Quantum Photonics SK2900

A general introduction for experimentalists

May 2024

Preface

Quantum photonics brings together fundamental and technological concepts to harness the power of light. The aim of these notes are to introduce students to the field and give them an understanding of the underlying physical concepts as well as the technical elements to allow them to understand what is going on in research laboratories. We follow the historical evolution of the field and consider the main concepts, look at the underlying theory and see how experiments are performed in the laboratory. An important aspect is the technological and experimental aspects where innovations are continuously pushing the limits of what can be realized and measured in quantum photonics.

Laboratory exercises should also be carried out in conjunction with studying these lecture notes. You will have the opportunity to perform several measurements in the lab starting with measurements on entangled pairs of photons generated with a non-linear crystal. This measurement will introduce you to the challenges associated with single photon detection and correlation measurements. The source of entangled photons can then be used to perform Hong-Ou Mandel measurements as well as to consider quantum key distribution schemes based on single and entangled photons.

After taking this course, you will have the knowledge needed to follow and discuss research articles in the field and will be able to start research projects in quantum photonics laboratories.

Chapter 1

Introduction

These notes are aimed at master students in physics with little knowledge in quantum physics but who are curious and eager to learn about the lively field of quantum photonics that is growing rapidly and is impacting many scientific and technological fields . It is based on the lecture notes for the course SK2900 Quantum Photonics I have given every year at the Royal Institute of Technology in Stockholm since 2016 and previously at the TU Delft.

We introduce notations, fundamental concepts, key scientific articles, experimental aspects and prepare students for hands-on experiments in the lab where they perform measurements on a source of entangled photons to measure quantum entanglement. Several key historical publications starting with the Einstein-Podolsky-Rosen paper are to be discussed in the class to understand how the field evolved over time and what new directions are emerging. For each topic, we cover the underlying theory, derive key formulas, mention historical developments, delve on the experimental aspects and discuss key publications.

Quantum photonics is a very broad subject stretching from the foundation of physics, where the nature of reality can be studied experimentally to an ever growing range of applications that include quantum communication, sensing and computation, with important potential societal impact. In quantum photonics, science is entangled with technology. Advances in single photon detection, photonics integration, new materials for single and entangled photons generation are enabling far more complex experiments and implementations than was thinkable just a decade ago. These technological advances in turn require more efforts on the theory side. It is therefore essential to combine knowledge in theory and experiment to play a role in the field, the course therefore includes an important practical part where the students are shown working laboratory experiments and offered to perform measurements themselves, this aims at making the technological aspect of the field along with the current technical limitations and challenges clear and visible.

At the end of the course, students should be proficient in quantum photonics: they will have the required basic knowledge to read and discuss research publications in the field of photonics, to understand the experimental requirements and challenges involved in state-of-the-art experiments and be able to discuss new advances in the field. In short, this course is the first step to educate the next generation of experts in quantum photonics who will make the world a better place.

Chapter 2

History and concept of entanglement

At the heart of quantum physics lie two new concepts: the superposition principle and quantum entanglement. These two concepts are readily observed with photons giving the field of photonics a head start in the study of quantum effects as will become clear in this chapter. Other systems such as solid state systems where decoherence can occur very quickly are usually not as convenient to generate, manipulate and detect quantum entanglement. Photons have this important advantage that they propagate quickly without loosing their coherence over arbitrarily long distances.

2.1 Superposition principle

The superposition principle tells us that a particle can be in the superposition of several states. For an electron, that could be a superposition of spin orientations. For a photon, the elementary particle of light, that could be a superposition of polarizations (horizontal and vertical polarization for instance). A famous and ancient example is the Schrödinger cat that is in a superposition of dead and alive, giving us an opportunity to introduce the bra-ket notation we will use throughout the lectures:

$$|\Psi\rangle = |Live\rangle + |Dead\rangle$$

While realizing such a state with a cat raises many questions, ethical and practical as a cat is a large cute macroscopic object, realizing such a superposition with a single photon, a single particle of light in terms of polarization is straightforward, given appropriate instruments.

2.2 Entanglement

In the famous Schrödinger cat gedanken experiment, a cat and a poison vial are placed in a box, taking us beyond a simple superposition. At some random time, given by the decay of a radioactive atom, the poison vial opens, killing the cat (figure 2.1). Because the box is entirely closed (no information can escape from the box), we cannot say with any possible measurement whether the poison vial has opened or not, the cat is therefore in a superposition of dead and alive, and the same goes for the poison vial. We therefore have the following equation that now shows *entanglement* between the cat and the poison vial, measuring one of the two (cat or vial) gives information on the other:

$$|\Psi\rangle = |Live, Closedvial\rangle + |Dead, openvial\rangle$$

Here, making a measurement on the cat (checking whether it is dead or alive) tells us right away about the state of the poison vial (opened or closed) without any need to make a measurement on the poison vial. We have our first quick and dirty definition of entanglement: measuring the state of one particle gives us information about the state of another particle, provided they are entangled.

Figure 2.1: The cruel Schoedinger cat experiment.

2.2.1 The Einstein Podolsky Rosen paper

Einstein, Podolsky and Rosen introduced the concept of entanglement in 1935 in an attempt to demonstrate that quantum mechanics is not a complete theory, this includes a discussion of what is reality and what is a complete physical theory. They suggested a gedanken experiment in the second half of the article. A particle decays into two particles of equal mass:

Figure 2.2: A particle breaks up into two equal particles.

Measuring the momentum of one particle gives information on the momentum of the other particle *instantaneously*. This of course was a problem for Einstein at it seems to violate relativity (nothing can travel faster than light, including information), and also the uncertainty principle as two independent measurements can be done on the same system. The first name 'Spuckhafte Fernwirkung' was coined by Einstein, the term 'Entanglement' was coined by Niels Bohr, an interesting discussion between Einstein and Bohr took place on this topic and was published in Physical Review, this discussion on the nature of reality still resonates today.

2.2.2 Bohm's concept

In 1951, David Bohm turned this concept into a spin $\frac{1}{2}$ particles problem, something measurable in the lab, as shown by Stern and Gerlach. Consider the dissociation of a spin zero two-atom molecule where each atom has spin $\frac{1}{2}$. After dissociation, the atoms travel in opposite directions, making it possible to label the atoms (1) and (2):

Figure 2.3: A particle breaks up into two equal particles.

Because the process must conserve angular momentum, there are only two possible outcomes:

- Particle (1) has spin Up and particle (2) has spin Down.
- Particle (1) has spin Down and particle (2) has spin Up.

Each of these two cases are equally likely, the wave function can be written:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}[|\uparrow\rangle_1 |\downarrow\rangle_2 + |\downarrow\rangle_1 |\uparrow\rangle_2] \tag{2.1}$$

Simpler notation:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}[|\uparrow_1\downarrow_2\rangle + |\downarrow_1\uparrow_2\rangle] = \frac{1}{\sqrt{2}}[|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle]$$

Paradox: The two atoms travel in opposite directions. After some time, they can no longer interact directly. But still, a measurement on one particle reveals to the experimenter what a measurement on the other particle

would give, wherever the other particle might be. At first glance, this seems to contradict relativity, however no information is sent faster than light. To be clear this does not enable communication faster than light, but it allows sharing randomness.

When measurements are carried out on one of the two particles in the entangled state given in equation 2.1, the outcome will be random: half of the time the measurement will give spin Up and half of the time spin Down. *However*, when both measurements are compared, something striking emerges: the results are always opposite. If measurement on particle 1 gives Up, the measurement on particle 2 gives Down and vice versa. This is the case whatever the distance between the two particles and the knowledge is gained instantaneously. There is nothing to worry about since no information travels faster than light here: we can't use this to communicate.

We can also see what makes a solid mathematical definition for an entangled state: *it is not factorizable*. While $[|\uparrow_1\downarrow_2\rangle + |\downarrow_1\uparrow_2\rangle]$ is not factorizable, the state $[|\uparrow_1\uparrow_2\rangle + |\uparrow_1\downarrow_2\rangle]$ for instance is not entangled and is factorizable: a measurement on particle 1 does not give us information on the state of particle 2 and we can factorize the state into $[|\uparrow_1\rangle |\uparrow_2 + \downarrow_2\rangle]$.

2.2.3 Entanglement beyond two particles

Entanglement is not limited to two particles. N particles can be entangled, for 3 particles and more, there are for instance the GHZ states named after Greenberger, Horne and Zeilinger:

$$|\Psi\rangle_{GHZ} = \frac{1}{\sqrt{2}}[|\uparrow_1\uparrow_2\uparrow_3\rangle + |\downarrow_1\downarrow_2\downarrow_3\rangle]$$

Here a measurement on one particle reveals the outcome of measurements on the other two particles, it is also not factorizable. Note that more than 3 particles can be used in a GHZ state.

2.2.4 Beyond spins

While spin is often used in entanglement experiments (photon spin $\approx$ polarization), continuous variables can also be entangled, such as position and linear momentum (as in the EPR paper). Or between two time bins where a particle can be in the superposition of two arrival times (time-bin entanglement).

2.2.5 Correlations

Correlations are crucial in entanglement measurements. For the state given in equation 2.1, measurements on individual particles give random results. However, measurements on pairs give correlated measurements. Correlations are therefore crucial in quantum entanglement studies: we need to make measurements on particles from the same entangled state. This raises a technological question: how does one measure correlations? We can look at two detectors and say that we have a correlation event if the two detectors give detection signals within a given time interval, this time interval will have to be made short enough to not mix up subsequent states. Here we require high time resolution, not only from light detectors but also from the electronics that can record the arrival times of single photons. It is now possible to routinely measure arrival times of single photons with 10 ps accuracy, quite an achievement when one thinks that light only travels 3 mm in 10 ps.

2.2.6 Hidden variables

Hidden variables have been proposed to explain the correlations observed in quantum entangled states. The hidden variables could be determined when the pairs are created and would then fool us, observers into believing there is entanglement. This is based on Einstein's concept 'God does not play dice', in his mind a theory is not complete if it is not able to fully predict the outcome of a measurement. Fully disproving hidden variables remains to be done in the lab, as one is free to assume that hidden variables could travel faster than light.. One question is how fast could hidden variables travel.

This opens the door for loopholes in entanglement measurements where for instance the *detection loophole* is based on the fact that only a tiny fraction of the particles are usually measured. While a measurement on all particles would not show entanglement, the few detected particles would behave differently and show entanglement. This concept could be refuted by detection a large fraction of the particles.

2.2.7 Hybrid entanglement

Different types particles can be entangled. For instance, an electron spin can be entangled with a photon polarization. In this case measuring the photon polarization would give information on the electron spin and vice versa.

2.2.8 Hyper entanglement

Two particles (or more) can share several types of entanglement. For instance, polarization and time-bin entanglement, this is called hyper entanglement.

2.2.9 Technological issues

To measure and produce the type of entanglement we are discussing here, one needs to be able to generate and detect light at the single photon level: we need single photon detectors and sources of pairs of entangled photons. The generation of single photons is an active field of research, a true single photon source on-demand, that would generate one and only one photon whenever required at a chosen wavelength and given polarization remains elusive but systems based on nanoscale quantum systems such as quantum dots are continuously improving. The generation of entangled photons can be done with several approaches: parametric down-conversion allows for random generation of entangled states while quantum dots can generate single and entangled photon pairs one at a time, on demand.

2.3 In the laboratory

Quick overview of the experimental setup that will be used in the laboratory: you will be using a system built by Qutools for the generation and measurement of entangled states.

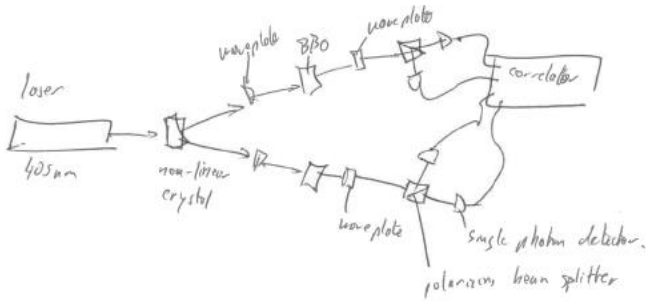


Figure 2.4: Schematic of the setup we will use to generate and measure entanglement. Each element and process will be discussed in the coming lectures.

The measurements are to be performed in groups of two students and a lab report will be written introducing the underlying theory, describing the experimental setup, the measurement process, the experimental data and its analysis to identify entanglement.

of lanthanum is 7/2, hence the nuclear magnetic moment as determined by this analysis is 2.5 nuclear magnetons. This is in fair agreement with the value 2.8 nuclear magnetons determined from La III hyperfine structures by the writer and N. S. Grace.[9]

[9] M. F. Crawford and N. S. Grace, Phys. Rev. **47**, 536 (1935).

This investigation was carried out under the supervision of Professor G. Breit, and I wish to thank him for the invaluable advice and assistance so freely given. I also take this opportunity to acknowledge the award of a Fellowship by the Royal Society of Canada, and to thank the University of Wisconsin and the Department of Physics for the privilege of working here.

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.

1.

ANY serious consideration of a physical theory must take into account the distinction between the objective reality, which is independent of any theory, and the physical concepts with which the theory operates. These concepts are intended to correspond with the objective reality, and by means of these concepts we picture this reality to ourselves.

In attempting to judge the success of a physical theory, we may ask ourselves two questions: (1) "Is the theory correct?" and (2) "Is the description given by the theory complete?" It is only in the case in which positive answers may be given to both of these questions, that the concepts of the theory may be said to be satisfactory. The correctness of the theory is judged by the degree of agreement between the conclusions of the theory and human experience. This experience, which alone enables us to make inferences about reality, in physics takes the form of experiment and measurement. It is the second question that we wish to consider here, as applied to quantum mechanics.

Whatever the meaning assigned to the term *complete*, the following requirement for a complete theory seems to be a necessary one: *every element of the physical reality must have a counterpart in the physical theory*. We shall call this the condition of completeness. The second question is thus easily answered, as soon as we are able to decide what are the elements of the physical reality.

The elements of the physical reality cannot be determined by *a priori* philosophical considerations, but must be found by an appeal to results of experiments and measurements. A comprehensive definition of reality is, however, unnecessary for our purpose. We shall be satisfied with the following criterion, which we regard as reasonable. *If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.* It seems to us that this criterion, while far from exhausting all possible ways of recognizing a physical reality, at least provides us with one

such way, whenever the conditions set down in it occur. Regarded not as a necessary, but merely as a sufficient, condition of reality, this criterion is in agreement with classical as well as quantum-mechanical ideas of reality.

To illustrate the ideas involved let us consider the quantum-mechanical description of the behavior of a particle having a single degree of freedom. The fundamental concept of the theory is the concept of *state*, which is supposed to be completely characterized by the wave function ψ, which is a function of the variables chosen to describe the particle's behavior. Corresponding to each physically observable quantity A there is an operator, which may be designated by the same letter.

If ψ is an eigenfunction of the operator A, that is, if

$$\psi' \equiv A\psi = a\psi, \tag{1}$$

where a is a number, then the physical quantity A has with certainty the value a whenever the particle is in the state given by ψ. In accordance with our criterion of reality, for a particle in the state given by ψ for which Eq. (1) holds, there is an element of physical reality corresponding to the physical quantity A. Let, for example,

$$\psi = e^{(2\pi i/h)p_0 x}, \tag{2}$$

where h is Planck's constant, p_0 is some constant number, and x the independent variable. Since the operator corresponding to the momentum of the particle is

$$p = (h/2\pi i)\partial/\partial x, \tag{3}$$

we obtain

$$\psi' = p\psi = (h/2\pi i)\partial\psi/\partial x = p_0\psi. \tag{4}$$

Thus, in the state given by Eq. (2), the momentum has certainly the value p_0. It thus has meaning to say that the momentum of the particle in the state given by Eq. (2) is real.

On the other hand if Eq. (1) does not hold, we can no longer speak of the physical quantity A having a particular value. This is the case, for example, with the coordinate of the particle. The operator corresponding to it, say q, is the operator of multiplication by the independent variable. Thus,

$$q\psi = x\psi \neq a\psi. \tag{5}$$

In accordance with quantum mechanics we can only say that the relative probability that a measurement of the coordinate will give a result lying between a and b is

$$P(a, b) = \int_a^b \bar{\psi}\psi dx = \int_a^b dx = b - a. \tag{6}$$

Since this probability is independent of a, but depends only upon the difference $b-a$, we see that all values of the coordinate are equally probable.

A definite value of the coordinate, for a particle in the state given by Eq. (2), is thus not predictable, but may be obtained only by a direct measurement. Such a measurement however disturbs the particle and thus alters its state. After the coordinate is determined, the particle will no longer be in the state given by Eq. (2). The usual conclusion from this in quantum mechanics is that *when the momentum of a particle is known, its coordinate has no physical reality.*

More generally, it is shown in quantum mechanics that, if the operators corresponding to two physical quantities, say A and B, do not commute, that is, if $AB \neq BA$, then the precise knowledge of one of them precludes such a knowledge of the other. Furthermore, any attempt to determine the latter experimentally will alter the state of the system in such a way as to destroy the knowledge of the first.

From this follows that either (1) *the quantum-mechanical description of reality given by the wave function is not complete* or (2) *when the operators corresponding to two physical quantities do not commute the two quantities cannot have simultaneous reality.* For if both of them had simultaneous reality—and thus definite values—these values would enter into the complete description, according to the condition of completeness. If then the wave function provided such a complete description of reality, it would contain these values; these would then be predictable. This not being the case, we are left with the alternatives stated.

In quantum mechanics it is usually assumed that the wave function *does* contain a complete description of the physical reality of the system in the state to which it corresponds. At first

sight this assumption is entirely reasonable, for the information obtainable from a wave function seems to correspond exactly to what can be measured without altering the state of the system. We shall show, however, that this assumption, together with the criterion of reality given above, leads to a contradiction.

2.

For this purpose let us suppose that we have two systems, I and II, which we permit to interact from the time $t=0$ to $t=T$, after which time we suppose that there is no longer any interaction between the two parts. We suppose further that the states of the two systems before $t=0$ were known. We can then calculate with the help of Schrödinger's equation the state of the combined system I+II at any subsequent time; in particular, for any $t>T$. Let us designate the corresponding wave function by Ψ. We cannot, however, calculate the state in which either one of the two systems is left after the interaction. This, according to quantum mechanics, can be done only with the help of further measurements, by a process known as the *reduction of the wave packet*. Let us consider the essentials of this process.

Let $a_1, a_2, a_3, \cdots$ be the eigenvalues of some physical quantity A pertaining to system I and $u_1(x_1), u_2(x_1), u_3(x_1), \cdots$ the corresponding eigenfunctions, where x_1 stands for the variables used to describe the first system. Then Ψ, considered as a function of x_1, can be expressed as

$$\Psi(x_1, x_2) = \sum_{n=1}^{\infty} \psi_n(x_2) u_n(x_1), \tag{7}$$

where x_2 stands for the variables used to describe the second system. Here $\psi_n(x_2)$ are to be regarded merely as the coefficients of the expansion of Ψ into a series of orthogonal functions $u_n(x_1)$. Suppose now that the quantity A is measured and it is found that it has the value a_k. It is then concluded that after the measurement the first system is left in the state given by the wave function $u_k(x_1)$, and that the second system is left in the state given by the wave function $\psi_k(x_2)$. This is the process of reduction of the wave packet; the wave packet given by the infinite series (7) is reduced to a single term $\psi_k(x_2)u_k(x_1)$.

The set of functions $u_n(x_1)$ is determined by the choice of the physical quantity A. If, instead of this, we had chosen another quantity, say B, having the eigenvalues $b_1, b_2, b_3, \cdots$ and eigenfunctions $v_1(x_1), v_2(x_1), v_3(x_1), \cdots$ we should have obtained, instead of Eq. (7), the expansion

$$\Psi(x_1, x_2) = \sum_{s=1}^{\infty} \varphi_s(x_2) v_s(x_1), \tag{8}$$

where φ_s's are the new coefficients. If now the quantity B is measured and is found to have the value b_r, we conclude that after the measurement the first system is left in the state given by $v_r(x_1)$ and the second system is left in the state given by $\varphi_r(x_2)$.

We see therefore that, as a consequence of two different measurements performed upon the first system, the second system may be left in states with two different wave functions. On the other hand, since at the time of measurement the two systems no longer interact, no real change can take place in the second system in consequence of anything that may be done to the first system. This is, of course, merely a statement of what is meant by the absence of an interaction between the two systems. Thus, *it is possible to assign two different wave functions* (in our example ψ_k and φ_r) *to the same reality* (the second system after the interaction with the first).

Now, it may happen that the two wave functions, ψ_k and φ_r, are eigenfunctions of two noncommuting operators corresponding to some physical quantities P and Q, respectively. That this may actually be the case can best be shown by an example. Let us suppose that the two systems are two particles, and that

$$\Psi(x_1, x_2) = \int_{-\infty}^{\infty} e^{(2\pi i/h)(x_1 - x_2 + x_0)p} dp, \tag{9}$$

where x_0 is some constant. Let A be the momentum of the first particle; then, as we have seen in Eq. (4), its eigenfunctions will be

$$u_p(x_1) = e^{(2\pi i/h)px_1} \tag{10}$$

corresponding to the eigenvalue p. Since we have here the case of a continuous spectrum, Eq. (7) will now be written

$$\Psi(x_1, x_2) = \int_{-\infty}^{\infty} \psi_p(x_2) u_p(x_1) dp, \tag{11}$$

where

$$\psi_p(x_2) = e^{-(2\pi i/h)(x_2 - x_0)p}. \tag{12}$$

This ψ_p however is the eigenfunction of the operator

$$P = (h/2\pi i)\partial/\partial x_2, \tag{13}$$

corresponding to the eigenvalue $-p$ of the momentum of the second particle. On the other hand, if B is the coordinate of the first particle, it has for eigenfunctions

$$v_x(x_1) = \delta(x_1 - x), \tag{14}$$

corresponding to the eigenvalue x, where $\delta(x_1 - x)$ is the well-known Dirac delta-function. Eq. (8) in this case becomes

$$\Psi(x_1, x_2) = \int_{-\infty}^{\infty} \varphi_x(x_2) v_x(x_1) dx, \tag{15}$$

where

$$\varphi_x(x_2) = \int_{-\infty}^{\infty} e^{(2\pi i/h)(x - x_2 + x_0)p} dp$$

$$= h\delta(x - x_2 + x_0). \tag{16}$$

This φ_x, however, is the eigenfunction of the operator

$$Q = x_2 \tag{17}$$

corresponding to the eigenvalue $x + x_0$ of the coordinate of the second particle. Since

$$PQ - QP = h/2\pi i, \tag{18}$$

we have shown that it is in general possible for ψ_k and φ_r to be eigenfunctions of two noncommuting operators, corresponding to physical quantities.

Returning now to the general case contemplated in Eqs. (7) and (8), we assume that ψ_k and φ_r are indeed eigenfunctions of some noncommuting operators P and Q, corresponding to the eigenvalues p_k and q_r, respectively. Thus, by measuring either A or B we are in a position to predict with certainty, and without in any way disturbing the second system, either the value of the quantity P (that is p_k) or the value of the quantity Q (that is q_r). In accordance with our criterion of reality, in the first case we must consider the quantity P as being an element of reality, in the second case the quantity Q is an element of reality. But, as we have seen, both wave functions ψ_k and φ_r belong to the same reality.

Previously we proved that either (1) the quantum-mechanical description of reality given by the wave function is not complete or (2) when the operators corresponding to two physical quantities do not commute the two quantities cannot have simultaneous reality. Starting then with the assumption that the wave function does give a complete description of the physical reality, we arrived at the conclusion that two physical quantities, with noncommuting operators, can have simultaneous reality. Thus the negation of (1) leads to the negation of the only other alternative (2). We are thus forced to conclude that the quantum-mechanical description of physical reality given by wave functions is not complete.

One could object to this conclusion on the grounds that our criterion of reality is not sufficiently restrictive. Indeed, one would not arrive at our conclusion if one insisted that two or more physical quantities can be regarded as simultaneous elements of reality *only when they can be simultaneously measured or predicted*. On this point of view, since either one or the other, but not both simultaneously, of the quantities P and Q can be predicted, they are not simultaneously real. This makes the reality of P and Q depend upon the process of measurement carried out on the first system, which does not disturb the second system in any way. No reasonable definition of reality could be expected to permit this.

While we have thus shown that the wave function does not provide a complete description of the physical reality, we left open the question of whether or not such a description exists. We believe, however, that such a theory is possible.

Chapter 3

Photon Statistics

We discus the nature of light, how to measure its statistics and show that light sources can be categorized along their photon emission statistics in three states: coherent, Fock and thermal states. We then consider the case of single photon sources and the measurement that can reveal the single photon nature of a light source.

When Maxwell published his four famous equations it seemed that the nature of light was finally fully understood: it was made of rather simple electromagnetic waves. However, the wave or particle nature of light, already discussed in the 17th century by Huygens and Newton, was still under discussion. There were valid arguments for both wave (Huygens' favorite that explains diffraction and Young's double slit experiment) and particle (Newton's favorite that could explain light's straight propagation and refraction, among other things) nature of light. Because Newton was such a prominent figure in physics his opinion in favor of the particle nature of light had a lasting impact. Planck's theory for black-body radiation was published 1901 followed by Einstein's interpretation of light as quantized electromagnetic radiation in 1905 that made a new quantum mechanical description of light necessary. The name photon was introduced in 1928 by Arthur Compton, it is derived from the Greek word $\phi\omega\sigma$ for light. Dirac gave the first quantum mechanical solution for the interaction between atoms and light fields in 1927 and shortly after, Fermi gave a complete review of quantum electrodynamics in 1932.

In quantum electrodynamics, the electromagnetic field is quantized and the photon is the smallest quantum of light. A complete derivation of the quantization of the light field can be found in several textbooks [Loudon1983, Fox2006]. We focus on photon statistics where the quantum description of light is required to fully classify different states of light and give a brief introduction to the quantization of the electromagnetic field. In simplified terms, we can replace the field amplitudes in the classical electrodynamics description with bosonic creation $\hat{a}^+$ and annihilation operators $\hat{a}$ that can add or remove a photon. Each mode of the light field (k, λ) can be described independently by a harmonic oscillator: we have an energy ladder with constant energy spacings whatever the number of photons already present. The consecutive operation of the annihilation and creation operator is equal to the operation of a new quantum mechanical operator $\hat{n}$, the photon number operator which gives the number of photons in one mode: $\hat{n} = \hat{a}^+\hat{a}$. The quantum mechanical approach allows to sum up all modes as independent quantum mechanical harmonic oscillators. The Hamiltonian of the electromagnetic field $\hat{H}_{em}$ for an arbitrary number of modes is given by:

$$\hat{H}_{\mathrm{em}} = \sum_k \sum_\lambda \frac{1}{2}\hbar\omega_k \left(\hat{a}_{k\lambda}\hat{a}^\dagger_{k\lambda} + \hat{a}^\dagger_{k\lambda}\hat{a}_{k\lambda}\right)$$

Where for each mode k we simply take the number of photons with wavelength λ to obtain the total amount of energy. If we consider only the fundamental mode, we can rewrite the Hamiltonian with the help of the photon number operator:

$$\hat{H}_{\mathrm{em}} = \hbar\omega\left(\hat{n} + \frac{1}{2}\right)$$

Just like in the quantum mechanical harmonic oscillator, we have a ground state with finite energy, called the vacuum state given by the term 1/2. The photon number operator $\hat{n}$ gives the number of photons with energy $\hbar\omega$ in the fundamental mode. The mean photon number of a mode $< n >$ is an important figure for the characterization of the light states. Together with the photon number variance $(\Delta n)^2$, we will identify different light states and use them to categorize light sources.

3.0.1 Number of Photons in a given Volume

To give an intuitive introduction to photon statistics, we consider a simple experiment taken from [Fox2006]. A light source emits photons that are detected by an ideal detector as shown in the figure below. The detector is sensitive down to the single photon level and produces a short electrical pulse in response to every single photon impinging the detector. Counting electronics records the number of electrical pulses and their arrival times within a defined time interval T. We will go deeper with single photon detection technology later.

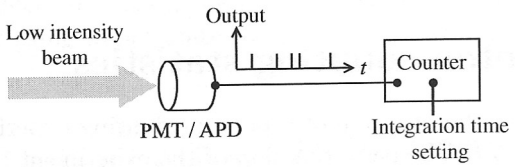


Figure 3.1: A single photon detector turns a stream of photons into electrical pulses that can be recorded and analyzed.

We start with a perfectly monochromatic light beam of frequency ω and constant intensity I and calculate the mean number of photons $< n(T) >$ passing through a cross section A of the beam in a given time interval T, set by the counting electronics:

$$< n(T) >= \frac{IAT}{\hbar\omega} = \frac{PT}{\hbar\omega}$$

where P is the power of the light beam, this equation represents the average properties of the beam and any light source will have fluctuations at short time scales. These fluctuations or differences in statistics of the photon numbers are used to characterize different light sources. Coming back to our example, we can calculate the constant photon flux Φ, i.e. the mean number of photons in a given cross-section of a beam of light with photon energy 1.0 eV and average power of 1 nW:

$$\Phi = \frac{< n(T) >}{T} = \frac{P}{\hbar\omega} = \frac{10^{-9}}{1.6.10^{-19}} = 6.2.10^{9} photons/s$$

Light travels at approximately 3.10^8 m/s, the photons are quite spread in space during this one second: We have a beam segment with a length of 3.10^8 m that contains $6.2.10^9$ photons. If we now reduce the volume we are interested, we only consider one meter instead of $3.10^8 m$ we have on average 20.67 photons in that volume. Since photons are the smallest quantum of light and are discrete, 20.67 mean photons does not make sense physically, instead there will be fluctuations in the number of photons and these fluctuations in mean photon numbers will increase the smaller we make the volume we are looking at. Similarly, one can also look at shorter and shorter time windows. Let us look at a segment of 1.5 m which on average contains 31 photons. We will divide the 1.5 m in 31 sub-segments. There are different options how the photons will be distributed within these sub-segments, here are three possible outcomes:

0 0 2 1 0 4 0 3 1 0 1 0 2 0 2 0 1 0 0 2 1 0 3 0 0 5 0 1 1 0 1
0 1 0 0 2 1 0 2 1 4 0 2 1 0 1 0 0 1 1 0 1 2 1 1 0 2 1 3 0 2 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

Even though in all 3 cases the mean photon number $< n >$ for each sub-segment is 1, the distribution function for each case is fundamentally different. In the first row it is super-Poissonian, in the second row it is Poissonian, and in the third row it is sub-Poissonian. We will now define these distributions.

3.1 Coherent state

A coherent state, or a Glauber state, describes the electromagnetic wave of a laser mode. In 1963, Roy Glauber provided a complete quantum mechanical description of these light states and got a Nobel prize for it. The coherent state is an eigenstate of the annihilation operator $\hat{a}$:

$$\hat{a}_i \left|\alpha_i\right\rangle = \alpha_i \left|\alpha_i\right\rangle$$

Being an eigenstate of $\hat{a}$, a coherent state *remains unchanged by the annihilation of a photon.* Additionally, since the vacuum state can be written as an eigenstate of the annihilation operator with $\alpha = 0$, all coherent

states have the same minimal uncertainty as the vacuum state. Linear superposition of these states allows for an expression of the coherent state in the basis of the photon number operator $\hat{n}$:

$$|\alpha_i\rangle = e^{-\frac{1}{2}|\alpha_i|^2} \sum_{n=0}^{\infty} \frac{\alpha_i^2}{\sqrt{n!}} |n_i\rangle$$

We can calculate the probability distribution P for n photons in a given mode i.

$$\begin{aligned} P_{coherent}(n) &= |\langle n \mid \alpha_i\rangle|^2 \\ &= \left| \exp\left(-\tfrac{1}{2}|\alpha_i|^2\right) \cdot \sum_m \frac{\alpha_i^m}{\sqrt{m!}} \langle n \mid m\rangle \right|^2 \\ &= \exp\left(-|\alpha_i|^2\right) \cdot \frac{|\alpha_i|^{2n}}{n!} \end{aligned}$$

This is the characteristic *Poisson statistics* used to describe coherent light states. The expected value of the photon number in one mode of a coherent state is therefore:

$$\langle n\rangle = \langle\alpha| \hat{n} |\alpha\rangle = |\alpha|^2$$

The variance of a coherent state is given as:

$$(\Delta n)^2_{\text{Glauber}} = \left\langle n^2 \right\rangle - \langle n\rangle^2 = |\alpha|^2 = \langle n\rangle$$

For a coherent state the maximum probability to find n photons in a mode is at the expected value $<n>$. The probability distribution of the photon number obeys a Poisson distribution. Any light state with larger (smaller) variance is called super (sub)- Poissonian light. The photon number distribution for a Glauber state is plotted below for 2 different mean photon numbers. We see that for a mean photon number of 1, we have as many 0 as 1 photon states and a rapidly decreasing probability of states with higher photon numbers. for a mean photon number of 5, the probability distribution is wider.

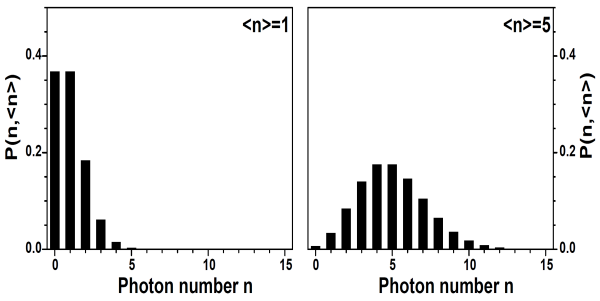


Figure 3.2: Photon number distribution for a coherent state with average photon number of 1 (left) and 5 (right).

3.2 Fock state

The Fock or photon number state, introduced by Vladimir Fock, results directly from the quantization of the electromagnetic field, since the Fock state is the eigenstate of the photon number operator $\hat{n}_i$:

$$\hat{n}_i |n_i\rangle = n_i |n_i\rangle$$

The eigenvalue n_i of the photon number operator describes the number of photons in a specific mode i. The probability $P_{Fock(n)}$ to find n_i photons in one mode is either 1 for $n = n_i$ or 0 for $n \neq n_i$, this is a very simnple and very clean state! A special characteristic of the Fock state: the photon number is precisely determined. Thus, the probability distribution of the photon number follows a δ-distribution. The expected value of the photon number in a Fock state is equal to the number of photons in the state:

$$\langle n \rangle = \langle n_i | \hat{n} | n_i \rangle = n_i$$

For the Fock state the variance is therefore zero, there is no variance only one number state is populated:

$$(\Delta n)^2_{\text{Fock}} = \left\langle n^2 \right\rangle - \langle n \rangle^2 = 0$$

The Fock state fulfills the inequality $\Delta n < \sqrt{n}$, showing a variance smaller than the coherent state. Such sub-Poisson statistics cannot be described by classical electromagnetic theory; thus such light is classified as non-classical light. The figure below shows the photon number distribution for two Fock states. Light emitters with a Fock state $n = 1$ are called single photon sources, since they can only emit one single photon at a time.

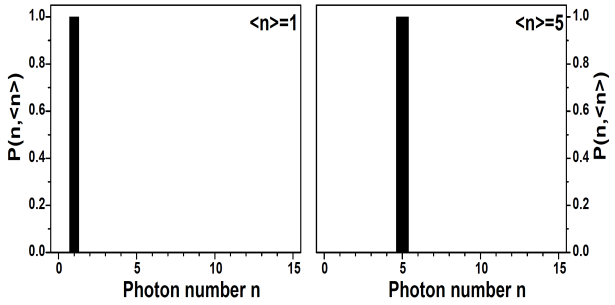


Figure 3.3: Photon number distribution for a Fock state with average photon number of 1 (left) and 5 (right). It can't get simpler than that: a Fock state with average photon number 1 only has single photon states and a Fock state with average photon number 5 only has 5 photon states.

3.3 Thermal state

The thermal state which is well described by the black-body radiation, it is an incoherent mixture of different photon number states. A quantum mechanical description of the thermal state takes advantage of the density matrix notation. The thermal state, being a quantum mechanical mixed state, can be written as the sum over all possible photon number states weighted with their occurrence probability:

$$\hat{\rho} = \sum_{n=0}^{\infty} P_n(n) \, |n\rangle \, \langle n|$$

where ρ is the density matrix operator and $P_n(n)$ gives the probability of finding n photons in a certain mode i of the thermal state. This is identical to the probability of having a certain photon number state occupied. $P(n)$ can be expressed as a function of n and $<n>$ for a single mode:

$$P(n, \langle n \rangle) = \frac{\langle n \rangle^n}{(1 + \langle n \rangle)^{n+1}}$$

$P(n, <n>)$ has the form of a Bose-Einstein distribution; the state with maximum probability is always the vacuum state with $n = 0$. The variance for a thermal state is given by:

$$(\Delta n)^2_{\text{Thermal}} = \langle n \rangle^2 + \langle n \rangle$$

It follows that fluctuations in photon number are typically larger than the mean photon number. Therefore, thermal light states are also called chaotic light. Since $\Delta n > \sqrt{n}$ one often describes *thermal state statistics as super-Poissonian statistics*. The thermal state distribution for 2 different mean photon numbers is plotted below. Finding zero photons in the mode always has the highest probability.

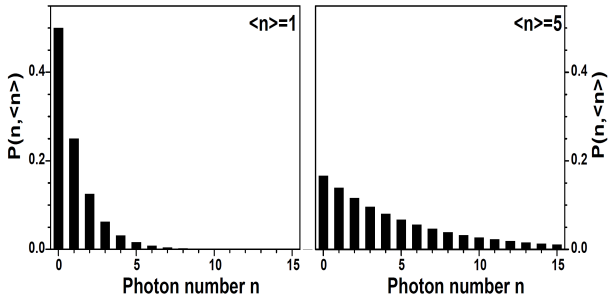


Figure 3.4: Photon number distribution for a thermal state with average photon number of 1 (left) and 5 (right).

3.4 Measuring light statistics

We have now seen the three possible photon statistics. But important questions remain: how do we measure photon statistics? How does one check in the lab that a light source is a single photon light source? We have seen that different light states are defined by their underlying photon statistics, photon probability distribution function and in the fluctuations of the photon numbers. With the help of the second-order correlation function $g^{(2)}(\tau)$ introduced by Glauber in 1963, we can classify the different light states. First, we introduce the classical second-order intensity correlation function:

$$g^{(2)}_{class}(\tau) = \frac{< I(t)I(t+\tau) >}{< I(t) >^2} = \frac{< E^*(t)E^*(t+\tau)E(t+\tau)E(t) >}{< E^*(t)E(t) >^2} \tag{3.1}$$

with $I \propto |E(t)|$ and $I(t+\tau)$ being the averaged intensities of the mode at a given time. Based on this definition the $g^{(2)}(\tau)$ function describes the correlation between two temporally separated intensity signals with time difference $\tau = t_2 - t_1$ from one light source. Using the transformation formalism from classical field quantities into equivalent quantum mechanical operators using the second quantization, we can rewrite the electric field $E(t)$ of a mode k with the help of annihilation $\hat{a}$ and creation $\hat{a}^+$ operators:

$$\hat{E}_k(t) = \hat{E}^{(+)}_k(t) + \hat{E}^{(-)}_k(t)$$

with

$$\begin{aligned} \hat{E}^{(+)}_k(t) &\propto \hat{a}_k \cdot \exp\left(-i\left(\omega_k t - \vec{k}\cdot\vec{r}\right)\right) \\ \hat{E}^{(-)}_k(t) &\propto (\hat{a}_k)^\dagger \cdot \exp\left(+i\left(\omega_k t - \vec{k}\cdot\vec{r}\right)\right) \end{aligned}$$

representing the 'positive' and 'negative' ωk frequency parts of the mode. For a single mode we can rewrite the $g^{(2)}(\tau)$ function using the commutator relation.

$$\begin{aligned} g^{(2)}_{QM}(\tau) &= \frac{\left\langle \hat{E}^{(-)}_k(t)\,\hat{E}^{(-)}_k(t+\tau)\,\hat{E}^{(+)}_k(t+\tau)\,\hat{E}^{(+)}_k(t)\right\rangle}{\left\langle \hat{E}^{(-)}_k(t)\,\hat{E}^{(+)}_k(t)\right\rangle^2} \\ &\overset{(\tau\to 0)}{=} \frac{\left\langle (\hat{a}_k)^\dagger (\hat{a}_k)^\dagger \hat{a}_k \hat{a}_k\right\rangle}{\left\langle (\hat{a}_k)^\dagger \hat{a}_k\right\rangle^2} = \frac{\langle n(n-1)\rangle}{\langle n\rangle^2} \ . \end{aligned}$$

Of particular interest is $g^{(2)}(0)$, since it represents the conditional probability how likely is it to detect a second photon at the same time one photon was already detected, it is a measure of the temporal photon coincidences, required to distinguish between different light states. Using the second factorial moment and the variance we can simplify the equation:

$$\begin{aligned} g^{(2)}_{QM}(0) &= \frac{\langle n^2\rangle - \langle n\rangle}{\langle n\rangle^2} \\ &= \frac{(\Delta n)^2 + \langle n\rangle^2 - \langle n\rangle}{\langle n\rangle^2} \\ &= 1 + \frac{(\Delta n)^2 - \langle n\rangle}{\langle n\rangle^2} \ . \end{aligned}$$

With the given variance of the different light states, we can now calculate the $g^{(2)}(0)$ value for the three different light states:

$$
\begin{aligned}
(\Delta n)^2_{thermal} = \langle n^2 \rangle + \langle n \rangle \quad &\Rightarrow \quad g^{(2)}_{QM}(0) = 2 \\
(\Delta n)^2_{coherent} = \langle n \rangle \quad &\Rightarrow \quad g^{(2)}_{QM}(0) = 1 \\
(\Delta n)^2_{Fock} = 0 \quad &\Rightarrow \quad g^{(2)}_{QM}(0) = 1 - \frac{1}{n} \quad (n \geq 1) \\
&\Rightarrow \quad g^{(2)}_{QM}(0) = 0 \quad (n = 0)
\end{aligned}
$$

Since in the Glauber state photon emission is completely uncorrelated, the $g^{(2)}(\tau)$ function is unity for all delay times τ , given an infinite coherence time of the state. As we can see from the equations above, the thermal state has a higher probability to emit more than one photon at the same time. However, this happens only in time periods shorter than the coherence time, which is typically very short for thermal/chaotic light. This effect is called *photon bunching*. In contrast, Fock states give $g_Fock^((2))(0) < 1$, leading to a reduced probability to emit two photons at the same time. This effect is called *photon antibunching*.

The graph below depicts the $g^{(2)}(\tau)$ function for three light states: thermal, coherent, and Fock state with a photon number of $n = 1$. If in this state a single photon is annihilated (e.g. detected), there is no photon left and no second photon can be detected. Fock states are therefore called non-classical light states and the first demonstration of photon antibunching by Kimble et al in 1977 was proof of the non-classical nature of light. Photon sources with $n = 1$ are single photon sources and important for the realization of different applications in photonic quantum technologies such as quantum key distribution.

We have seen that the statistics of light differs for different type of sources. Besides acquiring information from the spectrum, we can also gain information by measuring light statistics.

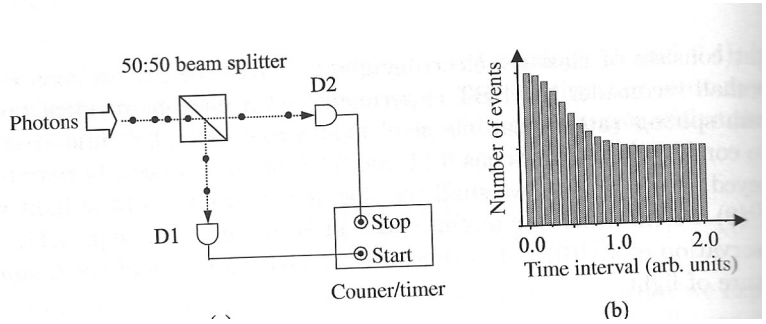


Figure 3.5: To identify a single photon emitter, a Hanbury-Brown Twiss setup (left) can be used where a 50-50 beamsplitter divides the incoming photon flux into two beams. Single photon detectors are placed at both outputs and correlations between the two detectors are measured. A histogram of the time intervals between the detection events can then be plotted (right).

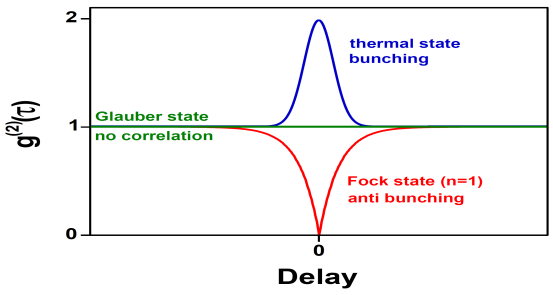


Figure 3.6: Schematic of the $g^{(2)}$ function for the three possible light statistics. The value around zero delay carries crucial information.

Chapter 4

Generating Single Photons

The development of single photon sources has been an active field of research for several decades. First demonstrations were done with atoms and molecules, intense efforts have followed with solid state based devices. A key element was the technological development that made it possible to detect the light emitted by a single photon emitter: the charge coupled device (CCD camera), the photomultiplier tube and the avalanche photodiode made it possible in the 1980s and 1990s to observe a single molecule.

An ideal single photon source should combine a wide range of properties: narrow emission spectrum, high brightness, repetition rate, polarization control, tunability, purity, room temperature operation are some elements one could wish for.

How can a single photon source be made? Because photons are bosons, there is no easy way to use interactions among photons to 'select' one single photon from a beam of light. Instead, what can be done is to isolate a single electron which is possible because of its charge and its fermionic nature and then use this electron to undergo a radiative transition. One single electron will undergo only one transition at a time and hence emit only one photon at a time. This can be done in a quantum dot, an 'artifical atom' or a 'quantum box' with nm sizes in all directions.

4.1 Solid State Single Photon Sources

Practical devices can be made with solid state single photon sources based on semiconductor quantum dots, single molecules, single defects, single ions and atoms. Intense research has been carried out and there are now commercial devices made by companies such as Sparrow Quantum and Quandela.

There are important remaining challenges: - the light extraction efficiency: semiconductors have large refractive indexes, light emitted inside a high refractive index material tends to stay trapped in the material because of total internal reflection. - electrical vs optical excitation: the easiest implementation is to excite the single photon emitter with a laser pulse. But a small, compact practical device should be electrically pumped, this is not easy. - higher operation temperature: because the confinement energy is usually limited and because competing processes have some activation energy, single photon sources tend to only operate at low temperatures and often at very low temperatures, at some Kelvins only. This requires the use of cryostats, high-performance fridges that add complexity, costs and power consumption to single photon sources. - operation at telecom wavelengths: the emission wavelength is crucial and most applications for single photon sources would be in the field of quantum communication, if one were to use optical fibers, one would require emission at telecom frequencies: around 1300 or 1550 nm. - Energy efficiency: the generation of single photons might well be the most inefficient thing ever done by man: to generate a stream of single photons containing only femto Watts of optical power, we operate cryostats and laser system consuming kilo Watts.

The first demonstration of single photon generation was performed with sodium atoms in 1977. This experiment was crucial in demonstrating the quantum nature of the photon.

Heralded single photons: By shining light on a non-linear crystal, we can have a down conversion process: each blue photon is turned into two red photons. When we detect one red photon in one output, we know that there is another photon in the other arm, that photon is 'heralded'. While the statistics of the light is the same as that of the incoming laser (Poissonian), we can use this approach to work with single photons. This has its limits as Poissonian statistics implies that two photons could very well be simultaneous.

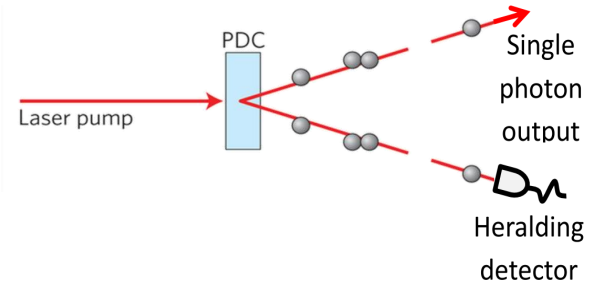


Figure 4.1: Parametric down conversion.

The Hanbury-Brown Twiss interferometer

How do we measure photon statistics? We use a Hanbury-Brown Twiss interferometer and measure time intervals between detection events on each detector. After acquiring a long list of events, we build a histogram of the time intervals.

we want to measure the g(2) function to see what type of light statistics we have, the second order correlation function is defined as:

$$g^{(2)}(\tau) = \frac{\langle : \hat{n}(t)\hat{n}(t+\tau) : \rangle}{\langle \hat{n} \rangle^2}$$

- $g^{(2)}(0)=1$ – **random**, no correlation
- $g^{(2)}(0)>1$ – **bunching**, photons arrive together
- $g^{(2)}(0)<1$ – **anti-bunching**, photons "repel"
- $g^{(2)}(\tau) \rightarrow 1$ at long times for all fields

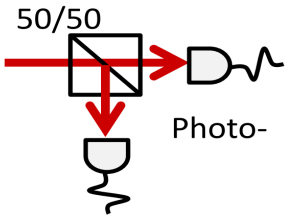
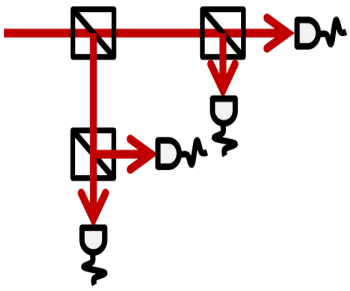


Figure 4.2: Hanbury Brown Twiss interferometer.

The term antibunched light applies to the case where there is always a minimum time interval between photons.

We can go beyond the g(2) function and measure g(n) which are correlations among n detectors. While this is possible, it still lacks a use and implies longer measurements.

Trick question: why not use only one single photon detector? This has to do with deadtime, after a detection event a detector is not able to detect another photon for a certain time. We need to rely on another detector during that time.



4.2 Generating Entangled Photons

While parametric down conversion as used in the laboratory provides entanglement, it has limitations: - The efficiency is very low: the probability that a laser photon is down converted into two entangled photons is less than one in a million, this is not energetically efficient and will prevent large scale use. - The statistics of the entanglement generation is Poissonian, we can't generate an entangled photon pair at a precise time. There is a solution: quantum dots, small pieces of semiconducting material whose energy levels are obtained by solving Schrödinger's equation. In quantum dots, we can excite an electron to a higher energy level and form an exciton. We can excite a second photon to a higher energy level and then have a bi-exciton. This bi exciton can then recombine and give us two photons in a cascade and these two photons can be entangled in polarization. By adjusting the size and composition of the quantum dot, we can tailor the emission wavelength and aim for particular values such as 1550 nm for optical fiber applications.

4.3 Solid state single photon sources

Solid state devices, usually based on semiconductor materials offer the possibility of realizing compact, scalable and stable devices that could be incorporated in large and complex architectures and would allow for long term and efficient operation. There are several types of emitters in the sold state that have been proven to be single photon sources each with their own advantages and disadvantages.

4.3.1 Quantum dots

Quantum dots, semiconductor nanostructures with dimensions in the nanometer range in all 3 directions can generate single as well as pairs of entangled photons. By varying the material composition, the emission energy can vary from the visible to the infrared, including the important telecom wavelengths of 1300 and 1550 nm that enable quantum communication in optical fibers. Quantum dots can be optically excited with light pulses or electrically pumped with LED structures.

4.3.2 Defects

Several defects have been shown to be single photon sources, the NV defect in diamond is well known, it has broad emission line but can be used at room temperature, the wavelength is not adapted to optical fiber communication.

4.3.3 Cryophobia

At this point, the best single photon sources all operate at low temperatures, of the order of a few degrees Kelvin. This cooling requirement adds complexity and costs but cooling techniques have evolved considerably over the past years and devices can be kept cold 24/7 in compact cryostats.

nature photonics

REVIEW ARTICLE

PUBLISHED ONLINE: 29 SEPTEMBER 2016 | DOI: 10.1038/NPHOTON.2016.186

Solid-state single-photon emitters

Igor Aharonovich[1,2]*, Dirk Englund[3] and Milos Toth[1,2]

Single-photon emitters play an important role in many leading quantum technologies. There is still no 'ideal' on-demand single-photon emitter, but a plethora of promising material systems have been developed, and several have transitioned from proof-of-concept to engineering efforts with steadily improving performance. Here, we review recent progress in the race towards true single-photon emitters required for a range of quantum information processing applications. We focus on solid-state systems including quantum dots, defects in solids, two-dimensional hosts and carbon nanotubes, as these are well positioned to benefit from recent breakthroughs in nanofabrication and materials growth techniques. We consider the main challenges and key advantages of each platform, with a focus on scalable on-chip integration and fabrication of identical sources on photonic circuits.

Photonic technologies are becoming increasingly prevalent in our daily lives. After decades of rapid advances, light sources — especially lasers and light-emitting diodes — have become high-performance, yet low-cost and reliable components, driving the Internet and lighting cities. A new frontier of research is the development of non-classical light sources: sources that produce streams of photons with controllable quantum correlations. A central building block, in particular, is a single-photon emitter (SPE) — a fundamental resource for many scalable quantum information technologies[1–6]. The ideal on-demand SPE emits exactly one photon at a time into a given spatiotemporal mode, and all photons are identical so that if any two are sent through separate arms of a beam-splitter, they produce full interference (a signature of indistinguishability). Such SPEs play a central role in a range of proposed quantum computing schemes, including linear[7,8] quantum simulation[9], quantum walks[10] and boson sampling[11], and precision measurement[12]. SPEs are also useful or necessary in many quantum secure communication schemes[13,14] and light flux metrology applications (such as defining the quantum candela — the SI base unit of luminous intensity) that do not require indistinguishability[15,16].

Over the years, various processes have been studied to generate single photons. The first demonstration of a SPE used an atomic transition of sodium atoms[17], though its reliability and efficiency were low. Today, it is possible to control cold atoms to efficiently produce single photons on-demand with near-identical wave packets[18]. Such sources, however, still require complex set-ups, and the loading of atoms or ions can be intermittent. The dynamics of atom-based sources is also relatively slow, leading to very low operation rates. Alternatively, single photons can be generated by heralding one of two photons produced using a nonlinear process such as spontaneous parametric down-conversion[19,20] or spontaneous four-wave mixing[21]. To overcome the unpredictable generation times of heralded photons, multiplexing schemes are being developed to rearrange them into regular intervals, though more work is needed to improve the single-photon purity and efficiency of such schemes, which are currently limited largely by losses in switching, photon storage and detection.

One of the most promising types of single-photon sources today are solid-state SPEs based on atom-like emitters — including fluorescent atomic defects and quantum dots (QDs) — which promise to combine the outstanding optical properties of atoms with the convenience and scalability of a solid-state host system[22–25]. But the complex mesoscopic environment of the solid state also entails numerous challenges, including inhomogeneous distributions that cause variability between photons from different emitters, and homogeneous linewidth broadening that gives rise to photon distinguishability from the same emitter. In addition, the extraction of photons, particularly from emitters in host materials with high refractive index, is challenging. Much research over the past decade has focused on mitigating these deleterious effects.

Over the past decade, efforts to engineer solid-state SPEs have expanded beyond the originally studied colour centres and QDs to include two-dimensional (2D) materials, carbon nanotubes (CNTs) and other solid-state host materials. A range of other source technologies are transitioning from discovery into engineering. This Review will identify key properties for evaluating and comparing SPEs, and will summarize recent progress of 'established' and emerging SPE technologies. In particular, we discuss the SPEs' photophysical properties as well as efforts towards scalable system integration, including electrical triggering and incorporation into optical resonators (metallic and dielectric).

We will first briefly review the available and most-studied solid-state systems, summarized in Fig. 1, and consider leading sources and their photophysical properties. We will then discuss important steps towards engineering scalable devices based on solid-state sources, with an emphasis on electrically triggered sources and integration of emitters with optical resonators (metallic and dielectric). We conclude with a discussion of challenges inherent to each system and highlight new research directions that are currently being explored.

Table 1 summarizes some of the most important properties of each system and serves as a roadmap for future studies of each system. It is clear that no single platform satisfies all prerequisites for an ideal SPE. For most applications, stable SPEs (which do not blink or bleach) are needed, with a high brightness and emission rate, as well as high single-photon purity and indistinguishability. The brightness of the source represents the maximum rate at which single photons can be emitted (or collected), while purity characterizes the multiphoton emission probability. Purity is quantified

[1]School of Mathematical and Physical Sciences, University of Technology Sydney, Ultimo, New South Wales 2007, Australia. [2]Institute for Biomedical Materials and Devices (IBMD), Faculty of Science, University of Technology Sydney, New South Wales 2007, Australia. [3]Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA.
*e-mail: igor.aharonovich@uts.edu.au

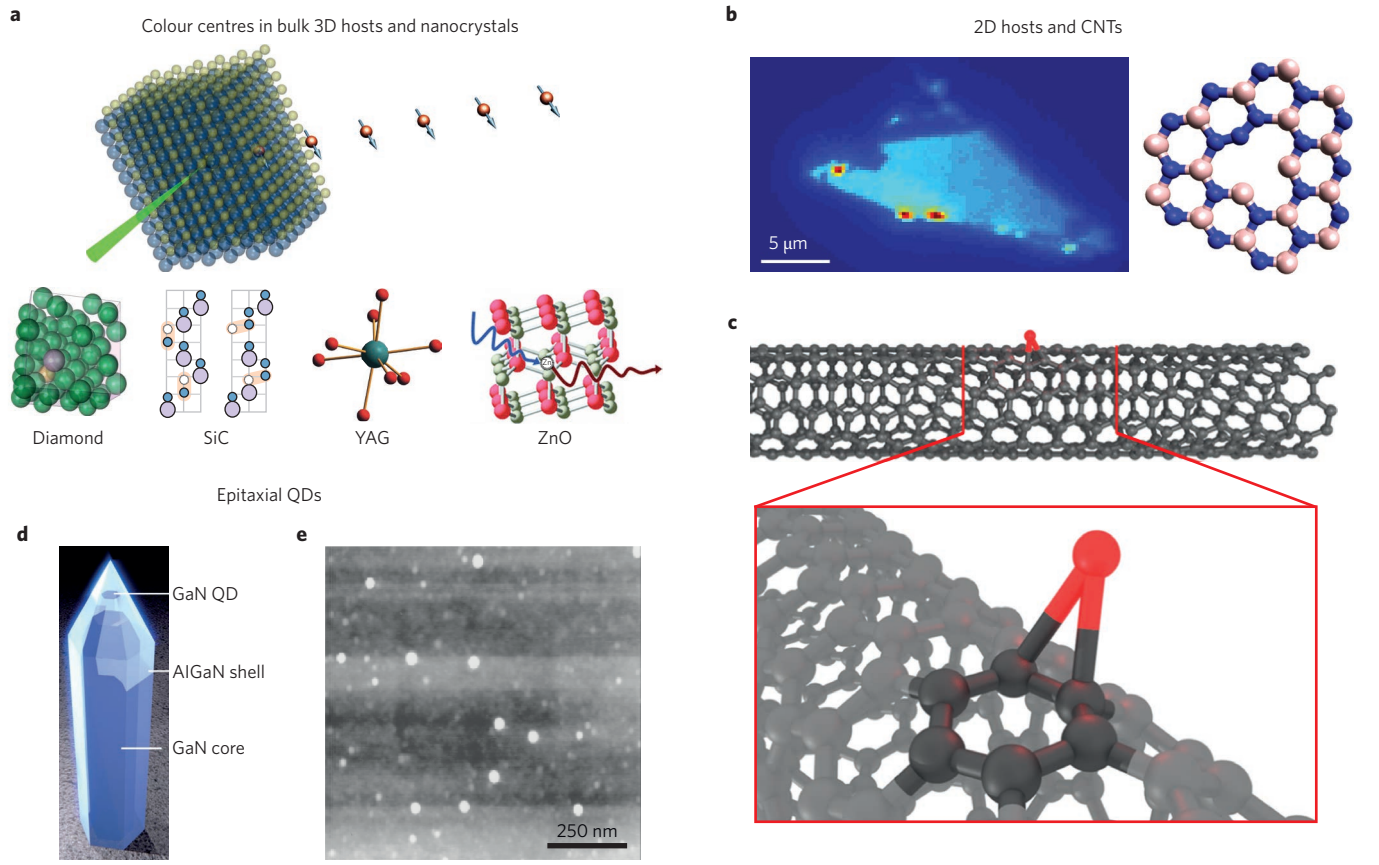


Figure 1 | Solid-state quantum systems emphasized in this Review. a, Defects in bulk 3D crystals and nanocrystals that emit single photons when excited with sub-bandgap light (illustrated with a green incoming laser beam). The insets show the most studied crystals — diamond, silicon carbide (SiC), yttrium aluminium garnet (YAG) and zinc oxide (ZnO). **b**, Emitters in 2D hosts. Single-photon emission at cryogenic temperatures was realized from localized excitons in several TMDCs including WSe_2 and $MoSe_2$, as shown in the confocal map (left). Room-temperature operation was realized from defects in monolayer hBN and few-layer flakes of hBN (right). **c**, Single-photon emission was recorded from excitons localized at oxygen-related defects in single-walled CNTs. **d**, Nitride QD embedded in a nanowire waveguide in order to enhance emission. **e**, Self-assembled InAs QDs. Both QD systems are representative of epitaxial (non-colloidal) QD-based SPE platforms. The InAs QDs were the first system used to demonstrate triggered SPEs. Figure reproduced with permission from: **a**(SiC), ref. 35, Nature Publishing Group; **a**(YAG), ref. 49, Nature Publishing Group; **a**(ZnO), ref. 44, American Chemical Society; **b**(left), ref. 61, OSA; **b**(right), ref. 56, Nature Publishing Group; **c**, ref. 68, Nature Publishing Group; **d**, ref. 85, American Chemical Society; **e**, ref. 74, APS.

by the dip of the second-order autocorrelation function, $g^{(2)}(\tau)$, at zero delay time, τ, while photon indistinguishability is quantified by a corresponding dip in the Hong–Ou–Mandel two-photon interference experiment that measures the extent of destructive interference between photons arriving simultaneously at a 50:50 beam splitter. These quantities are not consistently available, especially not under comparable experimental conditions (for example pump power) and especially not for emerging SPE systems. As the field of SPEs matures, it will become important to adopt consistent measurement and reporting standards to aid comparisons between SPE systems and for informing theoretical protocols. For the purpose of this Review, we have assembled the arguably most consistently reported SPE metrics in Table 1.

So far, only InGaAs QDs offer purities in excess of 99% (whereby $g^{(2)}(0) < 0.01$), corresponding to a 100-fold reduction in multiphoton emission compared with single-photon emission[24–27]. Most other systems suffer from increased multiphoton emission events with $g^{(2)}(0)$ in the range of 0.1–0.3, although many have very high emission rates of the order of 10^6 counts per second. Below, we discuss the key capabilities and limitations of the most promising systems.

Colour centres in crystals

A wide range of crystal colour centres — fluorescent point defects — exist at low enough density that SPEs can be isolated (Fig. 1a). Many of these emitters are stable even at room temperature if the electronic ground and excited states are far from the host crystal's valence and conduction bands. Among the most thoroughly studied SPEs are colour centres in diamond[28]. Stable room-temperature operation is one of the biggest advantages of these systems as it enables rapid characterization and thus fast research and development cycles used to improve the material. The nitrogen–vacancy (NV) and the silicon–vacancy (SiV) defects in diamond are the most studied, and their crystallographic and electronic structures are established[28]. These centres can occur naturally in diamond and can also be produced by ion implantation and subsequent annealing. At low temperature (<5 K), the zero-phonon emission lines of both emitters are narrow enough to allow two-photon interference between different emitters, although the visibility is poor[29,30] (72 ± 5% and 66 ± 10% for the SiV and the NV centres, respectively).

The NV centre has a non-zero electronic dipole moment that causes its optical frequencies to be sensitive to local strain and electric fields, which in turn contributes to homogeneous and inhomogeneous broadening. These can be mitigated by growing better diamond host material or engineering dynamical schemes to control and offset the fluctuations[31]. On the other hand, defects with an inversion symmetry such as the SiV centre in diamond are less susceptible to local environmental fluctuations. Indeed, multiple nearly identical SiV centres can be grown in the same crystal, as was

Table 1 | Summary of photophysical properties of solid-state SPEs.

	Maximum count rate (without a cavity, continuous wave) (counts s^{-1})	Lifetime (ns)	Homogeneous linewidth at 4 K	Indistinguishable photons (IP) and entanglement (E)	Spatial targeted fabrication of single emitters	Operation temperature	Integration of SPEs with dielectric cavities or plasmonic resonators
Colour centres in diamond	SiV: ~3×10^6 (ref. 138)* NV: ~1×10^6 (ref. 139)† For other sources see ref. 28	SiV: ~1 NV: ~12–22	NV, SiV lifetime-limited[29,30] Cr-related: 4 GHz (ref. 140)	NV: IP, E SiV: IP	Only for NV and SiV (ref. 28)	RT	Dielectric: NV, SiV only Plasmonics: NV only
Defects in SiC, ZnO and BN Rare earths in YAG/YOS	YAG: ~60×10^3 (ref. 141) ZnO: ~1×10^5 (ref. 44) SiC: ~2×10^6 (ref. 35) BN: ~3×10^6 (ref. 56)	19 (ref. 49)§ 1–4 (ref. 44) 1–4 (ref. 35) ~3 (ref. 56)	N/A	No	No	RT	No
Arsenide QDs	~1×10^7 (ref. 84)‡	~1 (refs 6,84)	Lifetime-limited	Yes	Yes	4 K	Yes
Nitride QDs	N/A	~0.3 (ref. 85)	~1.5 meV (ref. 85)	No	Yes	RT	Dielectric: yes Plasmonics: no
CNTs	~3×10^3 (ref. 68)	~0.4 (ref. 68)	N/A	No	No	RT	Dielectric: yes Plasmonics: no
2D TMDCs	~3.7×10^5 (ref. 57)	~1–3 (ref. 57)	N/A	No	No	4 K	No

The reported count rates for each system can be potentially optimized by integrating with cavities or improving collection optics. *Reported from a nanodiamond on iridium. †Recorded from a nanodiamond positioned on a solid immersion lens. Similar values obtained by etching a bullseye grating into a diamond membrane[142]. In both cases emitters in bulk diamond are dimmer. ‡Count rate at the objective, which is directly comparable to other systems. §Realized by optical upconversion to a short-lived excited state. N/A, not available; RT, room temperature.

recently demonstrated[29,32]. The SiV centre also has a strong zero-phonon line (ZPL), with ~70% of photons emitted into the ZPL. Emission into the ZPL is important for photon-mediated entanglement of internal quantum states of multiple emitters. The brightness of the SiV centre in bulk diamond is, however, still low, owing to low quantum efficiency of the defect[28]. Other defects with similar symmetry and optical properties, for example germanium–vacancy centres[33,34], are currently being investigated as promising alternatives.

An important challenge for other documented diamond colour centres is to reveal unambiguously the precise crystallographic structure, symmetry and charge state of each emitter. Several defects with known crystallographic structures, such as the nickel-related NE8 centre (ZPL ~793 nm) and the nitrogen-related H3 defect (ZPL ~503 nm), have been isolated at the single-defect level, but controlled fabrication of these defects as single sites is still missing[28]. Studies into the NV centre provide an excellent toolkit and a clear pathway to do so. These studies should include atomistic modelling to elucidate the level structure of the other atom-like defects in solids. These studies may also assist in identifying other NV-like systems with efficient optical spin readout at room temperature in diamond and other wide-bandgap crystal hosts. Subsequently, engineering these defects could be attempted in a controlled manner.

Much recent work has also focused on colour centres in the compound semiconductors. Silicon carbide (SiC) is of particular interest, as its many polytypes also have a large bandgap (typically 3–4 eV) and its nuclear spins can be spin-free (that is, a nuclear spin state of zero), allowing for colour-centre spin states with long coherence times. Of practical importance is that SiC is grown on an industrial scale for semiconductor applications. Consequently, the discovery[35] of a bright room-temperature SPE in SiC, tentatively attributed to the positively charged carbon antisite-vacancy (C_vC_{Si}) defect[36], was shortly followed by the first report of a pulsed room-temperature SPE diode[37]. Detection and manipulation of the spin state of SPEs in SiC has, however, been demonstrated so far only in comparatively low-brightness emitters attributed to Si vacancy and di-vacancy defects[38–42]. A conclusive correlation between the emission properties, spin properties and the precise crystallographic structure of each defect is yet to be established, and a topic of active research pursued by numerous groups[43].

The wide-bandgap (3.4 eV at room temperature) II–VI compound semiconductor ZnO has optoelectronic properties that could offer additional degrees of control over incorporated SPEs, including piezoelectric and spintronic properties, as well as mature commercial growth and processing. Several types of SPE have been reported in ZnO, but the structural origin of these luminescent centres is controversial, and most of the emitters reported so far suffer from blinking and bleaching[44–48]. Moreover, fabrication of high-quality, stable p-doped ZnO has remained elusive despite intense research efforts. This problem must be solved to enable the fabrication of ZnO p–n junctions and associated devices, a key potential benefit of this SPE host.

By comparison, rare-earth-ion impurities in crystals such as yttrium aluminium garnet (YAG) and yttrium orthosilicate (YOS) are well characterized and understood, with a range of properties that make them compelling candidates for SPEs[49–53]. These include narrow optical emission lines arising from transitions between excited states that are efficiently screened by outer-lying shells from the enclosing environment and hyperfine split ground states with very long coherence times[54,55]. Many of the garnet host materials have well-established growth protocols, driven by industrial applications such as solid-state laser gain materials. However, the excited-state lifetimes tend to be long, sometimes hundreds of milliseconds or more, resulting in low photon emission rates that make the detection of single ions challenging, and limit the maximum count rate of a practical SPE. This limitation has been partly circumvented in the case of Pr:YAG using a two-step upconversion process that has the mutual benefit of accessing a short-lived excited state and avoiding high background levels[49]. Nonetheless, maximum reported count rates are still moderate (~60×10^3; see Table 1) owing in part to a multitude of competing relaxation pathways.

The natural linewidths of all the colour centres need to be investigated in more detail. Although several lifetime-limited linewidths have been demonstrated in diamond, the existence of such linewidths has not been demonstrated for colour centres in other systems. Given the complexity of dielectric environments typically encountered in the proximity of defects, it is important to continue developing emitter systems that are inherently more tolerant to

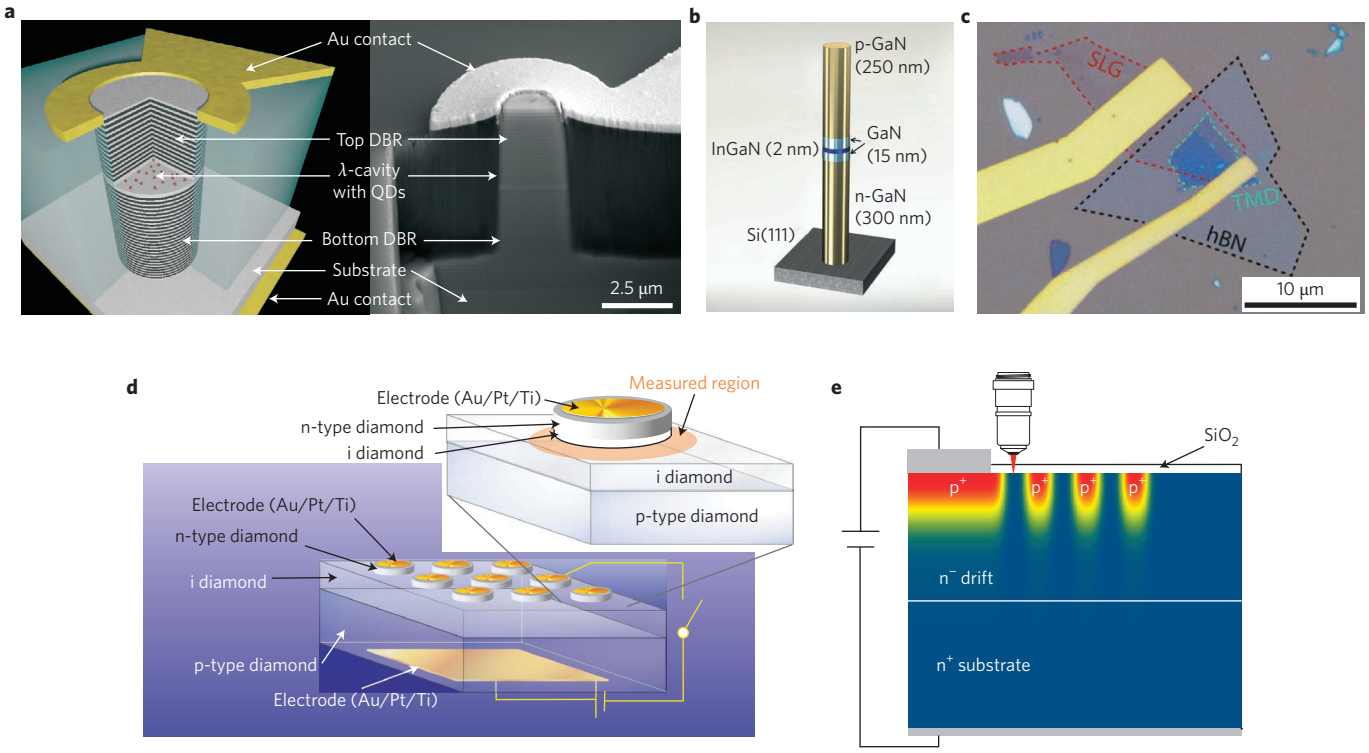


Figure 2 | Electrically driven single-photon emitters. a, InAs QDs embedded in an AlAs/GaAs Bragg-stack micropillar cavity that is doped to form a p–n structure used to electrically excite the QDs. DBR, distributed Bragg reflector. **b**, An InGaN QD embedded in a p–n nanowire made of p-GaN and n-GaN, grown on a silicon substrate. **c**, First demonstration of a quantum light-emitting device made using a 2D material. The TMDC is sandwiched between hBN and single-layer graphene (SLG). **d**, Diamond quantum LED realized by exciting the neutral NV centres in a diamond p–i–n structure. **e**, SiC-based quantum LED realized by creating a p^+–n^- junction and exciting emitters at the interface. Figure reproduced with permission from: **a**, ref. 94, AIP Publishing LLC; **b**, ref. 95, Nature Publishing Group; **c**, ref. 96, Nature Publishing Group; **d**, ref. 98, Nature Publishing Group; **e**, ref. 37, Nature Publishing Group.

stray electric fields, as well as active emitter stabilization methods to stabilize spectral drift[31].

Two-dimensional materials

Recently, a number of 2D materials have been shown to host SPEs[56–63] (Fig. 1b). The 2D hosts include transition metal dichalcogenides (TMDCs) in which the quantum defects are ascribed to localized, weakly bound excitons, and hexagonal boron nitride (hBN) in which SPEs have been associated with defects deep within the bandgap. Similarly to QDs, the TMDCs only exhibit quantum emission at cryogenic temperatures, whereas defects in hBN give rise to deep states that allow SPE operation at room temperature. The nature of SPEs in TMDCs is yet to be clarified. The emission is detuned by several millielectronvolts from the exciton transition and often appears at the 2D flake edges. The brightness varies from sample to sample, and most of the lines exhibit strong Zeeman shifts with applied magnetic field that could potentially be used to tune multiple emitters to the same frequency and realize photon indistinguishability. Several groups are pursuing this avenue of research[57–63].

Further research is required to explore limits of linewidth (for example through resonant excitation), photon purity and internal quantum efficiency of SPEs in 2D materials. Nevertheless, 2D materials offer a fascinating platform for quantum photonics. Given that the SPEs are embedded in a monolayer, total internal reflection can be avoided (which is a big problem with colour centres), and the light extraction efficiency can be very high. Moreover, integration with cavities and photonic waveguides is promising since manipulation of 2D materials on various substrates is now established. Another advantage of the defects in 2D materials is the great potential for coupling them to plasmonic structures. The thickness of the host material is particularly important for coupling to plasmonic tips or plasmonic gap cavities, as these require nanometre-scale proximity that is typically difficult for SPEs in bulk emitters in bulk crystals.

Defects in hBN are the most recent addition to the SPE library[64–67] and among the brightest SPEs reported so far[56]. Megahertz count rates at the detector have been recorded[56] with a very low excitation power of several hundred microwatts. The majority of photons are emitted into the ZPL, although the ZPL wavelength can vary from sample to sample. Rigorous modelling along with resonant excitation need to be carried out to reveal the electronic and crystallographic structure of the emitters. The natural linewidths of these emitters seem to be broadened by spectral diffusion, but these deficiencies may be resolved using dynamic stabilization[31].

Carbon nanotubes

Semiconducting CNTs (Fig. 1c) have also been shown to host SPEs[68–70]. The biggest promise for CNTs is the potential realization of optomechanical circuits since the CNT is a high-quality 1D mechanical resonator. Its mechanical properties are mostly known, and the growth of long CNTs is established. Another unique aspect of CNT SPEs is that the ZPLs can be above 1 μm in wavelength, potentially lowering the barrier for integration with existing telecom technologies.

The origin of these emitters is ascribed to excitons bound by shallow QD-like states generated by environmental fluctuations. These emitters therefore operate only at cryogenic temperatures and are highly susceptible to blinking, bleaching and dephasing. Recently, room-temperature quantum emission has been observed from deep O-related impurity states[68]. These emitters, however, require further characterization, and an outstanding challenge with all CNT emitters is to increase the brightness and stability of the SPEs.

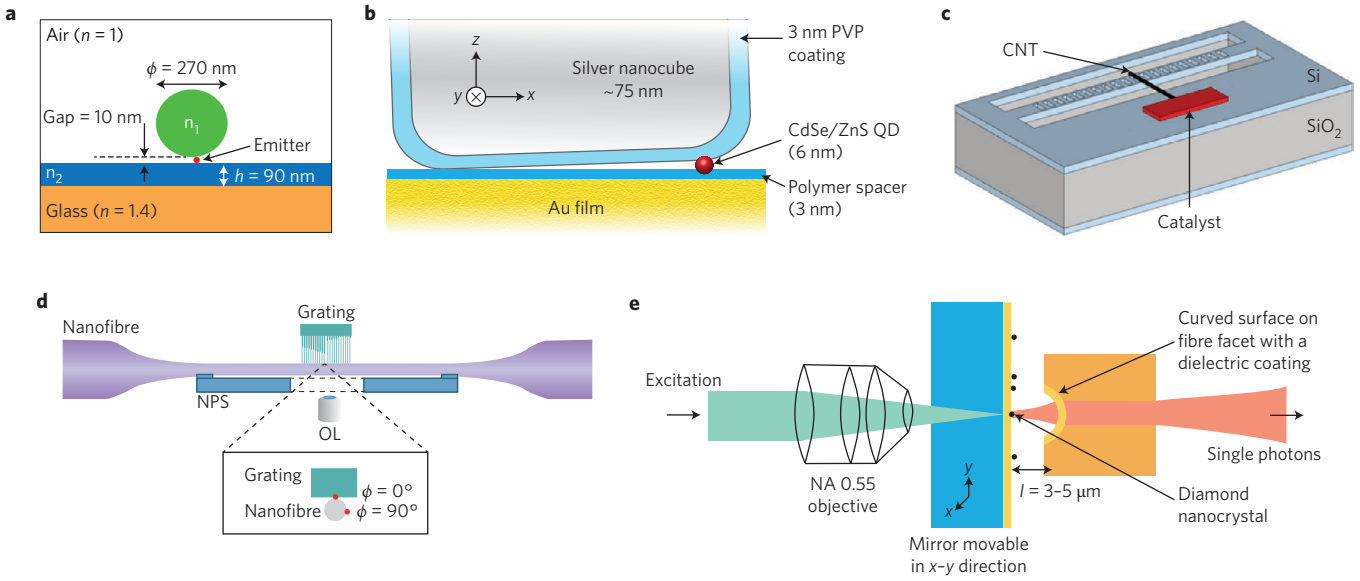


Figure 3 | Coupling single emitters to optical resonators. a, A single emitter (CdSe/ZnS QD) placed inside a dielectric slot cavity. The cavity is formed by positioning a silicon nanowire (n_1, green) on a ZnS slab (n_2, blue). The geometry enables a Purcell enhancement of up to 31. **b**, A CdSe/ZnS QD is placed in a nanogap spacer between a silver cube and a gold film. This geometry results in a 1,900-fold increase in emission rate. PVP, poly(vinyl pyrrolidone). **c**, A CNT hosting individual emitters positioned on top of a nanobeam cavity, resulting in a 10-fold enhancement of luminescence. **d**, A single QD is positioned in a grating, mounted on top of a nanofibre. This geometry enables coupling of the enhanced emission directly into the fibre-guided mode. OL, objective lens; NPS, nanopositioning stage. **e**, Nanodiamonds with single NV centres coupled to a fibre-based microcavity. This geometry can enable up to 65% of the NV emission to be channelled into the cavity mode. *l*, cavity length; NA, numerical aperture. Figure reproduced with permission from: **a**, ref. 107, American Chemical Society; **b**, ref. 108, American Chemical Society; **c**, ref. 109, Nature Publishing Group; **d**, ref. 110, APS; **e**, ref. 111, APS.

Other 1D hosts include QD-containing nanowires. A particularly interesting case is that of crystal-phase QDs, formed by modifying the crystallographic structure (from zinc blende to wurtzite) but not the chemical composition during the nanowire growth[71]. The quantum confinement originates from the bandgap differences at the domain interfaces within the nanowire.

Quantum dots

Self-assembled InAs/GaAs QDs (Fig. 1e) currently have the highest all-around SPE performance[72–75]. Emitted photons have been entangled to the spin degree of an additional electron loaded on the QD[4], and two-photon entangled states have been produced using bi-exciton cascade[76,77]. Under resonant excitation, recent demonstrations have achieved photon purity >99% (that is, $g^{(2)}(0) < 0.01$), and photon collection efficiency in excess of 75%[24,25,76–79]. In a recent report, over 1,000 consecutive emitted photons exhibited more than 92% indistinguishability[27]. A variety of methods have been developed to increase photon extraction efficiency above 50%, including coupling QDs to micropillars, nanowire antennas[80–82], microlenses[83] or circular Bragg grating bullseye cavities[84] defined on top of a pre-characterized dot. Moreover, strong coupling of single dots to photonic crystal cavities has been thoroughly investigated, bringing this platform one step closer towards integrated photonics on a single chip and engineering of spin/photon interfaces[1,2].

The production of many-photon quantum states can, to some extent, be achieved by time-delaying emissions from a single QD, but at the loss of overall rate. To maintain a high rate of multiphoton state generation, a key challenge for the InAs QDs is reproducibility of the samples and growth of multiple identical dots. To better interface with telecom systems, there has also been noticeable progress towards infrared emitters, and two-photon interference was recently demonstrated from InAs/InP SPEs in the telecom spectrum (1,550 nm)[26].

There has also been considerable progress in III-nitride QDs that operate even at room temperature[85–87]. But owing to challenges in growth of high-quality material and a higher emission energy of ~3 eV, their use as a reliable SPE platform with high signal-to noise ratio and a relatively low $g^{(2)}(0)$ is yet to be demonstrated.

Finally, perovskite QDs (not included in Table 1) have been shown to exhibit quantum emission[88] and operate at room temperature. However, the emitters blink and bleach, and the reported count rates are low. More materials development is required to optimize these emitters.

Electrically driven devices

Deployment of scalable single-photon technologies can benefit from electrically triggered devices integrated onto a single chip[89–93]. Figure 2 shows electrically driven quantum LEDs (QLEDs) that have been realized with QDs (Fig. 2a,b)[94,95], 2D TMDCs[96,97] (Fig. 2c) and defects in solids (Fig. 2d,e)[37,98,99]. One of the main challenges in QLEDs is to concentrate the electron–hole pair recombination current on the defect or QD of interest rather than on surrounding impurities. Therefore, material growth and site-specific emitter engineering are key to achieving working devices and technologies that are efficient and scalable. Indeed, generation of efficient QLEDs has been realized in the GaAs system[100], which allows for p- and n-type doping as well as positioning of QDs. Moreover, the QLEDs have been combined with photonic structures such as Bragg reflectors or nanowires that further enhance the overall efficiency of the devices (Fig. 2a,b). Entanglement between emitted photon pairs has also been recently reported — a hallmark of scalable quantum technologies[78].

In wide-bandgap systems, including diamond and silicon carbide, charge injection has so far resulted in increased background emission due to high defect concentration, and therefore reduced signal-to-noise ratio of the sources. A unique challenge for electrical driving concerns the control of the charge state, which greatly changes the emission spectrum in colour centres (whereas the shift between excitons and trions in QDs is typically smaller). While the negatively charged NV centre is of interest to the quantum photonic

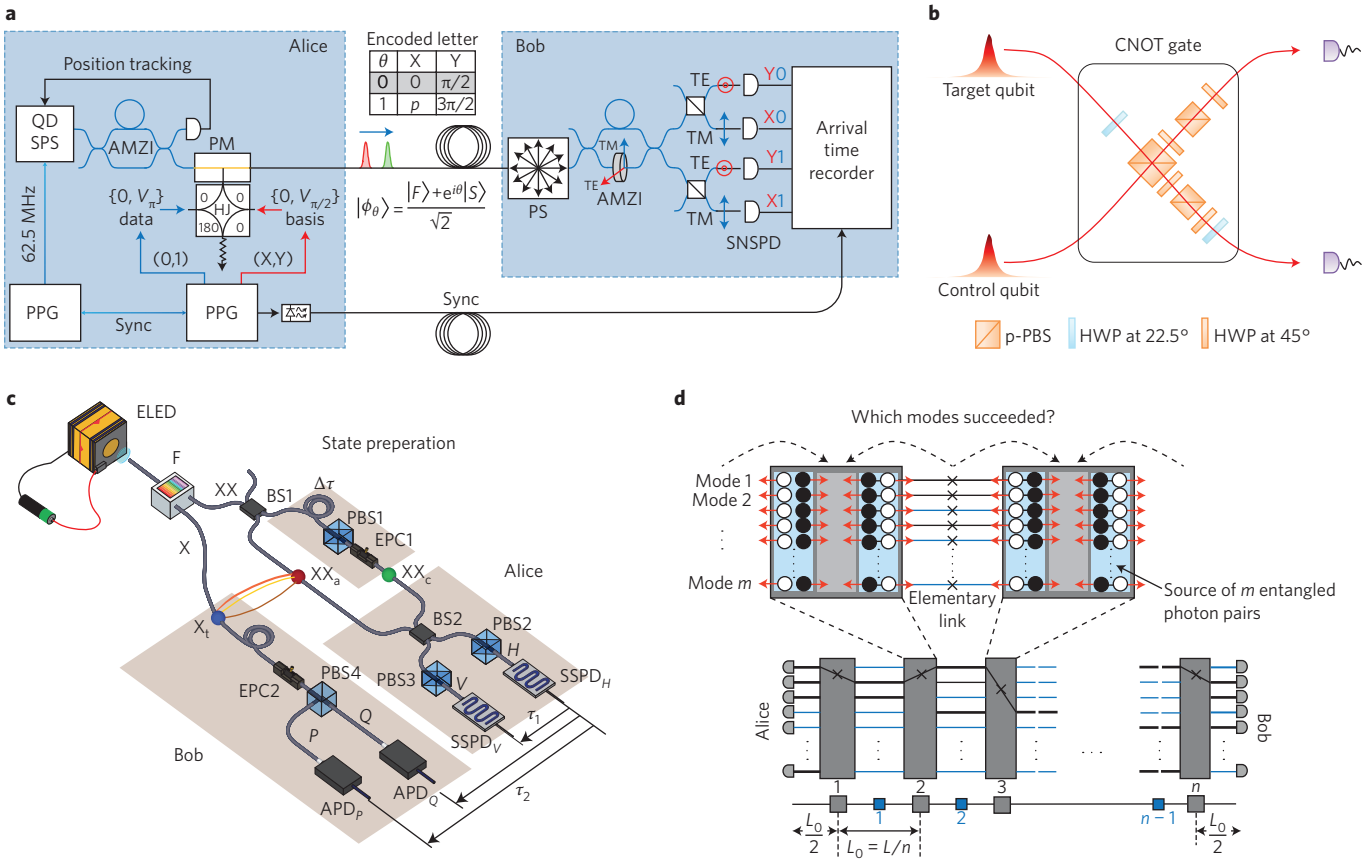


Figure 4 | Applications of quantum emitters. a, Quantum key distribution protocol realized over 120 km using an InAs/InP QD and a superconductor detector. AMZI, asymmetric Mach–Zehnder interferometer; HJ, hybrid junction; PPG, pulse pattern generator; PS, polarization scrambler; SPS, single-photon source; SNSPD, superconducting nanowire single-photon detector; TE, transverse electric; TM, transverse magnetic. **b**, A post-selected optical CNOT gate implemented using a nearly 'perfect' InAs QD. HWP, half-wave plate; PBS, polarizing beam-splitter. **c**, A quantum teleportation scheme realized with an electrically driven QD. APD, avalanche photodiode; BS, beam splitter; ELED, entangled-light-emitting diode; EPC, electrical polarization controller; F, spectral filter; SSPD, superconducting single-photon counting detector; *P*, *Q*, *V* and *H* are photons labelled by their polarization; τ, time delay. **d**, Schematic illustration of a quantum repeater. Chain of elementary links for a repeater architecture that uses quantum memories, Bell-pair sources, probabilistic Bell-state measurement, and multiplexing over *m* orthogonal qubit modes (parallel channels). Grey (blue) are major (minor) nodes. Figure reproduced with permission from: **a**, ref. 115, under a Creative Commons licence (http://creativecommons.org/licenses/by/4.0/); **b**, ref. 122, Nature Publishing Group; **c**, ref. 123, Nature Publishing Group; **d**, ref. 118, M. Pant *et al*.

community, only the neutral NV centre can be driven electrically. Electrical pumping of other colour centres — such as diamond Xe centres[101] or SiV centres[102] — appears promising.

Finally, 2D TMDCs provide another promising platform for QLED systems, as p–n junctions can now be fabricated in a wide range of homo- and heterojunctions, sheet conductivity can be high, and current could be injected with extremely high spatial resolution, at least in the out-of-plane dimension. In addition, charge control of individual shallow defects in hBN/graphene heterostructures using a high-resolution scanning tunnelling microscope has recently been shown[103]. This result opens interesting perspectives towards voltage-controlled emission from SPEs in hBN.

Integrated systems

In many applications, it is beneficial to integrate SPEs on-chip with other photonic devices, including photonic cavities, filters, waveguides, resonators and detectors. The integrated systems enable light guidance on a chip, enhancement of emission rates by modification of spontaneous emission, and efficient photonic interfaces to atom-like emitters in the strong Purcell and strong-coupling regimes[1,2,6,104]. Two broad approaches have been investigated to integrate quantum emitters and photonic integrated circuits (PICs): either a hybrid approach[105,106] whereby the SPE is heterogeneously integrated with a PIC made of a different material, or a homogeneous approach in which the SPE is monolithically grown in the PIC device[1,73]. Each approach offers advantages and disadvantages. In the following, we focus only on the hybrid approach as it offers more flexibility for realizing the final device. We note that colloidal QDs have been used in much of the proof-of-concept work done so far because they are relatively easy to fabricate and manipulate. Experiments to date have found unstable optical emission, however, and therefore we do not include them among the most promising SPEs in this Review.

Figure 3 summarizes several key experiments on hybrid integration of SPEs into cavities and waveguides. Figure 3a and b shows single colloidal CdSe/ZnS QDs coupled to a dielectric slot waveguide and a plasmonic gap cavity, respectively[107,108]. The latter results in a large emission rate enhancement of up to ~1,900 (ref. 108). Figure 3c shows a CNT that hosts a quantum emitter coupled to a nanobeam cavity in a low mode volume silicon photonic crystal that results in an emission enhancement, and a theoretical Purcell value of ~300 (ref. 109). Figure 3d and e shows examples of fibre-based cavities, realized with QDs[110] and nanodiamonds[111], respectively. Although such architectures are not easy to fabricate, they offer an interesting advantage in that the emission is directed into an optical fibre and can be easily integrated with other photonic components.

Table 2 | Summary of source requirements for different applications.

	Photon purity $g^{(2)}(0)$	Indistinguishability	Efficiency η	Repetition rate
Quantum key distribution	<0.1	Not critical, but consecutive photons must be uncorrelated	>0.5*	>GHz
Cluster-state quantum computing	<0.001 (more study needed on many-photon errors)	>0.99	>0.99 for reasonable resources	Ideally GHz to avoid long buffers, maximize experiment frequency
All-optical quantum repeater	<0.001	>0.99	>0.99	>GHz
Bell-state sources for memory-based repeaters	<0.01	>0.9	>0.9	Ideally GHz

*To be competitive against attenuated laser quantum key distribution with decoy state.

While the results presented in Fig. 3 are promising, there are several difficulties in assembling these hybrid nanophotonic systems. (1) The dipole orientation of the SPE within the solid-state particle is unknown, and once manipulated into a cavity, it is unlikely to experience the strongest electromagnetic field. (2) The SPEs are never located precisely in the 'middle' of the foreign particle, which poses limitations on the cavity design. (3) The actual placement of the particle in the strongest cavity field is often challenging. (4) The particles containing the SPEs scatter light, which degrades the cavity resonances and adds loss channels. The recently discovered SPEs in 2D materials may solve these problems, as the optical dipole is typically in-plane, aiding angular alignment, and the atomic thinness of the host material causes only minimal perturbations to the waveguide or cavity mode. Indeed, initial experiments on coupling exciton transitions of 2D materials to optical cavities are encouraging[112]. With improved control over lateral engineering of SPEs in these materials, high-precision deterministic coupling to cavities should become achievable.

Applications of SPEs

System-level demands on quantum light sources are far more stringent than for their classical counterparts, as reflected for example in the extremely high internal and extraction efficiency requirements in Table 2. For instance, most quantum key distribution (QKD) systems are nowadays run with attenuated laser sources, and can operate with a mean photon number per pulse of $\langle n \rangle \approx 0.5$ (using recently introduced decoy-state protocols[113,114] to counter the photon-number splitting side-channel attack). An ideal SPE could push this to $\langle n \rangle = 1$. Thus, to make SPEs worthwhile on the sender side (Alice), the efficiency from the source to the fibre, including all state preparation (for example polarization encoding), should be at least 0.5. Recent results demonstrated QKD with triggered SPEs over more than 120 km in fibres (Fig. 4a)[115]. The raw and secure key rates at 100 km were ~80 and 28 bits per second, respectively, realized with true pure SPEs ($g^{(2)}(0) \approx 10^{-3}$). But this rate is still 1–2 orders of magnitude slower than attenuated-laser QKD, pointing to the need for improvements in the source brightness and extraction efficiencies for SPEs to become competitive for QKD[113,115].

While QKD does not need — but could benefit from — SPEs, other applications require them. One important area is in the production of many-photon entangled states. For instance, heralded two-photon Bell states can be produced using linear optics and four single photons. Heralded Bell states are useful for certain types of quantum repeater protocols using atomic memories[116]. SPEs are also central resources for producing cluster states for all-optical quantum repeaters[117], although the latter is likely to require photon source efficiencies over 0.99 to keep the number of required sources manageable[118]. Fault-tolerant quantum computing imposes similar efficiency requirements on the source[88,119], as well as near-unity indistinguishability and probably very high photon purity, although the effect of multiphoton emissions on gate fidelities has not yet been thoroughly analysed[8]. Encouragingly, theoretical work on percolation-based generation of photonic cluster states shows significant loss tolerance. Even the best theoretical protocols, however, call for at least thousands of photons per encoded quantum bit, so many identical sources will need to work together efficiently, probably on PICs. A more forgiving application could be boson sampling and photonic quantum walks[9,120], which promise to beat today's classical computers at specialized tasks with more than ~40 photons; these applications can also tolerate lower indistinguishability[121].

Two-qubit logic gates and quantum-state teleportation (Fig. 4b,c)[122,123] represent operational primitives of photonic quantum information processing. A post-selected optical quantum-controlled NOT (CNOT) gate (analogous to a logic NOT gate) was recently demonstrated with indistinguishable SPEs (Fig. 4b). A heralded CNOT gate together with feed-forward and single-qubit rotation produces a universal set gate for quantum computing[7,117,118]. Finally, Fig. 4d illustrates the recently proposed concept of an all-optical quantum repeater for long-haul quantum cryptographic links. Quantum repeaters are analogous to amplifiers in classical channels[117]. They are proposed to be inserted between distant quantum nodes to generate a shared secret key to compensate for the losses in the channel[118]. Based on recent resource-cost analysis[118], millions of high-performance SPEs would be needed per repeater node to produce the required cluster states needed to beat the limits of repeaterless QKD. Additional theoretical work is needed to elucidate requirements on photon purity and indistinguishability, although errors in both will probably need to be much below 1%.

The early discovery of QD SPEs and their continued refinement has allowed these systems to lead the way in key quantum optics demonstrations, including CNOT gates and spin-photon entanglement experiments. However, the applications of atom-like defects in solids have grown in recent years far beyond single-photon emission. For example, defects in wide-bandgap systems (such as NV centres in diamond) have emerged as excellent systems for nanoscale sensing[124] and long-range electron-spin entanglement[125], while rare-earth-ion systems are being engineered as promising quantum memories for quantum repeaters.

Conclusions and outlook

SPEs have been, and remain, of central importance in many quantum optics applications. The basic physics of two-level optical systems is well established, but coaxing solid-state emitter systems, with their often complex mesoscopic environment, to simply fit such simple models has not been possible. Instead, the challenges of developing 'ideal' single-photon sources have prompted successful research that has greatly elucidated physical processes in open quantum systems and advanced our understanding on quantum–classical boundaries. These research efforts have also led to pleasant surprises — for instance, that the apparent 'nuisance' of emitter electron spins coupling to nearby nuclei actually allows controllable access of ancilla nuclear spins and related research activities.

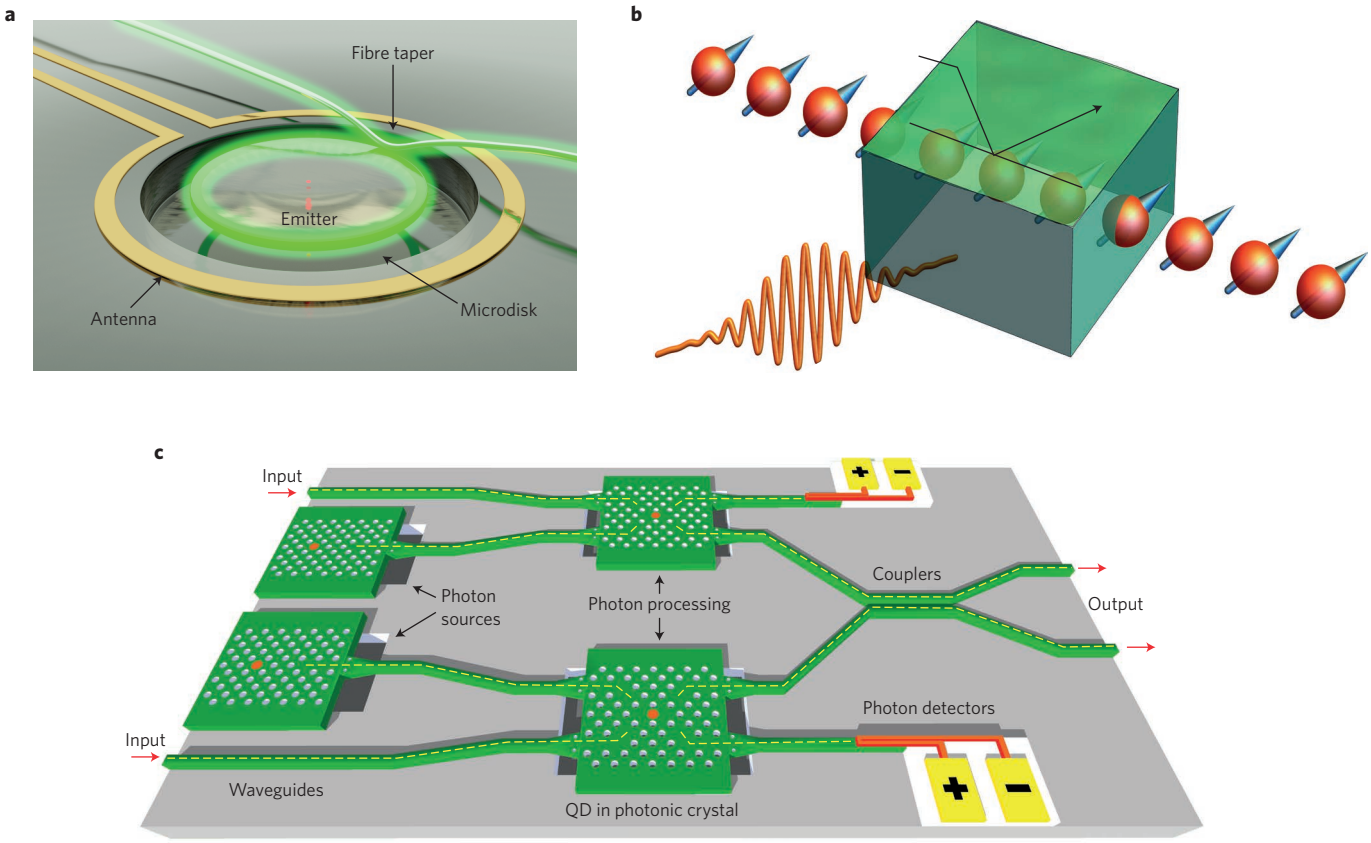


Figure 5 | Future applications of solid-state single emitters. a, Optomechanics with single photons. Coupling between single photons and single mechanical oscillations. Experiments of this type are already under way. **b**, Schematic illustration of a single-photon transistor. Such a device has been proposed and realized using Rydberg states in an ultracold Rb gas as well as single molecules. An analogous device is yet to be demonstrated using solid-state defect-based emitters. **c**, On-chip integrated quantum memory and quantum circuitry. Although such a memory has been realized with atomic vapour, and individual quantum memories have been demonstrated with both NV centres and QDs, on-chip integration is yet to be achieved. Figure courtesy of D. Lake and P. Barclay, Univ. of Calgary (**a**); R. Johne and A. Fiore, Eindhoven Univ. Technology (**c**).

Rapid progress in a range of SPE technologies has greatly improved key metrics — photon purity, efficiency and indistinguishability — as well as important practical matters including reproducibility, wavelength and electrical pumping. SPEs are now close to improving on state-of-the-art technologies, including photon-number-squeezed light sources for intensity standards or boson sampling and related applications. With sufficient overall internal and external photon efficiency, single-photon sources stand to become competitive for quantum communications — as sources for QKD and for augmenting quantum repeaters based on matter-based long-lived memories. Finally, when the key performance metrics of efficiency, indistinguishability and purity have errors below 1% or so, one may expect SPEs to enable scalable production of many-photon entangled states for advanced applications including all-optical repeaters and quantum repeating in linear optics.

Reaching the performance requirements for these applications requires continued basic research as well as engineering of already established systems. The crystallographic and electronic level structure of most of the current defects is still under debate. Rigorous atomistic modelling along with established spectroscopic, electron spin resonance and ion implantation studies is needed. The tremendous improvements in growth of arsenide-based systems can be extended to the increasingly important optoelectronic material system of III-nitrides, with a particular focus on reducing inhomogeneous broadening through improved material growth and methods for control of individual SPEs, particularly in attempts to grow identical QDs. After the discovery of a whole new class of SPEs in 2D materials with unique optical and material properties, experimental and theoretical work are needed to elucidate the photophysics, crystallographic and electronic properties, and methods of production. Growth of alternating layers promises multicolour SPEs on a chip, and recent progress in 2D-material electrical contacts promises high-performance electrically driven SPE devices. Thorough optical studies are needed, however, to understand the possible limits to efficiency, indistinguishability and photon purity. Ultimately, whereas miniaturization of electronic devices will reach the level of single charges, miniaturization of photonic and optoelectronic components will require manipulation of SPEs in a microscopic solid-state environment.

Among other promising applications in which SPEs can play a central role is quantum optomechanics, which may revolutionize today's sensing technologies[126]. Cooling an optomechanical resonator to its ground state has been demonstrated, and interfacing mechanical motion with spins and single photons is an exciting new direction of research. One promising avenue is to explore strain to mediate coupling between optical and mechanical resonances in a monolithic integrated device[127–129]. The mature nanofabrication capabilities of diamond or silicon carbide are promising for such devices (Fig. 5a)[130–133].

Another promising direction includes single-photon-level 'transistors' (Fig. 5b). Such advances will enable explorations of quantum nonlinearities and open the path for discoveries of new physical phenomena. Indeed, a single-photon transistor has been realized with trapped rubidium atoms[134] and single molecules[135], but is yet

to be realized in the solid state[136,137]. Finally, many proposals for cluster-state production would benefit greatly from an electrically triggered source of entangled photons that are guided and stored on a single chip (Fig. 5c). The required toolkit is in place, primarily because a vast library of SPEs has already been established. It is therefore the right time to dedicate resources to scalability, optimization and applicability of these emitters to real devices.

Received 29 June 2016; accepted 18 August 2016; published online 29 September 2016

References

1. O'Brien, J. L., Furusawa, A. & Vuckovic, J. Photonic quantum technologies. *Nat. Photon.* **3,** 687–695 (2009).
2. Lodahl, P., Mahmoodian, S. & Stobbe, S. Interfacing single photons and single quantum dots with photonic nanostructures. *Rev. Mod. Phys.* **87,** 347–400 (2015).
3. Koenderink, A. F., Alù, A. & Polman, A. Nanophotonics: shrinking light-based technology. *Science* **348,** 516–521 (2015).
4. Gao, W. B., Imamoglu, A., Bernien, H. & Hanson, R. Coherent manipulation, measurement and entanglement of individual solid-state spins using optical fields. *Nat. Photon.* **9,** 363–373 (2015).
5. Northup, T. E. & Blatt, R. Quantum information transfer using photons. *Nat. Photon.* **8,** 356–363 (2014).
6. Buckley, S., Rivoire, K. & Vuckovic, J. Engineered quantum dot single-photon sources. *Rep. Prog. Phys.* **75,** 126503 (2012).
7. Kok, P. *et al.* Linear optical quantum computing with photonic qubits. *Rev. Mod. Phys.* **79,** 135–174 (2007).
8. Gimeno-Segovia, M., Shadbolt, P., Browne, D. E. & Rudolph, T. From three-photon Greenberger–Horne–Zeilinger states to ballistic universal quantum computation. *Phys. Rev. Lett.* **115,** 020502 (2015).
9. Aspuru-Guzik, A. & Walther, P. Photonic quantum simulators. *Nat. Phys.* **8,** 285–291 (2012).
10. Aharonov, D., Ambainis, A., Kempe, J. & Vazirani, U. in *Proc. 33rd Annual ACM Symposium on Theory of Computing* 50–59 (ACM, 2001).
11. Aaronson, N. N. P. & Arkhipov, A. in *Proc. 43rd Annual ACM Symposium on Theory of Computing* 333–342 (ACM, 2011).
12. Giovannetti, V., Lloyd, S. & Maccone, L. Advances in quantum metrology. *Nat. Photon.* **5,** 222–229 (2011).
13. Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81,** 1301–1350 (2009).
14. Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photon.* **8,** 595–604 (2014).
15. Cheung, J. Y. *et al.* The quantum candela: a re-definition of the standard units for optical radiation. *J. Mod. Opt.* **54,** 373–396 (2007).
16. Chu, X.-L., Götzinger, S. & Sandoghdar, V. A high-fidelity photon gun: intensity-squeezed light from a single molecule. Preprint at https://arXiv.org/abs/1608.07980 (2016).
17. Kimble, H. J., Dagenais, M. & Mandel, L. Photon antibunching in resonance fluorescence. *Phys. Rev. Lett.* **39,** 691–695 (1977).
18. Kuhn, A., Hennrich, M. & Rempe, G. Deterministic single-photon source for distributed quantum networking. *Phys. Rev. Lett.* **89,** 067901 (2002).
19. Howell, J. C., Bennink, R. S., Bentley, S. J. & Boyd, R. W. Realization of the Einstein–Podolsky–Rosen paradox using momentum- and position-entangled photons from spontaneous parametric down conversion. *Phys. Rev. Lett.* **92,** 210403 (2004).
20. Kwiat, P. G. *et al.* New high-intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett.* **75,** 4337–4341 (1995).
21. Yan, Z. *et al.* Generation of heralded single photons beyond 1100 nm by spontaneous four-wave mixing in a side-stressed femtosecond laser-written waveguide. *Appl. Phys. Lett.* **107,** 231106 (2015).
22. Koehl, W. F., Seo, H., Galli, G. & Awschalom, D. D. Designing defect spins for wafer-scale quantum technologies. *MRS Bull.* **40,** 1146–1153 (2015).
23. Loredo, J. C. *et al.* Scalable performance in solid-state single-photon sources. *Optica* **3,** 433–440 (2016).
24. Somaschi, N. *et al.* Near-optimal single-photon sources in the solid state. *Nat. Photon.* **10,** 340–345 (2016).
25. Ding, X. *et al.* On-demand single photons with high extraction efficiency and near-unity indistinguishability from a resonantly driven quantum dot in a micropillar. *Phys. Rev. Lett.* **116,** 020401 (2016).
26. Kim, J.-H., Cai, T., Richardson, C. J. K., Leavitt, R. P. & Waks, E. Two-photon interference from a bright single-photon source at telecom wavelengths. *Optica* **3,** 577–584 (2016).
27. Wang, H. *et al.* Near-transform-limited single photons from an efficient solid-state quantum emitter. *Phys. Rev. Lett.* **116,** 213601 (2016).
28. Aharonovich, I. & Neu, E. Diamond nanophotonics. *Adv. Opt. Mater.* **2,** 911–928 (2014).
29. Sipahigil, A. *et al.* Indistinguishable photons from separated silicon-vacancy centers in diamond. *Phys. Rev. Lett.* **113,** 113602 (2014).
30. Sipahigil, A. *et al.* Quantum interference of single photons from remote nitrogen-vacancy centers in diamond. *Phys. Rev. Lett.* **108,** 143601 (2012).
31. Acosta, V. M. *et al.* Dynamic stabilization of the optical resonances of single nitrogen-vacancy centers in diamond. *Phys. Rev. Lett.* **108,** 206401 (2012).
32. Rogers, L. J. *et al.* Multiple intrinsically identical single-photon emitters in the solid state. *Nat. Commun.* **5,** 4739 (2014).
33. Ralchenko, V. G. *et al.* Observation of the Ge-vacancy color center in microcrystalline diamond films. *Bull. Lebedev Phys. Inst.* **42,** 165–168 (2015).
34. Iwasaki, T. *et al.* Germanium-vacancy single color centers in diamond. *Sci. Rep.* **5,** 12882 (2015).
35. Castelletto, S. *et al.* A silicon carbide room-temperature single-photon source. *Nat. Mater.* **13,** 151–156 (2014).
36. Umeda, T. *et al.* Identification of the carbon antisite–vacancy pair in 4H-SiC. *Phys. Rev. Lett.* **96,** 145501 (2006).
37. Lohrmann, A. *et al.* Single-photon emitting diode in silicon carbide. *Nat. Commun.* **6,** 7783 (2015).
38. Koehl, W. F., Buckley, B. B., Heremans, F. J., Calusine, G. & Awschalom, D. D. Room temperature coherent control of defect spin qubits in silicon carbide. *Nature* **479,** 84–87 (2011).
39. Falk, A. L. *et al.* Polytype control of spin qubits in silicon carbide. *Nat. Commun.* **4,** 1819 (2013).
40. Riedel, D. *et al.* Resonant addressing and manipulation of silicon vacancy qubits in silicon carbide. *Phys. Rev. Lett.* **109,** 226402 (2012).
41. Christle, D. J. *et al.* Isolated electron spins in silicon carbide with millisecond coherence times. *Nat. Mater.* **14,** 160–163 (2015).
42. Widmann, M. *et al.* Coherent control of single spins in silicon carbide at room temperature. *Nat. Mater.* **14,** 164–168 (2015).
43. Lienhard, B. *et al.* Bright and stable visible-spectrum single photon emitter in silicon carbide. *Optica* **3,** 768–774 (2016).
44. Morfa, A. J. *et al.* Single-photon emission and quantum characterization of zinc oxide defects. *Nano Lett.* **12,** 949–954 (2012).
45. Neitzke, O. *et al.* Investigation of line width narrowing and spectral jumps of single stable defect centers in ZnO at cryogenic temperature. *Nano Lett.* **15,** 3024–3029 (2015).
46. Jungwirth, N. R. *et al.* A single-molecule approach to ZnO defect studies: single photons and single defects. *J. Appl. Phys.* **116,** 043509 (2014).
47. Jungwirth, N. R., Chang, H.-S., Jiang, M. & Fuchs, G. D. Polarization spectroscopy of defect-based single photon sources in ZnO. *ACS Nano* **10,** 1210–1215 (2016).
48. Choi, S. *et al.* Single photon emission from ZnO nanoparticles. *Appl. Phys. Lett.* **104,** 261101 (2014).
49. Kolesov, R. *et al.* Optical detection of a single rare-earth ion in a crystal. *Nat. Commun.* **3,** 1029 (2012).
50. Xia, K. *et al.* All-optical preparation of coherent dark states of a single rare earth ion spin in a crystal. *Phys. Rev. Lett.* **115,** 093602 (2015).
51. Emanuel, E., Tobias, U., Stephan, G. & Vahid, S. Spectroscopic detection of single Pr^{3+} ions on the $^3H_4$–$^1D_2$ transition. *New J. Phys.* **17,** 083018 (2015).
52. Utikal, T. *et al.* Spectroscopic detection and state preparation of a single praseodymium ion in a crystal. *Nat. Commun.* **5,** 3627 (2014).
53. Kolesov, R. *et al.* Mapping spin coherence of a single rare-earth ion in a crystal onto a single photon polarization state. *Phys. Rev. Lett.* **111,** 120502 (2013).
54. Zhong, T., Kindem, J. M., Miyazono, E. & Faraon, A. Nanophotonic coherent light-matter interfaces based on rare-earth-doped crystals. *Nat. Commun.* **6,** 8206 (2015).
55. Longdell, J. J., Fraval, E., Sellars, M. J. & Manson, N. B. Stopped light with storage times greater than one second using electromagnetically induced transparency in a solid. *Phys. Rev. Lett.* **95,** 063601 (2005).
56. Tran, T. T., Bray, K., Ford, M. J., Toth, M. & Aharonovich, I. Quantum emission from hexagonal boron nitride monolayers. *Nat. Nanotech.* **11,** 37–41 (2016).
57. He, Y.-M. *et al.* Single quantum emitters in monolayer semiconductors. *Nat. Nanotech.* **10,** 497–502 (2015).
58. Srivastava, A. *et al.* Optically active quantum dots in monolayer WSe_2. *Nat. Nanotech.* **10,** 491–496 (2015).
59. Kumar, S., Kaczmarczyk, A. & Gerardot, B. D. Strain-induced spatial and spectral isolation of quantum emitters in mono- and bilayer WSe_2. *Nano Lett.* **15,** 7567–7573 (2015).
60. Koperski, M. *et al.* Single photon emitters in exfoliated WSe_2 structures. *Nat. Nanotech.* **10,** 503–506 (2015).
61. Tonndorf, P. *et al.* Single-photon emission from localized excitons in an atomically thin semiconductor. *Optica* **2,** 347–352 (2015).
62. Chakraborty, C., Kinnischtzke, L., Goodfellow, K. M., Beams, R. & Vamivakas, A. N. Voltage-controlled quantum light from an atomically thin semiconductor. *Nat. Nanotech.* **10,** 507–511 (2015).

63. Kern, J. *et al.* Nanoscale positioning of single-photon emitters in atomically thin WSe_2. *Adv. Mater.* **28,** 7101–7105 (2016).
64. Bourrellier, R. *et al.* Bright UV single photon emission at point defects in h-BN. *Nano Lett.* **16,** 4317–4321 (2016).
65. Jungwirth, N. R. *et al.* Temperature dependence of wavelength selectable zero-phonon emission from single defects in hexagonal boron nitride. Preprint at http://arXiv.org/abs/1605.04445 (2016).
66. Martinez, L. J. *et al.* Efficient single photon emission from a high-purity hexagonal boron nitride crystal. Preprint at http://arXiv.org/abs/1606.04124 (2016).
67. Tran, T. T. *et al.* Quantum emission from defects in single-crystalline hexagonal boron nitride. *Phys. Rev. Appl.* **5,** 034005 (2016).
68. Ma, X., Hartmann, N. F., Baldwin, J. K. S., Doorn, S. K. & Htoon, H. Room-temperature single-photon generation from solitary dopants of carbon nanotubes. *Nat. Nanotech.* **10,** 671–675 (2015).
69. Hogele, A., Galland, C., Winger, M. & Imamoglu, A. Photon antibunching in the photoluminescence spectra of a single carbon nanotube. *Phys. Rev. Lett.* **100,** 217401 (2008).
70. Jeantet, A. *et al.* Widely tunable single-photon source from a carbon nanotube in the Purcell regime. *Phys. Rev. Lett.* **116,** 247402 (2016).
71. Akopian, N., Patriarche, G., Liu, L., Harmand, J. C. & Zwiller, V. Crystal phase quantum dots. *Nano Lett.* **10,** 1198–1201 (2010).
72. Dory, C. *et al.* Complete coherent control of a quantum dot strongly coupled to a nanocavity. *Sci. Rep.* **6,** 25172 (2016).
73. Sun, S., Kim, H., Solomon, G. S. & Waks, E. A quantum phase switch between a single solid-state spin and a photon. *Nat. Nanotech.* **11,** 539–544 (2016).
74. Santori, C., Pelton, M., Solomon, G., Dale, Y. & Yamamoto, Y. Triggered single photons from a quantum dot. *Phys. Rev. Lett.* **86,** 1502–1505 (2001).
75. Strauf, S. *et al.* High-frequency single-photon source with polarization control. *Nat. Photon.* **1,** 704–708 (2007).
76. Muller, M., Bounouar, S., Jons, K. D., Glässl, M. & Michler, P. On-demand generation of indistinguishable polarization-entangled photon pairs. *Nat. Photon.* **8,** 224–228 (2014).
77. Versteegh, M. A. M. *et al.* Observation of strongly entangled photon pairs from a nanowire quantum dot. *Nat. Commun.* **5,** 5298 (2014).
78. Stevenson, R. M. *et al.* Indistinguishable entangled photons generated by a light-emitting diode. *Phys. Rev. Lett.* **108,** 040503 (2012).
79. Gazzano, O. *et al.* Bright solid-state sources of indistinguishable single photons. *Nat. Commun.* **4,** 1425 (2013).
80. Claudon, J. *et al.* A highly efficient single-photon source based on a quantum dot in a photonic nanowire. *Nat. Photon.* **4,** 174–177 (2010).
81. Reimer, M. E. *et al.* Bright single-photon sources in bottom-up tailored nanowires. *Nat. Commun.* **3,** 737 (2012).
82. Munsch, M. *et al.* Dielectric GaAs antenna ensuring an efficient broadband coupling between an InAs quantum dot and a Gaussian optical beam. *Phys. Rev. Lett.* **110,** 177402 (2013).
83. Gschrey, M. *et al.* Highly indistinguishable photons from deterministic quantum-dot microlenses utilizing three-dimensional *in situ* electron-beam lithography. *Nat. Commun.* **6,** 7662 (2015).
84. Sapienza, L., Davanco, M., Badolato, A. & Srinivasan, K. Nanoscale optical positioning of single quantum dots for bright and pure single-photon emission. *Nat. Commun.* **6,** 7833 (2015).
85. Holmes, M. J., Choi, K., Kako, S., Arita, M. & Arakawa, Y. Room-temperature triggered single photon emission from a III-nitride site-controlled nanowire quantum dot. *Nano Lett.* **14,** 982–986 (2014).
86. Kako, S. *et al.* A gallium nitride single-photon source operating at 200 K. *Nat. Mater.* **5,** 887–892 (2006).
87. Deshpande, S., Das, A. & Bhattacharya, P. Blue single photon emission up to 200 K from an InGaN quantum dot in AlGaN nanowire. *Appl. Phys. Lett.* **102,** 161114 (2013).
88. Park, Y.-S., Guo, S., Makarov, N. S. & Klimov, V. I. Room temperature single-photon emission from individual perovskite quantum dots. *ACS Nano* **9,** 10386–10393 (2015).
89. Nowak, A. K. *et al.* Deterministic and electrically tunable bright single-photon source. *Nat. Commun.* **5,** 3240 (2014).
90. Shambat, G. *et al.* Ultrafast direct modulation of a single-mode photonic crystal nanocavity light-emitting diode. *Nat. Commun.* **2,** 539 (2011).
91. Reithmaier, G. *et al.* On-chip generation, routing, and detection of resonance fluorescence. *Nano Lett.* **15,** 5208–5213 (2015).
92. Murray, E. *et al.* Quantum photonics hybrid integration platform. *Appl. Phys. Lett.* **107,** 171108 (2015).
93. Arcari, M. *et al.* Near-unity coupling efficiency of a quantum emitter to a photonic crystal waveguide. *Phys. Rev. Lett.* **113,** 093603 (2014).
94. Heindel, T. *et al.* Electrically driven quantum dot-micropillar single photon source with 34% overall efficiency. *Appl. Phys. Lett.* **96,** 011107 (2010).
95. Deshpande, S., Heo, J., Das, A. & Bhattacharya, P. Electrically driven polarized single-photon emission from an InGaN quantum dot in a GaN nanowire. *Nat. Commun.* **4,** 1675 (2013).
96. Palacios-Berraquero, C. *et al.* Atomically thin quantum light-emitting diodes. *Nat. Commun.* **7,** 12978 (2016).
97. Clark, G. *et al.* Single defect light-emitting diode in a van der Waals heterostructure. *Nano Lett.* **16,** 3944–3948 (2016).
98. Mizuochi, N. *et al.* Electrically driven single-photon source at room temperature in diamond. *Nat. Photon.* **6,** 299–303 (2012).
99. Lohrmann, A. *et al.* Diamond based light-emitting diode for visible single-photon emission at room temperature. *Appl. Phys. Lett.* **99,** 251106 (2012).
100. Salter, C. L. *et al.* An entangled-light-emitting diode. *Nature* **465,** 594–597 (2010).
101. Zaitsev, A. M., Bergman, A. A., Gorokhovsky, A. A. & Huang, M. B. Diamond light emitting diode activated with Xe optical centers. *Phys. Status Solidi A* **203,** 638–642 (2006).
102. Berhane, A. M. *et al.* Electrical excitation of silicon-vacancy centers in single crystal diamond. *Appl. Phys. Lett.* **106,** 171102 (2015).
103. Wong, D. *et al.* Characterization and manipulation of individual defects in insulating hexagonal boron nitride using scanning tunnelling microscopy. *Nat. Nanotech.* **10,** 949–953 (2015).
104. Pelton, M. Modified spontaneous emission in nanophotonic structures. *Nat. Photon.* **9,** 427–435 (2015).
105. Benson, O. Assembly of hybrid photonic architectures from nanophotonic constituents. *Nature* **480,** 193–199 (2011).
106. Englund, D. *et al.* Deterministic coupling of a single nitrogen vacancy center to a photonic crystal cavity. *Nano Lett.* **10,** 3922–3926 (2010).
107. Kolchin, P. *et al.* High Purcell factor due to coupling of a single emitter to a dielectric slot waveguide. *Nano Lett.* **15,** 464–468 (2015).
108. Hoang, T. B., Akselrod, G. M. & Mikkelsen, M. H. Ultrafast room-temperature single photon emission from quantum dots coupled to plasmonic nanocavities. *Nano Lett.* **16,** 270–275 (2016).
109. Miura, R. *et al.* Ultralow mode-volume photonic crystal nanobeam cavities for high-efficiency coupling to individual carbon nanotube emitters. *Nat. Commun.* **5,** 5580 (2014).
110. Yalla, R., Sadgrove, M., Nayak, K. P. & Hakuta, K. Cavity quantum electrodynamics on a nanofiber using a composite photonic crystal cavity. *Phys. Rev. Lett.* **113,** 143601 (2014).
111. Albrecht, R., Bommer, A., Deutsch, C., Reichel, J. & Becher, C. Coupling of a single nitrogen-vacancy center in diamond to a fiber-based microcavity. *Phys. Rev. Lett.* **110,** 243602 (2013).
112. Liu, X. *et al.* Strong light–matter coupling in two-dimensional atomic crystals. *Nat. Photon.* **9,** 30–34 (2015).
113. Schmitt-Manderbach, T. *et al.* Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.* **98,** 010504 (2007).
114. Lo, H. K., Ma, X. F. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94,** 230504 (2005).
115. Takemoto, K. *et al.* Quantum key distribution over 120 km using ultrahigh purity single-photon source and superconducting single-photon detectors. *Sci. Rep.* **5,** 14383 (2015).
116. Guha, S. *et al.* Rate-loss analysis of an efficient quantum repeater architecture. *Phys. Rev. A* **92,** 022357 (2015).
117. Azuma, K., Tamaki, K. & Lo, H.-K. All-photonic quantum repeaters. *Nat. Commun.* **6,** 6787 (2015).
118. Pant, M., Krovi, H., Englund, D. & Guha, S. Rate-distance tradeoff and resource costs for all-optical quantum repeaters. Preprint at https://arXiv.org/abs/1603.01353 (2016).
119. Li, Y., Humphreys, P. C., Mendoza, G. J. & Benjamin, S. C. Resource costs for fault-tolerant linear optical quantum computing. *Phys. Rev. X* **5,** 041007 (2015).
120. Peruzzo, A. *et al.* Quantum walks of correlated photons. *Science* **329,** 1500–1503 (2010).
121. Rohde, P. P. Boson sampling with photons of arbitrary spectral structure. *Phys. Rev. A* **91,** 012307 (2015).
122. He, Y.-M. *et al.* On-demand semiconductor single-photon source with near-unity indistinguishability. *Nat. Nanotech.* **8,** 213–217 (2013).
123. Nilsson, J. *et al.* Quantum teleportation using a light-emitting diode. *Nat. Photon.* **7,** 311–315 (2013).
124. Rondin, L. *et al.* Magnetometry with nitrogen-vacancy defects in diamond. *Rep. Prog. Phys.* **77,** 056503 (2014).
125. Bernien, H. *et al.* Heralded entanglement between solid-state qubits separated by three metres. *Nature* **497,** 86–90 (2013).
126. Aspelmeyer, M., Kippenberg, T. J. & Marquardt, F. Cavity optomechanics. *Rev. Mod. Phys.* **86,** 1391–1452 (2014).

127. Yeo, I. *et al.* Strain-mediated coupling in a quantum dot-mechanical oscillator hybrid system. *Nat. Nanotech.* **9,** 106–110 (2014).
128. Teissier, J., Barfuss, A., Appel, P., Neu, E. & Maletinsky, P. Strain coupling of a nitrogen-vacancy center spin to a diamond mechanical oscillator. *Phys. Rev. Lett.* **113,** 020503 (2014).
129. Ovartchaiyapong, P., Lee, K. W., Myers, B. A. & Jayich, A. C. B. Dynamic strain-mediated coupling of a single diamond spin to a mechanical resonator. *Nat. Commun.* **5,** 4429 (2014).
130. Khanaliloo, B. *et al.* Single-crystal diamond nanobeam waveguide optomechanics. *Phys. Rev. X* **5,** 041051 (2015).
131. MacQuarrie, E. R., Gosavi, T. A., Jungwirth, N. R., Bhave, S. A. & Fuchs, G. D. Mechanical spin control of nitrogen-vacancy centers in diamond. *Phys. Rev. Lett.* **111,** 227602 (2013).
132. Burek, M. J. *et al.* Diamond optomechanical crystals. Preprint at http://arXiv.org/abs/1512.04166 (2016).
133. Bracher, D. O. & Hu, E. L. Fabrication of high-*Q* nanobeam photonic crystals in epitaxially grown 4H-SiC. *Nano Lett.* **15,** 6202–6207 (2015).
134. Tiarks, D., Baur, S., Schneider, K., Dürr, S. & Rempe, G. Single-photon transistor using a Förster resonance. *Phys. Rev. Lett.* **113,** 053602 (2014).
135. Hwang, J. *et al.* A single-molecule optical transistor. *Nature* **460,** 76–80 (2009).
136. Fuechsle, M. *et al.* A single-atom transistor. *Nat. Nanotech.* **7,** 242–246 (2012).
137. Shomroni, I. *et al.* All-optical routing of single photons by a one-atom switch controlled by a single photon. *Science* **345,** 903–906 (2014).
138. Neu, E. *et al.* Single photon emission from silicon-vacancy centres in CVD-nano-diamonds on iridium. *New J. Phys.* **13,** 025012 (2011).
139. Schröder, T., Gädeke, F., Banholzer, M. J. & Benson, O. Ultrabright and efficient single-photon generation based on nitrogen-vacancy centres in nanodiamonds on a solid immersion lens. *New J. Phys.* **13,** 055017 (2011).
140. Siyushev, P. *et al.* Low-temperature optical characterization of a near-infrared single-photon emitter in nanodiamonds. *New J. Phys.* **11,** 113029 (2009).
141. Siyushev, P. *et al.* Coherent properties of single rare-earth spin qubits. *Nat. Commun.* **5,** 3895 (2014).
142. Luozhou, L. *et al.* Efficient photon collection from a nitrogen vacancy center in a circular bullseye grating. *Nano Lett.* **15,** 1493–1497 (2015).

Acknowledgements

We thank C.-Y. Lu for discussions, and G. Fuchs, P. Barclay, D. Lake, R. Johne and A. Fiore for assistance with images. Financial support from the Australian Research Council (via DP140102721, IH150100028, DE130100592), FEI Company, the Asian Office of Aerospace Research and Development grant FA2386-15-1-4044, the Army Research Laboratory, the Center for Distributed Quantum Information program and the Air Force Office of Scientific Research Multidisciplinary University Research Initiative (FA9550-14-1-0052) is gratefully acknowledged.

Additional information

Reprints and permissions information is available online at www.nature.com/reprints. Correspondence should be addressed to I.A.

Competing financial interests

The authors declare no competing financial interests.

Chapter 5

Bell basis and Photon Detection

For two-particle entanglement, there are four possible Bell states that define a basis:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}[|H_1H_2\rangle + |V_1V_2\rangle] \tag{5.1}$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}[|H_1H_2\rangle - |V_1V_2\rangle] \tag{5.2}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}[|H_1V_2\rangle + |V_1H_2\rangle] \tag{5.3}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}[|H_1V_2\rangle - |V_1H_2\rangle] \tag{5.4}$$

We can generalize these into:

$$|\Phi\rangle = \frac{1}{\sqrt{2}}[|H_1H_2\rangle + e^{i\theta}\,|V_1V_2\rangle] \tag{5.5}$$

$$|\Psi\rangle = \frac{1}{\sqrt{2}}[|H_1V_2\rangle + e^{i\theta}\,|V_1H_2\rangle] \tag{5.6}$$

The state $|\Phi\rangle$ has positive correlations: both measurements yield the same results. The state $|\Psi\rangle$ has negative correlations: each measurement yields opposite results.

But what is the physical meaning of the phase factor? Is there a measurable difference between $|\Phi^+\rangle$ and $|\Phi^-\rangle$?

To look for an answer, we can use another basis than H and V, we can use D and A: diagonal and anti-diagonal.

We express $|H\rangle$ and $|V\rangle$ in the $|D\rangle$ and $|A\rangle$ basis:

$$|H\rangle = \frac{1}{\sqrt{2}}[|D\rangle + |A\rangle] \tag{5.7}$$

$$|V\rangle = \frac{1}{\sqrt{2}}[|D\rangle - |A\rangle] \tag{5.8}$$

We can then express $|HH\rangle$ and $|VV\rangle$ in terms of $|A\rangle$ and $|D\rangle$:

$$|HH\rangle = |H\rangle\,|H\rangle \tag{5.9}$$

$$= \frac{1}{\sqrt{2}}[|D\rangle + |A\rangle][|D\rangle + |A\rangle] \tag{5.10}$$

$$= \frac{1}{\sqrt{2}}[|DD\rangle + |AA\rangle + |AD\rangle + |DA\rangle] \tag{5.11}$$

$$|VV\rangle = |V\rangle\,|V\rangle \tag{5.12}$$

$$= \frac{1}{\sqrt{2}}[|D\rangle - |A\rangle][|D\rangle - |A\rangle] \tag{5.13}$$

$$= \frac{1}{\sqrt{2}}[|DD\rangle - |AD\rangle - |DA\rangle + |AA\rangle] \tag{5.14}$$

We can rewrite the general state $|\Phi\rangle = \frac{1}{\sqrt{2}}[|HH\rangle + e^{i\theta}|VV\rangle]$ in the D,A basis:

$$|\Phi\rangle = \frac{1}{2\sqrt{2}}[|DD\rangle + |AA\rangle + |AD\rangle + |DA\rangle + e^{i\theta}(|DD\rangle - |DA\rangle - |AD\rangle + |AA\rangle)] \tag{5.15}$$

$$= \frac{1}{2\sqrt{2}}[(1+e^{i\theta})(|DD\rangle + |AA\rangle) + (1-e^{i\theta})(|DA\rangle - |AD\rangle)] \tag{5.16}$$

We see that θ has a physical meaning! For example, for $\theta = 0$ we measure high counts for positive correlations (DD and AA) but for $\theta = \pi$ that is $\phi^+ = HH + VV$ we measure high count rates for positive correlations (DD + AA). The phase therefore tells us about the type of correlations we have in the other basis.

5.1 Single Photon detection

A near infrared photon carries 10^{-19} Joules, a typical electrical pulse used for computer communication carries 10^{10} more energy. This means that to detect a single photon and process the detection event with conventional electronics, we need a very large amplification factor of the order of 10^{10}. It is under debate whether the human eye is able to detect single photons, it might be able to detect small numbers of photons but with a time resolution that makes it irrelevant for most experiments in physics.

The photo-multiplier tube (often referred to as PMT) has been used since the 1930s to detect single photons, it is based on the photoelectric effect where an incoming photon knocks off an electron from a metal that is then accelerated in vacuum towards another metal plate to release more electrons, this process is repeated several times to produce a macroscopic current. Note that Einstein was awarded the Nobel prize in 1922 for his discovery of the law of the photoelectric effect.

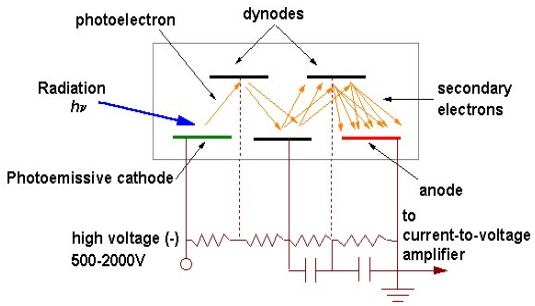


Figure 5.1: The photo-multiplier tube.

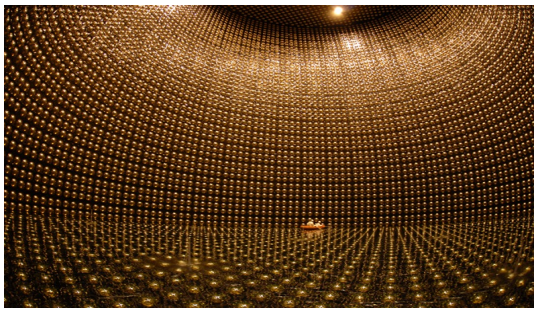


Figure 5.2: The Super Kamiokande: Photo Multiplier tubes are used to detect single photons linked to neutrinos.

A very important characteristic of a light detector is its detection efficiency, sometimes called quantum efficiency, this is the probability to generate a detection event when a photon reaches the detector. Limitations with the detection efficiency of the photo-multiplier tube were addressed with avalanche photo-diodes that are very compact, monolithic semiconductor devices and can therefore be mass produced with standard electronics fabrication processes. Detection efficiencies in excess of 60% can be achieved in the near-visible but time resolution and noise levels are not as good as one might wish for. The avalanche photo-diode is made of a pin semiconductor diode, Silicon can be used but then is limited by its bandgap of 1.1 eV: photons with energy lower than 1.1 eV are not absorbed by silicon and are not detected. Other semiconductors such as InGaAs can be used, with a lower bandgap to be able to detect light at telecom frequencies. These devices can be made very small and consume a small amount of power, they are however still not ideal as their detection efficiency is

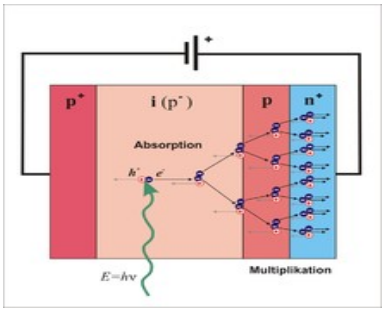


Figure 5.3: The avalanche photodiode.

still far below 100%, they have important dark counts (detection events generated in the absence of incoming light), they have limited time resolution (the timing between a photon reaching the detector and a detection pulse being generated fluctuates widely).

The most recent type of single photon detector to be developed is the superconducting single photon detector where superconducting nanostructures can switch from the superconducting state to the resistive state with the absorption of a single photon, this results in very high detection efficiencies approaching 100%, as well as very good time resolution better than 10 ps and in very law noise levels in the mHz range. It is interesting to note that 10 ps is the time it take light to travel 3 mm, this is particularly useful for LiDAR applications where a 3 dimensional image is created by measuring the return time of a laser pulse.

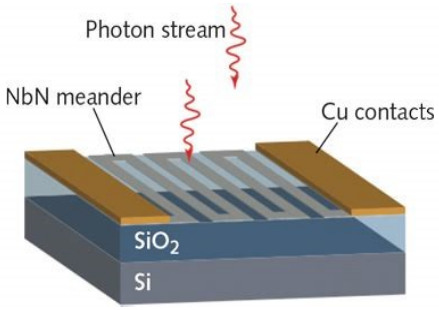


Figure 5.4: The Superconducting Nanowire Single Photon Detector (SNSPD).

Key performance indicators for single photon detectors: Time resolution: uncertainty in the timing of the output electrical pulse for a fixed photon absorption time. Dark noise: detection pulses generated by the detector in the absence of incident photons. On the order of hundreds of photons per second for a usual avalanche photodiode. The dark noise can be far less than one event per second for state of the art superconducting single photons. Dead time: time interval following a detection event where the detector is not able to detect an incoming photon. Quantum efficiency: probability for a photon to generate a detection event. Detection range: there is no device able to detect efficiently single photons from the UV to the mid-infrared. The detection range must also be taken into account. There are additional considerations such as size, cost, power consumption when selecting a single photon detector.

A practical photon number detector remains to be invented, all we have at our disposal today are 'click' detectors: if one photon or more impinges the detector, it generates a detection pulse, irrespective of the number of impinging photons. Note that resolving the number of photons is not impossible, a bolometer does just that, it measures the amount of heat deposited by a pulse of light on a detector (hence proportional to the number of photons). When operated very precisely with low enough noise, it is possible to distinguish the heat associated with one photon from the heat associated with two photons at optical frequencies. This can be done with a Transition Edge Sensor (TES) where the heat deposited on a nanoscale piece of Tungsten is measured with an accuracy that allows to distinguish the number of photons, this device is however very slow and operates at very low temperatures in the mK range, requiring bulky and expensive cooling systems.

Question: if the detection efficiency of a photon number resolving detector is less than unity, what happens to the fidelity of the measurement? For instance if a 2 photon state is incident on a detector with 50% detection efficiency, the probability that the two photons are detected is only 25%, this is the fidelity of the measurement. We see that for the fidelity to be high, we need very high detection efficiencies.

REVIEW ARTICLES | FOCUS
PUBLISHED ONLINE: 30 NOVEMBER 2009 | DOI: 10.1038/NPHOTON.2009.230
nature photonics

Single-photon detectors for optical quantum information applications

Robert H. Hadfield

The past decade has seen a dramatic increase in interest in new single-photon detector technologies. A major cause of this trend has undoubtedly been the push towards optical quantum information applications such as quantum key distribution. These new applications place extreme demands on detector performance that go beyond the capabilities of established single-photon detectors. There has been considerable effort to improve conventional photon-counting detectors and to transform new device concepts into workable technologies for optical quantum information applications. This Review aims to highlight the significant recent progress made in improving single-photon detector technologies, and the impact that these developments will have on quantum optics and quantum information science.

One of Einstein's key contributions to modern science was to recognize that light is fundamentally composed of individual packets of energy, now referred to as photons[1,2]. The energy of a single photon in the visible or near-infrared range is around 10^{-19} J. A single-photon detector is an extremely sensitive device capable of registering these quantum objects. Single-photon detectors now support and enable a host of applications at the frontiers of science and engineering. Conventional single-photon detectors are based on photomultipliers and avalanche photodiodes, and are used in a wide range of time-correlated single-photon counting (TCSPC) applications[3]. However, the major driver for single-photon detector development has been the rapidly expanding interest in optical quantum information (QI) applications[4]. Quantum information technologies use individual quantum objects (such as photons) to encode and manipulate information[5], and promise to have a dramatic technological impact in the twenty-first century[6]. The most mature of these innovations is quantum key distribution (QKD)[7,8], the most secure form of communication yet devised, and is now at the point of becoming commercially viable. Perhaps the most ambitious photonic QI application is linear optical quantum computing (LOQC)[9–11] — a scalable paradigm for QI processing and computation. LOQC remains a distant but tantalizing objective, and significant efforts have been mobilized worldwide towards this goal. A major reason that advanced QI technologies such as LOQC are so difficult to realize is the stringent demands these applications place on optical components such as single-photon detectors[12]. Significant improvements are required in terms of their signal-to-noise ratio, detection efficiency, spectral range and ability to resolve photon number (the number of photons reaching the detector simultaneously). Scientists and engineers around the world have taken up this challenge. Their efforts have led to considerable improvements in conventional single-photon detectors and to the emergence of new photon-counting technologies.

Quantifying the performance of single-photon detectors

The performance of a single-photon detector should be assessed[8,13] in terms of its spectral range, dead time, dark count rate, detection efficiency, timing jitter and ability to resolve photon number. We will consider these characteristics in detail, in particular with reference to the requirements of different optical QI applications. Spectral range, dead time, dark count rate, detection efficiency and timing jitter are all important general benchmarks for single-photon detectors, and the ability to resolve photon number is required in advanced QI protocols[10,11]. We will outline accurate measurement strategies for characterizing single-photon detectors and discuss an appropriate 'figure of merit' for quantifying detector performance.

Spectral range. A photon counter is only sensitive over a certain spectral range determined by its constituent materials. The operating wavelength of interest depends on the particular application. For free-space optical applications (either bench-top quantum optics experiments[13] or line-of-sight QKD through the atmosphere[8]) visible or near-infrared wavelengths are used to exploit the best commercially available detectors. Losses in optical fibre are lowest at a wavelength of 1,550 nm, making this wavelength a clear choice for long distance QKD in optical fibres[8]. Other advanced optical components such as on-chip waveguides are also tailored to telecommunications wavelengths. There is therefore considerable interest in the field of QI in telecommunications-wavelength detectors.

Dead time. The detector 'dead time' or recovery time, τ, is the time interval that follows the absorption of a photon, during which the detector is unable to reliably register a second photon. The factors influencing τ depend strongly on the detector type. In many cases, the measured value of τ is that of the bias circuit or the counting electronics, rather than the detector element itself. In semiconductor single-photon detectors, τ is deliberately lengthened to suppress afterpulsing, the spontaneous retriggering of the detector after an initial detection event. The dead time limits the maximum count rate of the detector but not the clock rate of the experiment, which can be much higher because TCSPC experiments are typically operated in the regime where the number of detected photons per clock cycle is much less than one.

Dark count rate. Most practical detector technologies have a finite probability of recording false counts, known as dark counts, dark noise or dark current, which arise either due to the materials properties of the detector, the biasing conditions or the susceptibility to external noise. In practical applications, the dark count rate of interest, D, is that measured with the detector embedded in the experiment — dark count measurements of completely shielded detectors can give unrealistic values that are of little help or guidance to potential users. D is usually given by a rate in hertz, but can be mitigated by gating or time-stamping the detection events. The minimum time interval for gating or time-stamping is set by the timing jitter of the detector.

Scottish Universities Physics Alliance and the School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, UK.
e-mail: r.h.hadfield@hw.ac.uk

Box 1 | Measurement of the detection efficiency, η

Measurement of η, the probability of registering a count if a photon arrives at the detector, can be achieved through two distinct methods.

Calibrated light source method

This method (Fig. B1a) relies on calibrating a light source with a power meter and then attenuating the output heavily to determine the incident power P. The number of incident photons per second is given by $R_{incident} = P\lambda/hc$, where λ is the wavelength and hc/λ is the energy per photon. One would expect that measurements using either pulsed or continuous wave (CW) sources should give the same reading. If, however, the detector recovery is affected by even a weak photon flux (as in the case of many semiconductor detectors where photon absorption affects the occupancy of low-lying trap states), then a pulsed measurement, in which the frequency f is lower than $1/\tau$ (where τ is the detector dead time), is the more reliable of the two measurements. Moreover, detector saturation or afterpulsing is easier to detect in a pulsed measurement. However, it is important to note that optical power meters are often only accurately calibrated for CW input power.

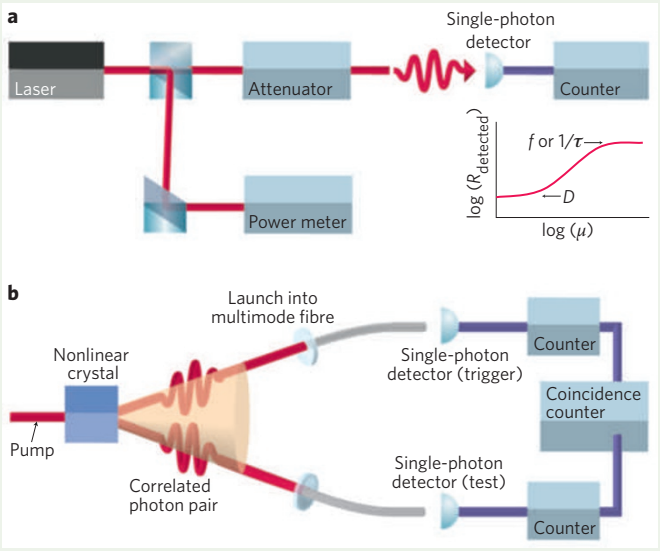


Figure B1 | Determination of single-photon detector efficiency. **a**, Calibrated laser method. A continuous wave or pulsed laser is measured using a calibrated power meter. A series of calibrated attenuators are then used to reduce the photon flux μ to less than one photon per time interval. The count rate of the detector $R_{detected}$ is recorded over a range of values of μ. Typically, $R_{detected}(\mu)$ will be of the form shown in the inset. In the continuous-wave case, $R_{detected}$ will saturate at the inverse of the detector (or counter) recovery time, τ. In the pulsed case, saturation should occur at the repetition frequency of the laser, f. At low values of μ, the residual count rate is due to dark counts in the detector. At intermediate values of μ, the signature of a single-photon detector is that $R_{detected}$ is proportional to μ. **b**, Correlated photon method. This method avoids the need for a calibrated power meter. A pair of correlated photons is produced from spontaneous parametric down-conversion source. The signal and idler photons are routed to the test and trigger detectors, then the respective count rates — including coincidences between the two channels — are recorded. The detection efficiency of the test detector channel is given by the coincidence rate divided by the count rate at the trigger detector.

Measurement using a CW source. For the case of a CW measurement of η, the fundamental time interval is set by τ. The mean photon number per time interval, μ, is

$$\mu = R_{incident}\,\tau$$

For a Poissonian light source in the limit of $\mu\eta << 1$, the count rate of an ideal detector is

$$R_{detected} = \frac{1}{\tau}(1-\exp(-\mu\eta)) \approx \frac{\mu\eta}{\tau}$$

The true count rate due to actual photodetection events, $R'_{detected}$, can be derived by correcting for the separately measured dark count rate D and the dead time τ, giving

$$R'_{detected} = \left(\frac{R_{detected}}{1 - R_{detected}\tau} - \frac{D}{1 - D\tau}\right)$$

The detection efficiency is therefore

$$\eta = \frac{R'_{detected}}{R_{incident}} = \tau\left(\frac{R_{detected}}{1 - R_{detected}\tau} - \frac{D}{1 - D\tau}\right)\Big/\mu$$

The parameters η, μ and τ can be determined by analysing a plot of $R_{detected}$ against the photon flux per time interval, μ (Fig. B1a, inset). At low numbers of detected photons ($\mu\eta << 1$) the signature of single-photon sensitivity is that $R_{detected} \propto \mu$, but a detector triggered by a two-photon event would give $R_{detected} \propto \mu^2$.

Measurement using a pulsed source. For a pulsed source of frequency $f << 1/\tau$ and a mean photon number per pulse μ,

$$R_{incident} = \mu f$$

$$R_{detected} = f(1-\exp(-\mu\eta)) \approx \mu\eta f$$

One would therefore expect the detector count rate to saturate under high photon flux at the clock rate of the source. In this case, the detection efficiency is given by

$$\eta = \frac{R_{detected}}{R_{incident}} = \left(\frac{R_{detected}}{1 - R_{detected}\tau} - \frac{D}{1 - D\tau}\right)\Big/\mu f$$

Correlated photon method

The correlated photon method (Fig. B1b) uses a source of correlated photons to characterize the detector[14,15]. Remarkably, this elegant technique requires no calibrated power meter. Photons from the pump laser of frequency ω_p are converted into signal and idler photons of frequency ω_s and ω_i, respectively, by spontaneous parametric down-conversion, which conserves energy and momentum such that $\omega_p = \omega_s + \omega_i$. The signal and idler photons are directed to the test and trigger detectors. Coincidences between the two detector channels are recorded. N is the number of photon pairs emitted in the counting period. The counts in the test and trigger detector are given by $N_1 = \eta_1 N$ and $N_2 = \eta_2 N$, respectively, and the total coincidence counts are given by $N_{coinc} = \eta_1\eta_2 N$. The detection efficiency of the test detector is therefore $\eta_1 = N_{coinc}/N_2$, which is independent of the efficiency of the trigger channel. This technique, however, only gives the overall efficiency of the test detector channel, which is problematic for small (<100 μm diameter) detectors.

NATURE PHOTONICS DOI: 10.1038/NPHOTON.2009.230

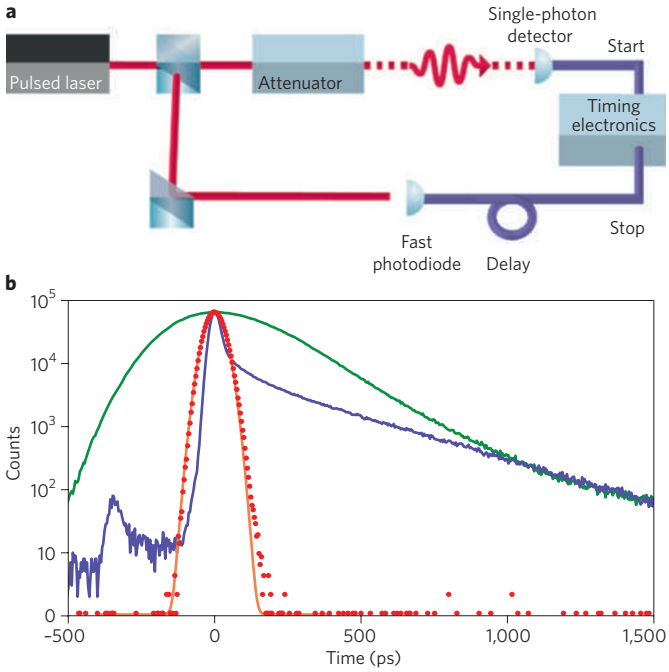


Figure 1 | Measurement of timing jitter. a, The timing jitter of a single-photon detector is the variation in delay between the absorption of a photon and the generation of an output electrical pulse. To measure the timing jitter accurately, a picosecond pulsed laser and high-resolution timing electronics are required to ensure that the dominant jitter is that of the detector. A count on the single-photon detector triggers the 'start' for the timing electronics, and the delayed clock pulse from the laser signals the 'stop'. A histogram of start–stop time intervals is accumulated over multiple clock cycles, giving the instrument response of the single-photon detector. **b**, Instrument responses of three types of single-photon detector, measured using a mode-locked Ti:Sapphire laser at 780 nm and picosecond timing electronics. The thick junction Si SPAD (green) has a FWHM response of ~400 ps, the shallow junction SPAD (blue) has a FWHM response of ~40 ps but with a strongly asymmetric instrument response function, and the superconducting nanowire single-photon detector (red) has a FWHM response of 68 ps with a Gaussian shape. Part **b** reproduced with permission from ref. 16, © 2009 AIP.

Detection efficiency. The detection efficiency, η, is defined as the overall probability of registering a count if a photon arrives at the detector. In most photon-counting applications a high value of η is certainly desirable, but it is by no means the only practical consideration. The maximum rate at which data can be accumulated in an experiment is governed by both the mean photon number per time interval, μ, and the maximum count rate of the detector, $1/\tau$. Moreover, signal-to-noise considerations are often the true determining factor as to whether an experiment is feasible. The exception is LOQC[9], where an extremely high value of η is essential. For scalable LOQC (even with new cluster-state protocols[10,11]), overall optical losses, including collection from the source, cannot fall below a 67% threshold[12].

Methods of accurately determining η are shown in Box 1, either by using a calibrated light source (Fig. B1a) or correlated photon pairs (Fig. B1b)[14,15]. In the ideal case, the detection efficiency is defined as $\eta = R_{\text{detected}}/R_{\text{incident}}$, where R_{detected} is the count rate and R_{incident} is the photon arrival rate. The intrinsic quantum efficiency of the actual device is not the paramount concern for the user; the practical detection efficiency η must include the optical coupling efficiency to the detector (through free-space optics or optical fibres). The overall detection efficiency η of a detector channel is therefore the product of coupling losses, η_{loss}, and the intrinsic quantum efficiency of the detector, η_{det}, such that $\eta = \eta_{\text{loss}}\,\eta_{\text{det}}$. When η is measured accurately, the dead time τ of the detector and the counting electronics must be considered. Furthermore, the measured count rate of the detector, R_{detected}, should be corrected for the finite dark count rate of the detector.

Timing jitter. This is the variation in the time interval between the absorption of a photon and the generation of an output electrical pulse from the detector. A reliable method of measuring Δt for a single-photon detector is shown in Fig. 1a. The full-width half-maximum (FWHM) of the detector instrument response function provides a benchmark for timing jitter. Many detectors have a non-Gaussian instrument response function, however, and this should be taken into account in any detailed analysis. The maximum clock rate of a photon counting experiment (where the mean detected photon number is given by $\eta\mu << 1$) is determined by the timing resolution, and jitter in the source or detector will cause counts to stray into neighbouring clock cycles. Typically, but not always, the detector jitter is dominant. Examples of instrument response functions for three detectors are shown in Fig. 1b[16].

Ability to resolve photon number. Most conventional single-photon detectors can only distinguish between zero or 'one or more' photons[10,17]. This binary response means that a multiphoton pulse triggers the same output signal as a single photon. QI protocols require single-photon states, which are difficult to prepare in practice because attenuated laser pulses obey Poissonian statistics; the probability of producing a photon state $|n\rangle$ is $P(n) = (\mu^n/n!)e^{-\mu}$, where $\mu = \langle n \rangle$ is the mean number of photons per pulse[2]. On-demand single-photon sources for QI applications are a highly active research field. Despite significant progress[18,19], current single-photon sources are imperfect because the second-order correlation function $g^{(2)}(0)$ is non-zero, implying residual multiphoton emission, and also because source emission rates are low (that is, $\mu << 1$). In QKD, multiphoton states represent a security 'loophole' that can be exploited by eavesdroppers. In LOQC[9–11], efficient detection of all photons is crucial for reducing errors. Photon number resolution has been achieved in two ways (Fig. 2). First, certain single-photon detector types (such as superconducting transition edge sensors) intrinsically produce a pulse proportional to the number of photons absorbed (Fig. 2a)[20]. The second method multiplexes conventional detectors[17]. This can be achieved either by combining the output signals of an array of detectors (spatial multiplexing; Fig. 2b)[21,22] or by splitting the multiphoton pulse via a cascade of beamsplitters and then delaying the signals so that they can be detected sequentially by a single detector (time multiplexing; Fig. 2c)[23]. The fidelity with which an n-photon state can be recorded scales as η^n — thus, high-efficiency detectors are desirable for these applications. In a multiplexed photon-number-resolving scheme, it is necessary to have a large number of pixels (or time bins) N, such that $N >> n$, to reduce the possibility that two or more photons were absorbed at any one pixel.

Figures of merit for single-photon detectors. The most widely quoted figure of merit for photodetectors is the noise equivalent power (NEP)[24], and this has proved useful for optical power measurements. For single-photon detectors, the NEP can be given by

$$\frac{h\nu}{\eta}\sqrt{2D}$$

where ν is the photon frequency and h is Planck's constant. The units of NEP are W $\text{Hz}^{-1/2}$, and the lowest possible value of NEP is desirable. However, a typical detector (one that does not resolve photon

number) does not measure optical power. Furthermore, NEP does not take into account the timing performance of the detector, nor does it relate D and η in a meaningful way for QI experiments. For example, in a QKD experiment, the detector contribution to the quantum-bit error rate (QBER) is the ratio of the dark count rate to the sifted detected photon rate (the detected rate after comparison of the transmission and receiving bases). Furthermore, D can be reduced by setting the timing window as small as possible. Unless some other factor (the jitter of a single-photon source, for example) has a dominant role, the minimum timing interval is usually limited by the timing jitter of the detector. We can therefore formulate a dimensionless figure of merit that takes all of these factors into consideration, giving

$$H = \eta/(D\Delta t)$$

This is a useful figure not only for QKD but also for a range of TCSPC measurements, both in QI applications and beyond. Better detectors have a higher value of H at the wavelength of interest.

This section has rigorously considered the characterization of single-photon detectors and devised an appropriate figure of merit for optical QI applications. It is crucial to understand these characteristics when selecting the best detector for a given experiment or application. Established and emerging single-photon detectors are compared through these metrics in Table 1.

Established single-photon detector technologies

This section reviews the current performance and future prospects of established single-photon detector technologies. In each case, the operating principle, performance, advantages and disadvantages of each detector type are discussed. Performance characteristics are shown in Table 1. New developments and the potential for further improvements in performance are also noted. Short reviews have been given previously elsewhere[10,17,18], and recent special issues devoted to the topic of photon-counting technologies are also recommended reading[4,25].

Photomultiplier tubes. The most long-established photon-counting technology is the photomultiplier tube (PMT). Single-photon counting in PMTs was demonstrated in 1949[26], and this development heralded the birth of the field of TCSPC[3,27]. Commercial PMT units are now widely available[28,29], and there are continued efforts to improve these devices. Photomultiplier tubes offer large active-areas (diameters of >10 mm) and cover the spectral range of 115–1,700 nm, but with large variations in performance.

A basic PMT consists of a vacuum tube with a photocathode for light absorption, from which electrons are liberated through the photoelectric effect (the energy of the incident photon must exceed the work function of the photocathode material). This single- or few-electron photocurrent is then multiplied by a cascade of secondary electron-emissions from dynodes — a series of electrodes, each one biased at a greater positive voltage than the one before — producing a macroscopic current pulse of $>10^6$ electrons. Traditional PMTs require large operating voltages around the kilovolt-level, and are fragile and expensive. In certain types of PMT, the excess noise of the multiplication process is sufficiently low to allow some discrimination between one or multiple photons. An alternative configuration is the microchannel plate photomultiplier tube, where glass capillaries are fused in parallel and coated with a secondary electron-emitting material to achieve a single continuous dynode under a bias voltage[30]. Microchannel plate PMTs offer improved timing jitter over basic PMTs, down to ~20 ps at FWHM[30].

Photomultiplier tubes have a maximum efficiency of around 40% at a wavelength of 500 nm in GaAsP photocathodes, and have dark

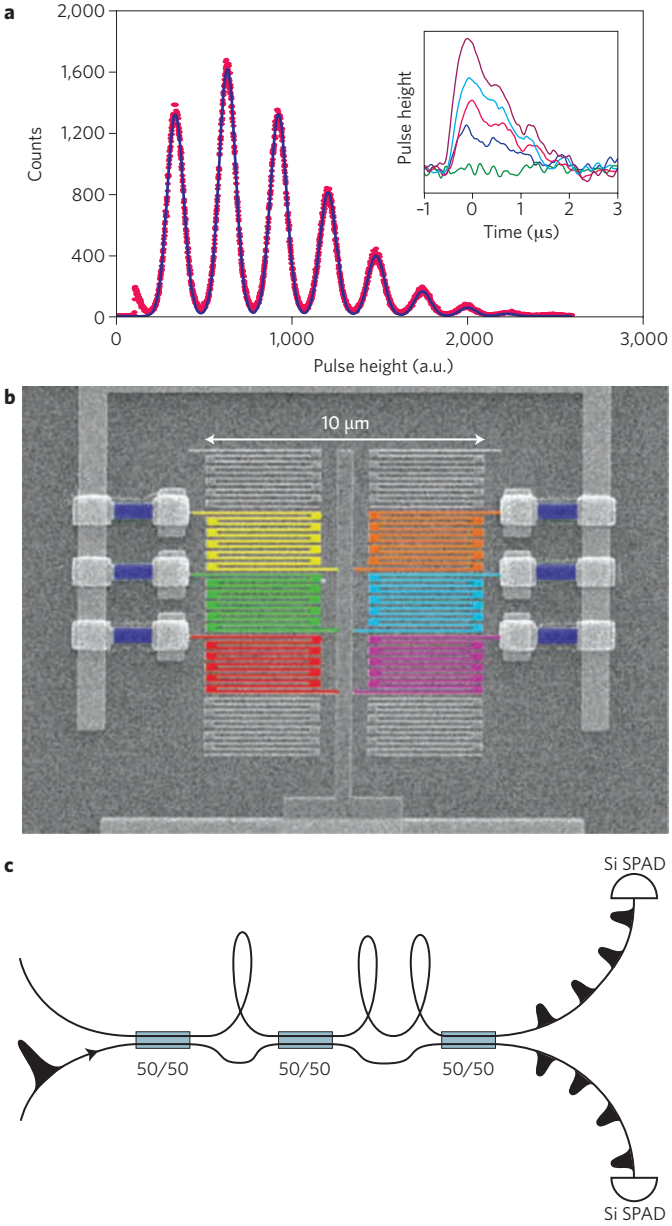


Figure 2 | Photon number resolution. Conventional single-photon detectors give a digital response — an output pulse or 'click' indicates the arrival of one or more photons. Determining the number of photons in a pulse requires a photon-number-resolving detector. **a**, True photon number resolution. Detectors with true photon number resolution give an output that depends on the number of photons absorbed. The superconducting TES is essentially a microcalorimeter — the height of the pulse is proportional to the number of photons at a given wavelength. The figure shows a TES measurement of Poissonian statistics with a mean photon number per pulse of 2.45 at 1,550 nm. The line shows a plot of best-fit to the data, convolving the Poissonian distribution with the energy resolution of the TES. Shown inset is the TES pulse heights for zero to four photons. **b**,**c**, Conventional single-photon detectors can be combined through spatial or temporal multiplexing to achieve photon number resolution. In spatial multiplexing (**b**), an array of detector pixels (in this case SNSPDs) are broadly illuminated and read-out in parallel. When several pixels are triggered simultaneously, the output pulses are summed. In temporal multiplexing (**c**), The input optical pulse is split via a network of delayed paths such that each photon can be picked out within the dead time interval of the detector pair. Image in **b** reproduced with permission from ref. 22, © 2008 NPG.

NATURE PHOTONICS DOI: 10.1038/NPHOTON.2009.230

Table 1 | Comparison of single-photon detectors.

Detector type	Operation temperature (K)	Detection efficiency, η	Jitter time, Δt (FWHM)	Dark count rate, D (ungated)	Figure of merit	Max. count rate	Resolves photon number?	Class of report
PMT (visible–near-infrared)[31]	300	40% @500 nm	300 ps	100 Hz	1.33×10^7	10 MHz	Yes	†
PMT (infrared)[32]	200	2% @1,550 nm	300 ps	200 kHz	3.33×10^2	10 MHz	Yes	†
Si SPAD (thick junction)[38]	250	65% @650 nm	400 ps	25 Hz	6.5×10^7	10 MHz	No	†
Si SPAD (shallow junction)[41]	250	49% @550 nm	35 ps	25 Hz	5.6×10^8	10 MHz	No	†
InGaAs SPAD (gated)[55]	200	10% @1,550 nm	370 ps	91 Hz	2.97×10^5	10 kHz	No	‡
InGaAs SPAD (self-differencing)[57]	240	10% @1,550 nm	55 ps	16 kHz	1.14×10^5	100 MHz	Yes	‡
Frequency up-conversion[65]	300	9% @1,550 nm	400 ps	13 kHz	1.7×10^4	10 MHz	No	‡
Frequency up-conversion[65]	300	2% @1,550 nm	40 ps	20 kHz	2.5×10^4	10 MHz	No	‡
VLPC[69]	6	88% @694 nm	—	20 kHz	—	—	Yes	§
VLPC*	6	34% @633 nm	270 ps	7 kHz	1.83×10^5	—	Yes	§
TES[76]	0.1	50% @1,550 nm	100 ns	3 Hz	1.67×10^6	100 kHz	Yes	‡
TES[20]	0.1	95% @1,550 nm	100 ns	—	—	100 kHz	Yes	§
SNSPD (meander)[90]	3	0.7% @1,550 nm	60 ps	10 Hz	1.16×10^7	100 MHz	No	‡
SNSPD (new)[87]	1.5	57% @1,550 nm	30 ps	—	—	1 GHz	No	§
QD (resonant tunnel diode)[96]	4	12% @550 nm	150 ns	2×10^{-3} Hz	4×10^9	250 kHz	No	§
QD (field-effect transistor)[93]	4	68% @805 nm	—	—	—	1 Hz	Yes	§

The class of report indicates the conditions under which the detector characteristics were measured; † represents a commercial product specification, ‡ represents the use of the detector in a practical experiment and § represents a measurement of device performance. *Unpublished data, Burm Baek, NIST, USA, 2009.

count rates as low as 100 Hz (ref. 31). The highest reported count rates are up to 10 MHz, and the typical jitter is 300 ps at FWHM[31]. PMTs are now available at telecommunications wavelengths[31] by cooling an InP/InGaAs photocathode to 200 K. Performance is poor compared with visible-wavelength PMTs, however, with a detection efficiency of 2% at 1,550 nm, a dark count rate of 200 kHz and a jitter of ~300 ps at FWHM. Another important development has been the hybrid photodetector, which combines a photocathode with a low-capacitance avalanche photodiode[33]. Hybrid photodetectors require low bias voltages of around 400 V, offer 46% efficiency at 500 nm, and have a timing jitter of 61 ps at FWHM and ~1 kHz dark count rates[33].

Single-photon avalanche photodiodes. Silicon single-photon avalanche photodiodes (Si SPADs; Fig. 3a,b)[34] are now a well-established alternative to PMTs in laboratory quantum optics experiments[13] and free-space QKD systems. These solid-state devices offer low dark count rates, high detection efficiencies and high count rates in the visible to near-infrared range. The long wavelength cut-off is a result of the semiconductor bandgap of Si. In the UV range, absorption occurs before the photon reaches the detection region.

The SPAD is based on an avalanche photodiode structure (a p–n or p–i–n junction). The diode is reverse-biased above the breakdown voltage, and this is known as Geiger mode operation. Carriers generated by photon absorption undergo avalanche gain, triggering a macroscopic breakdown of the diode junction[35]. To harness this effect in a practical device, the avalanche must be stopped and the device reset by a quenching circuit[34,36].

The highest efficiency commercial devices are based on a thick, 180-μm-diameter high-purity silicon absorber combined with an active quenching circuit and cooling in a single practical module[37,38]. These devices offer single-photon sensitivity in the 400–1,000 nm range and achieve a peak efficiency of 65% at ~650 nm (ref. 38). Dark count rates can be as low as 25 Hz (ref. 36) and the timing jitter is typically ~400 ps at FWHM[16] (Fig. 1b). The operating voltage is low at around 400 V. In Si SPADs the afterpulsing probability is low, with quenching times of approximately 50 ns. Although the excess noise of the multiplication process is too high in SPADs to achieve intrinsic photon number resolution, efforts have been made to achieve this indirectly by exploiting timing walk effects[39]or through spatial-[21] or temporal-multiplexing[23] schemes. Photon emission by hot carriers in an avalanche current ('backflash' photons) can potentially be exploited by eavesdroppers in QKD schemes[40].

A new generation of Si SPAD devices are now available[41]. These are shallow-junction planar devices[42] that have a diameter of 50 μm and require only low operating voltages. The timing is greatly improved to below 40 ps at FWHM (Fig. 1b), but the peak detection efficiency is reduced to 49% at 550 nm.

Silicon SPADs remain an active area of development[43]. Efforts are underway to integrate detector elements directly with quenching circuitry[44], and also to realize millimetre-scale SPAD arrays with low dark counts and minimal crosstalk[45]. The silicon photomultiplier device — an array of SPAD pixels that are read in parallel — can

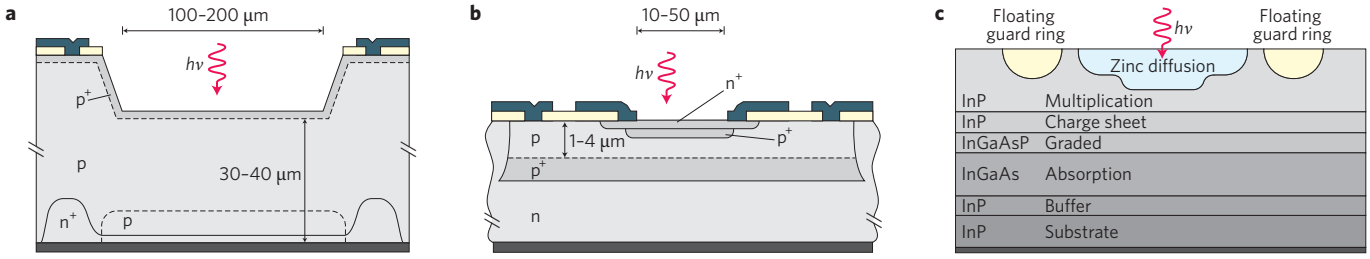


Figure 3 | Established photon-counting technologies based on reverse-biased avalanche photodiodes. a, Thick-junction Si SPAD, a device structure optimized for high detection efficiency and low dark counts. **b**, Shallow-junction planar Si SPAD, a device structure optimized for low timing jitter requiring low bias voltages. **c**, InGaAs/InP SPAD structure, where the use of a smaller-bandgap semiconductor extends single-photon sensitivity to telecommunications wavelengths. Figures reproduced with permission from: **a**,**b**, ref. 43, © 2004 Taylor & Francis; **c**, ref. 52, © 2006 IEEE.

offer extremely high count rates (~400 MHz) and photon number resolution, but suffer from elevated dark counts[46].

To extend the performance of SPADs to telecommunciations wavelengths (λ = 1,310 nm and 1,550 nm) it is necessary to use lower-bandgap semiconductor materials such as Ge and InGaAs. The best results have been achieved with an InGaAs absorption region and an InP multiplication layer, giving single-photon sensitivities across the 1,000–1,600 nm wavelength range and peak efficiencies of ~20% at 1,550 nm (refs 47–52). The diameter of the active device is ~40 μm, which is suitable for fibre coupling. Owing to materials defects, these devices suffer from dark count rates that are orders of magnitude higher than for their Si counterparts. As a result, InGaAs SPADs are typically operated in gated Geiger mode[51] — the quiescent device is biased beneath the breakdown voltage, then a short (~1 ns) pulse is applied, coincident with the expected arrival of a photon. The dark count rate can be reduced to ~10 kHz (including gating) by cooling to ~200 K, but this reduction in temperature exacerbates afterpulsing, causing long detector dead times of around 10 μs and reducing counting rates to ~100 kHz. These devices are now commercially available[53,54] and have allowed fibre QKD systems to reach distances beyond 100 km (ref. 55).

Much of the ongoing effort to improve InGaAs SPAD performance is targeted at QI applications such as QKD. Imaginative biasing and gating schemes, combined with higher-temperature operating schemes to reduce afterpulsing, have led to increased device clock rates[56–58], thus increasing overall bit-rates in QKD[57]. It is also possible to extract multiphoton sensitivity through such methods[59]. Passive quenching at low excess bias can enable free-running operation[60]. Looking ahead, SPADs based on new materials systems such as HgCdTe (ref. 61) may lead to improved long-wavelength performance.

Emerging single-photon detector technologies

We now review a selection of the most promising emerging single-photon detector technologies under consideration for use in QI applications. The operating principle, performance, advantages and disadvantages of each detector are detailed. Where possible, the properties of each emerging technology are compared with those of the established single-photon detector types in Table 1. Instances where these emerging technologies have been implemented in optical QI experiments are highlighted. Recent developments and the potential for future improvements of these technologies are also discussed.

Frequency up-conversion. The goal of frequency up-conversion single-photon detection schemes is to convert a telecommunications-wavelength photon to a shorter wavelength that can be more efficiently detected by a commercial single-photon detector. An example of such a scheme is illustrated in Fig. 4a. The mechanism used is sum-frequency generation in a nonlinear optical crystal: a weak signal at frequency ω_{in} is combined with a strong pump signal at frequency ω_{pump} to yield an output signal at the summation frequency of $\omega_{out} = \omega_{in} + \omega_{pump}$. If sufficient pump power is available, this frequency up-conversion can occur with near-unity efficiency. For example, in periodically poled lithium niobate, using a pump signal at 1,064 nm allows 1,550-nm photons to be converted to 630-nm photons with 90% efficiency[62]. There are several technical challenges in achieving high-efficiency up-conversion. The first is to achieve the desired field strength, either through a coincident pump and signal pulse[63], a continuous-wave pump pulse and a build up cavity[62], or by using a waveguide to concentrate the pump power into a small interaction region[64]. Drawbacks include the difficulty of stabilizing the nonlinear crystal, the presence of nonlinear processes that lead to fluorescence at the up-conversion wavelength (resulting in very high background count rates), and high in- and output coupling losses for waveguides. Up-conversion schemes using thick-junction Si SPADs have shown system detection efficiencies of 46% for 1,550-nm photons, with a jitter of 400-ps at FWHM and dark count rates of 800 kHz (ref. 65). Shallow-junction Si SPADs have also been used, achieving a system detection efficiency of 2% at 1,550 nm, a FWHM jitter of 40 ps and a dark count rate of 20 kHz (ref. 66). Low-jitter hybrid photodetectors have also been used in conjunction with up-conversion[67]. All three variants have been implemented in QKD demonstrations[65–67]. Recent studies have also shown that coherent up-conversion of quantum states is feasible[68], which is an important step for advanced QI applications.

Visible-light photon counters. The visible-light photon counter (VLPC) is a low-temperature semiconductor-based photon counting technology[69–71]. The device offers high-efficiency detection of single photons up to wavelengths of 1 μm, the ability to resolve photon number, good timing resolution and moderate dark counts.

The VLPC is based on an earlier concept called the solid-state photomultiplier, a blocked-impurity-band device based on As-doped silicon, which gives single-photon sensitivity from visible wavelengths up to 30 μm. Solid-state photomultiplier and VLPC devices operate at low voltage through a controlled single-carrier multiplication process, giving rise to a signal that is proportional to the photon number. In a VLPC the gain region and absorber are separate, maximizing the sensitivity in the wavelength range of 400–1,000 nm. A schematic of the device architechture is shown in Fig. 4b. An electron–hole pair is generated in the undoped (intrinsic) Si absorber region, and the resulting hole triggers an avalanche in the gain region through interaction with As impurity levels. This single-carrier multiplication process only requires a small bias voltage of 6–7.5 V, but the device temperature must be carefully tuned to around 6 K to achieve optimal performance. As the avalanche is confined to a 20-μm-wide filament and the overall device diameter is 1 mm, two photons can produce distinct concurrent avalanches if the focal spot is large. The low excess noise of the multiplication

NATURE PHOTONICS DOI: 10.1038/NPHOTON.2009.230

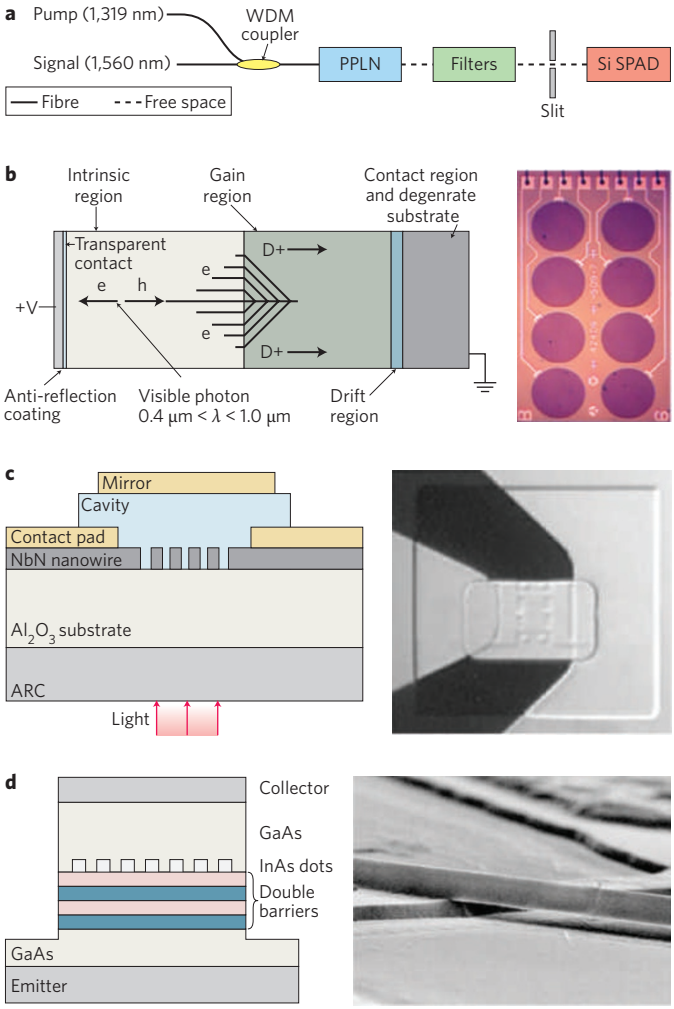


Figure 4 | Emerging single-photon detectors: a selection of promising technologies. a, Frequency up-conversion detector. A 1,560-nm photon is converted to a 715-nm photon through sum frequency generation in a periodically poled lithium niobate waveguide, and is detected by a Si SPAD. WDM, wavelength-division multiplexer. **b**, Visible-light photon counter. This is a low-tempertature semiconductor technology. The single-carrier multiplication process allows for photon number resolution. A device schematic (left) and an optical micrograph of eight VLPC pixels (right) are shown. **c**, A next-generation superconducting nanowire single-photon detector, showing the device schematic (left) and optical micrograph (right). A niobium nitride (NbN) SNSPD is embedded in a resonant cavity to enhance the detection efficiency. ARC, anti-reflection coating. **d**, A detector based on a quantum dot resonant tunelling diode, showing the device schematic (left) and a scanning electron micrograph of the cross-wire device structure (right). Figures reproduced with permission from: **a**, ref. 65, © 2005 IOP; **b**, ref. 71, © 2003 IEEE; **c**, ref. 87, © 2005 OSA; **d**, ref. 96, © 2005 APS.

process is close to the theoretical minimum, allowing up to five photons to be resolved[70,71]. VLPC detection efficiencies of up to 88% at 694 nm and 93% in the infrared have been observed, neglecting coupling losses and spectral filtering[69]. The dark count rate is ~20 kHz at the maximum detection efficiency. The dead time of the VLPC is ~100 ns, and therefore the upper limit to the count rate is ~100 kHz. The jitter of these devices has recently been measured at 633 nm (unpublished data, Burm Baek, NIST, USA, 2009), and the lowest value obtained is 250 ps at FWHM in the dark count range of 6.9–25 kHz, with a maximum fibre-coupled detection efficiency of 40%.

VLPCs are highly desirable for QI applications requiring high detection efficiency and photon number resolution. So far, VLPCs have been successfully used in studies of photon statistics in non-classical parametric down-conversion sources[72].

Superconducting transition-edge sensors. Superconducting transition-edge sensors (TESs) are low-temperature devices that offer very-high-efficiency single-photon detection with photon-number-resolving capability and low dark count rates. In a TES, the detector element is a superconducting film on the cusp of the superconducting transition, where any change in temperature will cause an abrupt change in resistance[73]. The absorption of an incident photon heats the device, causing the voltage-biased detector to draw a current that can be read out using a SQUID amplifier. The signal is proportional to the energy of the photon or, at fixed wavelength, the photon number[74]. This intrinsic ability to resolve photon number is illustrated in Fig. 2a[20]. These detectors operate at temperatures of around 100 mK and therefore require sophisticated cooling technology. The current tungsten-based detectors have a detection efficiency of 20%[75] — which increases to 95% efficiency at 1,550 nm (ref. 20) when they are embedded in an optical cavity structure — and have negligible dark counts. In practical implementations, the effective dark count rate may rise due to room-temperature blackbody radiation[76]. This effect can be mitigated by filtering, but this reduces the detection efficiency. The photon-number-resolving capabilities are excellent — up to eight photons can be resolved clearly[20]. High-efficiency devices for the near-infrared (~850 nm) have also recently been reported[77]. The timing properties of TES detectors are relatively poor, with jitter times of around 100 ns at FWHM. The dead time of the detector is limited by the thermal time constant of the detector element, and is typically ~1 μs. Faster detectors, with dead times around 100 ns, can be fabricated using films of higher transition temperatures[77], but these devices require faster SQUID read-out electronics.

TES detectors have so far been successfully implemented in quantum optics experiments[78] and long-distance QKD[76,79]. Owing to their near-unity detection efficiency and ability to resolve photon number, these detectors are highly promising candidates for fundamental tests of quantum mechanics, LOQC and optical quantum metrology applications.

Superconducting nanowire single-photon detectors Superconducting nanowire single-photon detectors (SNSPDs) offer single-photon sensitivity from visible to mid-infrared wavelengths, low dark counts, short recovery times and low timing jitter.

The detector element itself is a 100-nm-wide nanowire that is patterned by electron-beam lithography in an ultrathin niobium nitride superconducting film[80]. It operates in the temperature range of 1.5–4 K, well below the superconducting transition temperature of the niobium nitride film. The material is chosen because of its exceptionally fast photoresponsive properties[81]. The superconducting wire is biased just below its critical current, which is the point at which the wire becomes resistive. When a photon strikes the wire, a local resistive hotspot is formed, perturbing the current distribution and thus triggering a fast voltage-pulse[80] that can then be amplified and measured. The detection efficiency and dark count rate are both dependent on the bias point, with the dark count rate rising more steeply close to the critical current.

Current devices consist of a 'meander wire'[82] that covers an area of up to 20 μm × 20 μm (ref. 83) to achieve a high coupling efficiency between the nanowire and a single-mode optical fibre. The device is embedded in a microwave coplanar waveguide to facilitate the read-out of fast voltage pulses. Fabrication of large-area detectors is challenging

because the wire must be completely uniform along its length — a constriction at any point in the wire will negate the sensitivity of the rest of the detector[84]. The use of a single, long meander wire increases the overall inductance, lengthening the detector dead time[85] to around 10 ns for large-area detectors[86] — although this is a significant increase, it is still an order of magnitude faster than conventional photon counters. The intrinsic efficiency of small-area (3 μm × 3.3 μm) single-layer SNSPDs is as high as 20% at 1,550 nm, which is close to the expected absorption of the material[87]. Fibre-coupled large-area SNSPDs offer practical detection efficiencies of >1% at 1,550 nm, with dark count rates below 1 kHz (refs 83,86). The timing jitter of the device is extremely good (compared with Si SPADs[16]; Fig. 1b) — 65 ps at FWHM can be achieved in large-area devices[19], and 30 ps FWHM or less in small-area devices[87].

An exciting aspect of this technology is that considerable performance improvements are well within reach. SNSPDs have been integrated into low-Q optical cavity structures with back-reflector mirrors (the device architecture and an optical micrograph are shown in in Fig. 4c). This improves the intrinsic detection efficiency to as much as 57% for small-area devices[87]. The addition of a cavity does not degrade the timing performance of the detector. A limitation of current niobium nitride devices is that they must be grown on lattice-matched substrates (sapphire or MgO) at high temperatures (>600 °C). The demonstration of high-quality devices on alternative substrates, such as NbTiN deposited at room temperature on Si (ref. 88), will increase the versatility of this detector technology. Multipixel SNSPD devices have also recently been demonstrated[20,89]. Such devices provide spatially multiplexed photon number resolution, allowing larger detector areas to be achieved with both low timing jitter and short recovery times.

Basic meander-type SNSPDs[82] have now been widely implemented in optical QI applications. Fibre-coupled SNSPDs can be integrated into practical, closed-cycle refrigerator systems operating at ~3 K (ref. 86), widening the range of accessible applications. SNSPDs have had a major impact in the field of QKD, leading to record transmission distances and bit-rates in optical fibres[90]. As next-generation high-efficiency devices[87] become available, the importance of these detectors in optical QI science and technology is expected to continue increasing.

Single-photon detectors based on quantum dots and semiconductor defects. Another new class of devices utilize the trapping of charge in defects to achieve single-photon detection. Semiconductor heterostructures based on III–V compounds form the basic device architecture: either quantum dots (QDs) embedded in the material[91–97] or intrinsic defects[98] are exploited to achieve trapping. QDs are favoured as they can be controllably placed within the heterostructure to maximize internal efficiency and signal uniformity. Two main detection schemes have been realized. The first relies on a photoconductive gain mechanism that involves trapping charge in a defect or QD layer, which alters the conductance in a field-effect transistor structure[91–95,98]. These types of device have been operated at count rates of up to 400 kHz (ref. 92), and a high internal efficiency of up to 68% has been demonstrated at 805 nm (ref. 93). Resolution of up to three photons in such devices has also been shown[94,95].

The second scheme relies on photo-absorption in a QD, which alters the tunnelling probability in a resonant tunnel diode structure[96,97]. Quantum-dot-resonant tunnel diode devices have demonstrated single-photon detection efficiencies of up to 12% at 550 nm, jitter of 150 ns and very low dark count rates (down to 2×10^{-3} Hz). Devices of this type have recently been realized at telecommunications wavelengths[97].

These devices are currently at an early stage of development; the only successful demonstrations have been carried out at cryogenic temperatures (~4 K). Low dark count rates have been reported. Device performance seems to be limited by large timing jitter, and practical detection efficiencies are low because of the micrometre-scale device areas. Improvements are anticipated, however, and if sources of noise can be eliminated, higher temperature operation may be possible. Furthermore, resonant cavities may boost device efficiency. This class of detectors offers intriguing prospects for future QIP technologies. There is a clear compatibility with III–V semiconductor QD single-photon sources[19]. There is also potential for these types of structures to achieve spin-preserving photodetection[99]; transferring photon polarization to electron or hole spin is one possible candidate for emerging quantum memory and repeater technologies.

Outlook and conclusion

This review has summarized key performance parameters and defined a figure of merit for single-photon detectors in optical quantum information applications. The current performance of established and emerging detector technologies has also been reviewed. Semiconductor-based detectors such as single-photon avalanche diodes have attained a high level of maturity and are widely used in laboratory quantum optics and quantum information experiments. There are ongoing efforts to improve the performance of single-photon avalanche diodes at telecommunications wavelengths, for quantum information applications such as long-distance quantum key distribution in optical fibre. To meet the demands of new quantum information applications, a host of new single-photon detector technologies are being rapidly devised, developed, evaluated and deployed. As a result, low-temperature detectors with infrared sensitivity, excellent timing resolution and a high signal-to-noise ratio, such as superconducting nanowire single-photon detectors, have set new benchmarks in long distance, high-bit-rate quantum key distribution. Visible-light photon counters and superconducting transition-edge sensors now offer near-unity detection efficiency and the ability to resolve photon number, which are both prerequisites for scalable linear optical quantum computing. These improvements in detector technology are therefore having an immediate scientific impact, allowing the frontiers of quantum information science and quantum optics to be pushed forward. Moreover, these new single-photon detector technologies are poised to have a profound impact in a range of fields far beyond that of quantum information. There is widespread demand for improved single-photon detectors, particularly at infrared wavelengths; such technologies are eagerly awaited in fields as diverse as astronomy, laser ranging, remote sensing, classical communications and biomedical imaging.

References

1. Einstein, A. On a heuristic point of view about the creation and conversion of light. *Ann. Phys. (Leipz.)* **17,** 132–148 (1905).
2. Loudon, R. *Quantum Theory of Light* 3rd edn, Ch. 1 (Oxford Univ. Press, 2000).
3. Becker, W. *Advanced Time-Correlated Single Photon Counting Techniques* Ch. 2 (Springer, 2005).
4. Migdall, A. Introduction to journal of modern optics special issue on single-photon: detectors, applications, and measurement methods. *J. Mod. Opt.* **51,** 1265–1266 (2004).
5. Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* Ch. 1 (Cambridge Univ. Press, 2000).
6. Zoller, P. *et al.* Quantum information processing and communication. *Eur. Phys. J. D* **36,** 203–228 (2005).
7. Bennett, C. H. & Brassard, G. in *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing, Bangalore* 175–179 (1984).
8. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74,** 145–195 (2002).
9. Knill, E., Laflamme, R. & Milburn, G. J. A scheme for efficient quantum computation with linear optics. *Nature* **409**, 46–52 (2001).
10. Kok, P. *et al.* Linear optical quantum computing with photonic qubits. *Rev. Mod. Phys.* **79,** 135–175 (2007).
11. O'Brien, J. L. Optical quantum computing. *Science* **318,** 1567–1570 (2007).

12. Varnava, M., Browne, D. E. & Rudolph, T. How good must single photon sources and detectors be for efficient linear optical quantum computation? *Phys. Rev. Lett.* **100,** 060502 (2008).
13. Bachor, H.-A. & Ralph, T. C. *A Guide to Experiments in Quantum Optics* 2nd edn, Ch. 7 (Wiley-VCH, 2004).
14. Rarity, J. G., Ridley, K. D. & Tapster, P. R. Absolute measurement of detector quantum efficiency using parametric downconversion. *Appl. Opt.* **26,** 4616–4619 (1987).
15. Ware, M. & Migdall A. Single-photon detector characterization using correlated photons: the march from feasibility to metrology. *J. Mod. Opt.* **51,** 1549–1557 (2004).
16. Stevens, M. J. *et al.* Fast lifetime measurements of infrared emitters using a low-jitter superconducting single-photon detector. *Appl. Phys. Lett.* **89,** 031109 (2006).
17. Silberhorn, C. Detecting quantum light. *Contemp. Phys.* **48,** 143–156 (2007).
18. Kumar, P. *et al.* Photonic technologies for quantum information processing. *Quantum Inf. Process.* **3,** 215–231 (2004).
19. Shields, A. J. Semiconductor quantum light sources. *Nature Photon.* **1,** 215–223 (2007).
20. Lita, A. E., Miller, A. J. & Nam, S. W. Counting near-infrared single-photons with 95% efficiency. *Opt. Express* **16,** 3032–3040 (2008).
21. Jiang, L. A., Dauler, E. A. & Chang, J. T. Photon-number-resolving detector with 10 bits of resolution. *Phys. Rev. A* **75,** 062325 (2007).
22. Divochiy, A. *et al.* Superconducting nanowire photon-number-resolving detector at telecommunication wavelengths. *Nature Photon.* **2,** 302–306 (2008).
23. Achilles, D., Silberhorn, C., Sliwa, C., Banaszek, K. & Walmsley, I. A. Fiber-assisted detection with photon-number resolution. *Opt. Lett.* **28,** 2387–2389 (2003).
24. Donati, S. *Photodetectors: Devices, Circuits and Applications* Ch. 3 (Prentice Hall, 2000).
25. Cheung, J., Migdall, A. & Rastello, M.-L. Single-photon sources, detectors, applications and measurement methods. *J. Mod. Opt.* **56,** 139–140 (2009).
26. Morton, G. A. Photomultipliers for scintillation counting. *RCA Rev.* **10,** 525–553 (1949).
27. Poultney, S. K. Single-photon detection and timing: experiments and techniques. *Adv. Electron. El. Phys.* **31,** 39–117 (1972).
28. http://jp.hamamatsu.com/.
29. http://www.burle.com/index.html.
30. Kume, H., Koyama, K., Nakatsugawa, K., Suzuki, S. & Fatlowitz, D. Ultrafast microchannel plate photomultipliers. *Appl. Opt.* **27,** 1170–1178 (1988).
31. http://jp.hamamatsu.com/resources/products/etd/pdf/m-h7422e.pdf.
32. http://jp.hamamatsu.com/resources/products/etd/pdf/NIR-PMT_APPLI_TPMO1040E02.pdf.
33. Fukasawa, A., Haba, J., Kageyama, A., Nakazawa, H. & Suyama, M. High speed HPD for photon counting. *IEEE Trans. Nucl. Sci.* **55,** 758–762 (2008).
34. Cova, S., Longoni, A. & Andreoni, A. Towards picoseconds resolution with single-photon avalanche diodes. *Rev. Sci. Inst.* **52**, 408–412 (1981).
35. Haitz, R. H. Mechanisms contributing to the noise pulse rate of avalanche diodes. *J. Appl. Phys.* **36,** 3123–3131 (1965).
36. Brown, R. G. W., Jones, R., Rarity, J. G. & Ridley, K. D. Characterization of silicon avalanche photodiodes for photon correlation measurements 2: Active quenching. *Appl. Opt.* **26,** 2383–2389 (1987).
37. Daudet, H. *et al.* Photon counting techniques with silicon avalanche photodiodes. *Appl. Opt.* **32,** 3894–3900 (1993).
38. http://optoelectronics.perkinelmer.com/content/RelatedLinks/SpecificationSheets/SPC_PhotoDetectors.pdf.
39. Blazej, J. Photon number resolving in Geiger mode avalanche photodiode photon counters. *J. Mod. Opt.* **51,** 1491–1498 (2004).
40. Kurtsiefer, C., Zarda, P., Mayer, S. & Weinfurter, H. The breakdown flash of silicon avalanche photodiodes — a back door for eavesdropper attacks? *J. Mod. Opt.* **48,** 2039–2047 (2001).
41. http://www.microphotondevices.com/products_pdm.asp.
42. Cova, S., Lacaita, A., Ghioni, M., Ripamonti, G. & Louis, T. A. 20-ps timing resolution with single-photon avalanche diodes. *Rev. Sci. Inst.* **60,** 1104–1110 (1989).
43. Cova, S., Ghioni, M., Lotito, A., Rech, I. & Zappa, F. Evolution and prospects for single-photon avalanche diodes and quenching circuits. *J. Mod. Opt.* **51,** 1267–1288 (2004).
44. Zappa, F., Ghioni, M., Cova, S., Samori, C. & Giudice, A. C. An integrated active-quenching circuit for single-photon avalanche diodes. *IEEE Trans. Instr. Meas.* **49,** 1167–1175 (2000).
45. Rech, I. *et al.* Optical crosstalk in single photon avalanche diode arrays: a new complete model. *Opt. Express* **16,** 8381–8394 (2008).
46. Eraerds, P., Legré, M., Rochas, A., Zbinden, H. & Gisin, N. SiPM for fast photon-counting and multiphoton detection. *Opt. Express* **15,** 14539–14549 (2007).
47. Lacaita, A., Zappa, F., Cova, S. & Lovati, P. Single-photon detection beyond 1 μm: performance of commercially available InGaAs/InP detectors *Appl. Opt.* **35,** 2986–2996 (1996).
48. Ribordy, G., Gautier, J.-D., Zbinden, H. & Gisin, N. Performance of InGaAs/InP avalanche photodiodes as gated-mode photon counters. *Appl. Opt.* **37,** 2272–2277 (1998).
49. Rarity, J. G., Wall, T. E., Ridley, K. D., Owens, P. C. M. & Tapster, P. R. Single-photon counting for the 1300–1600-nm range by use of Peltier-cooled and passively quenched InGaAs avalanche photodiodes. *Appl. Opt.* **39,** 6746–6753 (2000).
50. Hiskett, P. A. *et al.* Performance and design of InGaAs/InP photodiodes for single-photon counting at 1.55 μm. *Appl. Opt.* **39,** 6818–6829 (2000).
51. Bethune, D. S. & Risk, W. P. An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light. *IEEE J. Quant. Elect.* **36,** 340–347 (2000).
52. Pellegrini S. *et al.* Design and performance of an InGaAs-InP single-photon avalanche diode detector. *IEEE J. Quant. Elect.* **42,** 397–403 (2006).
53. http://www.princetonlightwave.com/content/PGA-400%20V1.0.pdf.
54. http://www.idquantique.com/products/files/id201-specs.pdf.
55. Gobby, C., Yuan, Z. L. & Shields, A. J. Quantum key distribution over 122 km of standard telecom fiber. *Appl. Phys. Lett.* **84,** 3762–3764 (2004).
56. Namekata, N., Sasamori, S. & Inoue, S. 800 MHz single-photon detection at 1550-nm using an InGaAs/InP photodiode operated with a sine wave gating. *Opt. Express* **14,** 10043–10049 (2006).
57. Dixon, A. R., Yuan, Z. L., Dynes, J. F., Sharpe, A. W. & Shields, A. J. Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate. *Opt. Express* **16,** 18790–18797 (2008).
58. Thew, R. T., Stucki, D., Gautier, J.-D., Zbinden, H. & Rochas, A. Free-running InGaAs/InP avalanche photodiode with active quenching for single photon counting at telecom wavelengths. *Appl. Phys. Lett.* **91,** 201114 (2007).
59. Kardynał, B. E., Yuan, Z. L. & Shields, A. J. An avalanche-photodiode-based photon-number-resolving detector. *Nature Photon.* **2,** 425–428 (2008).
60. Warburton, R. E., Itzler, M. & Buller, G. S. Free-running room temperature operation of an InGaAs/InP single-photon avalanche diode. *Appl. Phys. Lett.* **94,** 071116 (2009).
61. Rogalski, A., Antoszewski, J. & Faraone, L. Third-generation infrared photodetector arrays. *J. Appl. Phys.* **105,** 091101 (2009).
62. Albota, M. A. & Wong, F. N. C. Efficient single-photon counting at1.55 μm by means of frequency upconversion. *Opt. Lett.* **29**, 1449–1451 (2004).
63. Vandevender, A. P. & Kwiat, P. G. High efficiency single-photon detection via frequency up-conversion. *J. Mod. Opt.* **51,** 1433–1445 (2004).
64. Langrock, C. *et al.* Highly efficient single-photon detection at communication wavelengths by use of upconversion in reverse-proton exchanged periodically poled $LiNbO_3$ waveguides. *Opt. Lett.* **30,** 1725–1727 (2005).
65. Takesue, H. *et al.* Differential phase shift quantum key distribution experiment over 105 km fibre. *New J. Phys.* **7,** 232–243 (2005).
66. Thew, R. T. *et al.* Low jitter up-conversion detectors for telecom wavelength GHz QKD. *New J. Phys.* **8,** 32–43 (2006).
67. Zhang, Q. *et al.* Megabits secure key rate quantum key distribution. *New J. Phys.* **11,** 045010 (2009).
68. Tanzilli, S. *et al.* A photonic quantum information interface. *Nature* **437,** 116–120 (2005).
69. Takeuchi, S., Kim, J., Yamamoto, Y. & Hogue H. H. Development of a high-quantum-efficiency single-photon counting system. *Appl. Phys. Lett.* **74**, 1063–1065 (1999).
70. Kim, J., Takeuchi, S., Yamamoto, Y. & Hogue, H. H. Multiphoton detection using visible light photon counter. *Appl. Phys. Lett.* **74,** 902–904 (1999).
71. Waks, E. *et al.* High-efficiency photon-number detection for quantum information processing. *IEEE J. Sel. Top. Quant.* **9,** 1502–1511 (2003).
72. Waks, E., Diamanti, E., Sanders, B. C., Bartlett, S. D. & Yamamoto, Y. Direct observation of nonclassical photon statistics in parametric down-conversion. *Phys. Rev. Lett.* **92,** 113602 (2004).
73. Cabrera, B. *et al.* Detection of single infrared, optical and ultraviolet photons using superconducting transition edge sensors. *Appl. Phys. Lett.* **73,** 735–737 (1998).
74. Miller, A. J., Nam, S. W., Martinis, J. M. & Sergienko, A. V. Demonstration of a low-noise near-infrared photon counter with multiphoton discrimination. *Appl. Phys. Lett.* **83**, 791–793 (2003).
75. Rosenberg, D., Lita, A. E., Miller, A. J. & Nam, S. W. Noise-free high-efficiency photon-number-resolving detectors. *Phys. Rev. A* **71**, 061803 (2005).
76. Rosenberg, D. *et al.* Long-distance decoy-state quantum key distribution in optical fiber. *Phys. Rev. Lett.* **98,** 010503 (2007).
77. Fukuda, D. *et al.* Photon number resolving detection with high speed and high quantum efficiency. *Metrologia* **46,** S288–S292 (2009).
78. Di Giuseppe, G. *et al.* Direct observation of photon pairs at a single output port of a beam-splitter interferometer. *Phys. Rev. A* **68,** 063817 (2003).

79. Rosenberg, D. *et al.* Quantum key distribution at telecom wavelengths with noise-free detectors. *Appl. Phys. Lett.* **88,** 021108 (2006).
80. Gol'tsman, G. N. *et al.* Picosecond superconducting single-photon optical detector. *Appl. Phys. Lett.* **79,** 705–707 (2001).
81. Il'in, K. S. *et al.* Picosecond hot-electron energy relaxation in NbN superconducting photodetectors. *Appl. Phys. Lett.* **76,** 2752–2754 (2000).
82. Verevkin, A. *et al.* Detection efficiency of large-active-area NbN single-photon superconducting detectors in the ultraviolet to near-infrared range. *Appl. Phys. Lett.* **80**, 4687–4689 (2002).
83. Miki, S. *et al.* Large sensitive-area NbN nanowire superconducting single-photon detectors fabricated on single-crystal MgO substrates. *Appl. Phys. Lett.* **92,** 061116 (2008).
84. Kerman, A. J. *et al.* Constriction-limited detection efficiency of superconducting nanowire single-photon detectors. *Appl. Phys. Lett.* **90,** 101110 (2007).
85. Kerman, A. J. *et al.* Kinetic-inductance-limited reset time of superconducting nanowire photon counters. *Appl. Phys. Lett.* **88,** 111116 (2006).
86. Hadfield, R. H. *et al.* Single photon source characterization with a superconducting single photon detector. *Opt. Express* **13,** 10846–10853 (2005).
87. Rosfjord, K. M. *et al.* Nanowire single-photon detector with an integrated optical cavity and anti-reflection coating. *Opt. Express* **14,** 527–534 (2006).
88. Dorenbos, S. N. *et al.* Low noise superconducting single photon detectors on silicon. *Appl. Phys. Lett.* **93,** 131101 (2008).
89. Dauler, E. A. *et al.* Photon-number-resolution with sub-30-ps timing using multi-element superconducting nanowire single photon detectors. *J. Mod. Opt.* **56,** 364–373 (2009).
90. Takesue, H. *et al.* Quantum key distribution over 40-dB channel loss using superconducting single-photon detectors. *Nature Photon.* **1,** 343–348 (2007).
91. Shields, A. J. *et al.* Detection of single photons using a field-effect transistor gated by a layer of quantum dots. *Appl. Phys. Lett.* **76,** 3673–3675 (2000).
92. Kardynał, B. E. *et al.* Low-noise photon counting with a radio-frequency quantum-dot field-effect transistor. *Appl. Phys. Lett.* **84,** 419–421 (2004).
93. Rowe, M. A. *et al.* Single-photon detection using a quantum dot optically gated field-effect transistor with high internal quantum efficiency. *Appl. Phys. Lett.* **89,** 253505 (2006).
94. Kardynal, B. E. *et al.* Photon number resolving detector based on a quantum dot field effect transistor. *Appl. Phys. Lett.* **90,** 181114 (2007).
95. Gansen, E. J. *et al.* Photon-number-discriminating detection using a quantum-dot, optically gated, field-effect transistor. *Nature Photon.* **1,** 585–588 (2007).
96. Blakesley, J. C. *et al.* Efficient single photon detection by quantum dot resonant tunneling diodes. *Phys. Rev. Lett.* **94**, 067401 (2005).
97. Li, H. W. *et al.* Quantum dot resonant tunneling diode for telecommunication wavelength single photon detection. *Appl. Phys. Lett.* **91,** 073516 (2007).
98. Kosaka, H. *et al.* Photoconduction quantization in a single-photon detector. *Phys. Rev. B* **65,** 201307 (2002).
99. Yablonovitch, E. *et al.* Optoelectronic quantum telecommunications based on spins in semiconductors. *Proc. IEEE* **91,** 761–780 (2003).

Acknowledgements

R.H.H. thanks colleagues at NIST, Boulder, USA, and Heriot-Watt University, Edinburgh, UK, for helpful discussions and comments. He also thanks colleagues who provided figures for the manuscript. His work is supported by the Royal Society of London through a University Research Fellowship and the UK Engineering and Physical Sciences Research Council.

Picosecond superconducting single-photon optical detector

G. N. Gol'tsman,[a] O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, and A. Dzardanov
Department of Physics, Moscow State Pedagogical University, Moscow 119435, Russia

C. Williams and Roman Sobolewski[b]
Department of Electrical and Computer Engineering and Laboratory for Laser Energetics, University of Rochester, Rochester, New York 14627-0231

(Received 22 January 2001; accepted for publication 1 June 2001)

We experimentally demonstrate a supercurrent-assisted, hotspot-formation mechanism for ultrafast detection and counting of visible and infrared photons. A photon-induced hotspot leads to a temporary formation of a resistive barrier across the superconducting sensor strip and results in an easily measurable voltage pulse. Subsequent hotspot healing in ~30 ps time frame, restores the superconductivity (zero-voltage state), and the detector is ready to register another photon. Our device consists of an ultrathin, very narrow NbN strip, maintained at 4.2 K and current-biased close to the critical current. It exhibits an experimentally measured quantum efficiency of ~20% for 0.81 μm wavelength photons and negligible dark counts. © *2001 American Institute of Physics.*
[DOI: 10.1063/1.1388868]

Superconducting devices are the natural choice for fast and ultrasensitive optical detection, because of their quantum nature and low-noise, cryogenic operation environment. The superconducting energy gap 2Δ is two to three orders of magnitude lower than in a semiconductor, thus, photon absorption in a superconducting detector creates an avalanche electron charge two to three orders of magnitude higher for the same photon energy. This results in an enhanced resolution in energy-resolving devices, such as superconducting tunnel junctions,[1] and extends the range of detectable energies well into the infrared for photodetectors.[2] In addition, as we have recently demonstrated, energy relaxation time constants of excited electrons in superconductors are in the picosecond range for both the low-temperature[3] and high-temperature[4] superconductors, assuring the gigahertz repetition rate for superconducting photon counters.

The dynamics of the hotspot formation in a superconductor at temperature T below its critical temperature T_C, at the position where the photon is absorbed has been described before[5] and the supercurrent-assisted mechanism experimentally demonstrated in this work was theoretically studied in Ref. 6. Therefore, we only mention that the absorption of a photon with energy $\hbar\omega \gg 2\Delta$ creates, through electron–electron and electron–Debye–phonon interactions, a local nonequilibrium perturbation with a large number of excited hot electrons (above 300 in the case of NbN, excited with 790 nm wavelength light),[2] and an increase of the average electron temperature above T_C. This initial thermalization phase for ultrathin NbN films is characterized by the thermalization time $\tau_T = 6.5$ ps (Ref. 3) and results in the formation of a hotspot—a local nonsuperconducting region of the thermalization length $2\lambda_T$ [Fig. 1(a)]. After the initial thermalization, the resistive hotspot size grows [Fig. 1(b)] as hot electrons diffuse out of its center. At the same time, the supercurrent is expelled from the hotspot volume and is concentrated in the "sidewalks" between the hotspot and the edges of the film [Fig. 1(c)]. If the bias current I_{bias} is sufficient to exceed the critical current in the sidewalks, the phase slip centers are sprung[7] and a nonsuperconducting barrier is formed across the entire width w of the device [Fig. 1(d)], giving rise to a voltage signal, due to a collaborative effect of the bias current and the radiation quantum. For a given experiment, the response magnitude is proportional to the barrier resistance, however, in general, the current-assisted hotspot process creates a nonlinear, multidimensional space of operating parameters, such as w, I_{bias}, $\hbar\omega$, and T.

The hotspot formation process competes, of course, with the cooling process, as electrons diffusing out of the hotspot lose their energy through electron–phonon scattering. Thus, after the time depending on both the diffusion rate and the quasiparticle relaxation dynamics,[6] the hotspot heals itself, leading to the restoration of the superconducting path along the microbridge. As a result of the hotspot creation and relaxation processes, the NbN device switches temporarily be-

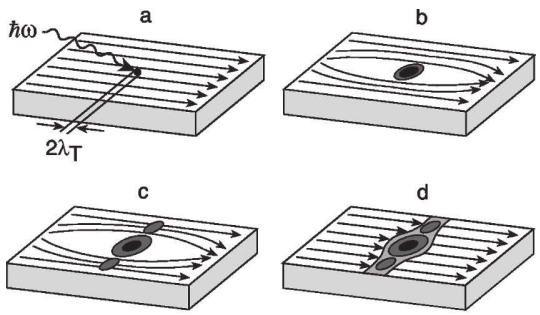


FIG. 1. Schematics of the supercurrent-assisted hotspot formation mechanism in an ultrathin and narrow superconducting strip, kept at temperature far below T_C are shown. The arrows indicate direction of the supercurrent flow.

[a]Also at: Department of Electrical and Computer Engineering and Laboratory for Laser Energetics, University of Rochester, Rochester, New York 14627-0231.
[b]Author to whom correspondence should be addressed: also at the Institute of Physics, Polish Academy of Sciences, PL-02904 Warszawa, Poland; electronic mail: sobolewski@ece.rochester.edu

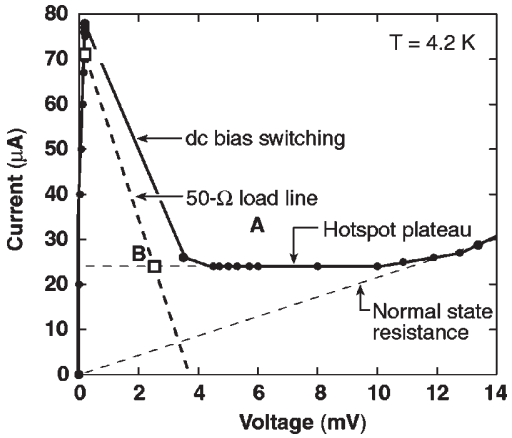


FIG. 2. $I-V$ characteristics of a 0.2 μm wide and 1.2 μm long NbN superconducting microbridge are shown. Point A denotes the initial detector bias level in the superconducting state and point B corresponds to the switched state upon absorbing a photon, leading a voltage pulse generation, before relaxing back to point A.

tween the superconducting and resistive states on a time scale of ~30 ps.

We have developed simple to manufacture, easy to operate, superconducting single photon detectors (SPDs) using nominally 0.2 μm wide and 1 μm long microbridges patterned from ultrathin (5 nm thick) NbN films deposited on sapphire substrate.[8] The microbridge was connected to the external circuit, via much thicker and larger, Au-coated contact pads. Figure 2 presents a current–voltage ($I-V$) characteristics of a NbN microbridge, operated at 4.2 K and biased using a voltage source. The characteristics are typical for a long superconducting constriction[9] and show that the bridge can be operated in either of the two distinct states: the superconducting (flux–flow) state *or* the resistive (hotspot) state. The hotspot plateau under dc conditions corresponds to the growing normal-state region, as the voltage across the device is increased, eventually reaching the bridge normal-state resistance, which in our case is approximately 500 Ω. The thick, dashed line represents a 50 Ω load line, when the device is connected to the output microwave transmission line. From Fig. 2, we see that the device I_C is approximately 78 μA.

For our experiments, a NbN SPD was mounted on a cold plate ($T=4.2$ K) inside an optical liquid-helium cryostat. We used two cold glass filters (inner glass window was at ~4.2 K) to block thermal radiation longer than 2.5 μm from the sample. The sample was dc biased through a bias tee and mounted on a rigid, 50 Ω coplanar transmission line with the ac output connected through a stainless-steel, semirigid coaxial cable to a cryogenic low-noise amplifier (placed inside the dewar), characterized by 30 dB gain and 1 to 2 GHz bandwidth. The noise temperature of our cryogenic amplifier was below 15 K, which yielded voltage fluctuations below 7 μV—several orders of magnitude below our signal levels. Outside the dewar, the signal passed through an isolator and a second broadband power amplifier (9 GHz; 20 dB gain) before going to a 6 GHz bandwidth single-shot oscilloscope for display, or to a 200 MHz voltage-level threshold counter for real-time event counting and statistical analysis. We worked with 100 fs wide, ~50 μm diameter optical pulses with a 1 kHz repetition rate at 0.4, 0.81, 1.55, and 2.1 μm wavelengths, with the bulk of the measurements performed using 0.81 μm photons. During our experiments, the fluence per pulse reaching the device plane inside the dewar was approximately $J_{\text{in}} \cong 1$ fJ/μm^2, and could be further attenuated using banks of neutral density filters, giving the total attenuation of 10^{-7}.

The actual fluence per pulse absorbed by our SPD, J_{abs}, can be estimated according to the relation $J_{\text{abs}}=J_{\text{in}}S_d\eta$, where S_d is the active area of the device and η is the radiation absorption coefficient of a metallic film, given by[10]

$$\eta=4(R_s/Z_0)/[(R_s/Z_0)(n_{\text{sub}}+1)+1]^2, \tag{1}$$

where n_{sub} is the index of refraction of the SPD substrate, R_s is the surface resistance of the NbN film measured just above T_C, and $Z_0=377\,\Omega$ is the free-space impedance. For our sapphire substrate ($n_{\text{sub}}=1.72$), $\eta_{\max}=37\%$. η is frequency independent as long as n_{sub} remains frequency independent and the film is much smaller than the radiation skin depth, and can be regarded as the intrinsic quantum efficiency (QE) of our device.

For a device biased near, but below I_C (point A in Fig. 2), photon absorption instigated the supercurrent-assisted hotspot formation leading to a temporary switch from the superconducting state to the hotspot resistive state (point B in Fig. 2) along the 50 Ω load line. As a result, an output voltage was generated with a magnitude corresponding to the voltage level at point B, and that was independent of the actual photon energy, as long as the photon energy was sufficient to form a hotspot large enough to trigger the supercurrent redistribution effect. The response time of the voltage pulses followed the formation and subsequent healing of the resistive state induced by the photon absorption.[6]

The measured response of our SPDs (not shown) was indeed "quantum" or "granular," in a sense that the voltage pulse amplitude was roughly the same (>400 mV after amplification, with a signal-to-noise ratio above 100:1) for all tested laser wavelengths. The response pulse width was ~100 ps, limited by the bandwidth of our chain of output amplifiers, and with negligible shot-to-shot jitter.

True single-photon counting requires that the photon detection probability has a linear dependence on the number of photons incident on the device. For a mean number of m photons per pulse, the probability $P(n)$ of absorbing n photons from a given pulse is $P(n)\sim(e^{-m}m^n)/(n!)$. When $m \ll 1$ (achieved by drastically attenuating the flux of photons incident on the SPD), the probability $P(n)$ simplifies to

$$P(n)\sim\frac{m^n}{n!}. \tag{2}$$

Consequently, the probability of absorbing one photon is proportional to m, the probability of detecting two photons is proportional to m^2, and so on.

Figure 3 shows the probability of the detector producing an output voltage pulse as a function of the average number $[J_{\text{in}}S_d/\hbar\omega]$ of 0.81 μm wavelength photons in a 100 fs pulse, incident on the device area, for two different values of I_{bias}. Since all photons arrive within the 100-fs-laser-pulse window, only spatial correlations (number of photons per device area) are important in the experiment. The left vertical

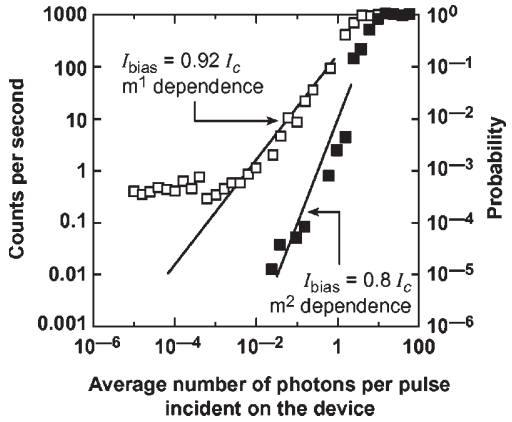


FIG. 3. Number of counts per second recorded by the NbN SPD versus the average number of photons per pulse incident upon the device, for two different bias current levels is shown. The solid lines correspond to the Eq. (4) theoretical predictions. The incident photon wavelength was 0.81 μm.

axis in Fig. 3 shows the experimental data i.e., the number of detector counts per second (equivalently, per 1000 laser pulses), based on the average number of counts detected by the SPD over a 10 s counting period for the highest photon doses, and up to 1000 s for the lowest. The counter threshold was adjusted to minimize spurious counts. The right vertical axis corresponds to the probability P of detecting an optical pulse. Open squares correspond to the SPD performance when it was biased at $0.92\,I_c$. For high incident photon fluxes, the detector managed to count all 1000 laser pulses in each second ($P=1$), without actually resolving the number of photons. For smaller fluxes, however, our experimental data show that for over four orders of magnitude, the detection probability decreases linearly with the decrease of the average number of incident photons, unambiguously demonstrating the single-photon detection mechanism. Since our experiment was performed in an optically unshielded environment (the detector was inside the dewar, but not in a dark box and only the main laboratory lights were off), at very low photon doses our experimental data points leveled off at 0.4 s^{-1} counts ($P=4\times10^{-4}$), which must be regarded as the laboratory single-photon background noise, where the background is essentially stray photons uncorrelated to the laser pulses. The intrinsic dark count rate of our SPD was below 0.001 s^{-1} ($P<10^{-6}$), which corresponded to zero number of detector responses over the time of 1000 s when its input was completely blocked.

From Fig. 3, we can estimate that the QE of our NbN microbridge is 20%, as the value corresponding to the probability of detecting a pulse containing an average of one photon incident upon the device. The practical detection efficiency of our SPD is, of course, much lower because of the very low S_d, as compared to the optical spot size. The maximization of detection efficiency is, however, strictly an engineering issue. Using proper coupling optics, the incident photon beam could be focused to a diffraction-limited spot size. At the same time, various geometrical configurations of the detector can be implemented, including a large-active-area meander-type design.

The 0.92-I_c detector bias was selected to achieve the single-photon detection with negligible dark counts (larger values of I_{bias}, resulted in dark counts associated with voltage oscillations in the metastable region). Lowering I_{bias}, on the other hand, led to the two-photon detection. Solid squares in Fig. 3 correspond to the same device, operated under the same conditions as discussed, but with $I_{\text{bias}}=0.8\,I_c$. We note immediately that our experimental data points now follow a quadratic dependence of detection probability showing the two-photon operation. The two-photon absorption, apparently, must form a larger hotspot size, needed to compensate for the smaller I_{bias}, but in this case, QE is significantly lower and is ~1%. At the same time, we do not see the laboratory photon background since the joint probability of two stray photons hitting the device area within the required space and time is negligibly small. Further reduction of I_{bias} (not shown in Fig. 3) resulted, unsurprisingly, in a cubic (three-photon detection) dependence of detection probability to the number of photons per pulse.

In conclusion, we have demonstrated that a supercurrent-assisted, hot-spot-formation mechanism can be implemented using an ultrathin NbN strip for ultrafast single-photon detection and counting of visible and infrared photons with an experimentally measured 20% QE for 0.81 μm photons and negligible dark counts. The bandwidth-limited measured response time was ~100 ps, corresponding to a 10 GHz photon counting rate. Already identified applications for our superconducting SPDs range from sensing ultraweak electroluminescence from submicron complementary metal–oxide–semiconductor very large scale integrated circuits,[11] to quantum communication systems.

The authors thank Aleksandr Verevkin, Kenneth Wilsher, Steven Kasapi, and Gerald Gilbert for helpful discussions and comments. This work was supported by Schlumberger SS, U.S. Office of Naval Research under Grant No. N00014-00-1-0237, and the NATO Linkage Grant No. CR-G.LG974662, and the Award No. RE-2227 of the U.S. Civilian Research and Development Foundation for the Independent States of the Former Soviet Union.

[1] A. Peacock, P. Verhoeve, N. Rando, A. van Dordrecht, B. G. Taylor, C. Erd, M. A. C. Perryman, R. Venn, J. Howlett, D. J. Goldie, J. Lumley, and M. Wallis, Nature (London) **381**, 135 (1996); R. J. Schoelkopf, S. H. Moseley, C. M. Stahle, P. Wahlgren, and P. Delsing, IEEE Trans. Appl. Supercond. **9**, 2935 (1999).
[2] K. S. Il'in, I. I. Milostnaya, A. A. Verevkin, G. N. Gol'tsman, E. M. Gershenzon, and R. Sobolewski, Appl. Phys. Lett. **73**, 3938 (1998).
[3] K. S. Il'in, M. Lindgren, M. Currie, A. D. Semenov, G. N. Gol'tsman, R. Sobolewski, S. I. Cherednichenko, and E. M. Gershenzon, Appl. Phys. Lett. **76**, 2752 (2000).
[4] M. Lindgren, M. Currie, C. Williams, T. Y. Hsiang, P. M. Fauchet, R. Sobolewski, S. H. Moffat, R. A. Hughes, J. S. Preston, and F. A. Hegmann, Appl. Phys. Lett. **74**, 853 (1999).
[5] A. M. Kadin and M. W. Johnson, Appl. Phys. Lett. **69**, 3938 (1996).
[6] A. D. Semenov, G. N. Gol'tsman, and A. Korneev, Physica C **351**, 349 (2001).
[7] M. Stuivinga, C. L. G. Ham, T. M. Klapwijk, and J. E. Mooij, J. Low Temp. Phys. **53**, 633 (1983).
[8] S. I. Cherednichenko, P. Yagoubov, K. S. Il'in, G. N. Gol'tsman, and E. M. Gershenzon, in *Proceedings of the Eighth International Symposium on Space Terahertz Technology* (Harvard University, Cambridge, MA, 1997), pp. 245–252.
[9] W. J. Skocpol, M. R. Beasley, and M. Tinkham, J. Appl. Phys. **45**, 4054 (1974).
[10] M. Born and E. Wolf, *Principles of Optics: Electromagnetic Theory of Propagation, Interference, and Diffraction of Light* 7th edition (Cambridge University Press, Cambridge, UK, 1999), pp. 752–758.
[11] J. C. Tsang and J. A. Kash, Appl. Phys. Lett. **70**, 889 (1997).

Chapter 6

The no-cloning theorem and light polarization

6.1 The no-cloning theorem

The no-cloning theorem was published in Nature in 1982 (Wooters , Nature 299, 802 (1982)). the question he addressed was: *Is there a physical limit to how perfect a copy can be made?* The answer is yes: in quantum physics, a perfect copy is impossible. Assume we have a 'quantum cloning machine': a copy operator U_{copy} that acts on a 'blank' state and makes a copy of a state:

$$U_{copy}(|V\rangle_1 |blank\rangle_2) = |V\rangle_1 |V\rangle_2 \tag{6.1}$$
$$U_{copy}(|H\rangle_1 |blank\rangle_2) = |H\rangle_1 |H\rangle_2 \tag{6.2}$$

This must also work for any superposition:

$$U_{copy}((a|H\rangle_1 + b|V\rangle_1)|blank\rangle_2) = \tag{6.3}$$
$$U_{copy}(a|H\rangle_1 |blank\rangle_2) + U_{copy}(b|V\rangle_1 |blank\rangle_2) \tag{6.4}$$
$$= a|H\rangle_1 |H\rangle_2 + b|V\rangle_1 |V\rangle_2 \tag{6.5}$$

But what should we really get for a cloning process?

$$(a|H\rangle_1 + b|V\rangle_1)(a|H\rangle_2 + b|V\rangle_2) =$$
$$a^2 |H\rangle_1 |H\rangle_2 + ab|H\rangle_1 |V\rangle_2 + ba|V\rangle_1 |H\rangle_2 + b^2 |V\rangle_1 |V\rangle_2 \tag{6.6}$$

We have a discrepancy between what a cloning machine would give for a superposition and what the cloning should give: the cloning machine misses the cross terms. Cloning only works for a=1 and b=0 (and vice versa), but not for all the other cases! General quantum cloning is impossible. This is good news for quantum cryptography: an eavesdropper cannot intercept a message, clone it, send a copy to the intended receiver and keep a copy without introducing errors.

While quantum cloning is impossible, quantum teleportation is possible (will be discussed in a coming lecture). In quantum teleportation, the original state is destroyed and a copy of that state is made, therefore not violating the no-cloning theorem.

6.2 Light Polarization

Polarization of light: We can decompose the electric field of a light field traveling along the x direction into Ey and Ez components. Depending on the phase between the two components, light is linearly, circularly or elliptically polarized, this is true for the electromagnetic field associated with an intense light beam as well as for a single photon. If Ey and Ez are in phase, we have linearly polarized light.

If Ey and Ez are out of phase by 90 degrees, we have circularly polarized light which can be left handed and right handed (+ or – 90 degrees phase difference): the electric field rotates.

The case between these two extremes gives elliptically polarized light. Light is therefore always elliptically polarized with circular and linear polarization being only two extremes. Polarization is reaedily measured with

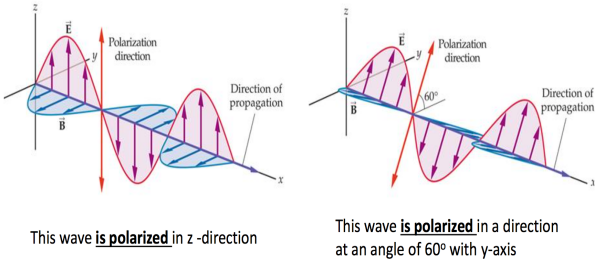


Figure 6.1: Linear polarization.

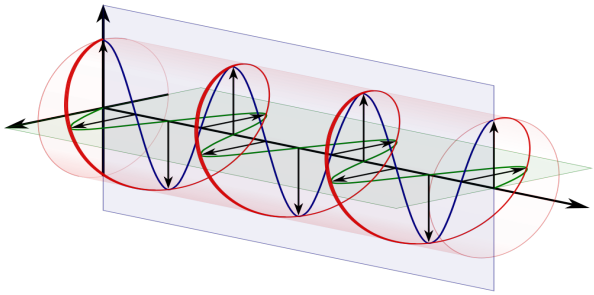


Figure 6.2: Circular polarization.

a polarimeter, an instrument that measures the Stokes vector and can neatly display the result on the Poincarre sphere. It is not possible to measure the exact polarization in one single measurement.

Polarization diffusion can be a problem in quantum optics when the polarization is not maintained during propagation. This can happen in deployed optical fibers because of vibrations, thermal fluctuations that evolve over time and result in time varying polarization evolution. In many cases, a feedback system is needed to counteract this effect.

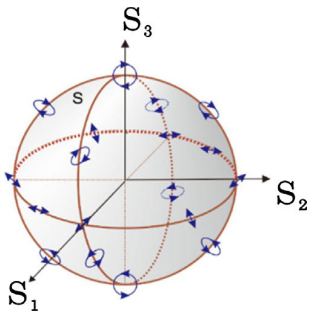


Figure 6.3: The Poincare Sphere.

6.2.1 Waveplates

Waveplates are made of birefringent materials. A birefringent material has two refractive indexes: n_o and n_e, for extraordinary and ordinary, respectively, along two different orientations. This can result in the effect seen below where two images are observed.

Calcite is a natural, birefringent crystal. This means that light propagating along a given direction can propagate at different velocities depending on its polarization. We can acquire a phase difference between the two polarizations during propagation:

$$\Delta\phi = \frac{2\pi d(n_e - n_o)}{\lambda} \tag{6.7}$$

where d is the thickness and $\Delta\phi$ is the retardance. A given waveplate thickness will introduce a given retardance. There are two thicknesses of special interest: the half-waveplate and the quarter-waveplate: - With a half-waveplate we can rotate linear polarization. When linearly polarized light propagates through

Figure 6.4: A birefringent calcite crystal: different polarizations have different refractive indexes.

a half-waveplate, its linear polarization rotates by 2θ where θ is the angle of the half-waveplate. - With a quarter-waveplate we can turn circular polarization into linear and vice versa. A half-waveplate is equivalent two quarter waveplates put together, so the quarter waveplate is the essential ingredient in polarization control.

Can we build an optical diode with waveplates and polarizers so that only one polarization can be transmitted? The answer is yes and can be realized by placing a waveplate after a polarizer such that light reflected back will pass a second time through the waveplate and have a polarization that is not transmitted through the polarizer, in this way light can only propagate in one direction, hence the name optical diode.

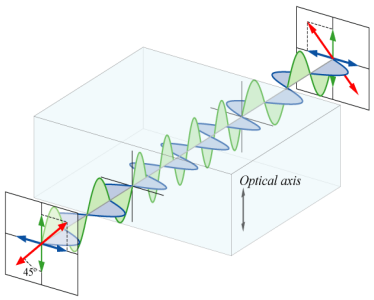


Figure 6.5: A waveplate: different polarizations polarizations see different refractive indexes.

A quarter waveplate turns linear polarization into circular polarization if placed at the correct angle.

To study polarization, we use polarizers such as polarizing beam splitters (PBS) that transmit one particular polarization and reflect the perpendicular polarization. The polarizing cube beam splitter is an excellent polarizer that offers very high selectivity: the output can be highly polarized.

All possible polarizations can be mapped on the Poincare sphere. We can use a halfwave plate to go from any linear polarization to any other linear polarization (to go from one point to another point on the equator).

Complete circular polarization is at the poles: right circular polarization on top, left circular polarization at the bottom. In the plane of the equator we have linear polarization. Between the equator and the poles, we have elliptical polarization. Unpolarized light is at the center of the sphere and fully polarized light on its surface. To go from any polarization to any other polarization, one solution is to use a quarter-waveplate to go down to the equator, followed by a half-waveplate to move along the equator and another quarter-waveplate to reach the polarization target.

Received 15 June; accepted 1 September 1982.

1. Kagi, J. H. R. & Nordberg, M. (eds) *Metallothionein* (Birkhauser, Basle, 1979).
2. Karin, M. & Herschman, H. R. *Science* **204,** 176–177 (1979).
3. Pulido, P., Kagi, J. H. R. & Vallee, B. L. *Biochemistry* **5,** 1768–1777 (1966).
4. Rudd, C. J. & Herschmann, H. R. *Tox. appl. Pharmac.* **47,** 273–278 (1979).
5. Karin, M. & Herschman, H. R. *Eur. J. Biochem.* **107,** 395–401 (1980).
6. Kissling, M. M. and Kagi, J. H. R. *FEBS Lett.* **82,** 247–250 (1977).
7. Karin, M. *et al. Nature* **286,** 295–297 (1980).
8. Karin, M., Slater, E. P. & Herschman, H. R. *J. cell. Physiol.* **106,** 63–74 (1981).
9. Durnam, D. M. & Palmiter, R. D. *J. biol. Chem.* **256,** 5712–2716 (1981).
10. Hager, L. J. & Palmiter, R. D. *Nature* **291,** 340–342 (1981).
11. Karin, M. & Richards, R. *Nucleic Acids Res.* **10,** 3165–3173 (1982).
12. Lawn, R. M. *et al. Cell* **15,** 1157–1174 (1978).
13. Southern, E. M. *J. molec. Biol.* **98,** 503–517 (1975).
14. Benton, W. D. & Davis, R. W. *Science* **196,** 180–182 (1977).
15. Glanville, N., Durnam, D. M. & Palmiter, R. D. *Nature* **292,** 267–269 (1981).
16. Breathnach, R. *et al. Proc. natn. Acad. Sci. U.S.A.* **75,** 4853–4857 (1978).
17. Weaver, R. F. & Weissman, C. *Nucleic Acids Res.* **5,** 1175–1193 (1979).
18. Kayb, K. E., Warren, R. & Palmiter, R. D. *Cell* **29,** 99–108 (1982).
19. Brinster, R. L. *et al. Nature* **296,** 39–42 (1982).
20. Kingsbury, R. & McKnight, S. L. *Science* **217,** 316–324 (1982).
21. Larsen, A. & Weintraub, H. *Cell* **29,** 609–672 (1982).
22. Proudfoot, N. J. & Brownlee, G. G. *Nature* **263,** 211–214 (1976).
23. Calos, M. P. & Miller, J. H. *Cell* **20,** 579–595 (1980).
24. Hollis, F. G. *et al. Nature* **296,** 321–325 (1982).
25. Leuders, K., Leder, A., Leder, P. & Kuff, E. *Nature* **295,** 426–428 (1982).
26. Van Arsdell, S. W. *et al. Cell* **26,** 11–17 (1981).
27. Jagadeeswaran, P., Forget, B. G. & Weissman, S. M. *Cell* **26,** 141–142 (1982).
28. Nishioka, Y., Leder, A. & Leder, P. *Proc. natn. Acad. Sci. U.S.A.* **77,** 2806–2809 (1980).
29. Wilde, C. D. *et al. Nature* **297,** 83–84 (1982).
30. Shaul, Y., Kaminichik, J. & Aviv, H. *Eur. J. Biochem.* **116,** 461–466 (1981).
31. Perry, R. P. *et al. Proc. natn. Acad. Sci. U.S.A.* **77,** 1937–1941 (1980).
32. Hofer, E. & Darnel, J. E. *Cell* **23,** 585–593 (1981).
33. Bell, G., Karam, J. H. & Rutter, W. J. *Proc. natn. Acad. Sci. U.S.A.* **78,** 5759–5763 (1981).
34. Rigby, P. W. J. *et al. J. molec. Biol.* **113,** 237–251 (1977).
35. Wahl, G. M., Stern, M. & Stark, G. R. *Proc. natn. Acad. Sci. U.S.A.* **76,** 3683–3687 (1979).
36. Maxam, A. & Gilbert, W. *Meth. Enzym.* **65,** 499–559 (1980).
37. Sanger, F., Nicklen, S. & Coulson, A. R. *Proc. natn. Acad. Sci. U.S.A.* **74,** 5463–5468 (1979).
38. Goodman, H. M. *Meth. Enzym.* **65,** 63–64 (1980).
39. Heidecker, G., Messing, J. & Gronenborn, B. *Gene* **10,** 69–73 (1980).
40. O'Farrel, P. *Focus* **3,** 1–3 (1981).

LETTERS TO NATURE

A single quantum cannot be cloned

W. K. Wootters*

Center for Theoretical Physics, The University of Texas at Austin, Austin, Texas 78712, USA

W. H. Zurek

Theoretical Astrophysics 130–33, California Institute of Technology, Pasadena, California 91125, USA

If a photon of definite polarization encounters an excited atom, there is typically some nonvanishing probability that the atom will emit a second photon by stimulated emission. Such a photon is guaranteed to have the same polarization as the original photon. But is it possible by this or any other process to amplify a quantum state, that is, to produce several copies of a quantum system (the polarized photon in the present case) each having the same state as the original? If it were, the amplifying process could be used to ascertain the exact state of a quantum system: in the case of a photon, one could determine its polarization by first producing a beam of identically polarized copies and then measuring the Stokes parameters[1]. We show here that the linearity of quantum mechanics forbids such replication and that this conclusion holds for all quantum systems.

Note that if photons could be cloned, a plausible argument could be made for the possibility of faster-than-light communication[2]. It is well known that for certain non-separably correlated Einstein–Podolsky–Rosen pairs of photons, once an observer has made a polarization measurement (say, vertical versus horizontal) on one member of the pair, the other one, which may be far away, can be for all purposes of prediction regarded as having the same polarization[3]. If this second photon could be replicated and its precise polarization measured as above, it would be possible to ascertain whether, for example, the first photon had been subjected to a measurement of linear or circular polarization. In this way the first observer would be able to transmit information faster than light by encoding his message into his choice of measurement. The actual impossibility of cloning photons, shown below, thus prohibits superluminal communication by this scheme. That such a scheme must fail for some reason despite the well-established existence of long-range quantum correlations[6–8], is a general consequence of quantum mechanics[9].

A perfect amplifying device would have the following effect on an incoming photon with polarization state $|s\rangle$:

$$|A_0\rangle|s\rangle \rightarrow |A_s\rangle|ss\rangle \tag{1}$$

Here $|A_0\rangle$ is the 'ready' state of the apparatus, and $|A_s\rangle$ is its final state, which may or may not depend on the polarization of the original photon. The symbol $|ss\rangle$ refers to the state of the radiation field in which there are two photons each having the polarization $|s\rangle$. Let us suppose that such an amplification can in fact be accomplished for the vertical polarization $|\updownarrow\rangle$ and for the horizontal polarization $|\leftrightarrow\rangle$. That is,

$$|A_0\rangle|\updownarrow\rangle \rightarrow |A_{\text{vert}}\rangle|\updownarrow\updownarrow\rangle \tag{2}$$

and

$$|A_0\rangle|\leftrightarrow\rangle \rightarrow |A_{\text{hor}}\rangle|\leftrightarrow\leftrightarrow\rangle \tag{3}$$

According to quantum mechanics this transformation should be representable by a linear (in fact unitary) operator. It therefore follows that if the incoming photon has the polarization given by the linear combination $\alpha|\updownarrow\rangle+\beta|\leftrightarrow\rangle$—for example, it could be linearly polarized in a direction 45° from the vertical, so that $\alpha=\beta=2^{-1/2}$—the result of its interaction with the apparatus will be the superposition of equations (2) and (3):

$$|A_0\rangle(\alpha|\updownarrow\rangle+\beta|\leftrightarrow\rangle) \rightarrow \alpha|A_{\text{vert}}\rangle|\updownarrow\updownarrow\rangle+\beta|A_{\text{hor}}\rangle|\leftrightarrow\leftrightarrow\rangle \tag{4}$$

If the apparatus states $|A_{\text{vert}}\rangle$ and $|A_{\text{hor}}\rangle$ are not identical, then the two photons emerging from the apparatus are in a mixed state of polarization. If these apparatus states are identical, then the two photons are in the pure state

$$\alpha|\updownarrow\updownarrow\rangle+\beta|\leftrightarrow\leftrightarrow\rangle \tag{5}$$

In neither of these cases is the final state the same as the state with two photons both having the polarization $\alpha|\updownarrow\rangle+\beta|\leftrightarrow\rangle$. That state, the one which would be required if the apparatus were to be a perfect amplifier, can be written as

$$2^{-1/2}(\alpha a^{+}_{\text{vert}}+\beta a^{+}_{\text{hor}})^2|0\rangle=\alpha^2|\updownarrow\updownarrow\rangle+2^{1/2}\alpha\beta|\updownarrow\leftrightarrow\rangle+\beta^2|\leftrightarrow\leftrightarrow\rangle$$

which is a pure state different from the one obtained above by superposition [equation (5)].

Thus no apparatus exists which will amplify an arbitrary polarization. The above argument does not rule out the possibility of a device which can amplify two special polarizations, such as vertical and horizontal. Indeed, any measuring device which distinguishes between these two polarizations, a Nicol prism for example, could be used to trigger such an amplification.

The same argument can be applied to any other kind of quantum system. As in the case of photons, linearity does not forbid the amplification of any given state by a device designed especially for that state, but it does rule out the existence of a device capable of amplifying an arbitrary state.

* Present address: Department of Physics and Astronomy, Williams College, Williamstown, Massachusetts 01267, USA.

Milonni (unpublished work) has shown that the process of stimulated emission does not lead to quantum amplification, because if there is stimulated emission there must also be—with equal probability in the case of one incoming photon—spontaneous emission, and the polarization of a spontaneously emitted photon is entirely independent of the polarization of the original.

It is conceivable that a more sophisticated amplifying apparatus could get around Milonni's argument. We have therefore presented the above simple argument, based on the linearity of quantum mechanics, to show that no apparatus, however complicated, can amplify an arbitrary polarization.

We stress that the question of replicating individual photons is of practical interest. It is obviously closely related to the quantum limits on the noise in amplifiers[10,11]. Moreover, an experiment devised to establish the extent to which polarization of single photons can be replicated through the process of stimulated emission is under way (A. Gozzini, personal communication; and see ref. 12). The quantum mechanical prediction is quite definite; for each perfect clone there is also one randomly polarized, spontaneously emitted, photon.

We thank Alain Aspect, Carl Caves, Ron Dickman, Ted Jacobson, Peter Milonni, Marlan Scully, Pierre Meystre, Don Page and John Archibald Wheeler for enjoyable and stimulating discussions.

This work was supported in part by the NSF (PHY 78-26592 and AST 79-22012-A1). W.H.Z. acknowledges a Richard Chace Tolman Fellowship.

Received 11 August; accepted 7 September 1982.

1. Born, M. & Wolf, E. *Principles of Optics* 4th edn (Pergamon, New York, 1970).
2. Herbert, N. *Found. Phys.* (in the press).
3. Einstein, A., Podolsky, B. & Rosen, N. *Phys. Rev.* **47**, 777–780 (1935).
4. Bohm, D. *Quantum Theory*, 611–623 (Prentice-Hall, Englewood Cliffs, 1951).
5. Kocher, C. A. & Commins, E. D. *Phys. Rev. Lett.* **18**, 575–578 (1967).
6. Freedman, S. J. & Clauser, J. R. *Phys. Rev. Lett.* **28**, 938–941 (1972).
7. Fry, E. S. & Thompson, R. C. *Phys. Rev. Lett.* **37**, 465–468 (1976).
8. Aspect, A., Grangier, P. & Roger, G. *Phys. Rev. Lett.* **47**, 460–463 (1981).
9. Bussey, P. J. *Phys. Lett.* **90A**, 9–12 (1982).
10. Haus, H. A. & Mullen, J. A. *Phys. Rev.* **128**, 2407–2410 (1962).
11. Caves, C. M. *Phys. Rev.* **D15**, (in the press).
12. Gozzini, A. *Proc. Symp. on Wave–Particle Dualism* (eds Diner, S., Fargue, D., Lochak, G. & Selleri, F) (Reidel, Dordrecht, in the press).

The Crab Nebula's progenitor

Ken'ichi Nomoto*, Warren M. Sparks†, Robert A. Fesen‡, Theodore R. Gull‡, S. Miyaji‡ & D. Sugimoto*

* Department of Earth Science and Astronomy, University of Tokyo, College of General Education, 3-8-1 Komaba, Meguro, Tokyo 153, Japan
† Group X-5, Mail Stop F669, Los Alamos National Laboratory, Los Alamos, New Mexico 87545, USA
‡ Laboratory for Astronomy and Solar Physics, Goddard Space Flight Center, Greenbelt, Maryland 20771, USA

The study of supernovae is hampered by an insufficient knowledge of the initial stellar mass for individual supernova. Because of large uncertainties in estimating both the total mass of a remnant (including the pulsar or black hole) and any mass loss during the pre-supernova stages, the main sequence mass of the progenitor cannot be accurately determined from observations alone. To calculate an initial mass, one must rely on a combination of both theory and observation. Limits on the progenitor's mass range can be estimated by the presence of a compact remnant and comparison of the observed nebular chemical abundances with detailed evolutionary calculations[1]. The Crab Nebula is an excellent choice for investigation because it contains a unique combination of characteristics: a central neutron star (pulsar) and a bright, well studied nebula having little or no swept-up interstellar material. In fact, several studies[1–4] have suggested an initial mass of $\sim 10\,M_\odot$ for the Crab progenitor. Recently, Davidson *et al.*[5], quoting two of us (K.N. and W.M.S.), state that the Crab's progenitor had a mass slightly larger than $8\,M_\odot$. Here we present in detail the reasoning behind this statement and suggest the explosion mechanism.

Briefly, the Crab consists of a pulsar (assumed here to have a mass of $\approx 1.4\,M_\odot$) and a nebula mass of $1.2\text{–}3.0\,M_\odot$ (refs 5, 6) which has a helium overabundance of $1.6 < X_{He}/X_H < 8$ (where X is an element's mass fraction). The oxygen abundance (X_O) is ~ 0.003 (refs 5, 6), which is less than the solar value of 0.007, while the oxygen-to-hydrogen ratio is approximately solar. The carbon-to-oxygen ratio is $0.4 < X_C/X_O < 1.1$ (ref. 5). Nitrogen may be slightly overabundant, while neon, sulphur and iron abundances are uncertain but are probably not greatly over- or underabundant. Because the Crab Nebula is helium-rich but not oxygen-rich, the hydrogen-rich (solar abundances) envelope and the helium layer of the progenitor star were ejected but the oxygen-rich layer below the helium layer was not. The lower layers must have formed the neutron star. The lower limit of the large helium-to-hydrogen ratio means that at least half of the ejected material must have come from the helium layer.

Arnett (ref. 7 and refs therein) systematically evolved helium cores of various masses (M_α) into late stages of evolution. He[1] compared Davidson's[8] derived abundances of the Crab nebula with calculated abundances from the $M_\alpha = 4.0\,M_\odot$ model, which was his lowest-massed, highly evolved helium core (corresponding to approximately a $15\,M_\odot$ star). Combining all the material above the helium-burning shell (his case B) with enough interstellar material to obtain $X_{He}/X_H = 8$, he found good agreement with X_N/X_{He} and X_O/X_{He} of Davidson's[8] 'model 1'. However, the calculated value of X_C/X_{He} was too large by a factor of 30. At that time, the Crab's carbon abundance had not been directly measured and Arnett suggested several possibilities: the inferred carbon abundance was too low, the carbon was hidden in the filaments, or a lower-mass helium core, $\sim 3\,M_\odot$, was more appropriate.

Using recent UV observations with the International Ultraviolet Explorer, Davidson *et al.*[5] have established that the carbon abundance is nearly solar. They also showed that the hydrogen and helium seemed to be fairly well mixed and, as carbon is convectively mixed in the helium layer, this would argue against carbon being hidden in the filaments. However, IR observations by Dennefeld and Andrillat[9] showed that the strength of [C I] λ9,850 relative to [S III] λ9,069 varied with position in the Crab. The strongest [C I] line would indicate a rather large carbon abundance if the ionizing flux is constant. Whether the IR observations indicate variation in the carbon abundance, variation in the ionizing flux, or high densities in neutral cores is not known. For the remainder of this report we will assume the carbon abundance as determined by Davidson *et al.*[5].

The existence of a pulsar in the Crab indicates that the progenitor's mass was larger than the upper mass limit ($8 \pm 1\,M_\odot$)[10] for degenerate carbon ignition. Degenerate carbon ignition results in carbon deflagration[11] which completely disrupts the star, leaving no compact remnant. Lower-mass stars that lose enough mass to avoid degenerate carbon burning eventually become white dwarfs. Stars massive enough ($\geq 8\,M_\odot$) to burn carbon non-degenerately will eventually undergo a core collapse initiated either by electron capture[12] onto Mg, Ne and O or by burn-out of all the available fuel[13,14]. When the collapsing core reaches neutron-star densities, stability is regained. Although detailed calculations of the collapse remain inconclusive, it is generally felt that the core will overshoot its equilibrium position and then rebound, initiating a shock wave[4]. This shock wave ejects the outer material but not the core, resulting in both a supernova nebula and a pulsar[15]. In more massive stars

Chapter 7

Bell's theorem

We need an experimental test to identify quantum entanglement. Correlations in one basis are not enough to identify quantum entanglement: imagine we have two independent single photon sources, each with a polarizer, the photons emitted by these two independent sources would not be entangled, yet the polarizers could be set so that photons measured by Alice and Bob have the same polarization.

Figure 7.1: An attempt to generate entangled photon pairs?

The (desperate) attempt shown above to fake entanglement would be easy to identify: in this case Alice always gets a V polarized photon and so does Bob. But when measuring in the AD basis, their measurements would be random, the correlations would be gone. For an entangled state, the correlations would also be there in any basis. To distinguish quantum entanglement, we need to measure in different bases: as we have seen, an entangled state in the HV basis is also entangled in the AD basis.

Another crucial question is whether there are hidden variables. John Bell came up with an answer: the Bell inequality that can test experimentally the question whether hidden variables set the outcome of a measurement. We assume that the measurement is a function of the photon polarization angle and the hidden variable λ:

- Measurement result for photon in the direction of Alice $A(a, \lambda) = \pm 1$
- Measurement result for photon in the direction of Bob $B(b, \lambda) = \pm 1$

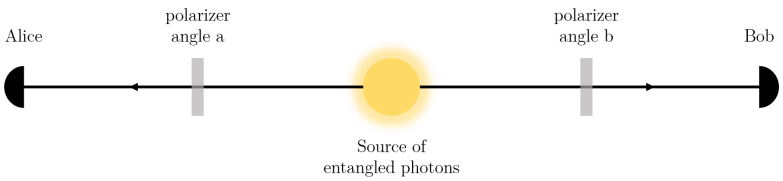


Figure 7.2: Experimental test of photon entanglement via a Bell measurement.

Considering the principle of locality, the result of a measurement on photon A does not depend on the setting b, provided the distance is large enough. Consequently, $B(b, \lambda)$ also does not depend on a, leading to $A(a, b, \lambda) = A(a, \lambda)$ and $B(a, b, \lambda) = B(b, \lambda)$.

For measurements performed in the lab, the outcomes could be defined as follows:

- $A(a, \lambda) = +1$ for a vertically polarized photon detection.
- $A(a, \lambda) = -1$ for a horizontally polarized photon detection.
- $B(b, \lambda) = +1$ for a vertically polarized photon detection.
- $B(b, \lambda) = -1$ for a horizontally polarized photon detection.

The probability of getting a +1 outcome is equal to getting a -1 outcome. We can also measure correlations between detection events in A and B for different polarizer settings and describe those with

$$C(a,b) = \int A(a,\lambda)\, B(b,\lambda)\, p(\lambda)\, d\lambda\,, \tag{7.1}$$

whereas $p(\lambda)$ corresponds to the normalized probability density of hidden variables ($\int p(\lambda)\, d\lambda = 1$). Next, we will consider the difference between correlations at varying polarization settings and make use of a generalized triangle inequality:

$$\begin{aligned} |C(a,b) - C(a,b')| &\leq \int |A(a,\lambda)\, B(b,\lambda) - A(a,\lambda)\, B(b',\lambda)|\, p(\lambda)\, d\lambda\,, \\ &\leq \int |A(a,\lambda)\, [B(b,\lambda) - B(b',\lambda)]\,|\, p(\lambda)\, d\lambda\,, \\ &\leq \int |B(b,\lambda) - B(b',\lambda)|\, p(\lambda)\, d\lambda\,. \end{aligned} \tag{7.2}$$

Consequently, the following holds for the sum of varying polarization settings:

$$\begin{aligned} |C(a',b) + C(a',b')| &\leq \int |A(a',\lambda)\, [B(b,\lambda) + B(b',\lambda)]\,|\, p(\lambda)\, d\lambda\,, \\ &\leq \int |B(b,\lambda) + B(b',\lambda)|\, p(\lambda)\, d\lambda\,. \end{aligned} \tag{7.3}$$

Due to the assumption of measurement results of $\pm$ 1, it follows that

$$|B(b,\lambda) - B(b',\lambda)| + |B(b,\lambda) + B(b',\lambda)| = 2\,. \tag{7.4}$$

Considering Equation 7.4, we can sum Equation 7.2 and Equation 7.3 to arrive at:

$$\begin{aligned} &|C(a,b) - C(a,b')| + |C(a',b) + C(a',b')| \leq \\ &|C(a,b) - C(a,b') + C(a',b) + C(a',b')| \leq 2\,, \end{aligned} \tag{7.5}$$

which constitutes the Bell inequality whereas the left-hand term is often denoted as S.

We have followed the CHSH (Clauser, Horne, Shimony and Holt) derivation introduced in 1969 where measurements only have two possible outcomes: +1 and -1. It can be generalized to the case of additional possible outcomes, for instance, in the case where a photon is not detected (one could imagine that hidden variables could determine photon detection). This opens the way to loopholes that provide alternative explanations, for example the detection loophole. Intuitively, we assume fair sampling: the detected photons give the same results as the undetected photons (and thus the whole ensemble of photons) would give. However, it could be that only photons that look 'entangled' are detected and that measuring all photons would not violate Bell's inequality anymore. This is the detection loophole, where one needs to measure (nearly) all the photons to close the loophole.

Another example is the communication loophole, where the setting on B might influence the measurement outcome on A, even for large distances. This was closed by Aspect et al. in 1982 using fast changing random polarizers that changed faster than light takes to travel from A to B. Nevertheless, one can still question how random the settings can be.

Experimentally, the question arises if S is bound by a maximum value and which angles one should for a, b, a' and b'. The upper bound for S, often called Cirel'son's (Tsirelson's) bound, can be derived as $S \leq 2\sqrt{2}$ (see e.g. Cirel'son, *Letters in Mathematical Physics* 4, 93–100, 1980). How can we rationalize this bound and validate it experimentally in a Bell test experiment? The quantum mechanical prediction for $C(a,b) = \cos[2(a-b)]$ with the derivation described in e.g. Duncan, Kleinpoppen, *Quantum Mechanics Versus Local Realism*, pp.175-218, Springer 1988. Consequently, we can evaluate S as

$$S = |\cos[2(a-b)] - \cos[2(a-b')] + \cos[2(a'-b)] + \cos[2(a'-b')]|\,. \tag{7.6}$$

To reach Cirel'son's bound $S = 2\sqrt{2}$, it follows that a, b, a' and b' should be chosen in equal steps of 22.5 ° or 67.5 °. When performing experimental Bell tests with entangled photon pairs in the lab, results between $2 < S < 2\sqrt{2}$ violate Bell's inequality and contradict theories based on local realism.

Another use for two-photon states: Absolute quantum efficiency measurements

The idea was first suggested by Klyshko in 1980 and was implemented in 1993 by Kwiat at al. (Phys. Rev. A 48, R867). It is based on a source of pairs of photons:

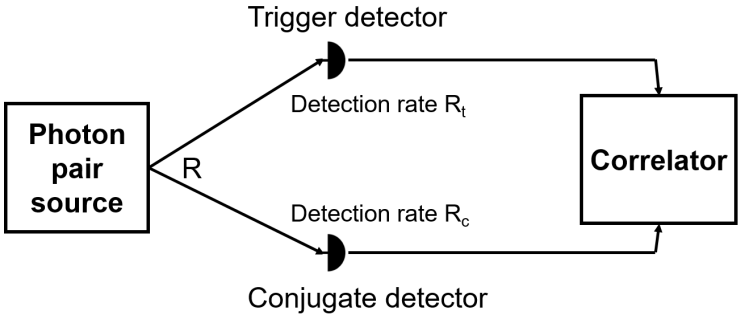


Figure 7.3: Quantum efficiency measurement with photon pairs.

We generate R photon pairs per second and consider the quantum efficiency η of the detectors, i.e. the probability for the detectors to detect a photon. η_t is the probability for the trigger detector to detect a photon, η_c is the probability for the conjugate detector to detect a photon. Thus, we can calculate

$$\begin{aligned} R_t &= R\eta_t\,, \\ R_c &= R\eta_c\,, \\ R_{tc} &= R\eta_t\eta_c\,, \\ \eta_t &= R_{tc}/R_c\,. \end{aligned} \tag{7.7}$$

The quantum efficiency is given by the ratio between the coincidence rate and the detection rate of the other detector. Thus, we do not need a low-fluctuation light source to obtain a precise measurement of the quantum efficiency, only a source of photon pairs (entanglement not required). Further, we don't even need to know the precise detection efficiency of a reference detector.

Note that this calculation does not take dark counts into account (detection events by the detector in the absence of an incoming photons). Considering dark count rates of X and Y for the two detectors, we arrive at the following expression:

$$\eta_t = (R_{tc} - X)/(R_c - Y)\,. \tag{7.8}$$

One remaining issue with this approach to determine the quantum efficiency is that that the value we get encompasses all losses on the way, not just the inefficiency of the detector but also losses in transmission between the light source and the detector (lenses, filters, optical fibers..).

PHYSICAL REVIEW
LETTERS

VOLUME 75 | 11 DECEMBER 1995 | NUMBER 24

New High-Intensity Source of Polarization-Entangled Photon Pairs

Paul G. Kwiat,* Klaus Mattle, Harald Weinfurter, and Anton Zeilinger
Institut für Experimentalphysik, Universität Innsbruck, Technikerstrasse 25, 6020 Innsbruck, Austria

Alexander V. Sergienko and Yanhua Shih
Department of Physics, University of Maryland Baltimore County, Baltimore, Maryland 21228
(Received 5 July 1995)

We report on a high-intensity source of polarization-entangled photon pairs with high momentum definition. Type-II noncollinear phase matching in parametric down conversion produces true entanglement: No part of the wave function must be discarded, in contrast to previous schemes. With two-photon fringe visibilities in excess of 97%, we demonstrated a violation of Bell's inequality by over 100 standard deviations in less than 5 min. The new source allowed ready preparation of all four of the EPR-Bell states.

PACS numbers: 03.65.Bz, 42.50.Dv

Entangled states of quantum particles highlight the nonseparability and nonlocality of quantum mechanics most vividly. A great number of experiments have investigated the production of entangled states of photons, particularly for use in tests of Bell's inequalities [1–3]. Recently, a whole wealth of curious and/or potentially useful applications of entangled states was proposed, from quantum communication, including cryptography [4] and transfer of two bits of information in one photon [5], to quantum teleportation [6] and "entanglement swapping" [7], to quantum computation [8].

Although entanglement in any degree of freedom is usually equally good in principle, polarization is often much easier to deal with in practice, due to the availability of high efficiency polarization-control elements and the relative insensitivity of most materials to birefringent thermally induced drifts. Unfortunately, as has been pointed out by several authors [9–12], no adequate source of polarization-entangled states has hitherto been reported. In particular, besides low brightness and difficulty in handling, the atomic cascade sources [1,2] suffer a degrade of the polarization correlations when the two photons are not emitted back to back (due to the recoil of the atom) [9]. This also results in a reduced collection efficiency for the pair. Nearly all previous experiments employing photons from parametric down conversion [3] have actually produced *product* states—they approximated an entangled state by post-selecting only *half* of the total state detected [13]. For example, one directs two orthogonally polarized photons onto a beam splitter, but considers only those cases where they leave via different output ports.

Three methods to avoid this problem by means of two down-conversion crystals have been proposed [10,14], but not yet carried out. Here we present a much simpler technique, relying on noncollinear type-II phase matching. The desired polarization-entangled state is produced *directly* out of a single nonlinear crystal [BBO (beta-barium borate) in our experiment], with no need for extra beam splitters or mirrors and no requirement of discarding detected pairs to observe nonlocal correlations. Verifying the correlations produced by the novel source, we have observed strong violations of Bell's inequalities (modulo the typical auxiliary assumptions), in some cases by more than 100 standard deviations. Using two extra birefringent elements, one can easily produce any of the four orthogonal "EPR-Bell states" [15].

To date, most of the experiments with photons from spontaneous parametric down conversion have used type-I phase matching, in which the correlated photons have the same polarization [16]. There, for the case of degenerate emission, a pair of photons with equal wavelength emerge on a cone [17], which is centered on the pump beam

0031-9007/95/75(24)/4337(5)$06.00

and whose opening angle depends on the angle θ_{pm} between the crystal optic axis and the pump. With type-II phase matching, the down-converted photons are emitted into *two* cones [10], one ordinary polarized, the other extraordinary polarized [17]. In the collinear situation the two cones are tangent to one another on exactly one line, namely, the pump beam direction [18]. If θ_{pm} is decreased, the two cones will separate from each other entirely. However, if the angle is *increased*, the two cones tilt toward the pump, causing an intersection along two lines (see Fig. 1) [19–21]. Along the two directions ("1" and "2"), where the cones overlap, the light can be essentially described by an entangled state:

$$|\psi\rangle = (|H_1, V_2\rangle + e^{i\alpha}|V_1, H_2\rangle)/\sqrt{2}, \quad (1)$$

where H and V indicate horizontal (extraordinary) and vertical (ordinary) polarization, respectively. The relative phase α arises from the crystal birefringence, and an overall phase shift is omitted.

Using an additional birefringent phase shifter (or even slightly rotating the down-conversion crystal itself), the value of α can be set as desired, e.g., to the values 0 or π. (Somewhat surprisingly, a net phase shift of π may be obtained by a 90° rotation of a *quarter* wave plate in one of the paths.) Similarly, a half wave plate in one path can be used to change horizontal polarization to vertical and vice versa. One can thus very easily produce any of the four EPR-Bell states,

$$|\psi^{\pm}\rangle = (|H_1, V_2\rangle \pm |V_1, H_2\rangle)/\sqrt{2},$$
$$|\phi^{\pm}\rangle = (|H_1, H_2\rangle \pm |V_1, V_2\rangle)/\sqrt{2}, \quad (2)$$

which form the complete maximally entangled basis of the two-particle Hilbert space, and which are important in many quantum communication and quantum information schemes.

The birefringent nature of the down-conversion crystal complicates the actual entangled state produced, since the ordinary and the extraordinary photons have different velocities inside the crystal, and propagate along different directions even though they become collinear outside the crystal (an effect well known from calcite prisms, for example). The resulting longitudinal and transverse walk-offs between the two terms in the state (1) are maximal for pairs created near the entrance face, which consequently acquire a relative time delay $\delta T = L(1/u_o - 1/u_e)$ (L is the crystal length, and u_o and u_e are the ordinary and extraordinary group velocities, respectively) and a relative lateral displacement $d = L\tan\rho$ (ρ is the angle between the ordinary and extraordinary beams inside the crystal). If $\delta T > \tau_c$, the coherence time of the down-conversion light, then the terms in (1) become, in principle, distinguishable by the order in which the detectors would fire, and no interference will be observable. Similarly, if d is larger than the coherence width, the terms can become partially labeled by their spatial location.

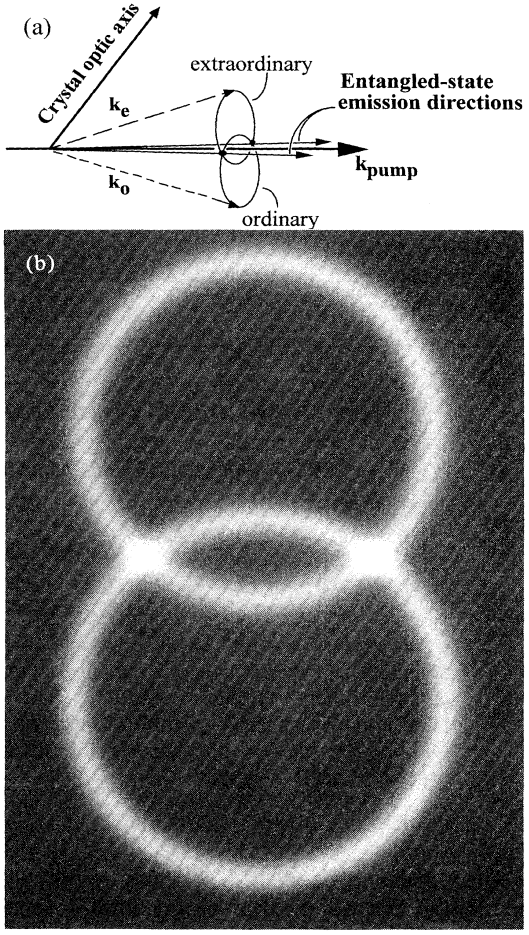


FIG. 1. (a) Spontaneous down-conversion cones present with type-II phase matching. Correlated photons lie on opposite sides of the pump beam. (b) A photograph of the down-conversion photons, through an interference filter at 702 nm (5 nm FWHM). The infrared film was located 11 cm from the crystal, with no imaging lens. (Photograph by M. Reck.)

Because the photons are produced coherently along the entire length of the crystal, one can *completely* compensate for the longitudinal walk-off [23]—after compensation, interference occurs pairwise between processes where the photon pair is created at distances $\pm x$ from the middle of the crystal. The ideal compensation therefore uses two crystals, one in each path, which are identical to the down-conversion crystal, but only half as long. If the polarization of the light is first rotated by 90° (e.g., with a half wave plate), the retardations of the o and the e components are exchanged and complete temporal indistinguishability is restored ($\delta T = 0$) [24]. The same method provides the optimal compensation for the transverse walk-off effect as well [25].

The experimental setup is shown in Fig. 2. The 351.1 nm pump beam (150 mW) originated in a single-mode argon ion laser, followed by a dispersion prism to remove

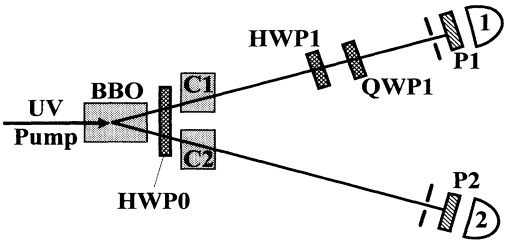


FIG. 2. Schematic of one method to produce and select the polarization-entangled state from the down-conversion crystal. The extra birefringent crystals C1 and C2, along with the half wave plate HWP0, are used to compensate the birefringent walk-off effects from the production crystal. By appropriately setting half wave plate HWP1 and quarter wave plate QWP1, one can produce all four of the orthogonal EPR-Bell states. Each polarizer P1 and P2 consisted of two stacked polarizing beam splitters preceded by a rotatable half wave plate.

unwanted laser fluorescence. Our 3 mm long BBO crystal (from Castech-Phoenix) was nominally cut at $\theta_{\rm pm} = 49.2°$ to allow collinear degenerate operation when the pump beam is precisely orthogonal to the surface. The optic axis was oriented in the vertical plane, and the entire crystal tilted (in the plane containing the optic axis, the surface normal, and the pump beam) by 0.72°, thus increasing the effective value of $\theta_{\rm pm}$ (inside the crystal) to 49.63°. The two cone-overlap directions, selected by irises before the detectors, were consequently separated by 6.0°. Each polarization analyzer consisted of two stacked polarizing beam splitters preceded by a rotatable half wave plate. The detectors were cooled silicon avalanche photodiodes operated in the Geiger mode. Coincidence rates $C(\theta_1, \theta_2)$ were recorded as a function of the polarizer settings θ_1 and θ_2.

In our experiment the transverse walk-off d (0.3 mm) was small compared to the coherent pump beam width (2 mm), so the associated labeling effect was minimal. However, it was necessary to compensate for longitudinal walk-off, since the 3.0 mm BBO crystal produced $\delta T = 385$ fs, while τ_c [determined by the collection irises and interference filters (centered at 702 nm, 5 nm FWHM)] was about the same. As discussed above, we used an additional BBO crystal (1.5 mm thickness) in each of the paths, preceded by a half wave plate to exchange the roles of the horizontal and vertical polarizations.

Under these conditions, we attained a maximum coincidence fringe visibility (as polarizer 2 was rotated, with polarizer 1 fixed at −45° [26]) of (97.8 ± 1.0)%, indicating the high quality of the source. Appropriately orienting the wave plates in path 1, we produced all four EPR-Bell states and observed the expected correlations (Table I, Fig. 3).

As is well known, the high-visibility sinusoidal coincidence fringes in such an experiment imply a violation of a suitable Bell inequality. In particular, according to the inequality of Clauser, Horne, Shimony, and Holt (CHSH) [27], $|S| \leq 2$ for any local realistic theory, where

TABLE I. The four EPR-Bell states, the associated coincidence rate predictions, and the measured value of the parameter S.

EPR-Bell state	$C(\theta_1, \theta_2)$	S[a]
$\|\psi^+\rangle$	$\sin^2(\theta_1 + \theta_2)$	−2.6489 ± 0.0064
$\|\psi^-\rangle$	$\sin^2(\theta_1 - \theta_2)$	−2.6900 ± 0.0066
$\|\phi^+\rangle$	$\cos^2(\theta_1 - \theta_2)$	2.557 ± 0.014
$\|\phi^-\rangle$	$\cos^2(\theta_1 + \theta_2)$	2.529 ± 0.013

[a]Data for the $|\phi^\pm\rangle$ states were taken with a single compensating crystal, data for the $|\psi^\pm\rangle$ states with a compensating crystal in each path (see text).

$$S = E(\theta_1, \theta_2) + E(\theta_1', \theta_2) + E(\theta_1, \theta_2') - E(\theta_1', \theta_2'), \tag{3a}$$

and $E(\theta_1, \theta_2)$ is given by [28]

$$\frac{C(\theta_1, \theta_2) + C(\theta_1^\perp, \theta_2^\perp) - C(\theta_1, \theta_2^\perp) - C(\theta_1^\perp, \theta_2)}{C(\theta_1, \theta_2) + C(\theta_1^\perp, \theta_2^\perp) + C(\theta_1, \theta_2^\perp) + C(\theta_1^\perp, \theta_2)}. \tag{3b}$$

The measured value of S is a figure of merit for the quality of the actual entangled state produced from the crystal. Therefore, for each of the four EPR-Bell states we took extensive data for the settings [29] $\theta_1 = -22.5°$, $\theta_1^\perp = 67.5°$; $\theta_1' = 22.5°$, $\theta_1'^\perp = 112.5°$; and $\theta_2 = -45°$, $\theta_2^\perp = 45°$; $\theta_2' = 0°$, $\theta_2'^\perp = 90°$. The CHSH inequality was strongly violated in all cases; see Table I.

For one of the Bell inequality measurements (ψ^+), a larger collection iris allowed us to accumulate the statistics necessary for a 102 standard deviation violation in less than 5 min. In particular, we were able to use elliptical collection irises (1.5 m from the crystal) with a horizontal opening of 3 mm, and a vertical opening of 10 mm, and still see visibilities of 95%. Therefore this source is more

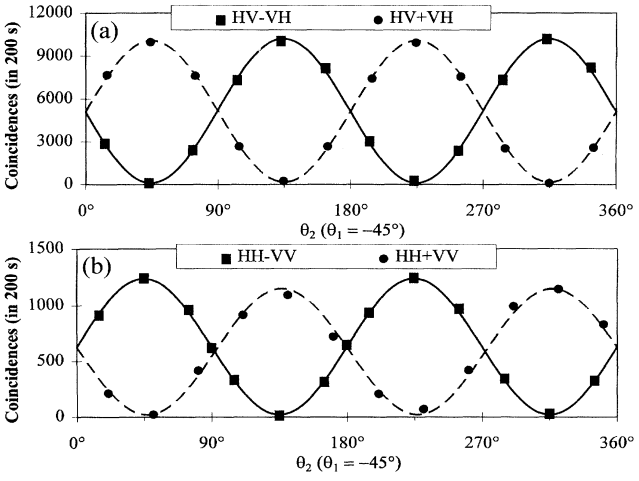


FIG. 3. Coincidence fringes for states (a) $(|H_1, V_2\rangle \pm |V_1, H_2\rangle)/\sqrt{2}$; (b) $(|H_1, H_2\rangle \pm |V_1, V_2\rangle)/\sqrt{2}$. The difference in the counting rates for the two plots is due to different collection geometries.

than an order of magnitude brighter than previous sources for polarization-entangled photons, with coincidence rates greater than 1500 s^{-1}. The high net detection efficiency ($> 10\%$) is an important step towards a loophole-free Bell-inequality experiment [9,10]. However, to achieve the requisite efficiency, it will almost certainly be necessary to employ a spatial-filtering scheme to take advantage of the momentum correlations of the photons.

Our source has a number of distinct advantages. As indicated above, it seems to be relatively insensitive to larger collection irises, an important practical advantage, and possibly crucial for a loophole-free test. In addition, due to its simplicity, the present scheme was much quicker to align than other down-conversion setups, and was remarkably stable. One of the reasons is that phase drifts are not detrimental to a polarization-entangled state unless they are *birefringent*, i.e., polarization dependent—this is a clear benefit over momentum-entangled or energy-time-entangled states. Moreover, one can, in fact, transform polarization-entangled states into momentum- or energy-time entangled states [12,30].

For these reasons, we expect that our technique will find immediate application in many experiments requiring a stable source of easily controllable entangled states of two particles, in particular, experiments on quantum communication, including quantum cryptography [4], encoding more than one bit of information in a photon [5], teleportation [6], "entanglement swapping" [7], and in the new field of quantum computation [8]. We believe that this source will significantly facilitate such experiments, as well as investigations of the foundations of quantum mechanics, even in student laboratories.

We would like to acknowledge Gregor Weihs for laboratory assistance, Ralph Höpfel for the helpful loan of a crystal in the first version of this experiment, Michael Reck for his photographic expertise, and Photo Gratl for developing the infrared film at night. This work was supported by the Austrian Science Foundation (FWF), Project No. S065/02, and by the U.S. National Science Foundation, Grant No. PHY92-13964. One of us (P. G. K.) was supported by FWF Lise Meitner Postdoctoral Fellowship, M0077-PHY.

*Current address: Physics Div., MS-H803, Los Alamos National Laboratory, Los Alamos, NM 87545.

[1] J. F. Clauser and A. Shimony, Rep. Prog. Phys. **41**, 1981 (1978), and references therein.

[2] A. Aspect, P. Grangier, and G. Roger, Phys. Rev. Lett. **47**, 460 (1981); **49**, 91 (1982); A. Aspect, J. Dalibard, and G. Roger, *ibid.* **49**, 1804 (1982).

[3] Z. Y. Ou and L. Mandel, Phys. Rev. Lett. **61**, 50 (1988); Y. H. Shih and C. O. Alley, *ibid.* **61**, 2921 (1988); P. G. Kwiat, A. M. Steinberg, and R. Y. Chiao, Phys. Rev. A **47**, R2472 (1993); J. Brendel, E. Mohler, and W. Martienssen, Europhys. Lett. **20**, 575 (1992); T. E. Kiess, Y. H. Shih, A. V. Sergienko, and C. O. Alley, Phys. Rev. Lett. **71**, 3893 (1993).

[4] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[5] C. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992); H. Weinfurter, Europhys. Lett. **25**, 559 (1994).

[6] C. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wooters, Phys. Rev. Lett. **70**, 1895 (1993).

[7] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993); M. Pavicic and J. Summhammer, *ibid.* **73**, 3191 (1994).

[8] A. Barenco, D. Deutsch, A. Ekert, and R. Jozsa, Phys. Rev. Lett. **74**, 4083 (1995); T. Sleator and H. Weinfurter, *ibid.* **74**, 4087 (1995); J. I. Cirac and P. Zoller, *ibid.* **74**, 4091 (1995).

[9] E. Santos, Phys. Rev. Lett. **68**, 894 (1992); Phys. Rev. A **46**, 3646 (1992).

[10] P. G. Kwiat, P. H. Eberhard, A. M. Steinberg, and R. Y. Chiao, Phys. Rev. A **49**, 3209 (1994).

[11] L. De Caro and A. Garuccio, Phys. Rev. A **50**, R2803 (1994).

[12] P. G. Kwiat, Phys. Rev. A **52**, 3380 (1995).

[13] One down-conversion source of *momentum*-entangled photons [M. A. Horne, A. Shimony, and A. Zeilinger, Phys. Rev. Lett. **62**, 2209 (1989)] does not suffer this minimum 50% decimation. However, the experimental realization [J. G. Rarity and P. R. Tapster, Phys. Rev. Lett. **64**, 2495 (1990)] suffered from poor visibility fringes ($\approx 80\%$), difficult alignment, and thermal instability.

[14] D. N. Klysko, Phys. Lett. A **132**, 299 (1988); L. Hardy, *ibid.* **161**, 326 (1992).

[15] S. L. Braunstein, A. Mann, and M. Revzen, Phys. Rev. Lett. **68**, 3259 (1992).

[16] R. Y. Chiao, P. G. Kwiat, and A. M. Steinberg, in *Advances in Atomic, Molecular and Optical Physics,* edited by B. Bederson and H. Walther (Academic Press, New York, 1994), Vol. 34.

[17] Because of transverse momentum conservation, the photons of each pair must lie on opposite sides of the pump beam.

[18] Y. H. Shih and A. V. Sergienko, Phys. Rev. A **50**, 2564 (1994);T. B. Pittman,Y. H. Shih, A. V. Sergienko, and M. H. Rubin, *ibid.* **51**, 3495 (1995).

[19] As θ_{pm} is increased to 90°, the two cones each become centered on the pump, and, in fact, overlap exactly. While this seems desirable, the actual down-conversion efficiency in a uniaxial crystal such as BBO varies as $\cos^2(\theta_{pm})$ [22], so that no down conversion takes place at this setting.

[20] A detailed calculation for vector phase matching in BBO [P. G. Kwiat, Ph. D. thesis, University of California at Berkeley, 1993] shows that the precise overlap only occurs *outside* the crystal, as a result of Snell's law at the exit face (assumed normal to the pump beam direction).

[21] Such a source has also been suggested by A. Garuccio [in *Fundamental Problems in Quantum Theory,* edited by D. Greenberger and A. Zeilinger, Annals of the New York Academy of Sciences, 755 (New York Academy of Sciences, New York, 1995)], Vol. 755, p. 632.

[22] V. G. Dmitriev, G. G. Gurzadyan, and D. N. Nikogosyan, *Handbook of Nonlinear Optical Crystals,* in *Springer*

Series in Optical Sciences, Vol. 64, edited by A. E. Siegman (Springer-Verlag, New York, 1991).

[23] M. H. Rubin, D. N. Klyshko, Y. H. Shih, and A. V. Sergienko, Phys. Rev. A **50**, 5122 (1994).

[24] It is also possible to compensate the longitudinal walk-off by using a *single* extra crystal, of length L, in only one of the arms. This will always cause one detector to fire before the other by the same amount δT, but now with the same firing order for both terms in the entanglement. Interference will be recovered whenever the coherence time of the pump is much longer than δT, for then the *processes* contributing to interference are indistinguishable. Tests made in this configuration displayed results nearly as good as those with two $L/2$ compensators.

[25] However, for a sufficiently long crystal, the o and e rays can separate by more than the coherence width of the pump beam, and it is then not possible to completely compensate the effects of walk-off.

[26] It is necessary to examine the case with one of the polarizers at $\pm 45°$ in order to demonstrate the quantum coherence between the terms in the entangled states (2).

[27] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[28] In normalizing to the sum of the four coincidence rates, we are invoking a particular version of the fair-sampling assumption [A. Garuccio and V. A. Rapisarda, Nuovo Cimento **65A**, 269 (1981)].

[29] Ideally, one would measure θ_i and $\theta_i^{\perp}$ simultaneously, e.g., by using both ports of the analyzing polarizing beam splitters, and four detectors. We approximated this situation by considering explicitly values of each polarizer separated by 90°; this requires the additional auxilliary assumption that the state from the source is independent of the analyzer settings.

[30] M. Zukowski and J. Pykacz, Phys. Lett. A **127**, 1 (1988).

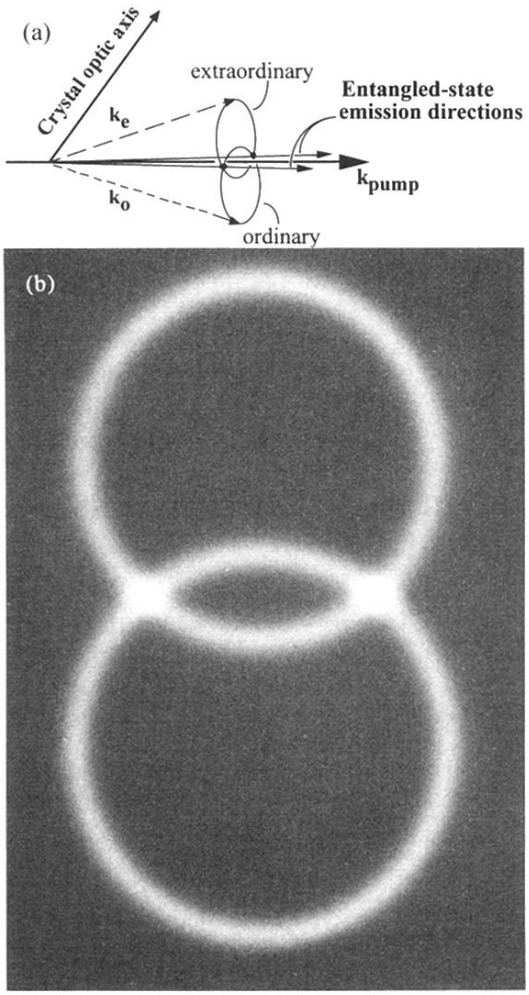


FIG. 1. (a) Spontaneous down-conversion cones present with type-II phase matching. Correlated photons lie on opposite sides of the pump beam. (b) A photograph of the down-conversion photons, through an interference filter at 702 nm (5 nm FWHM). The infrared film was located 11 cm from the crystal, with no imaging lens. (Photograph by M. Reck.)

Chapter 8

Quantum Cryptography, Quantum Money

A major application of quantum technologies is quantum cryptography where a secret key can be exchanged between A and B (Alice and Bob), eavesdropping (by Eve) without detection is impossible because of the laws of physics: the no-cloning theorem we recently demonstrated is at the heart of quantum communication and offers the first technique to guarantee data encryption with the laws of physics instead of mathematical tricks.

This is certainly the most mature of all quantum technologies, with a wide number of demonstrations and commercial devices already available. There are two families of quantum key distribution techniques: Discrete Variables (DV) and Continuous Variables (CV). In DV-QKD, single photons are sent one at a time and polarization can be encoded on the polarization of each photon as for the BB-84 and E-91 protocol we will see below. In CV-QKD, a continuous beam of light is sent and the amplitude and phase can encode information.

8.1 The BB84 protocol

The concept of quantum cryptography was proposed by Bennet and Brassard in 1984, this scheme is referred to as the BB84 scheme. It relies on single photons sent from Alice to Bob with controlled polarization. It must be noted that this technique generates a secret encryption key that is only shared between Alice and Bob, they can then use this secret key to encode their communication and share the encrypted message on a public channel. To make hacking impossible, each encryption key must be used only once (one time pad). This means there are two channels: a quantum channel to share quantum bits and a classical channel to distil the key and to share the encrypted message. Alice prepares an encryption key: a random number and sends that key to Bob by encoding each bit as a polarized single photon either in the HV basis (where H=1 and V=0) or in the AD (where D=1 and A=0) basis (she randomly chooses which basis to use for each photon). For every photon sent out, Alice needs two random bits: one for the state and one for the basis. Alice keeps her basis choices for herself. Bob measures the photons sent by Alice in random polarization basis (HV or DA) and keeps track of the detection events as well as the basis he used for each measurement. Note that the basis HV and DA must be agreed on between Alice and Bob and must be stable. Note also that the photon can be given a new name, more in line with quantum information: *a flying qubit.*

Alice then sends out on a public channel (accessible to everyone) the list of polarization bases she used: + X X ++X+X.... Alice and Bob only keep the bits measured in the same basis and discard the other half, the result is the sifted key. Alice and Bob then compare openly a part of their sifted key to make sure they are identical to check that no eavesdropper tried to intercept the message, this part that has been compared in public can obviously not be used anymore. Because of the no-cloning theorem, no eavesdropper can make perfect copies of Alice signal and send them to Bob. Comparing part of a key would therefore reveal any attempt at intercepting the message. It is therefore the no-cloning theorem that guarantees the BB84 protocol's security.

Alice has a random bit sequence she wants to share with Bob, she randomly selects polarization bases for each photon and sends a single photon to Bob with the corresponding polarization. The cases where Bob selected the same base than Alice allow them to share a secret bit. The resulting key can be used to encrypt a message, only Alice and Bob share this encryption key.

If Alice and Bob share the same polarization base, they share the bit. When different bases are used between Alice and Bob, the outcome is random.

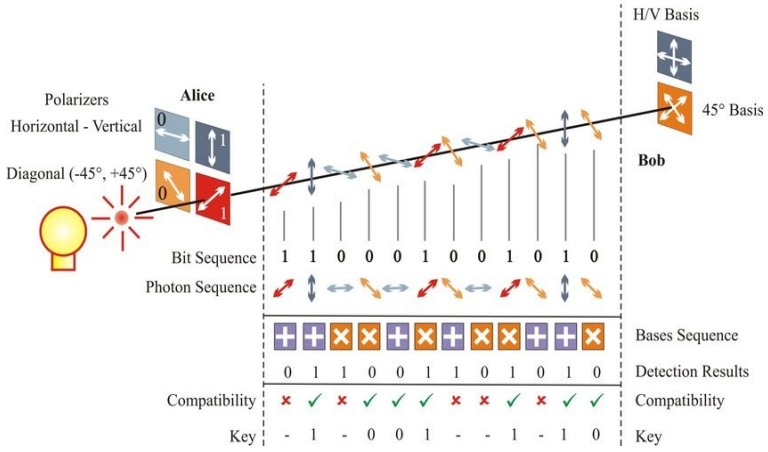


Figure 8.1: Concept of the BB84 protocol.

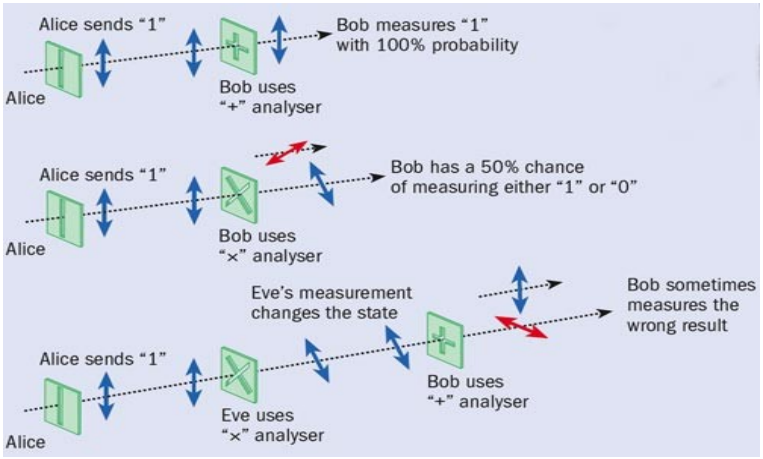


Figure 8.2: If Alice and Bob share the same polarization base, they share the bit. When Alice and Bob use different bases, the outcome is random.

8.2 The E91 protocol

Arthur Eckert came up with an improved version of the BB84 in 1991: the E91 protocol. We have seen that the BB84 protocol requires Alice to generate a random key and that half of the qubits are not used (Alice and Bob operate in different bases half of the time). This is solved using entangled photon pairs instead.

Figure 8.3: The E91 does not need Alice to choose random bases, this is taken care of with entanglement.

The entangled photon pair source can be located anywhere between Alice and Bob, the polarization randomness is given by quantum mechanics:

$$|HV\rangle + |VH\rangle$$

Like in the BB84, Alice and Bob measure either in HV or AD bases. They keep their results secret but publicly announce the base they used. Alice and Bob can then check that Bell's inequality is violated. If this is not the case, they deduce that an eavesdropper tried to intercept the photons and destroyed the entanglement (again, the no-cloning theorem). Note that with the E91 the key is produced by the measurement. A challenge for this implementation is the need for a bright source of entangled photons. It is very interesting to note that measuring entanglement in this case is useful to demonstrate the security of the quantum communication channel.

While quantum cryptography has been demonstrated in many laboratories around the world, it is not yet widely adopted. Among the drawbacks are the costs (need for single photon sources, detectors and direct

optical fibers from A to B), the limited bandwidth and the lack of a certification (there is not yet any central certification system for quantum technologies).

8.3 Quantum Money

Quantum money was proposed by Stephen Wiener in 1983. This was possibly the first ever quantum technology concept. Each issued banknote is given a classical serial number and a set of isolated quantum systems (qubits: electron spins, photon polarization...) A random number is written using two bases (HV or AD) and is preserved long enough (hours, months, years) until the authenticity of the banknote must be established. The bank keeps a record of the polarization bases used to write the random numbers as well as the random number itself associated with each serial number.

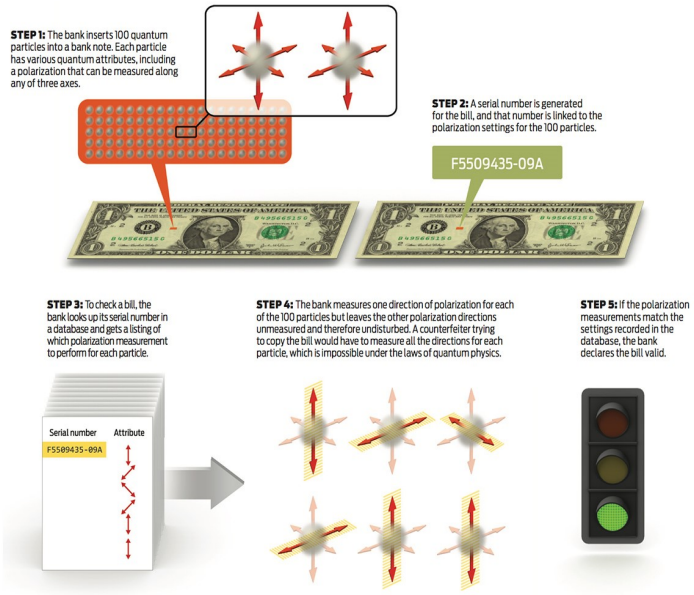


Figure 8.4: The concept of quantum money predates the BB84 and is based on similar concepts.

When a transaction takes place, the bank measures each qubit in the right base and finds exactly the initial random number, this shows that the banknote is not a counterfeit. If a counterfeiter tried to make a fake, half of the time he will measure the qubit in the wrong basis. For each qubit, the counterfeiter has probability 3/4 to duplicate each qubit correctly (1/2 in the right basis, when in the wrong basis 1/2 chance to guess right).

For N qubits, the probability to pass the bank test is $(3/4)^N$ For 20 qubits $(3/4)^{20} = 0.003$ this shows that a limited number of qubits are needed to be useful (compared to a quantum computer) but that their lifetime must be very long. Here again, the no-cloning theorem is used to certify the origin of a message.

Quantum money requires very long lived qubits to be implemented and preferably at room temperature.

Theoretical Computer Science 560 (2014) 7–11

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Quantum cryptography: Public key distribution and coin tossing ☆

Charles H. Bennett [a], Gilles Brassard [b]

[a] IBM Research, Yorktown Heights NY 10598, USA
[b] Département IRO, Université de Montréal, Montréal, QC, H3C 3J7 Canada

When elementary quantum systems, such as polarized photons, are used to transmit digital information, the uncertainty principle gives rise to novel cryptographic phenomena unachievable with traditional transmission media, e.g. a communications channel on which it is impossible in principle to eavesdrop without a high probability of disturbing the transmission in such a way as to be detected. Such a quantum channel can be used in conjunction with ordinary insecure classical channels to distribute random key information between two users with the assurance that it remains unknown to anyone else, even when the users share no secret information initially. We also present a protocol for coin-tossing by exchange of quantum messages, which is secure against traditional kinds of cheating, even by an opponent with unlimited computing power, but ironically can be subverted by use of a still subtler quantum phenomenon, the Einstein–Podolsky–Rosen paradox.

I. Introduction

Conventional cryptosystems such as ENIGMA, DES, or even RSA, are based on a mixture of guesswork and mathematics. Information theory shows that traditional secret-key cryptosystems cannot be totally secure unless the key, used once only, is at least as long as the cleartext. On the other hand, the theory of computational complexity is not yet well enough understood to prove the computational security of public-key cryptosystems.

In this paper we use a radically different foundation for cryptography, viz. the uncertainty principle of quantum physics. In conventional information theory and cryptography, it is taken for granted that digital communications in principle can always be passively monitored or copied, even by someone ignorant of their meaning. However, when information is encoded in non-orthogonal quantum states, such as single photons with polarization directions 0, 45, 90, and 135 degrees, one obtains a communications channel whose transmissions in principle cannot be read or copied reliably by an eavesdropper ignorant of certain key information used in forming the transmission. The eavesdropper cannot even gain partial information about such a transmission without altering it in a random and uncontrollable way likely to be detected by the channel's legitimate users.

Quantum coding was first described in [W], along with two applications: making money that is in principle impossible to counterfeit, and multiplexing two or three messages in such a way that reading one destroys the others. More recently [BBBW], quantum coding has been used in conjunction with public key cryptographic techniques to yield several schemes for unforgeable subway tokens. Here we show that quantum coding by itself achieves one of the main advantages of public key cryptography by permitting secure distribution of random key information between parties who share no secret information initially, provided the parties have access, besides the quantum channel, to an ordinary channel susceptible to passive but not active eavesdropping. Even in the presence of active eavesdropping, the two parties can still distribute key securely if they share some secret information initially, provided the eavesdropping is not so active as to suppress communications completely. We also present a protocol for coin tossing by exchange of quantum messages. Except where

☆ This paper appeared originally on pages 175–179 of the Proceedings of the *International Conference on Computers, Systems and Signal Processing*, which took place in Bangalore (now Bengalūru) in December 1984. It appears now for the first time in an archival journal, exactly as it was in its original 1984 version, except for fresh typesetting abiding to *Theoretical Computer Science* style, the correction of about one dozen typographical mistakes, as well as updated email addresses, affiliations and bibliographic publication data. A scan of the original manuscript is available as supplementary online material.

E-mail addresses: chdbennett@gmail.com (C.H. Bennett), brassard@iro.umontreal.ca (G. Brassard).

http://dx.doi.org/10.1016/j.tcs.2014.05.025

otherwise noted the protocols are provably secure even against an opponent with superior technology and unlimited computing power, barring fundamental violations of accepted physical laws.

Offsetting these advantages is the practical disadvantage that quantum transmissions are necessarily very weak and cannot be amplified in transit. Moreover, quantum cryptography does not provide digital signatures, or applications such as certified mail or the ability to settle disputes before a judge.

II. Essential properties of polarized photons

Polarized light can be produced by sending an ordinary light beam through a polarizing apparatus such as a Polaroid filter or calcite crystal; the beam's polarization axis is determined by the orientation of the polarizing apparatus in which the beam originates. Generating single polarized photons is also possible, in principle by picking them out of a polarized beam, and in practice by a variation of an experiment [AGR] of Aspect et al.

Although polarization is a continuous variable, the uncertainty principle forbids measurements on any single photon from revealing more than one bit about its polarization. For example, if a light beam with polarization axis α is sent into a filter oriented at angle β, the individual photons behave dichotomously and probabilistically, being transmitted with probability $\cos^2(\alpha-\beta)$ and absorbed with the complementary probability $\sin^2(\alpha-\beta)$. The photons behave deterministically only when the two axes are parallel (certain transmission) or perpendicular (certain absorption).

If the two axes are not perpendicular, so that some photons are transmitted, one might hope to learn additional information about α by measuring the transmitted photons again with a polarizer oriented at some third angle; but this is to no avail, because the transmitted photons, in passing through the β polarizer, emerge with exactly β polarization, having lost all memory of their previous polarization α.

Another way one might hope to learn more than one bit from a single photon would be not to measure it directly, but rather somehow amplify it into a clone of identically polarized photons, then perform measurements on these; but this hope is also vain, because such cloning can be shown to be inconsistent with the foundations of quantum mechanics [WZ].

Formally, quantum mechanics represents the internal state of a quantum system (e.g. the polarization of a photon) as a vector ψ of unit length in a linear space H over the field of complex numbers (Hilbert space). The inner product of two vectors $\langle\phi \mid \psi\rangle$ is defined as $\sum_j \phi_j^* \psi_j$, where * indicates complex conjugation. The dimensionality of the Hilbert space depends on the system, being larger (or even infinite) for more complicated systems. Each physical measurement M that might be performed on the system corresponds to a resolution of its Hilbert space into orthogonal subspaces, one for each possible outcome of the measurement. The number of possible outcomes is thus limited to the dimensionality d of the Hilbert space, the most complete measurements being those that resolve the Hilbert space into d 1-dimensional subspaces.

Let M_k represent the projection operator onto the kth subspace of measurement M, so that the identity operator on H can be represented as a sum of projections: $I = M_1 + M_2 + \ldots$. When a system in state ψ is subjected to measurement M, its behavior is in general probabilistic: outcome k occurs with a probability equal to $|M_k\psi|^2$, the square of the length of the state vector's projection into subspace M_k. After the measurement, the system is left in a new state $M_k\psi/|M_k\psi|$, which is the normalized unit vector in the direction of the old state vector's projection into subspace M_k. The measurement thus has a deterministic outcome, and leaves the state vector unmodified, only in the exceptional case that the initial state vector happens to lie entirely in one of the orthogonal subspaces characterizing the measurement.

The Hilbert space for a single polarized photon is 2-dimensional; thus the state of a photon may be completely described as a linear combination of, for example, the two unit vectors $r_1 = (1, 0)$ and $r_2 = (0, 1)$, representing respectively horizontal and vertical polarization. In particular, a photon polarized at angle α to the horizontal is described by the state vector $(\cos\alpha, \sin\alpha)$. When subjected to a measurement of vertical-vs.-horizontal polarization, such a photon in effect chooses to become horizontal with probability $\cos^2\alpha$ and vertical with probability $\sin^2\alpha$. The two orthogonal vectors r_1 and r_2 thus exemplify the resolution of a 2-dimensional Hilbert space into 2 orthogonal 1-dimensional subspaces; henceforth r_1 and r_2 will be said to comprise the 'rectilinear' basis for the Hilbert space.

An alternative basis for the same Hilbert space is provided by the two 'diagonal' basis vectors $d_1 = (0.707, 0.707)$, representing a 45-degree photon, and $d_2 = (0.707, -0.707)$, representing a 135-degree photon. Two bases (e.g. rectilinear and diagonal) are said to be 'conjugate' [W] if each vector of one basis has equal-length projections onto all vectors of the other basis: this means that a system prepared in a specific state of one basis will behave entirely randomly, and lose all its stored information, when subjected to a measurement corresponding to the other basis. Owing to the complex nature of its coefficients, the two-dimensional Hilbert space also admits a third basis conjugate to both the rectilinear and diagonal bases, comprising the two so-called 'circular' polarizations $c_1 = (0.707, 0.707i)$ and $c_2 = (0.707i, 0.707)$; but the rectilinear and diagonal bases are all that will be needed for the cryptographic applications in this paper.

The Hilbert space for a compound system is constructed by taking the tensor product of the Hilbert spaces of its components; thus the state of a pair of photons is characterized by a unit vector in the 4-dimensional Hilbert space spanned by the orthogonal basis vectors r_1r_1, r_1r_2, r_2r_1, and r_2r_2. This formalism entails that the state of a compound system is not generally expressible as the cartesian product of the states of its parts: e.g. the Einstein–Podolsky–Rosen state of two photons, $0.7071(r_1r_2 - r_2r_1)$, to be discussed later, is not equivalent to any product of one-photon states.

III. Quantum public key distribution

In traditional public-key cryptography, trapdoor functions are used to conceal the meaning of messages between two users from a passive eavesdropper, despite the lack of any initial shared secret information between the two users. In quantum public key distribution, the quantum channel is not used directly to send meaningful messages, but is rather used to transmit a supply of random bits between two users who share no secret information initially, in such a way that the users, by subsequent consultation over an ordinary non-quantum channel subject to passive eavesdropping, can tell with high probability whether the original quantum transmission has been disturbed in transit, as it would be by an eavesdropper (it is the quantum channel's peculiar virtue to compel eavesdropping to be active). If the transmission has not been disturbed, they agree to use these shared secret bits in the well-known way as a *one-time pad* to conceal the meaning of subsequent meaningful communications, or for other cryptographic applications (e.g. authentication tags) requiring shared secret random information. If transmission has been disturbed, they discard it and try again, deferring any meaningful communications until they have succeeded in transmitting enough random bits through the quantum channel to serve as a one-time pad.

In more detail one user ('Alice') chooses a random bit string and a random sequence of polarization bases (rectilinear or diagonal). She then sends the other user ('Bob') a train of photons, each representing one bit of the string in the basis chosen for that bit position, a horizontal or 45-degree photon standing for a binary zero and a vertical or 135-degree photon standing for a binary 1. As Bob receives the photons he decides, randomly for each photon and independently of Alice, whether to measure the photon's rectilinear polarization or its diagonal polarization, and interprets the result of the measurement as a binary zero or one. As explained in the previous section a random answer is produced and all information lost when one attempts to measure the rectilinear polarization of a diagonal photon, or vice versa. Thus Bob obtains meaningful data from only half the photons he detects—those for which he guessed the correct polarization basis. Bob's information is further degraded by the fact that, realistically, some of the photons would be lost in transit or would fail to be counted by Bob's imperfectly-efficient detectors.

Subsequent steps of the protocol take place over an ordinary public communications channel, assumed to be susceptible to eavesdropping but not to the injection or alteration of messages. Bob and Alice first determine, by public exchange of messages, which photons were successfully received and of these which were received with the correct basis. If the quantum transmission has been undisturbed, Alice and Bob should agree on the bits encoded by these photons, even though this data has never been discussed over the public channel. Each of these photons, in other words, presumably carries one bit of random information (e.g. whether a rectilinear photon was vertical or horizontal) known to Alice and Bob but to no one else.

Because of the random mix of rectilinear and diagonal photons in the quantum transmission, any eavesdropping carries the risk of altering the transmission in such a way as to produce disagreement between Bob and Alice on some of the bits on which they think they should agree. Specifically, it can be shown that no measurement on a photon in transit, by an eavesdropper who is informed of the photon's original basis only after he has performed his measurement, can yield more than $1/2$ expected bits of information about the key bit encoded by that photon; and that any such measurement yielding b bits of expected information ($b \leq 1/2$) must induce a disagreement with probability at least $b/2$ if the measured photon, or an attempted forgery of it, is later re-measured in its original basis. (This optimum tradeoff occurs, for example, when the eavesdropper measures and retransmits all intercepted photons in the rectilinear basis, thereby learning the correct polarizations of half the photons and inducing disagreements in $1/4$ of those that are later re-measured in the original basis.)

Alice and Bob can therefore test for eavesdropping by publicly comparing some of the bits on which they think they should agree, though of course this sacrifices the secrecy of these bits. The bit positions used in this comparison should be a random subset (say one third) of the correctly received bits, so that eavesdropping on more than a few photons is unlikely to escape detection. If all the comparisons agree, Alice and Bob can conclude that the quantum transmission has been free of significant eavesdropping, and those of the remaining bits that were sent and received with the same basis also agree, and can safely be used as a one-time pad for subsequent secure communications over the public channel. When this one-time pad is used up, the protocol is repeated to send a new body of random information over the quantum channel.

The following example illustrates the above protocol.

QUANTUM TRANSMISSION															
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	⤢	↕	⤡	↔	↕	↕	↔	↔	⤡	⤢	↕	⤡	⤢	⤢	↕
Random receiving bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)			1		1			0				1		0	1
Bob reveals some key bits at random					1									0	
Alice confirms them					OK									OK	
OUTCOME															
Remaining shared secret bits			1					0				1			1

The need for the public (non-quantum) channel in this scheme to be immune to *active* eavesdropping can be relaxed if Alice and Bob have agreed beforehand on a small secret key, which they use to create Wegman–Carter authentication tags [WC] for their messages over the public channel. In more detail the Wegman–Carter multiple-message authentication scheme uses a small random key to produce a message-dependent 'tag' (rather like a check sum) for an arbitrarily large message, in such a way that an eavesdropper ignorant of the key has only a small probability of being able to generate any other valid message–tag pairs. The tag thus provides evidence that the message is legitimate, and was not generated or altered by someone ignorant of the key. (Key bits are gradually used up in the Wegman–Carter scheme, and cannot be reused without compromising the system's provable security; however, in the present application, these key bits can be replaced by fresh random bits successfully transmitted through the quantum channel.) The eavesdropper can still prevent communication by suppressing messages in the public channel, as of course he can by suppressing or excessively perturbing the photons sent through the quantum channel. However, in either case, Alice and Bob will conclude with high probability that their secret communications are being suppressed, and will not be fooled into thinking their communications are secure when in fact they're not.

IV. Quantum coin tossing

'Coin Flipping by Telephone' was first discussed by Blum [Bl]. The problem is for two distrustful parties, communicating at a distance without the help of a third party, to come to agree on a winner and a loser in such a way that each party has exactly 50 percent chance of winning. Any attempt by either party to bias the outcome should be detected by the other party as cheating. Previous protocols for this problem are based on unproved assumptions in computational complexity theory, which makes them vulnerable to a breakthrough in algorithm design.

By contrast, we present here a scheme involving classical and quantum messages which is secure against traditional kinds of cheating, even by an opponent with unlimited computing power. Ironically, it can be subverted by a still subtler quantum phenomenon, the so-called Einstein–Podolsky–Rosen effect. This threat is merely theoretical, because it requires perfect efficiency of storage and detection of photons, which though not impossible in principle is far beyond the capabilities of current technology. The honestly-followed protocol, on the other hand, could be realized with current technology.

1. Alice chooses randomly one basis (say rectilinear) and a sequence of random bits (one thousand should be sufficient). She then encodes her bits as a sequence of photons in this same basis, using the same coding scheme as before. She sends the resulting train of polarized photons to Bob.
2. Bob chooses, independently and randomly for each photon, a sequence of reading bases. He reads the photons accordingly, recording the results in two tables, one of rectilinearly received photons and one of diagonally received photons. Because of losses in his detectors and in the transmission channel, some of the photons may not be received at all, resulting in holes in his tables. At this time, Bob makes his guess as to which basis Alice used, and announces it to Alice. He wins if he guessed correctly, loses otherwise.
3. Alice reports to Bob whether he won, by telling him which basis she had actually used. She certifies this information by sending Bob, over a classical channel, her entire original bit sequence used in step 1.
4. Bob verifies that no cheating has occurred by comparing Alice's sequence with both his tables. There should be perfect agreement with the table corresponding to Alice's basis and no correlation with the other table. In our example, Bob can be confident that Alice's original basis was indeed rectilinear as claimed.

Illustrating the protocol by a specific example, we have

Alice's bit string	1	0	1	0	0	1	1	1	0	1	0	1	1	0	0
Alice's random basis								Rectilinear							
Photons Alice sends	↕	↔	↕	↔	↔	↕	↕	↕	↔	↕	↔	↕	↕	↔	↔
Bob's random bases	R	D	D	D	R	R	D	R	R	D	R	R	D	D	R
Bob's rectilinear table	1					1					0				0
Bob's diagonal table		0		1						1			0		
Bob's guess								'Rectilinear'							
Alice's reply								'You win'							
Alice sends her original bit string to certify	'1	0	1	0	0	1	1	1	0	1	0	1	1	0	0'
Bob's rectilinear table	1					1					0				0
Bob's diagonal table		0		1						1			0		

In order to cheat, Bob would need to guess Alice's basis with probability greater than 1/2. This amounts to distinguishing a train of photons randomly polarized in one basis from a train randomly polarized in another basis. However, it can be shown that any measuring apparatus capable of making this distinction can also be used, in conjunction with the Einstein–Podolsky–Rosen effect described below, to transmit useful information faster than the speed of light, in violation of well-established physical laws.

Alice could attempt cheating either at step 1 or step 3. Let us first assume that she follows step 1 honestly and finds herself losing at the end of step 2, because Bob made the correct guess, here rectilinear. In order to pretend she has won, she would need to convince Bob that her photons were diagonally polarized, which she can only do by pro-

ducing a sequence of bits in perfect agreement with Bob's diagonal table. This she cannot do reliably because this table is the result of probabilistic behavior of the photons after they left her hands. Suppose she goes ahead anyway and sends Bob a new 'original' sequence, different from the one that she used in step 1, in the hope that it will by luck agree perfectly with Bob's diagonal table. This attempt to cheat requires Alice to be not only lucky but daring, because in the vast majority of cases, the gamble would fail and would be detected as cheating. By contrast, in traditional coin-tossing schemes, analogous attempts to seize a lucky victory from the jaws of defeat, though unlikely to succeed, are unaccompanied by any danger of detection.

It is easy to see that things are even worse for Alice if she attempts to cheat in step 1 by sending a mixture of rectilinear and diagonal photons, or photons which are polarized neither rectilinearly or diagonally. In this case she will not be able to agree with either of Bob's tables in step 3, since both tables will record the results of probabilistic behavior not under her control.

In order to say how Alice *can* cheat using quantum mechanics it is necessary to describe the Einstein–Podolsky–Rosen (EPR) effect [Bo,AGR], often called a paradox because it contradicts the common-sense notion that for two individually random events happening at distance from one another to be correlated, some physical influence must have propagated from the earlier event to the later, or else from some common random cause to both events.

The EPR effect occurs when certain types of atom or molecule decay with the emission of two photons, and consists of the fact that the two photons are always found to have opposite polarization, regardless of the basis used to observe them, provided both are observed in the same basis. For example, if both photons are measured rectilinearly, it will always be found that one is horizontal and the other vertical, though which is horizontal will vary randomly from one decay to the next. If both photons are measured diagonally, one will always be 135-degree and the other 45-degree. A moment's reflection will show that this behavior cannot be explained by assuming the decay produces a distribution over α of oppositely polarized (α and $\alpha + 90$) photons, since, in that case, if such a pair of photons were measured in an intermediate basis (say $\alpha + 45$), both would behave probabilistically so as to sometimes come out with the same polarization.

Probably the simplest, but paradoxical-sounding, verbal explanation of the EPR effect is to say that the two photons are produced in an initial state of undefined polarization; and when one of them is measured, the measuring apparatus forces it to choose a polarization (choosing randomly and equiprobably between the two characteristic directions offered by the apparatus) while simultaneously forcing the other unmeasured photon, no matter how far away, to choose the opposite polarization. This implausible-sounding explanation is supported by formal quantum mechanics, which represents the state of a pair of photons as a vector in a 4-dimensional Hilbert space obtained by taking the tensor product of two 2-dimensional Hilbert spaces. The EPR state produced by the decay is described by the vector $0.7071(r_1 r_2 - r_2 r_1)$, and the EPR effect is explained by the fact that this vector has anticorrelated projections into the 2-dimensional Hilbert spaces of the two photons no matter what basis is used to express the tensor product (e.g. the same state vector is demonstrably equal to $0.7071(d_1 d_2 - d_2 d_1)$, and to $0.7071(c_1 c_2 - c_2 c_1)$).

In order to cheat, Alice produces a number of EPR photon-pairs instead of individual random photons in step 1. In each case she sends Bob one member of the pair and stores the other herself, perhaps between perfectly reflecting mirrors. When Bob makes his guess (e.g. rectilinear) she then measures all her stored photons in the opposite (diagonal) basis, thereby obtaining results perfectly correlated with his diagonal table but uncorrelated with his rectilinear table. She then announces these results, pretending them to be the random bits she was supposed to have encoded in the photons in step 1, and thereby forces a win from which Bob cannot escape even by delaying his measurements until after his guess. This cheat requires that Alice be able to store the twin photons for a considerable time and then measure them with high detection efficiency, and thus would be possible only in principle, not in practice. Any photons lost by Alice during storage or measurement would result in holes in her pretended bit sequence, which she would have to fill by guessing, and these guesses would risk detection by Bob if they failed to agree with his tables.

Appendix A. Supplementary material

A scan of the original manuscript of this paper, which became known as BB84, is available as supplementary material. It can be found online at http://dx.doi.org/10.1016/j.tcs.2014.05.025.

References

[AGR] A. Aspect, P. Grangier, and G. Roger, 'Experimental Realization of the Einstein–Podolsky–Rosen–Bohm Gedankenexperiment: a New Violation of Bell's Inequalities', *Phys. Rev. Lett.* 49, 91–94 (1982).

[BBBW] C.H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, 'Quantum Cryptography, or Unforgeable Subway Tokens', to appear in *Advances in Cryptography: Proceedings of CRYPTOB2*, Plenum Press. [These CRYPTO82 Proceedings were published in 1983 and this paper was on pages 267–275.]

[Bl] Manuel Blum, 'Coin Flipping by Telephone — a Protocol for Solving Impossible Problems', *SIGACT News* 15:1, 23–27 (1983).

[Bo] David Bohm, *Quantum Theory* (Prentice-Hall, Englewood Cliffs, NJ, 1951), pp. 614–619.

[WC] M. Wegman and L. Carter, 'New Hash Functions and Their Use in Authentication and Set Equality', *J. Comp. Sys. Sci.* 22, 265–279 (1981).

[W] Stephen Wiesner, 'Conjugate Coding' (manuscript ca 1970); subsequently published in *SIGACT News* 15:1, 78–88 (1983).

[WZ] W.K. Wootters and W.H. Zurek, 'A Single Quantum Cannot be Cloned', *Nature* 299, 802–803 (1982).

RESEARCH ARTICLE

QUANTUM OPTICS

Satellite-based entanglement distribution over 1200 kilometers

Juan Yin,[1,2] Yuan Cao,[1,2] Yu-Huai Li,[1,2] Sheng-Kai Liao,[1,2] Liang Zhang,[2,3] Ji-Gang Ren,[1,2] Wen-Qi Cai,[1,2] Wei-Yue Liu,[1,2] Bo Li,[1,2] Hui Dai,[1,2] Guang-Bing Li,[1,2] Qi-Ming Lu,[1,2] Yun-Hong Gong,[1,2] Yu Xu,[1,2] Shuang-Lin Li,[1,2] Feng-Zhi Li,[1,2] Ya-Yun Yin,[1,2] Zi-Qing Jiang,[3] Ming Li,[3] Jian-Jun Jia,[3] Ge Ren,[4] Dong He,[4] Yi-Lin Zhou,[5] Xiao-Xiang Zhang,[6] Na Wang,[7] Xiang Chang,[8] Zhen-Cai Zhu,[5] Nai-Le Liu,[1,2] Yu-Ao Chen,[1,2] Chao-Yang Lu,[1,2] Rong Shu,[2,3] Cheng-Zhi Peng,[1,2]* Jian-Yu Wang,[2,3]* Jian-Wei Pan[1,2]*

Long-distance entanglement distribution is essential for both foundational tests of quantum physics and scalable quantum networks. Owing to channel loss, however, the previously achieved distance was limited to ~100 kilometers. Here we demonstrate satellite-based distribution of entangled photon pairs to two locations separated by 1203 kilometers on Earth, through two satellite-to-ground downlinks with a summed length varying from 1600 to 2400 kilometers. We observed a survival of two-photon entanglement and a violation of Bell inequality by 2.37 ± 0.09 under strict Einstein locality conditions. The obtained effective link efficiency is orders of magnitude higher than that of the direct bidirectional transmission of the two photons through telecommunication fibers.

Quantum entanglement, first recognized by Einstein, Podolsky, and Roson (*1*) and Schrödinger (*2*), is a physical phenomenon in which the quantum states of a many-particle system cannot be factorized into a product of single-particle wave functions, even when the particles are separated by large distances. Entangled states have been produced in laboratories (*3*–*5*) and exploited to test the contradiction between classical local hidden variable theory and quantum mechanics by using Bell's inequality (*6*). It is of fundamental interest to distribute entangled particles over increasingly large distances and study the behavior of entanglement under extreme conditions. Practically, large-scale dissemination of entanglement—eventually at a global scale—is useful as the essential physical resource for quantum information protocols such as quantum cryptography (*7*), quantum teleportation (*8*), and quantum networks (*9*).

Limitations on entanglement distribution

So far, entanglement distribution has only been achieved at a physical separation up to ~100 km (*10*) and is mainly limited by the photon loss in the channel (optical fibers or terrestrial free space), which normally scales exponentially with the channel length. For example, through bidirectional distribution of an entangled source of photon pairs with a 10-MHz count rate directly through two 600-km telecommunication fibers with a loss of 0.16 dB/km, eventually one would only obtain 10^{-12} two-photon coincidence events per second. When the transmitted photons are attenuated to a level comparable to the dark counts of the single-photon detectors, the entanglement cannot be established because of the low signal-to-noise ratio. To improve the signal-to-noise ratio, the entangled photons in the channel cannot simply be amplified because of the quantum noncloning theorem (*11*), but radically new methods to reduce the link attenuation must be developed.

One solution to improve the distribution is the protocol of quantum repeaters (*12*) that divide the whole transmission line into smaller segments and combine the functionalities of entanglement swapping (*13*), entanglement purification (*14*), and quantum storage (*15*). There has been considerable progress in the demonstrations of these building blocks (*16*–*18*) and proof-of-principle quantum repeater nodes (*19*, *20*). However, the practical usefulness of the quantum repeaters is still hindered by the challenges of simultaneously realizing and integrating all the key capabilities, including, most importantly, long storage time and high retrieval efficiency (*21*).

Satellite-based entanglement distribution

Another approach to global-scale quantum networks is making use of satellite- and space-based technologies. A satellite can conveniently cover two distant locations on Earth separated by thousands of kilometers. The key advantage of this approach is that the photon loss and turbulence predominantly occur in the lower ~10 km of the

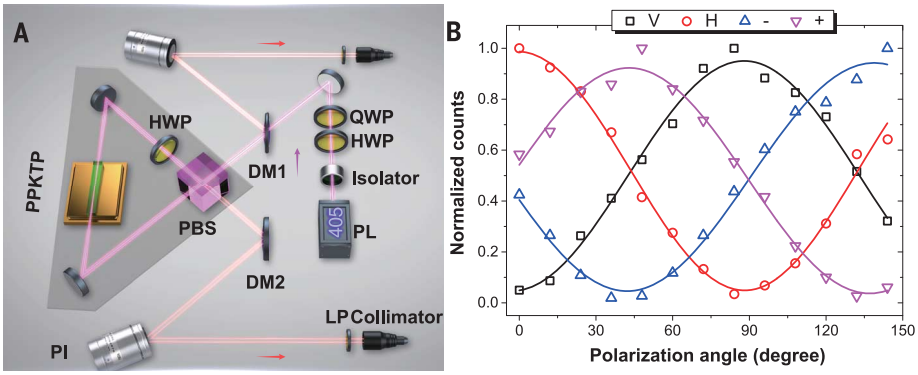


Fig. 1. Schematic of the spaceborne entangled-photon source and its in-orbit performance. (**A**) The thickness of the $KTiOPO_4$ (PPKTP) crystal is 15 mm. A pair of off-axis concave mirrors focus the pump laser (PL) in the center of the PPKTP crystal. At the output of the Sagnac interferometer, two dichromatic mirrors (DMs) and long-pass filters are used to separate the signal photons from the pump laser. Two additional electrically driven piezo steering mirrors (PIs), remotely controllable on the ground, are used for fine adjustment of the beam-pointing for an optimal collection efficiency into the single-mode fibers. QWP, quarter-wave plate; HWP, half-wave plate; PBS, polarizing beam splitter. (**B**) The two-photon correlation curves measured on-satellite by sampling 1% of each path of the entangled photons. The count rate measured from the overall 0.01% sampling is about 590 Hz, from which we can estimate the source brightness of 5.9 MHz.

[1]Department of Modern Physics and Hefei National Laboratory for Physical Sciences at the Microscale, University of Science and Technology of China, Hefei 230026, China. [2]Chinese Academy of Sciences (CAS) Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China. [3]Key Laboratory of Space Active Opto-Electronic Technology, Shanghai Institute of Technical Physics, Chinese Academy of Sciences, Shanghai 200083, China. [4]Key Laboratory of Optical Engineering, Institute of Optics and Electronics, Chinese Academy of Sciences, Chengdu 610209, China. [5]Shanghai Engineering Center for Microsatellites, Shanghai 201203, China. [6]Key Laboratory of Space Object and Debris Observation, Purple Mountain Observatory, Chinese Academy of Sciences, Nanjing 210008, China. [7]Xinjiang Astronomical Observatory, Chinese Academy of Sciences, Urumqi 830011, China. [8]Yunnan Observatories, Chinese Academy of Sciences, Kunming 650011, China.
*Corresponding author. Email: pcz@ustc.edu.cn (C.-Z.P.); jywang@mail.sitp.ac.cn (J.-Y.W.); pan@ustc.edu.cn (J.-W.P.)

atmosphere, and most of the photons' transmission path is virtually in vacuum, with almost zero absorption and decoherence. Previously, ground-based feasibility studies have demonstrated bidirectional distribution of entangled photon pairs through a two-link terrestrial free-space channel—with violations of Bell inequality—over distances of 600 m (*22*); 13 km, which goes beyond the effective atmospheric thickness (*23*); and 102 km with an ~80-dB effective channel loss, comparable to that of a satellite-to-ground two-downlink channel (*10*). In addition, quantum communications on moving platforms in a high-loss regime and under turbulent conditions were also tested (*24*, *25*). After these feasibility studies, a satellite dedicated for quantum science experiments, Micius [see the supplementary materials (*26*)], was developed and launched from Jiuquan, China, to an altitude of ~500 km.

For the mission of entanglement distribution, three ground stations are cooperating with the satellite, located in Delingha in Qinghai (37°22′44.43″N, 97°43′37.01″E; altitude, 3153 m); Nanshan in Urumqi, Xinjiang (43°28′31.66″N, 87°10′36.07″E; altitude, 2028 m); and Gaomeigu Observatory in Lijiang, Yunnan (26°41′38.15″N, 100°1′45.55″E; altitude, 3233 m). The physical distance between Delingha and Lijiang (Nanshan) is 1203 km (1120 km). The separation between the orbiting satellite and these ground stations varies from 500 to 2000 km. The effective laboratory space is thus greatly increased and provides a new platform for quantum networks, as well as for probing the validity of quantum mechanics.

By developing an ultrabright spaceborne two-photon entanglement source and high-precision acquiring, pointing, and tracking (APT) technology, we established entanglement between two single photons separated by 1203 km, with an average two-photon count rate of 1.1 Hz and state fidelity of 0.869 ± 0.085. Using the distributed entangled photons, we performed the Bell test at spacelike separation and without the locality and the freedom-of-choice loopholes.

Spaceborne entangled photons

In our design of a spaceborne entangled-photon source (Fig. 1A), a continuous-wave laser diode with a central wavelength of 405 nm and a linewidth of ~160 MHz is used to pump a periodically poled $KTiOPO_4$ crystal inside a Sagnac interferometer. The pump laser, split by a polarizing beam splitter, passes through the nonlinear crystal in the clockwise and anticlockwise directions simultaneously, which produces down-converted photon pairs at a wavelength of ~810 nm in polarization-entangled states close to the form $|\psi\rangle_{1,2} = (|H\rangle_1|V\rangle_2 + |V\rangle_1|H\rangle_2)/\sqrt{2}$, where $|H\rangle$ and $|V\rangle$ denote the horizontal and vertical polarization states, respectively, and the subscripts 1 and 2 denote the two output spatial modes. This source is robust against various vibration, temperature, and electromagnetic conditions (*26*). After launch, the source brightness and fidelity were tested by sampling ~1% of each path of the entangled photon pairs for on-satellite analysis (Fig. 1B). Under a pump power of ~30 mW, the source emits 5.9 million entangled photon pairs per second, with a state fidelity of 0.907 ± 0.007.

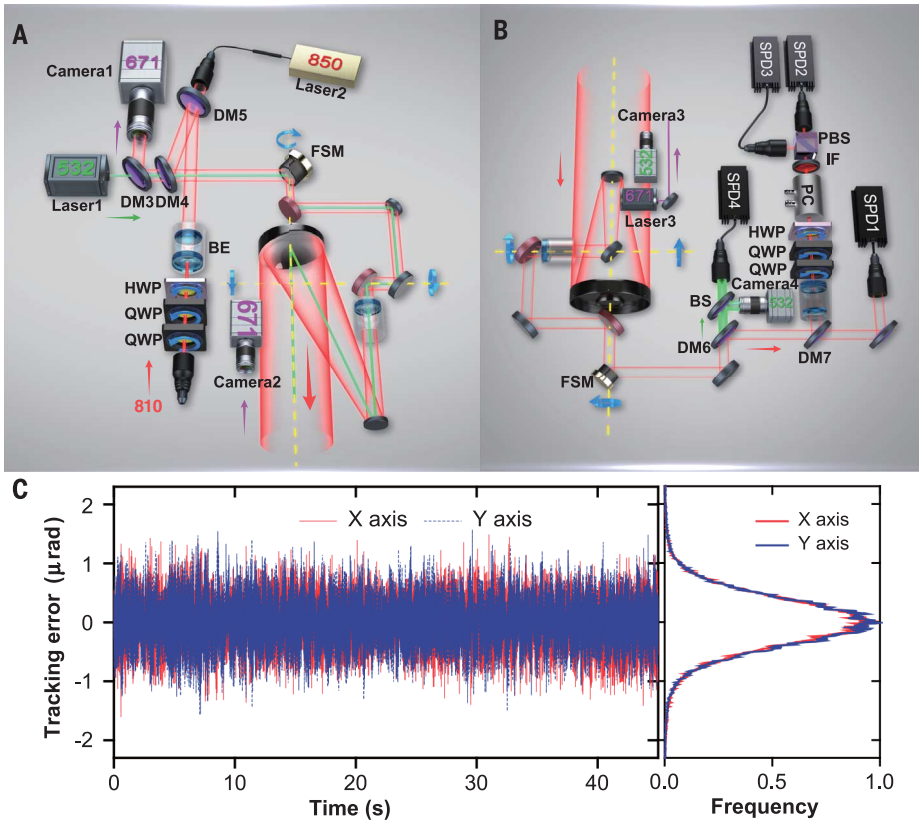


Fig. 2. The transmitters, receivers, and APT performance. (**A**) The entangled-photon beam (810 nm) is combined and co-aligned with a pulsed infrared laser (850 nm) for synchronization and a green laser (532 nm) for tracking by three DMs and sent out from an 8× telescope. For polarization compensation, two motorized QWPs and a HWP are remotely controlled. A fast steering mirror (FSM) and a two-axis turntable are used for closed-loop fine and coarse tracking, based on the 671-nm beacon laser images captured by cameras 1 and 2. BE, beam expander. (**B**) Schematic of the receiver at Delingha. The cooperating APT and polarization compensation systems are the same as those on the satellite. The tracking and synchronization lasers are separate from the signal photon and detected by single-photon detectors (SPDs). For polarization analysis along bases that are randomly switching quickly, two QWPs, a HWP, a Pockels cell (PC), and a PBS are used. BS, beam splitter; IF, interference filter. (**C**) The APT system starts tracking after the satellite reaches a 5° elevation angle. The left panel is a 50-s trace of the real-time image readout from the camera. Fine-tracking accuracy of ~0.41 μrad is achieved for both the *x* and *y* axes.

Establishing a space-to-ground two-downlink channel

As the entangled photons propagate from the satellite through the atmosphere to the two ground stations, each with a travel distance of 500 to 2000 km, several effects contribute to channel loss, including beam diffraction, pointing error, atmospheric turbulence, and absorption. Because the entangled photons cannot be amplified as classical signals, a robust and efficient satellite-to-ground entanglement distribution places more stringent requirements on the link efficiency than conventional satellite-based classical communications do. In particular, a satellite payload with two telescopes capable of establishing two independent satellite-to-ground quantum links simultaneously is required.

To optimize the link efficiency, we combined a narrow beam divergence with a high-bandwidth and high-precision APT technique. The two entangled beams were sent out with a near-diffraction-limited far-field divergence of ~10 μrad by two Cassegrain telescopes with apertures of 300 and 180 mm (Fig. 2A), which have been optimized to eliminate chromatic and spherical abbreviations at a wavelength of ~810 nm. The overall optical efficiencies of the two telescopes are 45 to 55%. At the Delingha, Lijiang, and Nanshan stations, the receiving telescopes have diameters of 1200, 1800, and 1200 mm, respectively. Our experiment has achieved entanglement distribution both between Delingha and Lijiang and between Delingha and Nanshan (*26*).

We designed cascaded multistage closed-loop APT systems in both the transmitters (Fig. 2A) and receivers (Fig. 2B). The transmitters use green (~532 nm) beacon lasers, whereas the receivers

use red (~671 nm) beacon lasers, pointing to each other with a divergence of ~1.2 mrad. The coarse pointing stages consist of a two-axis turntable or gimbal mirror and wide field-of-view cameras, and they achieve an accuracy better than 50 μrad. Further, the fine pointing stages with fast-steering mirrors and high-speed cameras reliably lock the remote telescopes by a feedback closed loop with a measured accuracy of 0.41 μrad for both the x and y axes (Fig. 2C), much smaller than the beam divergence (*26*). The APT systems are started when the satellite reaches a 5° elevation angle, and the measurement begins when it reaches a 10° elevation angle.

The motion of the satellite relative to the ground induces a drift in the arrival time and polarization rotation observed by the receivers. We kept track of the relative motion between the transmitters and the receivers, as well as all the optical elements in the optical paths, to calculate the polarization rotation angle offset and phase shift. Using a combination of motorized wave plates (two quarter-wave plates and one half-wave plate) for dynamical polarization compensation (*26*), we were able to recover the polarization contrast to 80:1. Synchronization of two ground stations was done with a 100-kHz pulsed laser, sent from the satellite and in good co-alignment with the signal photons. A synchronization jitter of 0.77 ns was obtained, which was used to tag the received signals and perform coincidence detection within a 2.5-ns time window. In addition to the temporal filtering, we placed 20-nm bandwidth filters in the receiving telescope to reduce the background noise. In our experiment, depending on the position of the Moon, the background noise ranged from 500 to 2000 counts/s in each detector.

The satellite flies along a sun-synchronous orbit and comes into both Delingha's and Lijiang's views once every night, starting at around 1:30 AM Beijing time and lasting for a duration of ~275 s. Figure 3A plots the physical distances from the satellite to Delingha and Lijiang during one orbit, together with the summed channel length of the two downlinks. Using a reference laser (*26*) on the satellite, we measured in real time the overall two-downlink channel attenuation, which varies from 64 to 82 dB (Fig. 3B). A slight asymmetry is evident in the attenuation curve—when the satellite moves closer to Lijiang, the link efficiency is higher, which is because the Lijiang station has a larger-aperture telescope. We observed an average two-photon count rate of 1.1 Hz, with a signal-to-noise ratio of ~8:1.

Compared with the previous method of entanglement distribution by direct transmission of the same two-photon source—using the best-performance (with a loss of 0.16 dB/km) and most common (with a loss of 0.2 dB/km) commercial telecommunication fibers, respectively—the effective link efficiency of our satellite-based approach within the 275-s coverage time is 12 and 17 orders of magnitude higher (*27*). The intrinsic physical loss limit of the silica optical fibers is estimated to be 0.095 to 0.13 dB/km (*28*). Even if such perfect optical fibers were produced in the future, our satellite-based method would still be four to eight orders of magnitude more efficient. In the future, satellites at higher orbits are expected to increase the area and time coverage.

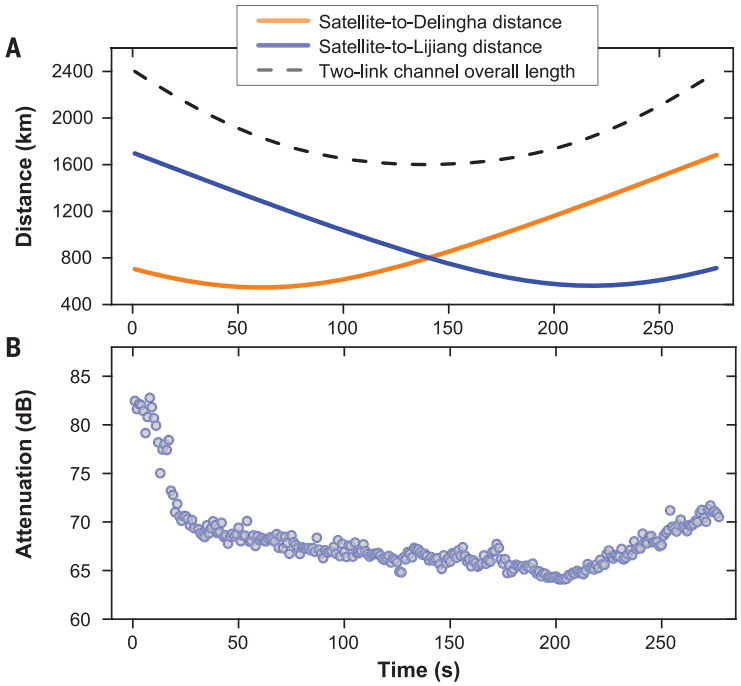


Fig. 3. Physical distances from the satellite to two ground stations and the measured channel attenuation. (**A**) A typical two-downlink transmission from the satellite to Delingha and Lijiang that lasted for about 275 s in one orbit. The distance from the satellite to Delingha varies from 545 to 1680 km. The distance from the satellite to Lijiang varies from 560 to 1700 km. The overall length of the two-downlink channel varies from 1600 to 2400 km. (**B**) The measured two-downlink channel attenuation in one orbit, using the high-intensity reference laser co-aligned with the entangled photons. The highest loss is ~82 dB at the summed distance of 2400 km, when the satellite has just reached a 10° elevation angle as seen from Lijiang station. Because the telescope has a diameter of 1.8 m (the largest) and thus has a higher receiving efficiency than other stations, when the satellite flies over Lijiang at an elevation angle of more than 15°, the channel loss remains relatively stable, from 64 to 68.5 dB.

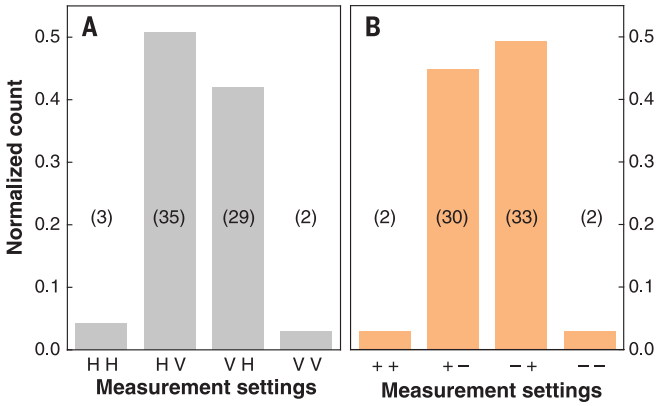


Fig. 4. Measurement of the received entangled photons after transmission by the two-downlink channel. (**A**) Normalized two-photon coincidence counts in the measurement setting of the $|H\rangle/|V\rangle$ basis. (**B**) Normalized counts in the diagonal $|\pm\rangle$ basis. Numbers in parentheses represent the raw coincidence counts of different measurement settings.

Verifying entanglement and Bell test

The received photons were analyzed by a half-wave plate, a polarizing beam splitter, and a Pockels cell, then coupled into a multimode fiber and detected by single-photon detectors with low dark counts (<100 Hz). The Pockels cells were driven by high-voltage pulses rapidly switching between zero- and half-wave voltages, controlled by fast (4 megabits/s) random numbers. Such a setting allows measurements of polarization at the basis of $\cos\theta|H\rangle + \sin\theta|V\rangle$. To verify whether the two photons, after traveling the overall distance ranging from 1600 to 2400 km, were still entangled, we analyzed their polarizations in the $|H\rangle/|V\rangle$

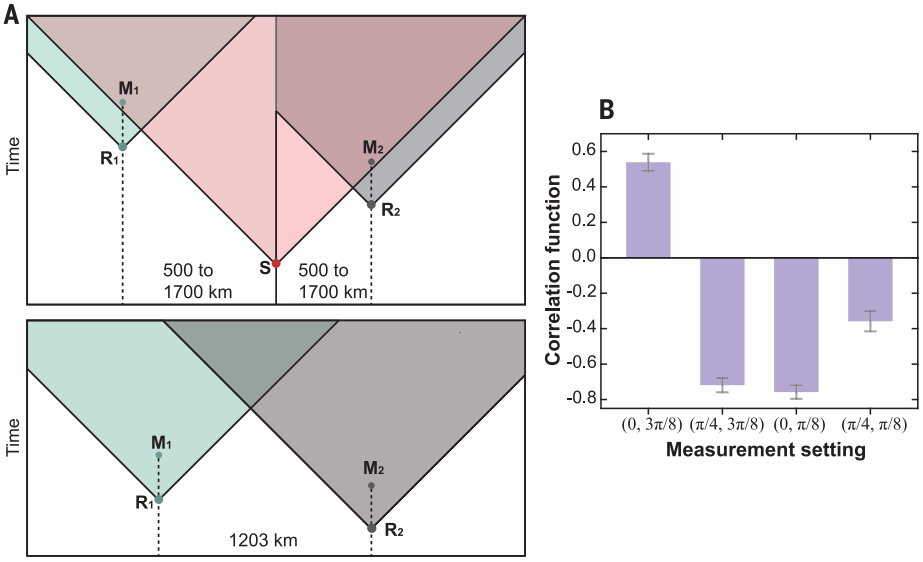


Fig. 5. Space-time diagram and Bell inequality violation. (**A**) The top panel illustrates the space-time relationship among the entanglement generation point (S), the quantum random-number generation points (R1 and R2), and the measurement results points (M1 and M2). The horizontal axis represents the distances between the ground stations and the satellite, which vary from 500 to 1700 km. In our experimental configuration, M1 and M2 are about 100 ns behind the light cone of S. The rate of quantum random-number generation is 5 kHz with an output delay below 200 ns. That is, the duration between R1 (R2) and M1 (M2) is in the range of 0.2 to 200.2 μs. Therefore, R1 (R2) and S are spacelike-separated, which implies that the freedom-of-choice loophole is distinctly closed, under the additional assumption that all the possible hidden variables must originate together with the entangled particles. The bottom panel illustrates the relationship between two ground stations, which are 1203 km apart. Taking into account the orbit height of 500 km, the length difference between the two free-space channels does not exceed 944 km. Thus, the spacelike criterion is satisfied between R1 and R2, R1 and M2, M1 and R2, and M1 and M2. As a result, the locality loophole is addressed. (**B**) Correlation functions of a CHSH-type Bell inequality for entanglement distribution. The measurement settings are the angles (φ_1, φ_2) used for the measurement of the polarization of photons by the Delingha and Lijiang stations, respectively. Error bars are one standard deviation, calculated from propagated Poissonian counting statistics of the raw photon detection events.

and $|\pm\rangle = (|H\rangle \pm |V\rangle)/\sqrt{2}$ bases. We obtained 134 coincidence counts—raw data without subtracting background noise—during an effective time of 250 s in satellite-orbit shadow time (Fig. 4). We found that, in good agreement with the state $|\psi\rangle_{1,2}$, the $|H\rangle_1|V\rangle_2$ and $|V\rangle_1|H\rangle_2$ populations dominate in the $|H\rangle/|V\rangle$ basis (Fig. 4A). Further, the coherence of the state is evident in Fig. 4B, where the measured $|+\rangle_1|+\rangle_2$ and $|-\rangle_1|-\rangle_2$ counts dominate over $|+\rangle_1|-\rangle_2$ and $|-\rangle_1|+\rangle_2$ at a ratio of 16:1. From these measurements, we can estimate the state fidelity [defined as the wave function overlap of the experimentally obtained states with the ideal $|\psi\rangle_{1,2}$ (*29*)] of the two photons distributed over 1203 km: $F \geq 0.87 \pm 0.09$, which is well above the threshold for both confirming the two-particle entanglement and violating Bell inequalities.

We used the distributed entangled photons for the Bell test with the Clauser-Horne-Shimony-Holt (CHSH)–type inequality (*30*), which is given by

$$S = |E(\varphi_1,\varphi_2) - E(\varphi_1,\varphi_2') + E(\varphi_1',\varphi_2) + E(\varphi_1',\varphi_2')| \leq 2$$

where $E(\varphi_1,\varphi_2)$, $E(\varphi_1,\varphi_2')$, and so forth are the joint correlations at the two remote locations with respective measurement angles of (φ_1,φ_2), (φ_1,φ_2'), and so forth. The angles are randomly selected among $(0, \pi/8)$, $(0, 3\pi/8)$, $(\pi/4, \pi/8)$, and $(\pi/4, 3\pi/8)$, quickly enough to close the locality (*31*) and freedom-of-choice loopholes (Fig. 5A). We ran 1167 trials of the Bell test during an effective time of 1059 s. The data observed in the four settings are summarized in Fig. 5B, from which we found $S = 2.37 \pm 0.09$, with a violation of the CHSH-type Bell inequality $S \leq 2$ by four standard deviations. The result again confirms the nonlocal feature of entanglement and excludes the models of reality that rest on the notions of locality and realism—on a previously unattained scale of thousands of kilometers.

Concluding remarks

We have demonstrated the distribution of two entangled photons from a satellite to two ground stations that are physically separated by 1203 km and have observed the survival of entanglement and violation of Bell inequality. The distributed entangled photons are readily useful for entanglement-based quantum key distribution (*7*), which, so far, is the only way that has been demonstrated to establish secure keys between two distant locations with a separation of thousands of kilometers on Earth without relying on trustful relay. Another immediate application is to exploit the distributed entanglement to perform a variant of the quantum teleportation protocol (*32*) for remote preparation and control of quantum states, which can be a useful ingredient in distributed quantum networks. The satellite-based technology that we developed opens up a new avenue to both practical quantum communications and fundamental quantum optics experiments at distances previously inaccessible on the ground (*33*, *34*).

REFERENCES AND NOTES

1. A. Einstein, B. Podolsky, N. Rosen, *Phys. Rev.* **47**, 777–780 (1935).
2. E. Schrödinger, *Naturwissenschaften* **23**, 807–812 (1935).
3. C. S. Wu, I. Shaknov, *Phys. Rev.* **77**, 136 (1950).
4. S. J. Freedman, J. F. Clauser, *Phys. Rev. Lett.* **28**, 938–941 (1972).
5. A. Aspect, P. Grangier, G. Roger, *Phys. Rev. Lett.* **49**, 91–94 (1982).
6. J. S. Bell, *Physics* **1**, 195 (1964).
7. A. K. Ekert, *Phys. Rev. Lett.* **67**, 661–663 (1991).
8. C. H. Bennett *et al.*, *Phys. Rev. Lett.* **70**, 1895–1899 (1993).
9. H. J. Kimble, *Nature* **453**, 1023–1030 (2008).
10. J. Yin *et al.*, *Nature* **488**, 185–188 (2012).
11. W. K. Wootters, W. H. Zurek, *Nature* **299**, 802–803 (1982).
12. H.-J. Briegel, W. Dür, J. I. Cirac, P. Zoller, *Phys. Rev. Lett.* **81**, 5932–5935 (1998).
13. M. Zukowski, A. Zeilinger, M. A. Horne, A. K. Ekert, *Phys. Rev. Lett.* **71**, 4287–4290 (1993).
14. J.-W. Pan, C. Simon, C. Brukner, A. Zeilinger, *Nature* **410**, 1067–1070 (2001).
15. L. M. Duan, M. D. Lukin, J. I. Cirac, P. Zoller, *Nature* **414**, 413–418 (2001).
16. J.-W. Pan, D. Bouwmeester, H. Weinfurter, A. Zeilinger, *Phys. Rev. Lett.* **80**, 3891–3894 (1998).
17. J.-W. Pan, S. Gasparoni, R. Ursin, G. Weihs, A. Zeilinger, *Nature* **423**, 417–422 (2003).
18. C. H. van der Wal *et al.*, *Science* **301**, 196–200 (2003).
19. Z.-S. Yuan *et al.*, *Nature* **454**, 1098–1101 (2008).
20. C.-W. Chou *et al.*, *Science* **316**, 1316–1320 (2007).
21. S.-J. Yang, X.-J. Wang, X.-H. Bao, J.-W. Pan, *Nat. Photonics* **10**, 381 (2016).
22. M. Aspelmeyer *et al.*, *Science* **301**, 621–623 (2003).
23. C.-Z. Peng *et al.*, *Phys. Rev. Lett.* **94**, 150501 (2005).
24. J.-Y. Wang *et al.*, *Nat. Photonics* **7**, 387–393 (2013).
25. S. Nauerth *et al.*, *Nat. Photonics* **7**, 382–386 (2013).
26. The supplementary materials provide more details about payloads in the satellite, receiving ground stations, and the polarization compensation method, as well as relevant supporting data.
27. H.-L. Yin *et al.*, *Phys. Rev. Lett.* **117**, 190501 (2016).
28. K. Tsujikawa, K. Tajima, J. Zhou, *Opt. Fiber Technol.* **11**, 319–331 (2005).
29. B. B. Blinov, D. L. Moehring, L. Duan, C. Monroe, *Nature* **428**, 153–157 (2004).
30. J. F. Clauser, M. A. Horne, A. Shimony, R. A. Holt, *Phys. Rev. Lett.* **23**, 880–884 (1969).
31. G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, A. Zeilinger, *Phys. Rev. Lett.* **81**, 5039–5043 (1998).
32. D. Boschi, S. Branca, F. De Martini, L. Hardy, S. Popescu, *Phys. Rev. Lett.* **80**, 1121–1125 (1998).
33. D. P. Rideout *et al.*, *Class. Quantum Gravity* **29**, 224011 (2012).
34. S. K. Joshi *et al.*, Space QUEST mission proposal: Experimentally testing decoherence due to gravity. arXiv:1703.08036 [math.FA] (26 April 2017).

ACKNOWLEDGMENTS

We thank many colleagues at the National Space Science Center, National Astronomical Observatories, and China Xi'an Satellite Control Center, especially B.-M. Xu, J. Li, J.-C. Gong, B. Chen,

J. Liu, X.-J. Jiang, and T. Xi for their management and coordination. We thank Q. Zhang, L. Li, and S. Chen for helpful discussions. This work was supported by the Strategic Priority Research Program on Space Science of the Chinese Academy of Sciences and by the National Natural Science Foundation of China. C.-Z.P. and J.-W.P. conceived the research. C.-Z.P., J.-Y.W., and J.-W.P. designed the experiments. J.Y., Y.C., G.-B.L., Z.-Q.J., M.L., C.-Z.P., and J.-W.P. developed the spaceborne entangled-photon source. J.Y., Y.C., S.-K.L., L.Z., W.-Q.C., G.-B.L., Z.-Q.J., M.L., J.-J.J., Y.-L.Z., Z.-C.Z., R.S., C.-Z.P., J.-Y.W., and J.-W.P. designed and developed the satellite and payloads. L.Z., J.-J.J., R.S., C.-Z.P., and J.-Y.W. developed the transmitters and the ATP technique. S.-K.L., W.-Q.C., W.-Y.L., and C.-Z.P. developed the software. J.Y., Y.C., L.Z., Y.-H.L., C.-Z.P., and J.-W.P. developed the polarization compensation method. C.-Y.L., C.-Z.P., and J.-W.P. analyzed the data and wrote the manuscript, with input from J.Y., Y.C., and Y.-H.L. All authors contributed to the data collection, discussed the results, and reviewed the manuscript. J.-W.P. supervised the whole project.

SUPPLEMENTARY MATERIALS

www.sciencemag.org/content/356/6343/1140/suppl/DC1
Materials and Methods
Figs. S1 to S11
Table S1
Reference (*35*)

28 March 2017; accepted 22 May 2017
10.1126/science.aan3211

Science

Satellite-based entanglement distribution over 1200 kilometers

Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, Guang-Bing Li, Qi-Ming Lu, Yun-Hong Gong, Yu Xu, Shuang-Lin Li, Feng-Zhi Li, Ya-Yun Yin, Zi-Qing Jiang, Ming Li, Jian-Jun Jia, Ge Ren, Dong He, Yi-Lin Zhou, Xiao-Xiang Zhang, Na Wang, Xiang Chang, Zhen-Cai Zhu, Nai-Le Liu, Yu-Ao Chen, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang and Jian-Wei Pan

Science **356** (6343), 1140-1144.
DOI: 10.1126/science.aan3211

Space calling Earth, on the quantum line

A successful quantum communication network will rely on the ability to distribute entangled photons over large distances between receiver stations. So far, free-space demonstrations have been limited to line-of-sight links across cities or between mountaintops. Scattering and coherence decay have limited the link separations to around 100 km. Yin *et al.* used the Micius satellite, which was launched last year and is equipped with a specialized quantum optical payload. They successfully demonstrated the satellite-based entanglement distribution to receiver stations separated by more than 1200 km. The results illustrate the possibility of a future global quantum communication network.

Science, this issue p. 1140

Science (print ISSN 0036-8075; online ISSN 1095-9203) is published by the American Association for the Advancement of Science, 1200 New York Avenue NW, Washington, DC 20005.

npj | Quantum Information

www.nature.com/npjqi

REVIEW ARTICLE OPEN

Practical challenges in quantum key distribution

Eleni Diamanti[1], Hoi-Kwong Lo[2], Bing Qi[3,4] and Zhiliang Yuan[5,6]

Quantum key distribution (QKD) promises unconditional security in data communication and is currently being deployed in commercial applications. Nonetheless, before QKD can be widely adopted, it faces a number of important challenges such as secret key rate, distance, size, cost and practical security. Here, we survey those key challenges and the approaches that are currently being taken to address them.

npj Quantum Information (2016) **2,** 16025; doi:10.1038/npjqi.2016.25; published online 8 November 2016

INTRODUCTION

Why quantum key distribution?

For thousands of years, human beings have been using codes to keep secrets. With the rise of the Internet and recent trends to the Internet of Things, our sensitive personal financial and health data as well as commercial and national secrets are routinely being transmitted through the Internet. In this context, communication security is of utmost importance. In conventional symmetric cryptographic algorithms, communication security relies solely on the secrecy of an encryption key. If two users, Alice and Bob, share a long random string of secret bits—the key—then they can achieve unconditional security by encrypting their message using the standard one-time-pad encryption scheme. The central question then is: how do Alice and Bob share a secure key in the first place? This is called the key distribution problem. Unfortunately, all classical methods to distribute a secure key are fundamentally insecure because in classical physics there is nothing preventing an eavesdropper, Eve, from copying the key during its transit from Alice to Bob. On the other hand, standard asymmetric or public-key cryptography solves the key distribution problem by relying on computational assumptions such as the hardness of factoring. Therefore, such schemes do not provide information-theoretic security because they are vulnerable to future advances in hardware and algorithms, including the construction of a large-scale quantum computer.[1]

We remark that some secrets, for instance, census data, need to be kept secret for decades (e.g. 92 years in Canada (Statistical Canada webpage. Release of personal data after 92 years, URL: http://www12.statcan.gc.ca/census-recensement/2011/ref/about-apropos/personal-personnels-eng.cfm)). Currently, however, data transmitted in 2016 is vulnerable to technological advances made in the future as Eve might simply save the transcripts of communication in her memory and wait for the construction, for example, of a quantum computer some time before 2,108 (92 years from 2016). This is highly probable. Recall that ENIAC, the first general purpose electronics computer,[2] which was largely inferior to modern computers, was invented only 70 years ago. The US National Security Agency is taking the threat of quantum computing seriously and has recently announced transition plans to quantum-resistant classical algorithms[3] (These algorithms are typically based on hard computational problems involving for instance the structure of some specific lattices. Despite important progress in the development of such algorithms, it is still an open question whether they are secure against a quantum computer).

Quantum cryptography, or more specifically, quantum key distribution (QKD),[4–7] promises in principle unconditional security —the Holy Grail of communication security—based on the laws of physics only.[8–10] QKD has the advantage of being future-proof:[11] unlike classical key distribution, it is not possible for an eavesdropper to keep a transcript of quantum signals sent in a QKD process, owing to the quantum non-cloning theorem.[12,13] For this reason, QKD is an essential element of the future quantum-safe infrastructure, which will include both quantum-resistant classical algorithms and quantum cryptographic solutions. In the bigger context of quantum information, there has been tremendous scientific and engineering effort towards the long-term vision of a global quantum internet.[14] Imagine a world where only a few large-scale quantum computers are available (just like the early days of classical computing when only a few classical computers were available and in line with the current trend towards cloud computing); users will have to access those powerful quantum computers at long distances via a quantum internet. QKD will have a central role in securing data communication links in such a quantum internet.

The potential applications of QKD include securing critical infrastructures (for instance, the Smart Grid), financial institutions and national defense. Experimental QKD has been performed over distances on the order of 100 km in standard telecom fibres as well as in free space, while the secure key rate has now reached a few Mbits per second. QKD has leaped out of the lab.[15] In China, the deployment of a 2,000 km QKD network between Shanghai and Beijing is underway; in Europe, after the SECOQC network demonstration in 2008,[16] the UK is now creating a quantum network facilitating device and system trials, and the integration of quantum and conventional communications; in Japan, QKD technologies will be put into test to secure transmission of

[1]Laboratoire Traitement et Communication de l'Information, CNRS, Télécom ParisTech, Université Paris-Saclay, Paris, France; [2]Center for Quantum Information and Quantum Control, Department of Physics and Department of Electrical & Computer Engineering, University of Toronto, Toronto, Canada; [3]Quantum Information Science Group, Computational Sciences and Engineering Division, Oak Ridge National Laboratory, Oak Ridge, TN, USA; [4]Department of Physics and Astronomy, University of Tennessee, Knoxville, TN, USA; [5]Toshiba Research Europe Limited, Cambridge, UK and [6]Corporate Research & Development Center, Toshiba Corporation, Kawasaki, Japan.
Correspondence: H-K Lo (hklo@ece.utoronto.ca)
Received 7 December 2015; revised 5 May 2016; accepted 29 May 2016

sensitive genome data; and the US has also started installing its own QKD network.

Why practical challenges in QKD?

In this review, we will focus on practical issues in QKD. We remark that, historically, practical considerations in QKD have led to ground-breaking inventions. For example, the need to counter the photon-number-splitting attack[17] triggered the invention of the decoy-state protocol,[18–20] which allows efficient distillation of secure keys using weak coherent pulse based QKD systems that once were vulnerable. As another example, the need to counter detector side-channel attacks has led to the discovery of measurement device independent (MDI) QKD.[21] New theory that is due to practical advances in QKD also includes, for instance, the quantum de Finetti theorem,[22] while security loopholes in QKD are closely related to loopholes in Bell inequality tests[23]—a key subject in the foundations of quantum mechanics. These issues are therefore of great interest to mathematicians and theoretical physicists.

QKD is clearly of interest to engineers too. For instance, practical QKD is closely linked to the development of new single-photon detection technologies such as superconducting nanowire single-photon detectors (SNSPDs),[24] superconducting transition-edge sensors (TES),[25] frequency up-conversion single photon detectors,[26,27] and self-differencing InGaAs avalanche photodiodes,[28] as well as of high-performance homodyne detection techniques.[29] It is also the motivation for high-speed quantum random number generators[30] and broadband entangled photon sources.[31]

Practical QKD has steered innovation and is a precursor in the field of Quantum Information Processing.

Outline of the review

Despite the important theoretical and experimental achievements, a number of key challenges remain for QKD to be widely used for securing everyday interactions. For instance, much effort is being put into increasing the communication rate and range of QKD and making QKD systems low cost, compact and robust. New hardware such as chip-based QKD and new software such as novel protocols are being studied and developed. The security of practical QKD systems is another important challenge. In order to foil quantum hackers, protocols such as MDI-QKD and loss-tolerant QKD[32] have been developed and are currently being experimentally implemented. Yet, a comprehensive theory of the model of a QKD source remains to be constructed. To further extend the reach of QKD, two different approaches—quantum repeaters and ground-to-satellite QKD—are being pursued. In view of the proliferation of mobile computing devices including smart phones, mobile QKD applications have also attracted recent attention. Furthermore, the standardisation of QKD components is currently being pursued in European Telecommunications Standards Institute.[33] In what follows, we will highlight some of the above challenges and the various approaches that are being taken to tackle them.

MAIN PROTOCOLS AND IMPLEMENTATIONS

We begin our discussion with a brief overview of the main QKD protocols currently studied and the state-of-the-art in their practical implementations. As our main focus here is the current challenges in the field, we refer the reader to a recent review[7] for the necessary background on the rigorous information-theoretic (or, unconditional) security definition of QKD in the composable framework, secure communication schemes including the one-time pad, the standard BB84 QKD protocol, and basic QKD components.

QKD protocols can be in essence divided with respect to the detection technique required to recover the key information encoded in the properties of light (Figure 1a). In discrete-variable (DV) protocols information is typically encoded in the polarisation or phase of weak coherent pulses simulating true single-photon states; hence the corresponding implementations employ single-photon detection techniques. The previously mentioned BB84 and decoy-state protocols are prominent examples in this category. Single-photon detection techniques are also necessary for the so-called distributed-phase-reference protocols, such as the coherent-one-way[34] and differential-phase-shift (DPS)[35] protocols, where the key information is encoded in photon arrival times or in the phase between adjacent weak coherent pulses. On the other hand, in continuous-variable (CV) QKD protocols information is encoded in the quadratures of the quantised electromagnetic field, such as those of coherent states,[36,37] and homodyne or heterodyne detection techniques are used in this case. Such detectors are routinely deployed in classical optical communications, hence the CV approach offers the possibility for implementations based only on mature telecom components. All these protocols are prepare-and-measure in the sense that the transmitter, Alice, sends the encoded pulses to the receiver, Bob, who decodes as required by the specific protocol. On the contrary, in entanglement-based protocols,[5] both parties receive parts of an entangled state and perform suitable measurements. More details on all protocols can be found in refs 6,7,38,39.

When it comes to practical demonstrations, performance of point-to-point links is assessed by the distance over which secret keys can be distributed and the rate of their distribution for a given security level. The security level is determined by the type of attacks considered in the corresponding security proof; demonstrating security against the so-called collective attacks[6] is an important challenge for an implementation; however, information-theoretic security is achieved only when security against the most general (or coherent) attacks is proven. Hence, the ultimate goal is to provide this level of security at a speed and a distance that are compatible with practical applications. Some recent implementations have provided high levels of security: several QKD protocols have been demonstrated to provide composable security against collective attacks using reasonable data block sizes and practical setups, including decoy-state BB84,[40] coherent-one-way,[41] and CV-QKD.[42,43] Among those protocols, the security of decoy-state BB84 QKD has been extended to cover coherent attacks, for realistic block sizes and with a minimal sacrifice in the secret key rate.[44,45] Unfortunately, for coherent-one-way, the best security proof against coherent attacks currently gives a secret key rate that only scales quadratically with the loss.[46] For CV-QKD with coherent states and heterodyne detection, a composable security proof against the most general attacks has recently been provided,[47] but the current proof techniques do not allow a positive key rate for realistic block sizes in this case. Extending the security proofs for the latter protocols is therefore a pressing task in the theoretical study of QKD.

Figure 1b,c shows examples of advanced fibre-optic QKD systems allowing for real-time secret key generation over distances of 50 km with Mbit/s rates. In Figure 1d we summarise some important experimental achievements from both established and emerging QKD protocols (discussed in the following sections). Although the security assumptions and technological maturity vary in these implementations, these results illustrate the diversity of protocols and experimental solutions that the research community has invented to push the performance of QKD technology. Indeed, tremendous progress has been achieved in recent years, and avenues for further progress will be discussed in the next section. We remark, however, that there are fundamental limitations on what can be ultimately achieved. Over optical fibre networks, the attenuation of light in standard fibres at the telecom wavelength of 1,550 nm is 0.2 dB/km (or 0.16 dB/km in newly developed ultralow loss fibres). This unavoidable loss will not

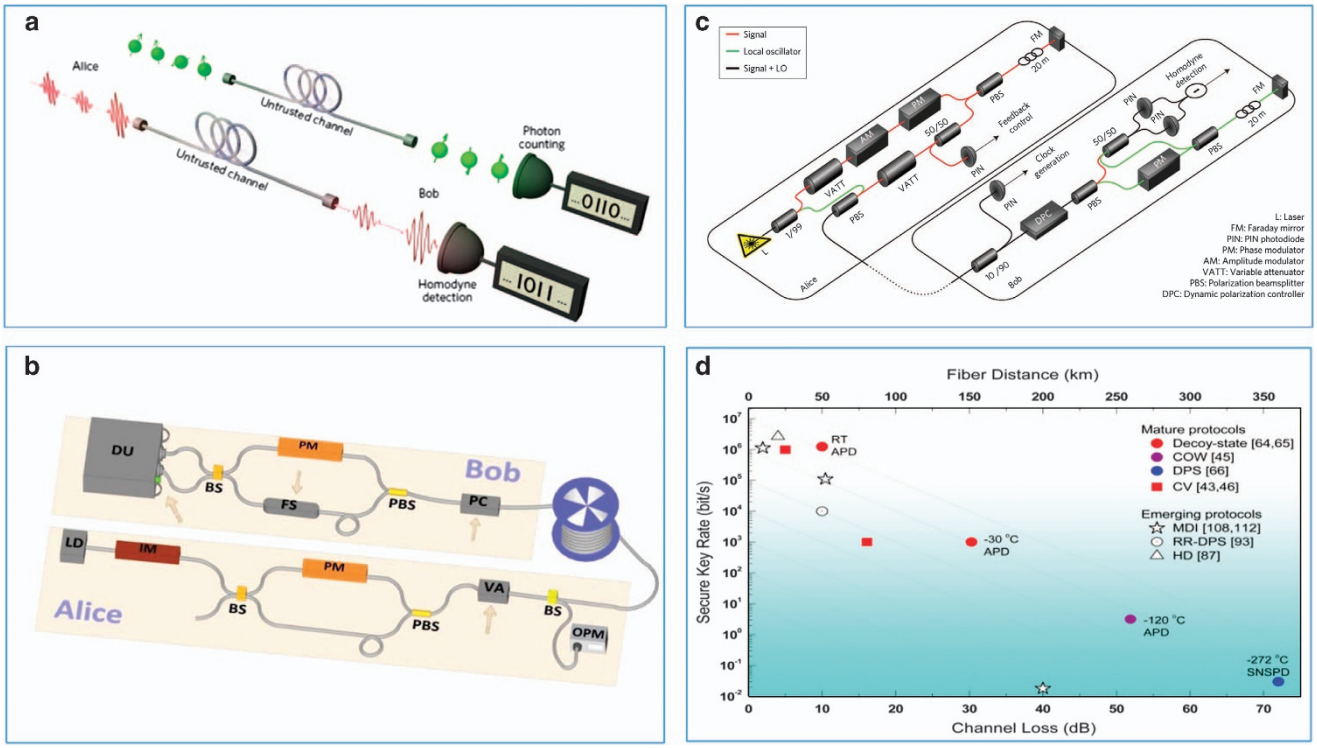


Figure 1. (**a**) Quantum key distribution systems use discrete-variable (DV) single-photon state encoding and single-photon detection techniques or continuous-variable (CV) quadrature field amplitude encoding and homodyne (or heterodyne) detection techniques. (**b**) State-of-the-art experimental setup for the implementation of the decoy-state BB84 QKD protocol.[40] (**c**) State-of-the-art experimental setup for the implementation of the coherent state CV-QKD protocol.[42] (**d**) Secret key generation rates demonstrated in some representative recent QKD experiments. Note that this figure is not meant to provide an exhaustive list of QKD implementations. Furthermore, protocol performance cannot be directly compared as different security assumptions are considered; for instance, decoy-state BB84 is secure against general coherent attacks while coherent-one-way (COW) and CV-QKD are secure against collective attacks. QKD is a subject of active ongoing research and so further developments are likely to occur in the near future. The loss coefficient of 0.2 dB/km in standard single-mode fibres at telecom wavelengths is assumed in this figure. Figures adapted with permission from: (**a**), ref. 180 © 2013 NPG, courtesy of Ping Koy Lam; (**b**), ref. 40 © 2013 OSA; (**c**) ref. 42 © 2013 NPG.

allow the range of point-to-point QKD links to exceed a few hundreds of kilometres as with overly excessive channel loss it would take several years to generate just one bit even using perfect light sources and detectors. Furthermore, with a practical lossy channel, the ultimate key rate is upper bounded by the so-called TGW bound[48] (see also ref. 49 for a more recent result, quoted as the PLOB bound). These bounds provide a useful benchmark for the performance of all QKD protocol implementations.

MAJOR CHALLENGES IN PERFORMANCE AND COST

In the quest for high performance and low-cost QKD systems, both hardware and software solutions are currently being pursued.

Hardware development

Key rate. Encryption keys generated by QKD can be used in a symmetric cipher scheme, such as Advanced Encryption Standard, which is quantum resistant, for enhanced security, or they can be combined with the one-time-pad encryption scheme for unconditional security. In both cases, the secure key rate achieved by the underlying QKD layer in a typical application scenario is crucial. Higher secure rates allow for a more frequent update of encryption keys in symmetric ciphers, and for a proportional increase in the one-time-pad communication bandwidth as this scheme requires the key to be as long as the message.

Presently, strong disparity exists between the classical and QKD communication rates. Classical optical communications delivering speeds of 100 Gbit/s per wavelength channel are currently being deployed,[50] and a field trial featuring 54.2 Tbit/s aggregated data rate has recently been performed.[51] On the other hand, the Mbit/s rates achieved by QKD systems today are sufficient, for instance, for video transmission; however, it is clear that if we want in the longer term to encrypt high volumes of classical network traffic using the one-time-pad, major developments on the secure key rate generated by QKD will be required.

The obtained key rate depends crucially on the performance of the detectors used. For QKD systems employing single-photon detection techniques, high efficiency and short dead time of the detectors are essential for reaching a high bit rate. The latest developments on high efficiency detectors[52–54] are extremely promising; quantum efficiencies as high as 93% at telecom wavelengths have been reported for SNSPDs,[53] and devices based on this technology with short dead time, low dark count, low time jitter and high detection efficiency are commercially available[55] (Figure 2a,b). These results may allow for as much as a fourfold increase in the secret key rate, which currently stands at 1 Mbit/s over a 50 km fibre (or 10 dB loss) achieved using self-differencing InGaAs avalanche photodiodes with an ultrashort dead time[40] (Figure 2c). Further key rate increase is possible using wavelength or spatial mode multiplexing technologies that have been routinely used for increasing the bandwidth in data communications.[50,56,57] For CV-QKD systems, increasing the bandwidth of the homodyne or heterodyne detectors, while keeping at the

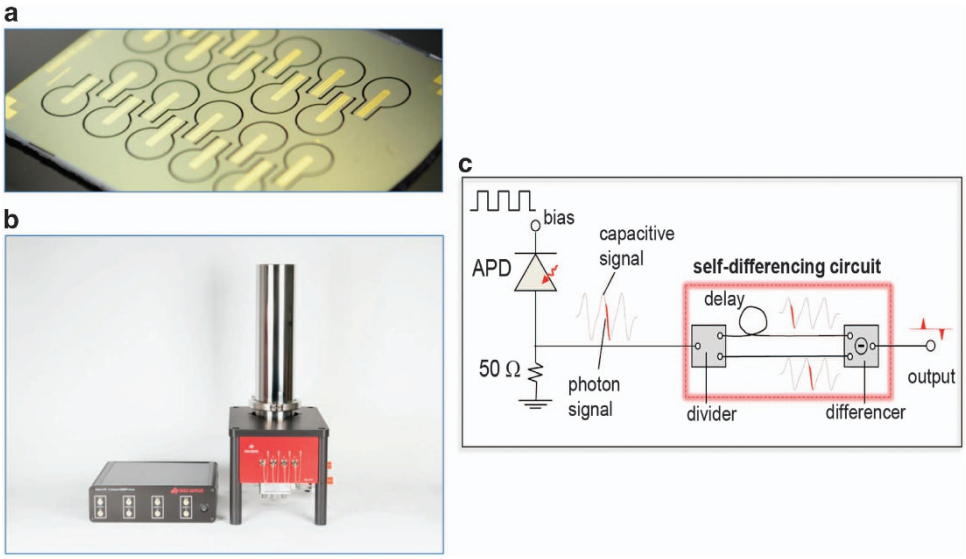


Figure 2. (**a**) Superconducting nanowire chips. (**b**) Commercial SNSPDs with high detection efficiency. (**c**) Characterisation circuit for self-differencing InGaAs avalanche photodiodes.[69] Figures adapted with permission from: (**a**) http://www.photonspot.com/, courtesy of Vikas Anant; (**b**) http://www.singlequantum.com/products, courtesy of Jessie Qin-Dregely.

same time the electronic noise low, is a necessary step for increasing the key rate beyond the 1 Mbit/s over 25 km that has been achieved.[43] Further progress continues to be pursued, targeting also higher efficiency, which is currently around 60% for fibre-coupled detectors at telecom wavelengths.[42] Furthermore, as shown in Figure 1c, a practical issue in these systems is that the strong phase reference pulse (or local oscillator) needs to be transmitted together with the signal at high clock rates; recent proposals that avoid this and use instead a local oscillator generated at Bob's site[58–60] are promising and will lead to more practical, high performance implementations.

Distance. Extending the communication range of QKD systems is a major driving factor for technological developments in view of future network applications. QKD systems based on single-photon detection champion the point-to-point communication distance (or channel loss). Here the low noise of single-photon detectors is the key enabling factor; in particular, the attainable range depends on the type and operation temperature of the detectors. InGaAs avalanche photodiodes can tolerate losses of 30 and 52 dB when cooled to −30 and −120 °C,[41,61] respectively, whereas SNSPDs cooled to cryogenic temperatures have been demonstrated to withstand a record loss of 72 dB.[62] This loss is equivalent to 360 km of standard single mode fibre or about 450 km of ultralow loss fibre. Although technologically possible, further extending the point-to-point distance is increasingly unappealing because the channel loss will inevitably reduce the key rate to a level of little practical relevance. This is also true for CV-QKD systems, which are in general more sensitive to losses. Here it is crucial to keep the excess noise—the noise exceeding the fundamental shot noise of coherent states—low and especially to be able to estimate the noise value precisely, which becomes increasingly difficult with the distance.[38,42]

We remark that advances towards high-performance QKD systems in terms of key rate and distance are coupled with the security guarantees offered by these systems. For instance, achieving composable security against general attacks requires in practice being able to perform efficient post-processing, including parameter estimation, over large data blocks with stable setups. Particularly for CV-QKD, performing efficient error correction and precise parameter estimation is of utmost importance.[38,63]

Cost and robustness. For QKD systems to be used in real world applications, low cost and robustness are indispensable features alongside high performance. Several avenues are currently being pursued. First, QKD systems have been shown to coexist with intense data traffic in the same fibre,[64–67] thus eliminating the need for dark fibres that are not only expensive but also often unavailable. Access network architecture allows simultaneous access by a multitude of QKD users, and importantly they are compatible with full power Gigabit Passive Optical Network traffic in the same network.[61,68] Room-temperature single-photon detectors have been shown to be suitable for DV-QKD over up to 100 km fibre, thus removing cooling requirements for the entire QKD system;[44,69] for CV-QKD cooling is unnecessary. All these developments help reduce deployment cost as well as system complexity, footprint and power consumption.

Another important avenue to address the issue of cost and robustness is photonic integration.[70] Chip-scale integration will bring high level of miniaturisation, leading to compact and light-weight QKD modules that can be mass-manufactured at low cost. Two main integration platforms are currently being explored, namely silicon (Si)[71] and indium phosphide (InP),[72] whereas alternative techniques include lithium niobate ($LiNbO_3$) integration and glass waveguide technologies. For QKD protocols employing single-photon detection, the main difficulty comes from the receiver side so initial experiments have focused on transmitter integration. A $LiNbO_3$ integrated polarisation controller was used for state preparation in a QKD implementation,[73] whereas several techniques were combined to construct a hand-held QKD sender module in ref. 74. More recently, a QKD transmitter chip that is reconfigurable to accommodate the state preparation for several QKD protocols, including decoy-state BB84, coherent-one-way and DPS, has been developed on InP[75] (Figure 3), and Si transmitters have also been demonstrated independently by the U. of Toronto[76] and also by Bristol group. (C. Erven and M. Thompson, private communication.)

Chip-scale QKD receivers are also progressing. Low-loss planar-lightwave-circuits based on silica-on-silicon technology have been routinely used to replace fibre-based asymmetric Mach–Zehnder interferometres,[75,77,78] a key enabling component for phase-based QKD protocols. Research efforts are currently focused on the integration of single-photon detectors using the aforementioned

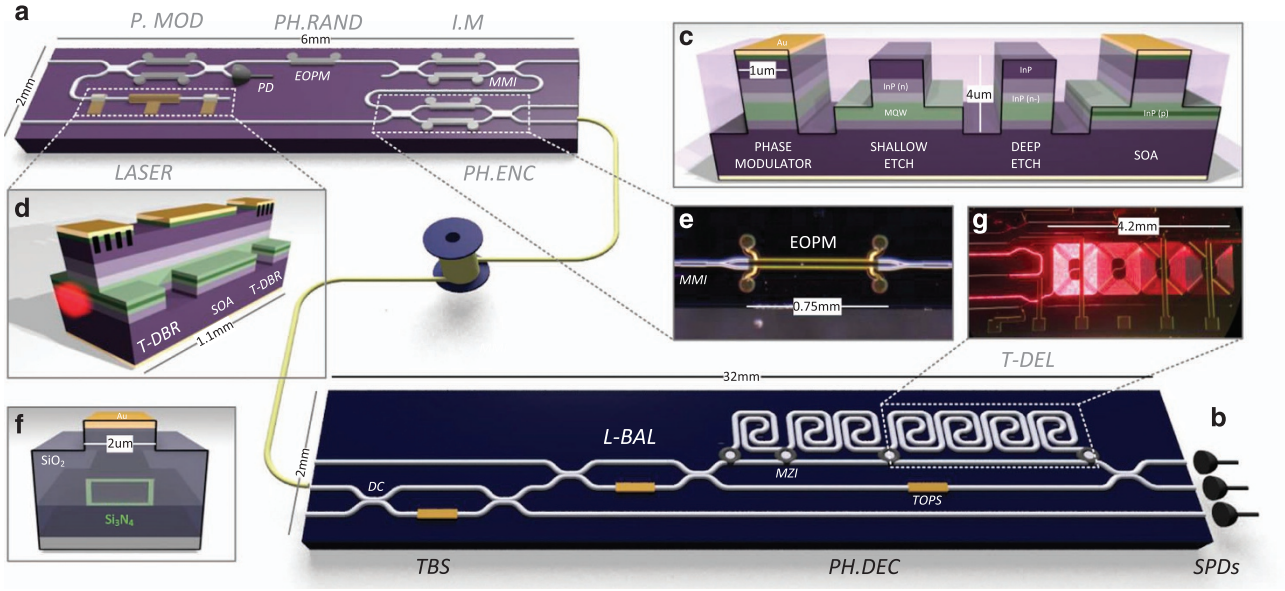


Figure 3. Chip architecture combining several integrated photonic devices for the implementation of DV-QKD. (**a**) A monolithically integrated In-dium phosphide (InP) transmitter for GHz clock rate, reconfigurable, multi-protocol QKD. (**b**) A silicon oxynitride (Triplex) photonic receiver circuit for reconfigurable, multi-protocol QKD that passively decodes the quantum information with on-chip single-photon detectors. (**c**) The InP technology platform waveguide cross-section. (**d**) Wavelength tunable continuous-wave laser, formed from two tuneable distributed Bragg reflectors (T-DBR) and a semiconductor optical amplifier (SOA). (**e**) Microscopic image of electro-optic phase modulators in Mach-Zehnder interferometer. (**f**) The SiOxNy Triplex waveguide cross-section, with metalisation for heating elements. (**g**) Microscopic image of the receiver delay lines. Caption and Figure adapted with permission from ref. 75, courtesy of Philip Sibson, Chris Erven and Mark Thompson.

techniques, which will be essential for developing complete integrated systems. CV-QKD systems are particularly well suited for this objective because they only require the use of standard components. Indeed, Si photonic chips integrating many functionalities of a CV-QKD setup, including active elements such as amplitude and phase modulators and homodyne/heterodyne detectors based on germanium (Ge) photodiodes, have been developed.[79]

Development of chip-scale QKD is still at its early stages. Further research in this direction will help bring the QKD technology closer to its wide adoption.

New QKD protocols

In parallel to hardware development, much effort has also been devoted to novel QKD protocols aiming to outperform the established ones. Encouragingly, this line of research has led to protocols that may exhibit advantages when certain technical constraints are in place. Below, we discuss two protocols featuring high photon information capacity or noise tolerance.

High dimension-QKD. High dimension-QKD allows retrieval of more than 1 bit from each detected photon, thus offering an advantage in the photon information capacity when the photon rate is restrained.[80–82] The choice for encoding is to use the arrival times of time-energy entangled photon pairs,[83] whose continuous nature permits encoding of extremely large alphabets. A security proof against collective attacks has been developed,[84] which was followed by a laboratory experiment demonstrating a photon information capacity of up to 6.9 bits per coincidence and a key rate of 2.7 Mbit/s over a 20 km fibre.[85] Although this development has narrowed the key rate gap between entanglement based and prepare-and-measure QKD systems, its viability in a field environment will face a challenge to maintain the near unity interference visibility which was key to the obtained information capacity. High dimension-QKD without entanglement is also possible by exploiting the spatial degree of freedom, but its potential is restricted by the availability of high speed modulators.[86,87]

RR-DPS-QKD. The Round-Robin (RR) DPS protocol, which was proposed in 2014,[88] removes the need for monitoring the channel disturbance to establish security, in stark contrast with conventional QKD protocols (see Figure 4a for the principle). Instead, Eve's information can be tightly set, even to an arbitrarily low level, by just choosing experimental parameters. In theory, a positive key rate is possible for any quantum bit error rate (QBER) $< 50\%$. This extraordinary QBER tolerance makes it attractive for deployment when large systematic errors cannot be avoided. Shortly after its introduction the protocol has stimulated a number of experimental demonstrations.[89–92] The RR-DPS-QKD protocol uses a transmitter identical to that found in a conventional DPS system,[35] but requires a receiver that is capable of measuring the differential phase between any two pulses within a pulse group sent by Alice. Two different approaches are adopted. In the first, direct approach, a combination of optical switches and delay lines is used to bring the intended pulses into temporal overlap and then let them interfere[90–92] (see for example Figure 4b). A more ingenious approach is to let a common phase reference interfere with all pulses sent by Alice, and then determine the differential phase between those pulses whose interference with the common reference produces a photon click.[89] This latter approach avoids many problems associated with the direct one, such as loss and phase instability caused by optical delay lines and switches, but it will require remote optical phase locking for optimal performance. As it currently stands, the best key rate for RR-DPS-QKD is around 10 kbit/s for a 50 km distance in fibre[91] and cannot compete with the more mature decoy-state BB84 protocol. RR-DPS-QKD has the advantage of being robust against encoding errors,[93] but it is vulnerable to attacks on detectors, which will be discussed in the next section.

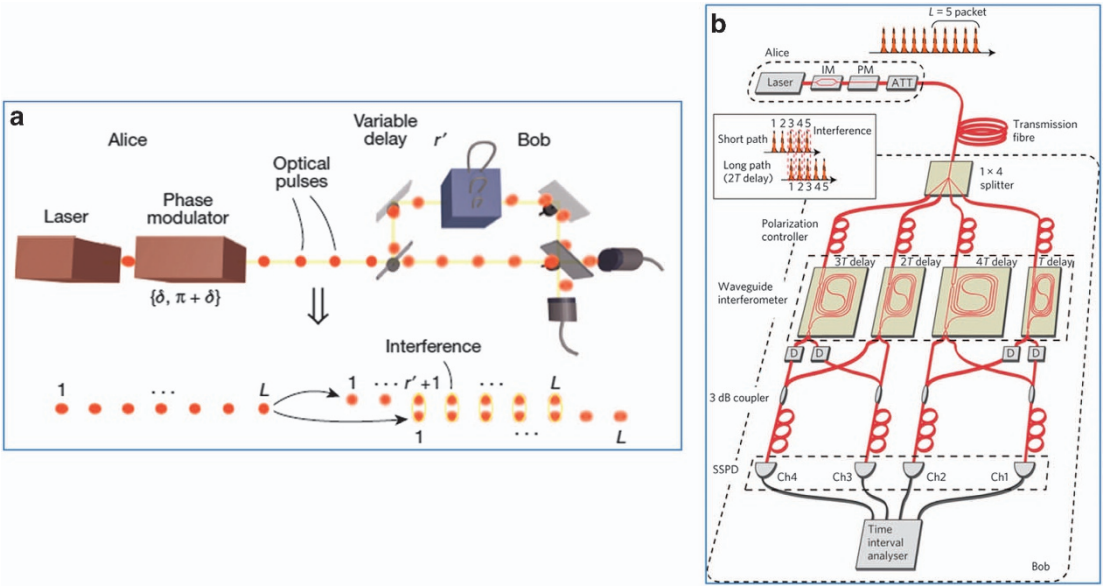


Figure 4. (**a**) Basic principle of RR-DPS QKD protocol.[88] (**b**) Example of experimental implementation of the RR-DPS QKD protocol.[90] Figures adapted with permission from: (**a**), ref. 88 © 2014 NPG; (**b**), ref. 90 © 2015 NPG. Courtesy of Masato Koashi.

MAJOR CHALLENGES IN PRACTICAL SECURITY

Although the security of a QKD protocol can be proven rigorously, its real-life implementation often contains imperfections that may be overlooked in the corresponding security proof. By exploiting such imperfections, various attacks, targeting either the source or the detectors, have been proposed; some of them have even been demonstrated to be effective against commercial systems.[94–96] We refer the reader to a recent review[7] for more details on quantum hacking and also countermeasures. To regain security in practical QKD, several solutions, including QKD based on testable assumptions,[7] device independent (DI) QKD[97,98] (see also ref. 99) and MDI-QKD,[21] have been proposed. In the following, we discuss some important recent developments in this direction.

MDI-QKD

One promising long-term solution to side-channel attacks is DI-QKD, where the security relies on the violation of a Bell inequality and can be proven without knowing the implementation details. While recent loophole-free Bell experiments[23,100,101] imply that DI-QKD could be implemented, the expected secure key rate is nevertheless impractically low even at short distances. A more practical solution is MDI-QKD, which is inherently immune to all side-channel attacks targeting the measurement device, usually the most vulnerable part in a QKD system. In fact, the measurement device in MDI-QKD can be treated as a 'black box' which could even be manufactured and operated by Eve. Building upon refs 102,103; ref. 21 proposed a practical scheme with weak coherent pulses and decoy states (Figure 5a), whose security against the most general coherent attacks, taking into account the finite data size effect, has been proved in ref. 104 (see also ref. 99, which studied an entanglement-based representation with general finite-dimensional systems, and ref. 105, which proposed a DI-QKD protocol with local Bell test).

MDI-QKD[21] is a natural building block for multi-user QKD networks, since the most expensive and complicated measurement device can be placed in an untrusted relay and shared among many QKD users.[68] Several groups have demonstrated its feasibility. In particular, DV MDI-QKD was demonstrated over 200 km telecom fibre[106] and 404 km of ultralow loss fibre[107] in lab conditions, and over 30 km of deployed fibre.[108] With highly efficient single-photon detectors, the tolerable channel loss can be as high as 60 dB, which corresponds to 300 km of standard telecom fibre.[109] A real-life fibre based multi-user MDI-QKD network was also implemented recently[110] (Figure 5c). Moreover, a 1 Mbit/s proof-of-principle MDI-QKD experiment was performed,[111] thus illustrating the high key rate potential of DV MDI-QKD. This was also studied in ref. 112 for MDI-QKD employing state-of-the-art SNSPDs; in Figure 5b, simulation results of the secret key rate in this case show an achievable key rate of 0.01 bit per pulse over 25 km. With a transmission rate of 1 GHz, this corresponds to a secret key rate of 10 Mbit/s, which is sufficient for many cryptographic applications. As a comparison, we also present in Figure 5b the previously mentioned fundamental upper bounds per optical mode.[48,49] We see that the key rate of DV MDI-QKD is only about 2 orders of magnitude away from the TGW bound at a practical distance, hence this protocol is suitable for high speed communications in metropolitan area networks.

It is important to emphasise that one fundamental assumption in MDI-QKD is that Eve cannot interfere with Alice and Bob's state preparation processes. To prevent Eve from having access to quantum signals entering Alice's or Bob's labs and interfering with the state preparation process, MDI-QKD is commonly implemented using independent laser sources for Alice and Bob. Recently, gigahertz-clocked, phase-randomised pulses from independent gain-switched lasers have been demonstrated to interfere with high visibility, by control of the frequency chirp and/or emission jitter.[111,113]

DDI-QKD. One drawback of MDI-QKD is that its key rate scales quadratically with the detector efficiency. This is because in most of existing MDI-QKD protocols (except for ref. 114), secure keys are distilled from two-fold coincidence detection events (In MDI-QKD, the secure key rate R scales as $T_A \times \eta \times T_B \times \eta$, where T_A is the channel transmission from Alice to the measurement device, T_B is the channel transmission from Bob to the measurement device, and η is the single-photon detection efficiency (assuming that all detectors have the same efficiency). The overall transmission of the whole channel (from Alice to Bob) is $T = T_A \times T_B$, hence the key rate R of MDI-QKD scales as $T \times \eta^2$. This means that the key rate of MDI-QKD scales linearly with the whole channel transmittance (same as the case of conventional QKD and DDI-QKD), but

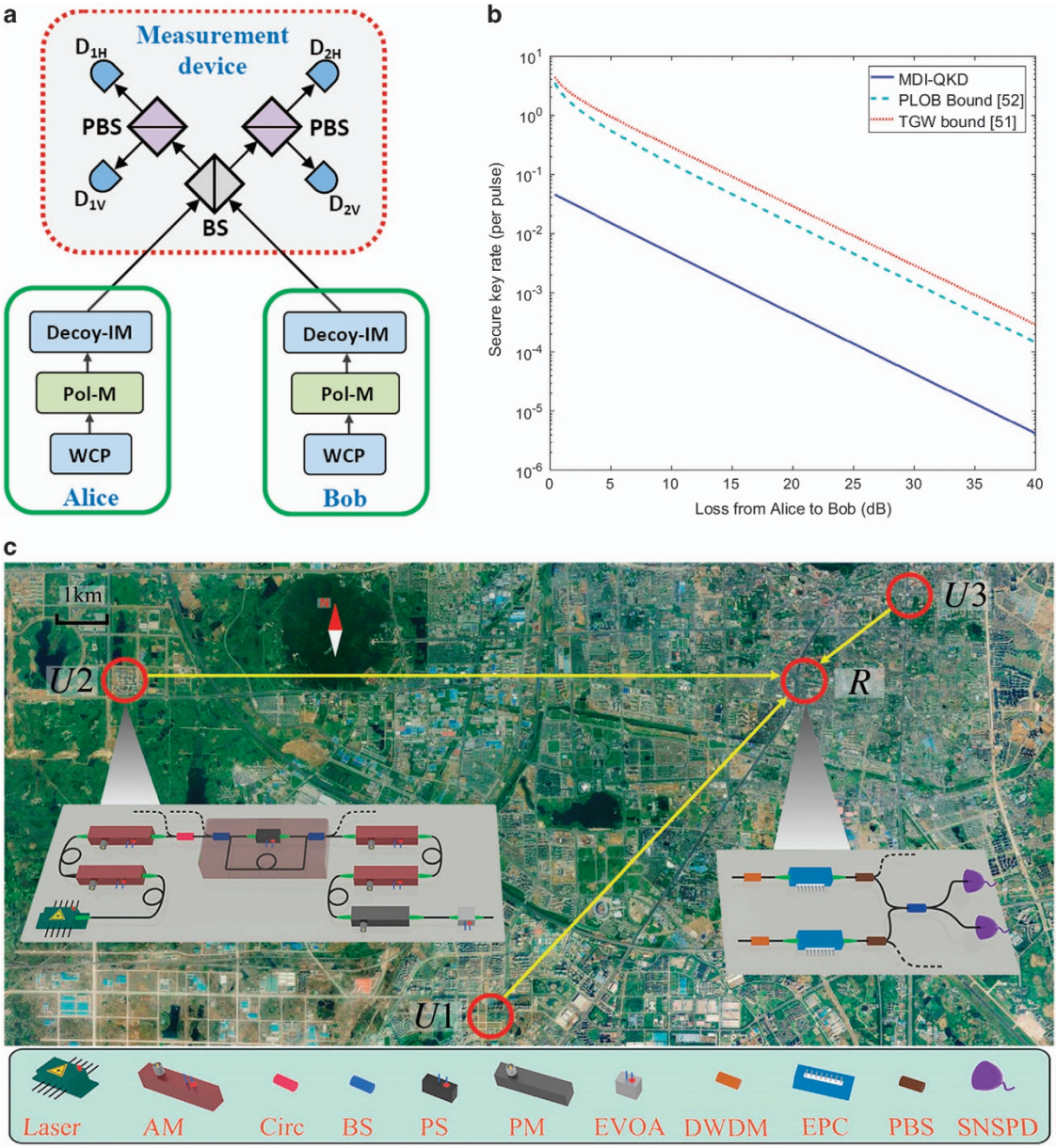


Figure 5. (**a**) The schematic diagram of DV MDI-QKD proposed in ref. 21. (**b**) Simulation results of MDI-QKD and the TGW and PLOB bounds. DV MDI-QKD has a high key rate and is suitable for metropolitan networks. The achievable key rate is about 0.01 bit per pulse at a channel loss of 5 dB (which corresponds to 25 km telecom fibre). The key rate of DV MDI-QKD is only about 2 orders of magnitude away from the TGW bound at a practical distance. The simulation corresponds to the symmetric MDI-QKD case where the channels between Alice and Charlie and Charlie and Bob have the same amount of losses. It assumes high-efficiency SNSPDs with detection efficiency of 93% and dark count probability of 10^{-6} (per pulse),[53] and an intrinsic error rate of 0.1%.[106] The efficiency of error correction is assumed to be 1.16. Note that if the detection efficiency is reduced, for instance, to 50%, this induces a drop of the key rate of about a factor of 4. This means that for the metropolitan applications of DV MDI-QKD, the requirement on detector efficiency is not stringent. (**c**) MDI-QKD metropolitan area network experimental field test with untrusted relays.[110] Figures adapted with permission from: (**a**) ref. 21, © 2012 APS; (**b**) ref. 112 courtesy of Feihu Xu; (**c**) ref. 110 courtesy of Qiang Zhang.

quadratically with the detector efficiency.). Recently, the detector-device-independent (DDI) QKD protocol, designed to bridge the strong security of MDI-QKD with the high efficiency of conventional QKD, was proposed.[115–117] In this protocol, the legitimate receiver employs a trusted linear optics network to decode information on photons received from an insecure quantum channel, and then performs a Bell state measurement (BSM) using uncharacterised detectors. One important advantage of this approach is that its key rate scales linearly with the detector efficiency. This is achieved by replacing the two-photon BSM scheme in the original MDI-QKD protocol (Figure 5a) by a single-photon BSM scheme.[118] However, its ability to completely remove detector side-channel attacks has yet to be proven. Either countermeasures to Trojan horse attacks[119] or some trustworthiness to the BSM device is still required to establish the security of DDI-QKD.[120] In fact, mathematically the standard BB84 QKD protocol based on a four-state modulation scheme can be formulated into a DDI-QKD protocol.[121] This highlights the underlying connection between DDI-QKD and the BB84 protocol. Finally, we remark that the advantage of DDI-QKD compared with MDI-QKD becomes insignificant if high detection efficiency detectors are used in both schemes.

CV MDI-QKD. The MDI-QKD scheme has been extended recently to the CV framework[122] (see also refs 123,124 for a more restricted security analysis). In the CV framework, both Alice and Bob prepare Gaussian-modulated coherent states and send them to an untrusted third party, Charlie, who measures the correlation between the incoming quantum states. The CV MDI-QKD system requires high efficiency ($>85\%$) homodyne detectors for a positive key rate.[112] This efficiency requirement has been met in recent proof-of-principle laboratory free-space experiments.[122,125] However, achieving the required efficiencies in a fibre-based optical network setting is more challenging, owing to the detector coupling loss and losses by fibre network interconnects and components[110] (see also ref. 126 for a different perspective). When high efficiency detectors are in place, CV MDI-QKD would require an asymmetric configuration, where Charlie needs to be located close to one of the users. Even in this case, the expected key rate of the state-of-the-art CV MDI-QKD system drops to zero when the channel loss is above 6 dB (corresponding to 30 km standard telecom fibre).[112,122] Therefore, for long distance (>30 km) applications, DV MDI-QKD is currently the only option available for MDI-QKD. A reliable phase reference between Alice and Bob also needs to be established in CV MDI-QKD, and may be possible to realise using recently proposed techniques for standard CV-QKD.[58–60] Despite these challenges, CV MDI-QKD has the potential for very high key rates, within one order of magnitude from the TGW and PLOB bounds, at relatively short communication distances.

QKD with imperfect sources

Given that the security loopholes associated with the measurement device can be closed by MDI-QKD, an important remaining question is how to justify the assumption of trustable quantum state preparation, including single-mode operation, perfect global phase randomisation, no side channels, etc. On one hand, the imperfections in quantum state preparation need to be carefully quantified and taken into account in the security proof; on the other hand, practical countermeasures are required to prevent Trojan horse attacks[119] on the source.

To address imperfections in quantum state preparation in QKD, a loss-tolerant protocol was proposed in ref. 32, which makes QKD tolerable to channel loss in the presence of source flaws (see also studies in refs 127,128). On the basis of the assumption that the single-photon components of the states prepared by Alice remain inside a two-dimensional Hilbert space, it was shown that Eve cannot enhance state preparation flaws by exploiting the channel loss and Eve's information can be bounded by the rejected data analysis.[129] The intuition for the security of loss-tolerant QKD protocol can be understood in the following manner. By assuming that the state prepared by Alice is a qubit, it becomes impossible for Eve to perform an unambiguous state discrimination (USD) attack.[130] Indeed, in order for Eve to perform a USD attack, the states prepared by Alice must be linearly independent; but by having three or more states in a two-dimensional space, in general the set of states prepared by Alice is linearly dependent, thus making USD impossible.

The above loss-tolerant protocol has been further developed and demonstrated experimentally in ref. 131, where the authors implemented decoy-state QKD with imperfect state preparation and employed tight finite-key security bounds with composable security against coherent attacks. The work in ref. 32 has also been extended to the finite-key regime in ref. 132, where a wide range of imperfections in the laser source, such as the intensity fluctuations, have been taken into account. In ref. 133, a rigorous security proof of QKD systems using discrete-phase-randomised coherent states was given, thus removing the requirement for perfect phase randomisation. With respect to this, we note that gain-switched laser diodes are presently the de facto QKD light source, capable of naturally providing phase-randomised coherent pulses at a clock rate of up to 2.5 GHz.[134,135]

Progress has also been made on enhancing the security of QKD by carefully examining source imperfections in implementations. Refs 136,137 studied the risk of Trojan horse attacks due to back reflections from commonly used optical components in QKD. Similar research was also conducted for CV-QKD.[138] In ref. 139, by using laser-induced damage threshold of single-mode optical fibre to bound the photon numbers in Eve's Trojan horse pulses, the authors provided quantitative security bounds and a purely passive solution against a general Trojan horse attack.

All the above advances strongly suggest the feasibility of long-distance secure quantum communication with imperfect sources. A promising research direction is to apply the above techniques for QKD with imperfect sources to MDI-QKD leading to practical side-channel-free QKD. To achieve this goal, it is necessary to establish a comprehensive list of assumptions on the sources, and verify them one by one. In a recent experimental demonstration,[140] the loss-tolerant protocol is applied to a MDI-QKD setting. Such an experiment thus addresses source and detector flaws at the same time.

We end our discussion on practical security by noting that in both classical and quantum cryptography, it is also important to carefully address the risks of side-channel attacks on the electronics and post-processing layers. Various side-channel attacks discovered in classical cryptography, such as the timing attack,[141] the power-monitoring attack,[142] and acoustic cryptanalysis,[143] can also pose threats to quantum cryptography. Closing these side channels requires substantial future efforts.

NETWORK QKD

So far, our discussion has been largely limited to point-to-point QKD links. Although these links are useful for some applications, QKD network structures must be considered in order to enable access by a greater many users and also to extend the reach and geographical coverage. In addition, the incorporation of mobile QKD nodes for key transports will add to network connection flexibility and allow even greater geographical coverage. In the following, we discuss approaches for building a QKD network and possibilities for future mobile QKD deployment.

Building QKD networks

An important issue in a network setting is the topology that allows for multiple users to access the network. A star topology is suitable for this purpose for relatively short distance (up to 400 km). Imagine a star network where there is at most one intermediate node between any two users, allowing for secure quantum communication among all users without the need for the relay to be trusted. In fact, this approach has already been demonstrated based on the MDI-QKD protocol.[110] The long-term vision is for each user to use a simple and cheap transmitter and outsource all the complicated devices for network control and measurement to an untrusted network operator. As only one set of measurement devices will be needed for such a network that is shared by many users, the cost per user could be kept relatively low. The network provider would then be in a favourable position to deploy state-of-the-art technologies including high detection efficiency SNSPDs to enhance the performance of the network and to perform all network management tasks. The important advantage is that the network operator can be completely untrusted without compromising security. Experimental demonstrations of network MDI-QKD, either in optical fibres[110] or in free space, are a major step towards such QKD networks with untrusted relays.

Nonetheless, MDI-QKD is limited in distance, hence in order to address the great challenge of extending the distance of secure QKD, three further approaches are possible. The first and the

simplest approach is to use trusted relays. This is already feasible with current technology and indeed has been used as the standard in existing QKD networks.[16,144] By setting up trusted nodes, for instance, every 50 km, to relay secrets, it is possible to achieve secure communication over arbitrarily long distances. The QKD network currently under development between Shanghai and Beijing is based on this approach.

The second approach is quantum repeaters, which remove the need for the users to trust the relay nodes. Quantum repeaters are beyond current technology, but have been a subject of intense research efforts in recent years. The long-term vision here is to construct a global quantum internet as described, for example, in ref. 14. Research efforts on quantum repeaters have focused on matter quantum memories and their interface with photonic flying qubits.[145,146] However, new recent approaches manage to reduce the need for a quantum memory[147] or to completely remove it by using all-photonic quantum repeaters.[148]

Finally, the third approach is ground-to-satellite QKD. By using one or a few trusted satellites as relay stations, it is possible to extend the distance of secure QKD to the global scale. To this end, several free-space studies, including experiments with low earth orbit (LEO) satellites, have been conducted.[149–155] China, the EU and Canada are all currently exploring experimental ground-to-satellite QKD in ambitious long-term projects involving LEO satellites.

Mobile QKD

The studies in free-space QKD may also open the door to mobile QKD networks, which can be useful in many applications, such as ship-to-ship communication, airport traffic control, communication between autonomous vehicles, etc. In such a network, the mobility of QKD platforms requires the network to be highly reconfigurable—the QKD users should be able to automatically determine the optimal QKD route in real time based on their locations. Fast-beam tracking systems are indispensable. Furthermore, due to the strong ambient light, an effective filtering scheme is required to selectively detect quantum signals. Recent studies analyze the effect of fading and of atmospheric turbulence to CV-QKD[156] and show that CV-QKD with coherent detection could be robust against ambient noise photons due to the intrinsic filtering function of the local oscillator.[157] We also note that preliminary studies suggest that QKD at microwave wavelengths, which are widely used in wireless communications, might be feasible over short distances.[158–160] Driven by various potential applications, we expect that mobile QKD will become an active research topic in the coming years.

CONCLUSION

In this review, we have discussed important challenges in practical QKD. These range from extending security proofs to the most general attacks allowed by quantum mechanics to developing photonic chips as well as side-channel-free systems and global-scale QKD networks. Addressing these challenges using some of the approaches that we have presented will open the way to the use of QKD technology for securing everyday interactions.

As the lead application of the field of Quantum Information Processing, advances in QKD will have important implications in many other applications too. For example, a great range of quantum communication protocols beyond QKD have been studied in recent years[161] and their development has directly benefited from research in QKD. These include, for instance, quantum bit commitment,[162–164] quantum secret sharing,[165–167] quantum coin flipping,[168,169] quantum fingerprinting,[170,171] quantum digital signatures,[172,173] blind quantum computing[174,175] and position-based quantum cryptography.[176–178] It is known that some of those protocols, such as quantum bit commitment and position-based quantum cryptography, cannot be perfectly achieved with unconditional security. However, other security models exist, such as, for instance, those based on relativistic constraints or on noisy storage assumptions,[179] where by assuming that it is impossible for an eavesdropper to store quantum information for a long time, one can retrieve security for such protocols.

Determining the exact power and limitations of quantum communication is the subject of intense research efforts worldwide. The formidable developments that can be expected in the next few years will mark important milestones towards the quantum internet of the future.

Notes added in proof

After a completion of a preliminary version of this paper, a recent preprint[181] has been posted on the arXiv that demonstrates the insecurity of DDI-QKD protocol. In addition, it has come to our attention that DI-QKD remains vulnerable to covert channels such as memory attack.[182]

ACKNOWLEDGEMENTS

We acknowledge helpful comments from many colleagues including Romain Alléaume, Hoi-Fung Chau, Marcos Curty, Philippe Grangier, Anthony Leverrier, Charles Ci Wen Lim, Marco Lucamarini, Xiongfeng Ma, Joyce Poon, Li Qian, Kiyoshi Tamaki and Feihu Xu. We thank our colleagues including Ping Koy Lam, Vikas Anant, Jessie Qin-Dregely, Chris Erven, Masato Koashi, Philip Sibson, Mark Thompson and Qiang Zhang for allowing us to reproduce some of their figures. We thank Warren Raye of Nature Partner Journals for securing the permission for reproductions of figures from various publishers. We acknowledge financial support from NSERC, CFI, ORF, the US Office of Naval Research (ONR), the Laboratory Directed Research and Development (LDRD) Program of Oak Ridge National Laboratory (managed by UT-Battelle LLC for the US Department of Energy), the City of Paris, the French National Research Agency, the Ile-de-France Region, the France-USA Partner University Fund, and the Commissioned Research of National Institute of Information and Communications Technology (NICT), Japan.

COMPETING INTERESTS

Owing to the employments and consulting activities of some of the authors, they have financial interests in the commercial applications of quantum key distribution.

REFERENCES

1. Shor, P. W. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (ed. Goldwasser, S.) 124–134 (IEEE Computer Society Press, 1994).
2. Encyclopedia Britannica. ENIAC. https://www.britannica.com/technology/ENIAC.
3. Cesare, C. Encryption faces quantum foe. *Nature* **525**, 167–168 (2015).
4. Bennett, C. H. & Brassard, G. *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (ed. Goldwasser, S.) 175–179 (IEEE Press, 1984).
5. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
6. Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301 (2009).
7. Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photon.* **8**, 595–604 (2014).
8. Mayers, D. Unconditional security in quantum cryptography. *J. ACM* **48**, 351–406 (2001).
9. Lo, H.-K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283**, 2050–2056 (1999).
10. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441–444 (2000).
11. Unruh, D. Advances in Cryptology—Crypto 2013. Vol. 8043, 380–397 (Springer, 2013).
12. Wootters, W. K. & Zurek., W. H. A single quantum cannot be cloned. *Nature* **299**, 802–803 (1982).
13. Dieks, D. Communication by EPR devices. *Phys. Lett.* **92A**, 271–272 (1982).
14. Kimble., H. J. The quantum internet. *Nature* **453**, 1023–1030 (2008).

15. Qiu, J. Quantum communications leap out of the lab. *Nature* **508**, 441–442 (2014).
16. Peev, M. *et al.* The SECOQC quantum key distribution in vienna. *New J. Phys.* **11**, 075001 (2009).
17. Huttner, B., Imoto, N., Gisin, N. & Mor, T. Quantum cryptography with coherent states. *Phys. Rev. A* **51**, 1863–1869 (1995).
18. Hwang, W.-Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91**, 057901 (2003).
19. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
20. Wang, X.-B. Beating photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).
21. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
22. Christandl, M., Koenig, R., Mitchison, G. & Renner, R. One-and-a-half quantum de Finetti theorems. *Commun. Math. Phys* **273**, 473–498 (2007).
23. Hensen, B. *et al.* Experimental loophole-free violation of a Bell inequality using entangled electron spins separated by 1.3 km. *Nature* **526**, 682 (2015).
24. Gol'Tsman, G. N. *et al.* Picosecond superconducting single-photon optical detector. *Appl. Phys. Lett.* **79**, 705–707 (2001).
25. Lita, A. E., Miller, A. J. & Nam., S. W. Counting near-infrared single-photons with 95% efficiency. *Opt. Express* **16**, 3032–3040 (2008).
26. Albota, M. A. & Wong, F. N. C. Efficient single-photon counting at 1.55 μm by means of frequency upconversion. *Opt. Lett.* **29**, 1449–1451 (2004).
27. Langrock, C. *et al.* Highly efficient single-photon detection at communication wavelengths by use of upconversion in reverse-proton-exchanged periodically poled $LiNbO_3$ waveguides. *Opt. Lett.* **30**, 1725–1727 (2005).
28. Yuan, Z. L., Kardynal, B. E., Sharpe, A. W. & Shields, A. J. High speed single photon detection in the near infrared. *Appl. Phys. Lett.* **91**, 041114 (2007).
29. Hansen, H. *et al.* Ultrasensitive pulsed, balanced homodyne detector: application to time-domain quantum measurements. *Opt. Lett.* **26**, 1714–1716 (2001).
30. Jennewein, T., Achleitner, U., Weihs, G., Weinfurter, H. & Zeilinger, A. A fast and compact quantum random number generator. *Rev. Sci. Instrum.* **71**, 1675–1680 (2000).
31. Zhu, E. Y. *et al.* Poled-fiber source of broadband polarization-entangled photon pairs. *Opt. Lett.* **38**, 4397–4400 (2013).
32. Tamaki, K., Curty, M., Kato, G., Lo, H.-K. & Azuma, K. Loss-tolerant quantum cryptography with imperfect sources. *Phys. Rev. A* **90**, 052314 (2014).
33. Alléaume, R. *et al.* Worldwide standardization activity for quantum key distribution. In *Proceedings of the IEEE Globecom Workshops (GC Wkshps)*, 656–551 (2014).
34. Stucki, D., Brunner, N., Gisin, N., Scarani, V. & Zbinden, H. Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.* **87**, 194108 (2005).
35. Inoue, K., Waks, E. & Yamamoto, Y. Differential phase shift quantum key distribution. *Phys. Rev. Lett.* **89**, 037902 (2002).
36. Grosshans, F. & Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **88**, 057902 (2002).
37. Grosshans, F. *et al.* Quantum key distribution using gaussian-modulated coherent states. *Nature* **421**, 238 (2003).
38. Diamanti, E. & Leverrier, A. Distributing secret keys with quantum continuous variables: principle, security and implementations. *Entropy* **17**, 6072–6092 (2015).
39. Ma, X., Fung, C.-H. F. & Lo, H.-K. Quantum key distribution with entangled photon sources. *Phys. Rev. A* **76**, 012307 (2007).
40. Lucamarini, M. *et al.* Efficient decoy-state quantum key distribution with quantified security. *Opt. Express* **21**, 24550–24565 (2013).
41. Korzh, B. *et al.* Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nat. Photon.* **9**, 163–168 (2015).
42. Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. & Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photon.* **7**, 378 (2013).
43. Huang, D. *et al.* Continuous-variable quantum key distribution with 1 Mbit/s secure key rate. *Opt. Express* **23**, 17511–17519 (2015).
44. Lim, C. C. W., Curty, M., Walenta, N., Xu, F. & Zbinden, H. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **89**, 022307 (2014).
45. Lucamarini, M., Dynes, J. F., Fröhlich, B., Yuan, Z. & Shields, A. J. Security bounds for efficient decoy-state quantum key distribution. *IEEE J. Sel. Topics Quantum Electron* **21**, 6601408 (2015).
46. Moroder, T. *et al.* Security of distributed-phase-reference quantum key distribution. *Phys. Rev. Lett.* **109**, 260501 (2012).
47. Leverrier, A. Composable security proof for continuous-variable quantum key distribution with coherent states. *Phys. Rev. Lett.* **114**, 070501 (2015).
48. Takeoka, M., Guha, S. & Wilde, M. M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* **5**, 5235 (2014).
49. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi., L. The ultimate rate of quantum cryptography. Preprint at arXiv:1510.08863 (2015).
50. Winzer, P. J. Scaling optical fiber networks: Challenges and solutions. *Opt. Photon. News* **26**, 28–35 (2015).
51. Huang, M. F. *et al.* Terabit/s Nyquist superchannels in high capacity fiber field trials using DP-16QAM and DP-8QAM modulation formats. *J. Lightw. Technol.* **32**, 776–782 (2014).
52. Pernice, W. H. P. *et al.* High-speed and high-efficiency travelling wave single-photon detectors embedded in nanophotonic circuits. *Nat. Commun.* **3**, 1325 (2012).
53. Marsili, F. *et al.* Detecting single infrared photons with 93% system efficiency. *Nat. Photon.* **7**, 210–214 (2013).
54. Comandar, L. C. *et al.* Gigahertz-gated InGaAs/InP single-photon detector with detection efficiency exceeding 55% at 1550 nm. *J. Appl. Phys.* **117**, 083109 (2015).
55. Scontel Superconducting nanotechnology. http://www.scontel.ru/; Single Quantum. http://www.singlequantum.com/; ID Quantique. http://www.idquantique.com/; Photon Spt. http://www.photonspot.com/ Accessed 19 October, 2016.
56. Bahrani, S., Razavi, M. & Salehi, J. A. Orthogonal frequency-division multiplexed quantum key distribution. *J. Lightw. Technol.* **33**, 4687–4698 (2015).
57. Dynes, J. F. *et al.* Quantum key distribution over multicore fiber. *Opt. Express* **24**, 8081–8087 (2016).
58. Qi, B., Lougovski, P., Pooser, R., Grice, W. & Bobrek, M. Generating the local oscillator 'locally' in continuous-variable quantum key distribution based on coherent detection. *Phys. Rev. X* **5**, 041009 (2015).
59. Soh, D. B. S. *et al.* Self-referenced continuous-variable quantum key distribution. *Phys. Rev. X* **5**, 041010 (2015).
60. Huang, D., Huang, P., Lin, D., Wang, C. & Zeng., G. High-speed continuous-variable quantum key distribution without sending a local oscillator. *Opt. Lett.* **40**, 3695–3698 (2015).
61. Fröhlich, B. *et al.* Quantum secured gigabit optical access networks. *Sci. Rep.* **5**, 18121 (2015).
62. Shibaba, H., Honjo, T. & Shimizu, K. Quantum key distribution over a 72 dB channel loss using ultralow dark count superconducting single-photon detectors. *Opt. Lett.* **39**, 5078–5081 (2014).
63. Jouguet, P., Elkouss, D. & Kunz-Jacques, S. High bit rate continuous-variable quantum key distribution. *Phys. Rev. A* **90**, 042329 (2014).
64. Patel, K. A. *et al.* Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks. *Appl. Phys. Lett.* **104**, 051123 (2014).
65. Choi, I. *et al.* Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber. *Opt. Express* **22**, 23121–23128 (2014).
66. Qi, B., Zhu, W., Qian, L. & Lo, H.-K. Feasibility of quantum key distribution through a dense wavelength division multiplexing network. *New J. Phys.* **12**, 103042 (2010).
67. Kumar, R., Qin, H. & Alléaume, R. Coexistence of continuous variable QKD with intense DWDM classical channels. *New J. Phys.* **17**, 043027 (2015).
68. Fröhlich, B. *et al.* A quantum access network. *Nature* **501**, 69–72 (2013).
69. Comandar, L. C. *et al.* Room temperature single-photon detectors for high bit rate quantum key distribution. *Appl. Phys. Lett.* **104**, 021101 (2014).
70. Hughes, R. J. *et al.* Network-centric quantum communications with applications to critical infrastructure protection. Preprint at arXiv:1305.0305 (2013).
71. Lim, A. E.-J. *et al.* Review of silicon photonics foundry efforts. *IEEE J. Sel. Topics Quantum Electron* **20**, 405–416 (2014).
72. Smit, M. *et al.* An introduction to InP-based generic integration technology. *Semicond. Sci. Technol.* **29**, 083001 (2014).
73. Zhang, P. *et al.* Reference-frame-independent quantum-key-distribution server with a telecom tether for an on-chip client. *Phys. Rev. Lett.* **112**, 130501 (2014).
74. Vest, G. *et al.* Design and evaluadtion of a handheld quantum key distribution sender module. *IEEE J. Sel. Topics Quantum Electron* **21**, 6600607 (2014).
75. Sibson, P. *et al.* Chip-based quantum key distribution. Preprint at arXiv:1509.00768 (2015).
76. Ma, C. *et al.* Integrated silicon photonic transmitter for polarization-encoded quantum key distribution. Optica (in press). Preprint on-line available at https://arxiv.org/abs/1606.04407.
77. Takesue, H. *et al.* Differential phase shift quantum key distribution experiment over 105 km fibre. *New J. Phys.* **7**, 232 (2005).
78. Nambu, Y., Yoshino, K. & Tomita, A. Quantum encoder and decoder for practical quantum key distribution using a planar lightwave circuit. *J. Mod. Opt.* **55**, 1953–1970 (2008).
79. Ziebell, M. *et al. CLEO/Europe* (EQEC, Munich, Germany, 2015).
80. Bechmann-Pasquinucci, H. & Tittel, W. Quantum cryptography using larger alphabets. *Phys. Rev. A* **61**, 062308 (2000).
81. Bourennane, M., Karlsson, A. & Björk, G. Quantum key distribution using multilevel encoding. *Phys. Rev. A* **64**, 012306 (2001).

82. Cerf, N. J., Bourennane, M., Karlsson, A. & Gisin, N. Security of quantum key distribution using *d*-level systems. *Phys. Rev. Lett.* **88**, 127902 (2002).
83. Zhang, L., Silberhorn, C. & Walmsley, I. A. Secure quantum key distribution using continuous variables of single photons. *Phys. Rev. Lett.* **100**, 110504 (2008).
84. Zhang, Z., Mower, J., Englund, D., Wong, F. N. C. & Shapiro, J. H. Unconditional security of time-energy entanglement quantum key distribution using dual-basis interferometry. *Phys. Rev. Lett.* **112**, 120506 (2014).
85. Zhong, T. *et al.* Photon-efficient quantum key distribution using time-energy entanglement with high-dimensional encoding. *New J. Phys.* **17**, 022002 (2015).
86. Mirhosseini, M. *et al.* High-dimensional quantum cryptography with twisted light. *New J. Phys.* **17**, 033033 (2015).
87. Etcheverry, S. *et al.* Quantum key distribution session with 16-dimensional photonic states. *Sci. Rep.* **3**, 2316 (2013).
88. Sasaki, T., Yamamoto, Y. & Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature* **509**, 475–478 (2014).
89. Guan, J. Y. *et al.* Experimental passive round-robin differential phase-shift quantum key distribution. *Phys. Rev. Lett.* **114**, 180502 (2015).
90. Takesue, H., Sasaki, H., Tamaki, K. & Koashi, M. Experimental quantum key distribution without monitoring signal disturbance. *Nat. Photon.* **9**, 827—831 (2015).
91. Wang, S. *et al.* Experimental demonstration of quantum key distribution without signal disturbance monitoring. *Nat. Photon.* **9**, 832–836 (2015).
92. Li, Y. H. *et al.* Experimental round-robin differential phase-shift quantum key distribution. *Phys. Rev. A* **93**, 030302(R) (2016).
93. Mizutani, A., Imoto, N. & Tamaki, K. Robustness of round-robin differential phase-shift quantum key distribution protocol against source flaws. *Phys. Rev. A* **92**, 060303 (2015).
94. Zhao, Y., Fung, C.-H. F., Qi, B., Chen, C. & Lo, H.-K. Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A* **78**, 042333 (2008).
95. Lydersen, L. *et al.* Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photon.* **4**, 686–689 (2010).
96. Xu, F., Qi, B. & Lo, H.-K. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New J. Phys.* **12**, 113026 (2010).
97. Mayers, D. & Yao, A. Quantum cryptography with imperfect apparatus. in *Proceedingsof the 39th Annual Symposium on Foundations of Computer Science, 1998*. 503–509 (IEEE, 1998).
98. Can, A. *et al.* Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).
99. Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012).
100. Shalm, L. K. *et al.* A strong loophole-free test of local realism. *Phys. Rev. Lett.* **115**, 250402 (2015).
101. Giustina, M. *et al.* A significant-loophole-free test of Bell's theorem with entangled photons. *Phys. Rev. Lett.* **115**, 250401 (2015).
102. Biham, E., Huttner, B. & Mor, T. Quantum cryptographic network based on quantum memories. *Phys. Rev. A* **54**, 2651 (1996).
103. Inamori, H. Security of practical time-reversed EPR quantum key distribution. *Algorithmica* **34**, 340 (2002).
104. Curty, M. *et al.* Finite-key analysis for measurement-device-independent quantum key distribution. *Nat. Commun.* **5**, 3732 (2014).
105. Lim, C. C. W., Portmann, C., Tomamichel, M., Renner, R. & Gisin, N. Device-independent quantum key distribution with local Bell test. *Phys. Rev. X* **3**, 031006 (2013).
106. Tang, Y.-L. *et al.* Measurement-device-independent quantum key distribution over 200 km. *Phys. Rev. Lett.* **113**, 190501 (2014).
107. Yin, H.-L. *et al.* Measurement device independent quantum key distribution over 404 km optical fibre. Preprint at arXiv:1606.06821 (2016).
108. Tang, Y.-L. *et al.* Field test of measurement-device-independent quantum key distribution. *IEEE J. Sel. T. Quantum Electron.* **21**, 6600407 (2014).
109. Valivarthi, R. *et al.* Measurement-device-independent quantum key distribution: from idea towards application. *J. Mod. Opt.* **62**, 1141–1150 (2015).
110. Tang, Y.-L. *et al.* Measurement-device-independent quantum key distribution over untrustful metropolitan network. *Phys. Rev. X* **6**, 011024 (2015).
111. Comandar, L. C. *et al.* Quantum cryptography without detector vulnerabilities using optically-seeded lasers. *Nat. Photon.* **10**, 312–315 (2016).
112. Xu, F., Curty, M., Qi, B., Qian, L. & Lo, H.-K. Discrete and continuous variables for measurement-device-independent quantum cryptography. *Nat. Photon.* **9**, 772 (2015).
113. Yuan, Z.-L. *et al.* Interference of short optical pulses from independent gain-switched laser diodes for quantum secure communications. *Phys. Rev. Applied* **2**, 064006 (2014).
114. Tamaki, K., Lo, H.-K., Fung, C.-H. F. & Qi, B. Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw. *Phys. Rev. A* **85**, 042307 (2012).
115. González, P. *et al.* Quantum key distribution with untrusted detectors. *Phys. Rev. A* **92**, 022337 (2015).
116. Lim, C. C. W. *et al.* Detector-device-independent quantum key distribution. *Appl. Phys. Lett.* **105**, 221112 (2014).
117. Cao, W.-F. *et al.* Highly efficient quantum key distribution immune to all detector attacks. Preprint at arXiv:1410.2928v1 (2014).
118. Kim, Y.-H. Single-photon two-qubit entangled states: Preparation and measurement. *Phys. Rev. A* **67**, 040301(R) (2003).
119. Gisin, N., Fasel, S., Kraus, B., Zbinden, H. & Ribordy, G. Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A* **73**, 022320 (2006).
120. Qi, B. Trustworthiness of detectors in quantum key distribution with untrusted detectors. *Phys. Rev. A* **91**, 020303(R) (2015).
121. Liang, W.-Y. *et al.* Simple implementation of quantum key distribution based on single-photon bell state measurement. *Phys. Rev. A* **92**, 012319 (2015).
122. Pirandola, S. *et al.* High-rate measurement-device-independent quantum cryptography. *Nat. Photon.* **9**, 397–402 (2015).
123. Li, Z., Zhang, Y.-C., Xu, F., Peng, X. & Guo, H. Continuous-variable measurement-device-independent quantum key distribution. *Phys. Rev. A* **89**, 052301 (2014).
124. Ma, X.-C., Sun, S.-H., Jiang, M.-S., Gui, M. & Liang, L.-M. Gaussian-modulated coherent-state measurement-device-independent quantum key distribution. *Phys. Rev. A* **89**, 042335 (2014).
125. Gehring, T. *et al.* Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks. *Nat. Commun.* **6**, 8795 (2015).
126. Pirandola, S. *et al.* Reply to 'Discrete and continuous variables for measurement-device-independent quantum cryptography'. *Nat. Photon.* **9**, 773 (2015).
127. Yin, Z.-Q. *et al.* Measurement-device-independent quantum key distribution with uncharacterized qubit sources. *Phys. Rev. A* **88**, 062322 (2013).
128. Yin, Z.-Q. *et al.* Mismatched-basis statistics enable quantum key distribution with uncharacterized qubit sources. *Phys. Rev. A* **90**, 052319 (2014).
129. Barnett, S. M., Huttner, B. & Phoenix, S. Eavesdropping strategies and rejected-data protocols in quantum cryptography. *J. Mod. Opt.* **40**, 2501 (1993).
130. Dušek, M., Jahma, M. & Lütkenhaus, N. Unambiguous state discrimination in quantum cryptography with weak coherent states. *Phys. Rev. A* **62**, 022306 (2000).
131. Xu, F. *et al.* Experimental quantum key distribution with source flaws. *Phys. Rev. A* **92**, 032305 (2015).
132. Mizutani, A., Curty, M., Lim, C. C. W., Imoto, N. & Tamaki, K. Finite-key security analysis of quantum key distribution with imperfect light sources. *New J. Phys.* **17**, 093011 (2015).
133. Cao, Z., Zhang, Z., Lo, H.-K. & Ma, X. Discrete-phase-randomized coherent state source and its application in quantum key distribution. *New J. Phys.* **17**, 053014 (2015).
134. Yuan, Z. L. *et al.* Robust random number generation using steady-state emission of gain-switched laser diodes. *Appl. Phys. Lett.* **104**, 261112 (2014).
135. Yuan, Z. L. *et al.* A directly phase-modulated light source. *Phys. Rev. X* **6**, 031044 (2016).
136. Jain, N. *et al.* Trojan-horse attacks threaten the security of practical quantum cryptography. *New J. Phys.* **16**, 123030 (2014).
137. Jain, N. *et al.* Risk analysis of trojan-horse attacks on practical quantum key distribution systems. *IEEE J. Sel. Topics Quantum Electron* **21**, 6600710 (2015).
138. Stiller, B. *et al.* in *2015 Conference on Lasersand Electro-Optics (CLEO)* (ed. Goldwasser, S.) (Optical Society of America, 2015).
139. Lucamarini, M. *et al.* Practical security bounds against the Trojan-horse attack in quantum key distribution. *Phys. Rev. X* **5**, 031030 (2015).
140. Tang, Z., Wei, K., Bedroya, O., Qian, L. & Lo, H.-K. Experimental measurement-device-independent quantum key distribution with imperfect sources. *Phys. Rev. A* **93**, 042308 (2016).
141. Paul, C. K. in *Advances in Cryptology—CRYPTO 1996* 104–113 (Springer, 1996).
142. Kocher, P., Jaffe, J. & Jun, B. in *Advances in Cryptology—CRYPTO 1999* 388–397 (Springer, 1999).
143. Genkin, D., Shamir, A. & Tromer, E. in *Advances in Cryptology—CRYPTO 2014* 444–461 (Springer, 2014).
144. Sasaki, M. *et al.* Field test of quantum key distribution in the Tokyo QKD network. *Opt. Express* **19**, 10387 (2011).
145. Northup, T. E. & Blatt, R. Quantum information transfer using photons. *Nat. Photon.* **8**, 356 (2014).
146. Bussières, F. *et al.* Quantum teleportation from a telecom-wavelength photon to a solid-state quantum memory. *Nat. Photon.* **8**, 775 (2014).

147. Munro, W. J., Stephens, A. M., Devitt, S. J., Harrison, K. A. & Nemoto, K. Quantum communication without the necessity of quantum memories. *Nat. Photon.* **6**, 777–781 (2012).
148. Azuma, K., Tamaki, K. & Lo, H.-K. All-photonic quantum repeaters. *Nat. Commun.* **6**, 6787 (2015).
149. Buttler, W. T. *et al.* Daylight quantum key distribution over 1.6 km. *Phys. Rev. Lett.* **84**, 5652 (2000).
150. Nauerth, S. *et al.* Air-to-ground quantum communication. *Nat. Photon.* **7**, 382–386 (2013).
151. Wang, J.-Y. *et al.* Direct and full-scale experimental verifications towards ground-satellite quantum key distribution. *Nat. Photon.* **7**, 387–393 (2013).
152. Vallone, G. *et al.* Experimental satellite quantum communications. *Phys. Rev. Lett.* **115**, 040502 (2015).
153. Meyers, R. E. in *Advanced Free Space Optics (FSO)* 343–387 (Springer, 2015).
154. Elser, D. *et al.* in *IEEE ICSOS 2015*, (New Orleans, USA, 2015).
155. Bourgoin, J. P. *et al.* Free-space quantum key distribution to a moving receiver. *Opt. Express* **23**, 33437–33447 (2015).
156. Usenko, V. C. *et al.* Entanglement of Gaussian states and the applicability to quantum key distribution over fading channels. *New J. Phys.* **14**, 093048 (2012).
157. Heim, B. *et al.* Atmospheric continuous-variable quantum communication. *New J. Phys.* **16**, 113018 (2014).
158. Usenko, V. C. & Filip, R. Feasibility of continuous-variable quantum key distribution with noisy coherent states. *Phys. Rev. A* **81**, 022318 (2010).
159. Weedbrook, C., Pirandola, S., Lloyd, S. & Ralph, T. C. Quantum cryptography approaching the classical limit. *Phys. Rev. Lett.* **105**, 110501 (2010).
160. Weedbrook, C., Pirandola, S. & Ralph, T. C. Continuous-variable quantum key distribution using thermal states. *Phys. Rev. A* **86**, 022318 (2012).
161. Broadbent, A. & Schaffner, C. Quantum cryptography beyond quantum key distribution. *Des. Codes Cryptogr.* **78**, 351–382 (2016).
162. Mayers, D. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.* **78**, 3414–3417 (1997).
163. Lo, H.-K. & Chau, H. F. Is quantum bit commitment really possible? *Phys. Rev. Lett.* **78**, 3410–3413 (1997).
164. Lunghi, T. *et al.* Practical relativistic bit commitment. *Phys. Rev. Lett.* **115**, 030502 (2015).
165. Cleve, R., Gottesman, D. & Lo, H.-K. How to share a quantum secret. *Phys. Rev. Lett.* **83**, 648–651 (1999).
166. Hillery, M., Bužek, V. & Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **59**, 1829–1834 (1999).
167. Bell, B. A. *et al.* Experimental demonstration of graph-state quantum secret sharing. *Nat. Commun.* **5**, 5480 (2014).
168. Berlin, G. *et al.* Flipping quantum coins. *Nat. Commun.* **2**, 561 (2011).
169. Pappa, A. *et al.* Experimental plug and play quantum coin flipping. *Nat. Commun.* **5**, 3717 (2014).
170. Buhrman, H., Cleve, R., Watrous, J. & Wolf, R. D. Quantum fingerprinting. *Phys. Rev. Lett.* **87**, 167902 (2001).
171. Xu, F. *et al.* Experimental quantum fingerprinting. *Nat. Commun.* **6**, 8735 (2015).
172. Gottesman, D. & Chuang, I. Quantum digital signatures. Preprint at quant-ph/0105032 (2001).
173. Donaldson, R. J. *et al.* Experimental demonstration of kilometer-range quantum digital signatures. *Phys. Rev. A* **93**, 012329 (2016).
174. Broadbent, A., Fitzsimons, J. & Kashefi, E. in *Proceedings of the 50th Annual Symposium on Foundations of Computer Science* 517–526 (IEEE, 2009).
175. Barz, S. *et al.* Experimental demonstration of blind quantum computing. *Science* **335**, 303 (2012).
176. Lau, H.-K. & Lo, H.-K. Insecurity of position-based quantum-cryptography protocols against entanglement attacks. *Phys. Rev. A* **83**, 012322 (2011).
177. Buhrman, H. *et al.* Position-based quantum cryptography: Impossibility and constructions. *SIAM J. Comput.* **43**, 150–178 (2014).
178. Chakraborty, K. & Leverrier, A. Practical position-based quantum cryptography. *Phys. Rev. A* **92**, 052304 (2015).
179. Wehner, S., Curty, M., Schaffner, C. & Lo, H.-K. Implementation of two-party protocols in the noisy-storage model. *Phys. Rev. A* **81**, 052336 (2010).
180. Lam, P.-K. & Ralph, T. Quantum cryptography: Continuous improvement. *Nat. Photon.* **7**, 350 (2013).
181. Sajeed, S, Huang, A, Sun, S, Xu, F, Makarov, V & Curty, M. Insecurity of detector-device-independent quantum key distribution. https://arxiv.org/abs/1607.05814 (2016).
182. Barrett, J., Colbeck, R. & Kent, A. Memory attacks on device-independent quantum cryptography. *Phys. Rev. Lett.* **110**, 010503 (2013).

Chapter 9

Quantum teleportation and Quantum dense coding

9.1 Quantum teleportation

Quantum teleportation was first realized in 1997 in Vienna in the Zeilinger group. It relies on a pair of entangled photons.

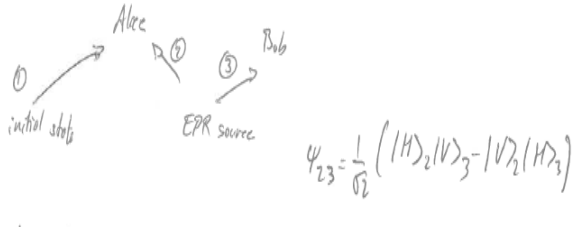


Figure 9.1: In quantum teleportation, the arbitrary polarization state of photon 1 is teleported on photon 3.

$|\Psi\rangle_1 = a\,|H\rangle_1 + b\,|V\rangle_1$ is the arbitrary state we want to teleport to Bob. We let particles 1 and 2 interact on a beam splitter to get:

$$|\Psi\rangle_{12} = \frac{1}{\sqrt{2}}[|H_1V_2\rangle - |V_1H_2\rangle]$$

Once particles 1 and 2 are in the state $|\Psi\rangle_{12}$, particle 3 is projected into the initial state of particle 1.

Particle 2 is in a state opposite to 1 and 3 is opposite to 2. Hence particle 3 is in the same state than particle 1. Note that Ψ_1 is destroyed, otherwise the no-cloning theorem would forbid us from making a perfect copy.

We see that after Alice measures on 1 and 2, she can tell Bob which of the four possible measurements she performed and send this information over a public channel. Bob can then complete the teleportation.

$$|\Psi\rangle = |\Psi_1\rangle \otimes |\Psi_{23}\rangle$$

$$= (\frac{a}{\sqrt{2}})[|V_1V_2H_3\rangle - |V_1H_2V_3\rangle] + (\frac{b}{\sqrt{2}})[|H_1V_2H_3\rangle - |H_1H_2V_3\rangle]$$

$$= \frac{1}{2}(|V_1H_2\rangle - |H_1V_2\rangle)(-a\,|V_3\rangle - b\,|H_3\rangle) +$$
$$(|V_1H_2\rangle + |H_1H_2\rangle)(-a\,|V_3\rangle - b\,|H_3\rangle) +$$
$$(|V_1V_2\rangle - |H_1H_2\rangle)(a\,|H_3\rangle - b\,|V_3\rangle) +$$
$$(|V_1V_2\rangle + |H_1H_2\rangle)(a\,|H_3\rangle - b\,|V_3\rangle)]$$

Experimental quantum teleportation

Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter & Anton Zeilinger

Institut für Experimentalphysik, Universität Innsbruck, Technikerstr. 25, A-6020 Innsbruck, Austria

Quantum teleportation—the transmission and reconstruction over arbitrary distances of the state of a quantum system—is demonstrated experimentally. During teleportation, an initial photon which carries the polarization that is to be transferred and one of a pair of entangled photons are subjected to a measurement such that the second photon of the entangled pair acquires the polarization of the initial photon. This latter photon can be arbitrarily far away from the initial one. Quantum teleportation will be a critical ingredient for quantum computation networks.

The dream of teleportation is to be able to travel by simply reappearing at some distant location. An object to be teleported can be fully characterized by its properties, which in classical physics can be determined by measurement. To make a copy of that object at a distant location one does not need the original parts and pieces—all that is needed is to send the scanned information so that it can be used for reconstructing the object. But how precisely can this be a true copy of the original? What if these parts and pieces are electrons, atoms and molecules? What happens to their individual quantum properties, which according to the Heisenberg's uncertainty principle cannot be measured with arbitrary precision?

Bennett *et al.*[1] have suggested that it is possible to transfer the quantum state of a particle onto another particle—the process of quantum teleportation—provided one does not get any information about the state in the course of this transformation. This requirement can be fulfilled by using entanglement, the essential feature of quantum mechanics[2]. It describes correlations between quantum systems much stronger than any classical correlation could be.

The possibility of transferring quantum information is one of the cornerstones of the emerging field of quantum communication and quantum computation[3]. Although there is fast progress in the theoretical description of quantum information processing, the difficulties in handling quantum systems have not allowed an equal advance in the experimental realization of the new proposals. Besides the promising developments of quantum cryptography[4] (the first provably secure way to send secret messages), we have only recently succeeded in demonstrating the possibility of quantum dense coding[5], a way to quantum mechanically enhance data compression. The main reason for this slow experimental progress is that, although there exist methods to produce pairs of entangled photons[6], entanglement has been demonstrated for atoms only very recently[7] and it has not been possible thus far to produce entangled states of more than two quanta.

Here we report the first experimental verification of quantum teleportation. By producing pairs of entangled photons by the process of parametric down-conversion and using two-photon interferometry for analysing entanglement, we could transfer a quantum property (in our case the polarization state) from one photon to another. The methods developed for this experiment will be of great importance both for exploring the field of quantum communication and for future experiments on the foundations of quantum mechanics.

The problem

To make the problem of transferring quantum information clearer, suppose that Alice has some particle in a certain quantum state $|\psi\rangle$ and she wants Bob, at a distant location, to have a particle in that state. There is certainly the possibility of sending Bob the particle directly. But suppose that the communication channel between Alice and Bob is not good enough to preserve the necessary quantum coherence or suppose that this would take too much time, which could easily be the case if $|\psi\rangle$ is the state of a more complicated or massive object. Then, what strategy can Alice and Bob pursue?

As mentioned above, no measurement that Alice can perform on $|\psi\rangle$ will be sufficient for Bob to reconstruct the state because the state of a quantum system cannot be fully determined by measurements. Quantum systems are so evasive because they can be in a superposition of several states at the same time. A measurement on the quantum system will force it into only one of these states—this is often referred to as the projection postulate. We can illustrate this important quantum feature by taking a single photon, which can be horizontally or vertically polarized, indicated by the states $|\leftrightarrow\rangle$ and $|\updownarrow\rangle$. It can even be polarized in the general superposition of these two states

$$|\psi\rangle = \alpha|\leftrightarrow\rangle + \beta|\updownarrow\rangle \qquad (1)$$

where α and β are two complex numbers satisfying $|\alpha|^2 + |\beta|^2 = 1$. To place this example in a more general setting we can replace the states $|\leftrightarrow\rangle$ and $|\updownarrow\rangle$ in equation (1) by $|0\rangle$ and $|1\rangle$, which refer to the states of any two-state quantum system. Superpositions of $|0\rangle$ and $|1\rangle$ are called qubits to signify the new possibilities introduced by quantum physics into information science[8].

If a photon in state $|\psi\rangle$ passes through a polarizing beamsplitter—a device that reflects (transmits) horizontally (vertically) polarized photons—it will be found in the reflected (transmitted) beam with probability $|\alpha|^2$ ($|\beta|^2$). Then the general state $|\psi\rangle$ has been projected either onto $|\leftrightarrow\rangle$ or onto $|\updownarrow\rangle$ by the action of the measurement. We conclude that the rules of quantum mechanics, in particular the projection postulate, make it impossible for Alice to perform a measurement on $|\psi\rangle$ by which she would obtain all the information necessary to reconstruct the state.

The concept of quantum teleportation

Although the projection postulate in quantum mechanics seems to bring Alice's attempts to provide Bob with the state $|\psi\rangle$ to a halt, it was realised by Bennett *et al.*[1] that precisely this projection postulate enables teleportation of $|\psi\rangle$ from Alice to Bob. During teleportation Alice will destroy the quantum state at hand while Bob receives the quantum state, with neither Alice nor Bob obtaining information about the state $|\psi\rangle$. A key role in the teleportation scheme is played by an entangled ancillary pair of particles which will be initially shared by Alice and Bob.

Suppose particle 1 which Alice wants to teleport is in the initial state $|\psi\rangle_1 = \alpha|\leftrightarrow\rangle_1 + \beta|\updownarrow\rangle_1$ (Fig. 1a), and the entangled pair of particles 2 and 3 shared by Alice and Bob is in the state:

$$|\psi^-\rangle_{23} = \frac{1}{\sqrt{2}}\left(|\leftrightarrow\rangle_2|\updownarrow\rangle_3 - |\updownarrow\rangle_2|\leftrightarrow\rangle_3\right) \quad (2)$$

That entangled pair is a single quantum system in an equal superposition of the states $|\leftrightarrow\rangle_2|\updownarrow\rangle_3$ and $|\updownarrow\rangle_2|\leftrightarrow\rangle_3$. The entangled state contains no information on the individual particles; it only indicates that the two particles will be in opposite states. The important property of an entangled pair is that as soon as a measurement on one of the particles projects it, say, onto $|\leftrightarrow\rangle$ the state of the other one is determined to be $|\updownarrow\rangle$, and vice versa. How could a measurement on one of the particles instantaneously influence the state of the other particle, which can be arbitrarily far away? Einstein, among many other distinguished physicists, could simply not accept this "spooky action at a distance". But this property of entangled states has now been demonstrated by numerous experiments (for reviews, see refs 9, 10).

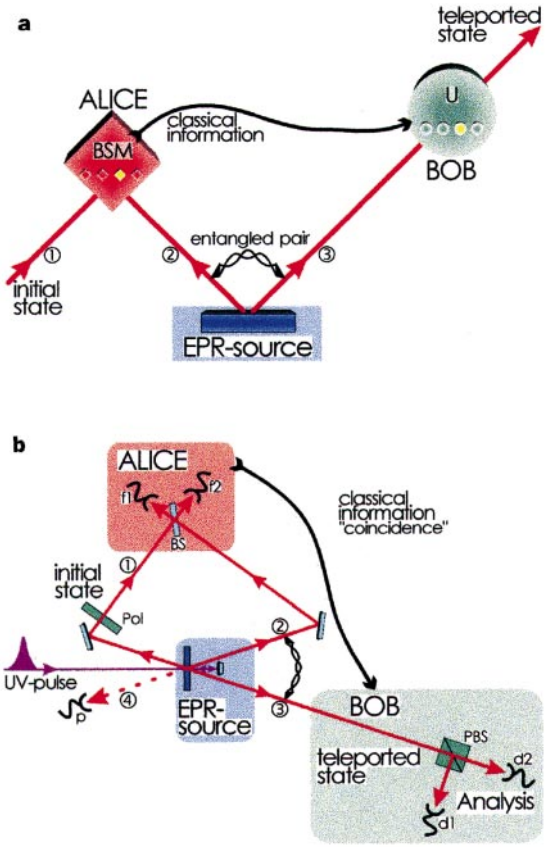


Figure 1 Scheme showing principles involved in quantum teleportation (**a**) and the experimental set-up (**b**). **a**, Alice has a quantum system, particle 1, in an initial state which she wants to teleport to Bob. Alice and Bob also share an ancillary entangled pair of particles 2 and 3 emitted by an Einstein–Podolsky–Rosen (EPR) source. Alice then performs a joint Bell-state measurement (BSM) on the initial particle and one of the ancillaries, projecting them also onto an entangled state. After she has sent the result of her measurement as classical information to Bob, he can perform a unitary transformation (U) on the other ancillary particle resulting in it being in the state of the original particle. **b**, A pulse of ultraviolet radiation passing through a nonlinear crystal creates the ancillary pair of photons 2 and 3. After retroflection during its second passage through the crystal the ultraviolet pulse creates another pair of photons, one of which will be prepared in the initial state of photon 1 to be teleported, the other one serving as a trigger indicating that a photon to be teleported is under way. Alice then looks for coincidences after a beam splitter BS where the initial photon and one of the ancillaries are superposed. Bob, after receiving the classical information that Alice obtained a coincidence count in detectors f1 and f2 identifying the $|\psi^-\rangle_{12}$ Bell state, knows that his photon 3 is in the initial state of photon 1 which he then can check using polarization analysis with the polarizing beam splitter PBS and the detectors d1 and d2. The detector p provides the information that photon 1 is under way.

The teleportation scheme works as follows. Alice has the particle 1 in the initial state $|\psi\rangle_1$ and particle 2. Particle 2 is entangled with particle 3 in the hands of Bob. The essential point is to perform a specific measurement on particles 1 and 2 which projects them onto the entangled state:

$$|\psi^-\rangle_{12} = \frac{1}{\sqrt{2}}\left(|\leftrightarrow\rangle_1|\updownarrow\rangle_2 - |\updownarrow\rangle_1|\leftrightarrow\rangle_2\right) \quad (3)$$

This is only one of four possible maximally entangled states into which any state of two particles can be decomposed. The projection of an arbitrary state of two particles onto the basis of the four states is called a Bell-state measurement. The state given in equation (3) distinguishes itself from the three other maximally entangled states by the fact that it changes sign upon interchanging particle 1 and particle 2. This unique antisymmetric feature of $|\psi^-\rangle_{12}$ will play an important role in the experimental identification, that is, in measurements of this state.

Quantum physics predicts[1] that once particles 1 and 2 are projected into $|\psi^-\rangle_{12}$, particle 3 is instantaneously projected into the initial state of particle 1. The reason for this is as follows. Because we observe particles 1 and 2 in the state $|\psi^-\rangle_{12}$ we know that whatever the state of particle 1 is, particle 2 must be in the opposite state, that is, in the state orthogonal to the state of particle 1. But we had initially prepared particle 2 and 3 in the state $|\psi^-\rangle_{23}$, which means that particle 2 is also orthogonal to particle 3. This is only possible if particle 3 is in the same state as particle 1 was initially. The final state of particle 3 is therefore:

$$|\psi\rangle_3 = \alpha|\leftrightarrow\rangle_3 + \beta|\updownarrow\rangle_3 \quad (4)$$

We note that during the Bell-state measurement particle 1 loses its identity because it becomes entangled with particle 2. Therefore the state $|\psi\rangle_1$ is destroyed on Alice's side during teleportation.

This result (equation (4)) deserves some further comments. The transfer of quantum information from particle 1 to particle 3 can happen over arbitrary distances, hence the name teleportation. Experimentally, quantum entanglement has been shown[11] to survive over distances of the order of 10 km. We note that in the teleportation scheme it is not necessary for Alice to know where Bob is. Furthermore, the initial state of particle 1 can be completely unknown not only to Alice but to anyone. It could even be quantum mechanically completely undefined at the time the Bell-state measurement takes place. This is the case when, as already remarked by Bennett *et al.*[1], particle 1 itself is a member of an entangled pair and therefore has no well-defined properties on its own. This ultimately leads to entanglement swapping[12,13].

It is also important to notice that the Bell-state measurement does not reveal any information on the properties of any of the particles. This is the very reason why quantum teleportation using coherent two-particle superpositions works, while any measurement on one-particle superpositions would fail. The fact that no information whatsoever is gained on either particle is also the reason why quantum teleportation escapes the verdict of the no-cloning theorem[14]. After successful teleportation particle 1 is not available in its original state any more, and therefore particle 3 is not a clone but is really the result of teleportation.

A complete Bell-state measurement can not only give the result that the two particles 1 and 2 are in the antisymmetric state, but with equal probabilities of 25% we could find them in any one of the three other entangled states. When this happens, particle 3 is left in one of three different states. It can then be brought by Bob into the original state of particle 1 by an accordingly chosen transformation, independent of the state of particle 1, after receiving via a classical communication channel the information on which of the Bell-state

results was obtained by Alice. Yet we note, with emphasis, that even if we chose to identify only one of the four Bell states as discussed above, teleportation is successfully achieved, albeit only in a quarter of the cases.

Experimental realization

Teleportation necessitates both production and measurement of entangled states; these are the two most challenging tasks for any experimental realization. Thus far there are only a few experimental techniques by which one can prepare entangled states, and there exist no experimentally realized procedures to identify all four Bell states for any kind of quantum system. However, entangled pairs of photons can readily be generated and they can be projected onto at least two of the four Bell states.

We produced the entangled photons 2 and 3 by parametric down-conversion. In this technique, inside a nonlinear crystal, an incoming pump photon can decay spontaneously into two photons which, in the case of type II parametric down-conversion, are in the state given by equation (2) (Fig. 2)[6].

To achieve projection of photons 1 and 2 into a Bell state we have to make them indistinguishable. To achieve this indistinguishability we superpose the two photons at a beam splitter (Fig. 1b). Then if they are incident one from each side, how can it happen that they emerge still one on each side? Clearly this can happen if they are either both reflected or both transmitted. In quantum physics we have to superimpose the amplitudes for these two possibilities. Unitarity implies that the amplitude for both photons being reflected obtains an additional minus sign. Therefore, it seems that the two processes cancel each other. This is, however, only true for a symmetric input state. For an antisymmetric state, the two possibilities obtain another relative minus sign, and therefore they constructively interfere[15,16]. It is thus sufficient for projecting photons 1 and 2 onto the antisymmetric state $|\psi^-\rangle_{12}$ to place detectors in each of the outputs of the beam splitter and to register simultaneous detections (coincidence)[17–19].

To make sure that photons 1 and 2 cannot be distinguished by their arrival times, they were generated using a pulsed pump beam and sent through narrow-bandwidth filters producing a coherence time much longer than the pump pulse length[20]. In the experiment, the pump pulses had a duration of 200 fs at a repetition rate of 76 MHz. Observing the down-converted photons at a wavelength of 788 nm and a bandwidth of 4 nm results in a coherence time of 520 fs. It should be mentioned that, because photon 1 is also produced as part of an entangled pair, its partner can serve to indicate that it was emitted.

How can one experimentally prove that an unknown quantum state can be teleported? First, one has to show that teleportation works for a (complete) basis, a set of known states into which any other state can be decomposed. A basis for polarization states has just two components, and in principle we could choose as the basis horizontal and vertical polarization as emitted by the source. Yet this would not demonstrate that teleportation works for any general superposition, because these two directions are preferred directions in our experiment. Therefore, in the first demonstration we choose as the basis for teleportation the two states linearly polarized at −45° and +45° which are already superpositions of the horizontal and vertical polarizations. Second, one has to show that teleportation works for superpositions of these base states. Therefore we also demonstrate teleportation for circular polarization.

Results

In the first experiment photon 1 is polarized at 45°. Teleportation should work as soon as photon 1 and 2 are detected in the $|\psi^-\rangle_{12}$ state, which occurs in 25% of all possible cases. The $|\psi^-\rangle_{12}$ state is identified by recording a coincidence between two detectors, f1 and f2, placed behind the beam splitter (Fig. 1b).

If we detect a f1f2 coincidence (between detectors f1 and f2), then photon 3 should also be polarized at 45°. The polarization of photon 3 is analysed by passing it through a polarizing beam splitter selecting +45° and −45° polarization. To demonstrate teleportation, only detector d2 at the +45° output of the polarizing beam splitter should click (that is, register a detection) once detectors f1 and f2 click. Detector d1 at the −45° output of the polarizing beam splitter should not detect a photon. Therefore, recording a three-fold coincidence d2f1f2 (+45° analysis) together with the absence of a three-fold coincidence d1f1f2 (−45° analysis) is a proof that the polarization of photon 1 has been teleported to photon 3.

To meet the condition of temporal overlap, we change in small

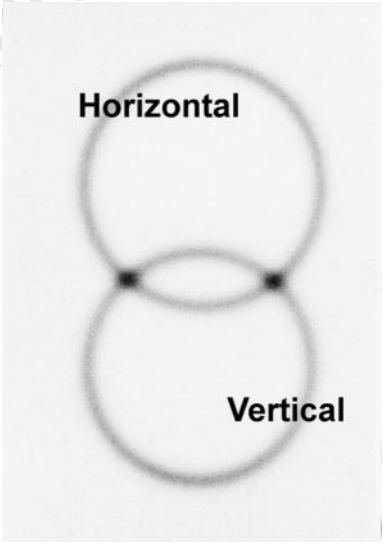


Figure 2 Photons emerging from type II down-conversion (see text). Photograph taken perpendicular to the propagation direction. Photons are produced in pairs. A photon on the top circle is horizontally polarized while its exactly opposite partner in the bottom circle is vertically polarized. At the intersection points their polarizations are undefined; all that is known is that they have to be different, which results in entanglement.

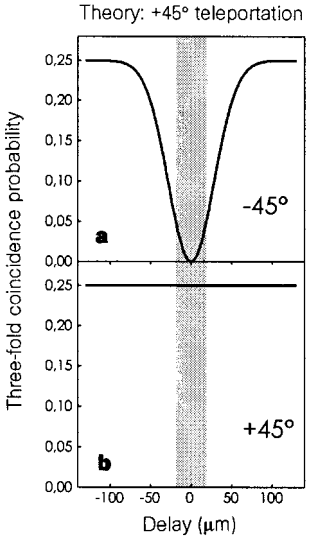


Figure 3 Theoretical prediction for the three-fold coincidence probability between the two Bell-state detectors (f1, f2) and one of the detectors analysing the teleported state. The signature of teleportation of a photon polarization state at +45° is a dip to zero at zero delay in the three-fold coincidence rate with the detector analysing –45° (d1f1f2) (**a**) and a constant value for the detector analysis +45° (d2f1f2) (**b**). The shaded area indicates the region of teleportation.

steps the arrival time of photon 2 by changing the delay between the first and second down-conversion by translating the retroflection mirror (Fig. 1b). In this way we scan into the region of temporal overlap at the beam splitter so that teleportation should occur.

Outside the region of teleportation, photon 1 and 2 each will go either to f1 or to f2 independent of one another. The probability of having a coincidence between f1 and f2 is therefore 50%, which is twice as high as inside the region of teleportation. Photon 3 should not have a well-defined polarization because it is part of an entangled pair. Therefore, d1 and d2 have both a 50% chance of receiving photon 3. This simple argument yields a 25% probability both for the −45° analysis (d1f1f2 coincidences) and for the +45° analysis (d2f1f2 coincidences) outside the region of teleportation. Figure 3 summarizes the predictions as a function of the delay. Successful teleportation of the +45° polarization state is then characterized by a decrease to zero in the −45° analysis (Fig. 3a), and by a constant value for the +45° analysis (Fig. 3b).

The theoretical prediction of Fig. 3 may easily be understood by realizing that at zero delay there is a decrease to half in the coincidence rate for the two detectors of the Bell-state analyser, f1 and f2, compared with outside the region of teleportation. Therefore, if the polarization of photon 3 were completely uncorrelated to the others the three-fold coincidence should also show this dip to half. That the right state is teleported is indicated by the fact that the dip goes to zero in Fig. 3a and that it is filled to a flat curve in Fig. 3b.

We note that equally as likely as the production of photons 1, 2 and 3 is the emission of two pairs of down-converted photons by a single source. Although there is no photon coming from the first source (photon 1 is absent), there will still be a significant contribution to the three-fold coincidence rates. These coincidences have nothing to do with teleportation and can be identified by blocking the path of photon 1.

The probability for this process to yield spurious two- and three-fold coincidences can be estimated by taking into account the experimental parameters. The experimentally determined value for the percentage of spurious three-fold coincidences is 68% ± 1%. In the experimental graphs of Fig. 4 we have subtracted the experimentally determined spurious coincidences.

Table 1 Visibility of teleportation in three fold coincidences

Polarization	Visibility
+45°	0.63 ± 0.02
–45°	0.64 ± 0.02
0°	0.66 ± 0.02
90°	0.61 ± 0.02
Circular	0.57 ± 0.02

The experimental results for teleportation of photons polarized under +45° are shown in the left-hand column of Fig. 4; Fig. 4a and b should be compared with the theoretical predictions shown in Fig. 3. The strong decrease in the −45° analysis, and the constant signal for the +45° analysis, indicate that photon 3 is polarized along the direction of photon 1, confirming teleportation.

The results for photon 1 polarized at −45° demonstrate that teleportation works for a complete basis for polarization states (right-hand column of Fig. 4). To rule out any classical explanation for the experimental results, we have produced further confirmation that our procedure works by additional experiments. In these experiments we teleported photons linearly polarized at 0° and at 90°, and also teleported circularly polarized photons. The experimental results are summarized in Table 1, where we list the visibility of the dip in three-fold coincidences, which occurs for analysis orthogonal to the input polarization.

As mentioned above, the values for the visibilities are obtained after subtracting the offset caused by spurious three-fold coincidences. These can experimentally be excluded by conditioning the three-fold coincidences on the detection of photon 4, which effectively projects photon 1 into a single-particle state. We have performed this four-fold coincidence measurement for the case of teleportation of the +45° and +90° polarization states, that is, for two non-orthogonal

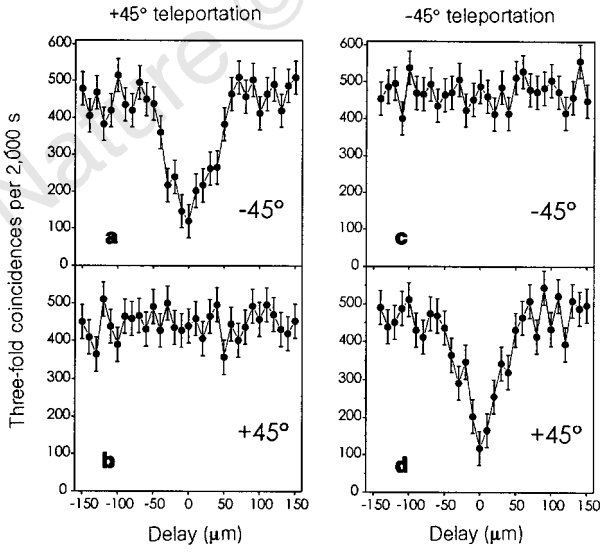


Figure 4 Experimental results. Measured three-fold coincidence rates d1f1f2 (–45°) and d2f1f2 (+45°) in the case that the photon state to be teleported is polarized at +45° (**a** and **b**) or at –45° (**c** and **d**). The coincidence rates are plotted as function of the delay between the arrival of photon 1 and 2 at Alice's beam splitter (see Fig. 1b). The three-fold coincidence rates are plotted after subtracting the spurious three-fold contribution (see text). These data, compared with Fig. 3, together with similar ones for other polarizations (Table 1) confirm teleportation for an arbitrary state.

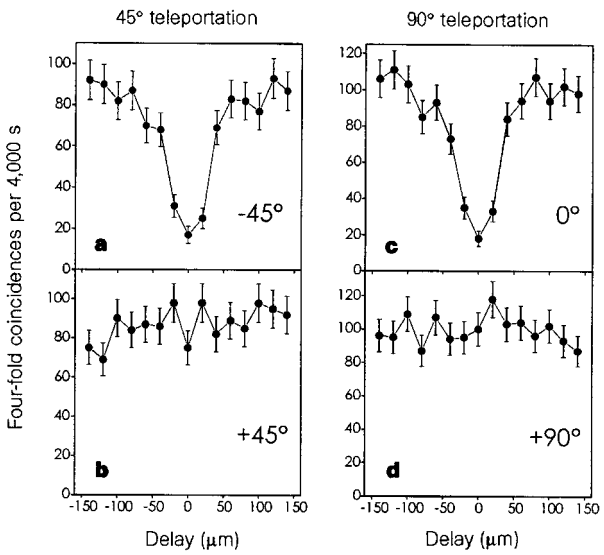


Figure 5 Four-fold coincidence rates (without background subtraction). Conditioning the three-fold coincidences as shown in Fig. 4 on the registration of photon 4 (see Fig. 1b) eliminates the spurious three-fold background. **a** and **b** show the four-fold coincidence measurements for the case of teleportation of the +45° polarization state; **c** and **d** show the results for the +90° polarization state. The visibilities, and thus the polarizations of the teleported photons, obtained without any background subtraction are 70% ± 3%. These results for teleportation of two non-orthogonal states prove that we have demonstrated teleportation of the quantum state of a single photon.

states. The experimental results are shown in Fig. 5. Visibilities of 70% ± 3% are obtained for the dips in the orthogonal polarization states. Here, these visibilities are directly the degree of polarization of the teleported photon in the right state. This proves that we have demonstrated teleportation of the quantum state of a single photon.

The next steps

In our experiment, we used pairs of polarization entangled photons as produced by pulsed down-conversion and two-photon interferometric methods to transfer the polarization state of one photon onto another one. But teleportation is by no means restricted to this system. In addition to pairs of entangled photons or entangled atoms[7,21], one could imagine entangling photons with atoms, or phonons with ions, and so on. Then teleportation would allow us to transfer the state of, for example, fast-decohering, short-lived particles, onto some more stable systems. This opens the possibility of quantum memories, where the information of incoming photons is stored on trapped ions, carefully shielded from the environment.

Furthermore, by using entanglement purification[22]—a scheme of improving the quality of entanglement if it was degraded by decoherence during storage or transmission of the particles over noisy channels—it becomes possible to teleport the quantum state of a particle to some place, even if the available quantum channels are of very poor quality and thus sending the particle itself would very probably destroy the fragile quantum state. The feasibility of preserving quantum states in a hostile environment will have great advantages in the realm of quantum computation. The teleportation scheme could also be used to provide links between quantum computers.

Quantum teleportation is not only an important ingredient in quantum information tasks; it also allows new types of experiments and investigations of the foundations of quantum mechanics. As any arbitrary state can be teleported, so can the fully undetermined state of a particle which is member of an entangled pair. Doing so, one transfers the entanglement between particles. This allows us not only to chain the transmission of quantum states over distances, where decoherence would have already destroyed the state completely, but it also enables us to perform a test of Bell's theorem on particles which do not share any common past, a new step in the investigation of the features of quantum mechanics. Last but not least, the discussion about the local realistic character of nature could be settled firmly if one used features of the experiment presented here to generate entanglement between more than two spatially separated particles[23,24]. □

Received 16 October; accepted 18 November 1997.

1. Bennett, C. H. *et al*. Teleporting an unknown quantum state via dual classic and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70,** 1895–1899 (1993).
2. Schrödinger, E. Die gegenwärtige Situation in der Quantenmechanik. *Naturwissenschaften* **23,** 807–812; 823–828; 844–849 (1935).
3. Bennett, C. H. Quantum information and computation. *Phys. Today* **48(10),** 24–30, October (1995).
4. Bennett, C. H., Brassard, G. & Ekert, A. K. Quantum Cryptography. *Sci. Am.* **267(4),** 50–57, October (1992).
5. Mattle, K., Weinfurter, H., Kwiat, P. G. & Zeilinger, A. Dense coding in experimental quantum communication. *Phys. Rev. Lett.* **76,** 4656–4659 (1996).
6. Kwiat, P. G. *et al*. New high intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett.* **75,** 4337–4341 (1995).
7. Hagley, E. *et al*. Generation of Einstein-Podolsky-Rosen pairs of atoms. *Phys. Rev. Lett.* **79,** 1–5 (1997).
8. Schumacher, B. Quantum coding. *Phys. Rev. A* **51,** 2738–2747 (1995).
9. Clauser, J. F. & Shimony, A. Bell's theorem: experimental tests and implications. *Rep. Prog. Phys.* **41,** 1881–1927 (1978).
10. Greenberger, D. M., Horne, M. A. & Zeilinger, A. Multiparticle interferometry and the superposition principle. *Phys. Today* August, 22–29 (1993).
11. Tittel, W. *et al*. Experimental demonstration of quantum-correlations over more than 10 kilometers. *Phys. Rev. Lett.* (submitted).
12. Zukowski, M., Zeilinger, A., Horne, M. A. & Ekert, A. "Event-ready-detectors" Bell experiment via entanglement swapping. *Phys. Rev. Lett.* **71,** 4287–4290 (1993).
13. Bose, S., Vedral, V. & Knight, P. L. A multiparticle generalization of entanglement swapping. preprint.
14. Wootters, W. K. & Zurek, W. H. A single quantum cannot be cloned. *Nature* **299,** 802–803 (1982).
15. Loudon, R. *Coherence and Quantum Optics VI* (eds Everly, J. H. & Mandel, L.) 703–708 (Plenum, New York, 1990).
16. Zeilinger, A., Bernstein, H. J. & Horne, M. A. Information transfer with two-state two-particle quantum systems. *J. Mod. Optics* **41,** 2375–2384 (1994).
17. Weinfurter, H. Experimental Bell-state analysis. *Europhys. Lett.* **25,** 559–564 (1994).
18. Braunstein, S. L. & Mann, A. Measurement of the Bell operator and quantum teleportation. *Phys. Rev. A* **51,** R1727–R1730 (1995).
19. Michler, M., Mattle, K., Weinfurter, H. & Zeilinger, A. Interferometric Bell-state analysis. *Phys. Rev. A* **53,** R1209–R1212 (1996).
20. Zukowski, M., Zeilinger, A. & Weinfurter, H. Entangling photons radiated by independent pulsed sources. *Ann. NY Acad. Sci.* **755,** 91–102 (1995).
21. Fry, E. S., Walther, T. & Li, S. Proposal for a loophole-free test of the Bell inequalities. *Phys. Rev. A* **52,** 4381–4395 (1995).
22. Bennett, C. H. *et al*.Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.* **76,** 722–725 (1996).
23. Greenberger, D. M., Horne, M. A., Shimony, A. & Zeilinger, A. Bell's theorem without inequalities. *Am. J. Phys.* **58,** 1131–1143 (1990).
24. Zeilinger, A., Horne, M. A., Weinfurter, H. & Zukowski, M. Three particle entanglements from two entangled pairs. *Phys. Rev. Lett.* **78,** 3031–3034 (1997).

Acknowledgements. We thank C. Bennett, I. Cirac, J. Rarity, W. Wootters and P. Zoller for discussions, and M. Zukowski for suggestions about various aspects of the experiments. This work was supported by the Austrian Science Foundation FWF, the Austrian Academy of Sciences, the TMR program of the European Union and the US NSF.

Correspondence and requests for materials should be addressed to D.B. (e-mail: Dik.Bouwmeester@uibk.ac.at).

9.2 Quantum dense coding

Can we make use of entanglement to increase the bandwidth of a communication channel?

Bennett introduced in 1992 the concept of quantum dense coding to communicate 4 bits while sending only one photon from Alice to Bob, this requires the photon traveling from Alice to Bob to be entangled with a second photon that travels to Bob.

Figure 9.2: In quantum dense coding, one photon from an entangled pair is sent to Alice who can control its polarization, the other goes directly to Bob.

Paradox: we can only control the polarization of one photon (=1 bit of information) but we can exchange 4 bits of information. Our EPR source generates

$$|\Psi\rangle = |H_A H_B\rangle + |V_A V_B\rangle$$

Alice can perform any of 4 transformations on her photon:

$$I[|H_A H_B\rangle + |V_A V_B\rangle] = |H_A H_B\rangle + |V_A V_B\rangle$$

The I transformation corresponds to doing nothing: very easy to implement.

$$X[|H_A H_B\rangle + |V_A V_B\rangle] = |V_A H_B\rangle + |H_A V_B\rangle$$

The X transformation corresponds to rotating the polarization of photon A by 90 degrees. This can be implemented with a half-wave plate at the right angle.

$$Y[|H_A H_B\rangle + |V_A V_B\rangle] = |V_A H_B\rangle - |H_A V_B\rangle$$

The Y transformation corresponds to rotating the polarization of photon A by 90 degrees and introducing a phase shift.

$$Z[|H_A H_B\rangle + |V_A V_B\rangle] = |H_A H_B\rangle - |V_A V_B\rangle$$

The Z transformation corresponds to introducing a phase shift.

Alice does no measurements, she only performs a transformation on one photon and sends her photon to Bob. Bob measures in which of the four possible Bell states the entangled pair is. Bob then finds out which of the four transformations Alice applied, this gives 4 possible values and hence 2 bits of information. But only one photon travelled from Alice to Bob!

But can it be done? Bob needs to identify which of the four Bell states he gets in one shot (one single measurement on only one photon pair). While possible in principle, it has not yet been done.

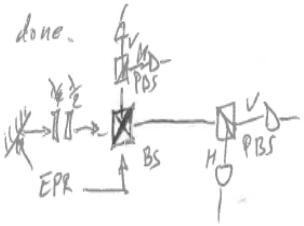


Figure 9.3: Implementation of quantum dense coding.

The photons leave the beam splitter in the same output (HOM) or in each output. Only $|\Psi\rangle^- = \frac{1}{\sqrt{2}}[|H_A V_B\rangle - |V_A H_B\rangle]$ is anti-symmetric, only this state gives photons in each port. What counts here is the symmetry of the state that has to be taken into account with the beam splitter transformation. For the 3 other states, both photons come out in the same port of the beam splitter. We can therefore identify $|\Psi\rangle^-$ as this state will result in one detection event in each arm.

$|\Psi\rangle^+ = \frac{1}{\sqrt{2}}[|H_A V_B\rangle + |V_A H_B\rangle]$ can be distinguished from the others with the addition of polarizing beam splitters (PBS). $|\Phi\rangle^+$and $|\Phi\rangle^-$ give the same outcome and cannot be distinguished, we can only guess. This enables 1.5 bits per photon to be transferred from A to B. Note that to measure photon number (that is to distinguish one from two photons) we can stack detectors:

Figure 9.4: Chaining beam splitters and detectors can help to measure photon number to distinguish a one photon state from a two photon state for example.

Dense Coding in Experimental Quantum Communication

Klaus Mattle,[1] Harald Weinfurter,[1] Paul G. Kwiat,[1,2] and Anton Zeilinger[1]
[1]*Institut für Experimentalphysik, Universität Innsbruck, A-6020 Innsbruck, Austria*
[2]*Los Alamos National Laboratory, P-23, MS-H803, Los Alamos, New Mexico 87545*
(Received 22 November 1995)

Classically, sending more than one bit of information requires manipulation of more than one two-state particle. We demonstrate experimentally that one can transmit one of three messages, i.e., 1 "trit" ≈ 1.58 bit, by manipulating only one of two entangled particles. The increased channel capacity is proven by transmitting ASCII characters in five trits instead of the usual 8 bits. [S0031-9007(96)00478-4]

PACS numbers: 03.65.–w, 89.70.+c

While the strikingly nonclassical properties of entangled states lead to more and more novel demonstrations of fundamental properties of quantum mechanical systems [1], the young field of quantum information exploits such entangled quantum states for new types of information transmission and information processing [2]. In the present paper, we report the first experimental realization of quantum communication, verifying the increased capacity of a quantum information channel by "quantum dense coding." The scheme, theoretically proposed by Bennett and Wiesner [3], utilizes two entangled two-state systems. Suppose that, as was the case in our experiment, the two states are horizontal (H) and vertical (V) polarizations of a photon. Then, classically, the four possible polarization combinations for a pair of photons are HH, HV, VH, and VV. Identifying each with different information implies that we can encode two bits of information by manipulating both photons.

Quantum mechanics allows one to encode the information also in superpositions of the classical combinations, an appropriate basis is formed by the maximally entangled Bell states

$$\begin{aligned} |\Psi^+\rangle &= (|H\rangle|V\rangle + |V\rangle|H\rangle)/\sqrt{2}, \\ |\Psi^-\rangle &= (|H\rangle|V\rangle - |V\rangle|H\rangle)/\sqrt{2}, \\ |\Phi^+\rangle &= (|H\rangle|H\rangle + |V\rangle|V\rangle)/\sqrt{2}, \\ |\Phi^-\rangle &= (|H\rangle|H\rangle - |V\rangle|V\rangle)/\sqrt{2}. \end{aligned} \tag{1}$$

The Hilbert space spanned by these orthogonal states is still four dimensional, implying that using the two particles we again can encode 2 bits of information, yet, now by manipulating only *one* of the two particles. This is achieved in the following quantum communication scheme for transmitting 2 bits of information per two state: Initially, Alice and Bob each obtain one particle of an entangled pair, say, in the state $|\Psi^+\rangle$. Bob then performs one out of four possible unitary transformations on his particle alone. For polarized photons, four such transformations are (i) identity operation; (ii) polarization flip ($|H\rangle \rightarrow |V\rangle$ and $|V\rangle \rightarrow |H\rangle$, changing the two-photon state to $|\Phi^+\rangle$); (iii) polarization-dependent phase shift (differing by π for $|H\rangle$ and $|V\rangle$ and transforming to $|\Psi^-\rangle$); and (iv) rotation and phase shift together (giving the two-photon state $|\Phi^-\rangle$). Since the four manipulations result in the four orthogonal Bell states, four distinguishable messages, i.e., 2 bits of information, can be sent via Bob's two-state particle to Alice, who finally reads the encoded information by determining the Bell state of the two-particle system.

This scheme enhances the information capacity of the transmission channel to 2 bits compared to the classical maximum of 1 bit [4]. The problem clearly is how to identify the four Bell states. Unique determination of the state would be possible by coupling the two particles in a similar way as in certain quantum logic operations. However, reversing the process of down-conversion and combining two photons conditionally in a nonlinear crystal [3] has to fail due to low efficiency ($\approx 10^{-6}$). Also, cavity-QED techniques [5] still lack the necessary strong coupling, and the recently developed ion-trap quantum logic gates [6] impose other severe restrictions for the present application. On the other hand, two-particle interferometry can provide a solution to this problem [7]. Different interference effects allow one to identify two of the four Bell states, with the other two giving the same, third, measurement signal. Such an interferrometric state analyzer therefore allows Alice to read three different messages sent via Bob's particle.

In this Letter we report the realization of quantum dense coding transmission with entangled photon pairs as produced by parametric down-conversion. We choose polarization entanglement [8] because of the higher stability and the more reliable methods for manipulating polarized beams, as opposed to experimental Bell-state analysis of momentum-entangled photons [9]. The reduction of phase drifts, and especially the simpler configuration of the Bell-state analyzer, results in better interference visibility.

The experiment consists of three distinct parts (Fig. 1): the EPR source generating entangled photons in a well-defined state; Bob's station for encoding the messages by a unitary transformation of his particle; and, finally, Alice's Bell-state analyzer to read the signal sent by Bob. The polarization-entangled photons were produced by

 0031-9007/96/76(25)/4656(4)$10.00

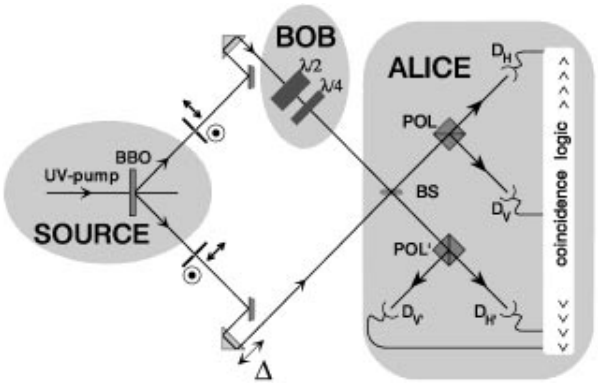


FIG. 1. Experimental setup for quantum dense coding. Because of the nature of the Si-avalanche photodiodes, the extension shown in the inset of Fig. 4 is necessary for identifying two-photon states in one of the outputs.

degenerate noncollinear type-II down-conversion in a nonlinear BBO crystal. A UV beam ($\lambda = 351$ nm) from an argon-ion laser is down-converted into pairs of photons ($\lambda = 702$ nm) with orthogonal polarization. We obtained the entangled state $|\Psi^+\rangle$ after compensation of birefringence in the BBP crystal along two distinct emission directions (carefully selected by 2 mm irises, 1.5 m away from the crystal [10]). One beam was first directed to Bob's encoding station, the other directly to Alice's Bell-state analyzer; in the alignment procedure optical trombones were employed to equalize the path lengths to well within the coherence length of the down-converted photons ($\ell_c \approx 100$ μm), in order to observe the two-photon interference.

For polarization encoding, the necessary transformation of Bob's particle was performed using a half-wave retardation plate for changing the polarization and a quarter-wave plate to generate the polarization-dependent phase shift [11]. The beam manipulated in this way in Bob's encoding station was then combined with the other beam at Alice's Bell-state analyzer. It consisted of a single beam splitter followed by two-channel polarizers in each of its outputs and proper coincidence analysis between four single photon detectors.

Such a configuration allows one to distinguish between the Bell states due to the different outcomes of the interference at the beam splitter and the subsequent polarization analysis. The spatial part of the state determines the photon statistics behind the (polarization insensitive) beam splitter. This results either in both photons leaving the beam splitter via the same output beam for a symmetric spatial part or in one photon exiting into each output for an antisymmetric spatial component of the state [12]. Since only the state $|\Psi^-\rangle$ has an antisymmetric spatial part, only this state will be registered by coincidence detection between the different outputs of the beam splitter (i.e., coincidence between detectors D_H and $D_{V'}$ or between $D_{H'}$ and D_V). For the remaining three states, both photons exit into the same output port of the beam splitter. The state $|\Psi^+\rangle$ can easily be distinguished from the other two due to the different polarizations of the two photons, giving, behind the two-channel polarizer, a coincidence between detectors D_H and D_V or between $D_{H'}$ and $D_{V'}$. The two states $|\Phi^+\rangle$ and $|\Phi^-\rangle$ both result in a two-photon state being absorbed by a single detector and thus cannot be distinguished. Table I gives an overview of the different manipulations and detection probabilities of Bob's encoder and Alice's receiver.

The experiments were performed by first setting the output state of the source such that the state $|\Psi^+\rangle$ left Bob's encoder when both retardation plates were set to vertical orientation, the other Bell states could then be generated with the respective settings (Table I). To characterize the interference observable at Alice's Bell-state analyzer, we varied the path length difference Δ of the two beams with the optical trombone. For $\Delta \gg \ell_c$ no interference occurs, and one obtains classical statistics for the coincidence count rates at the detectors. For optimal path-length tuning ($\Delta = 0$), interference enables one to read the encoded information. Figures 2 and 3 show the dependence of the coincidence rates C_{HV} (●) and $C_{HV'}$ (○) on the path length difference for $|\Psi^+\rangle$ and $|\Psi^-\rangle$, respectively (the rates $C_{H'V'}$ and $C_{H'V}$ display analogous behavior; we use the notation C_{AB} for the coincidence rate between detectors D_A and D_B). At $\Delta = 0$, C_{HV} reaches its maximum for $|\Psi^+\rangle$ (Fig. 2) and vanishes (aside from noise) for $|\Psi^-\rangle$ (Fig. 3). $C_{HV'}$ displays the opposite dependence and clearly signifies $|\Psi^-\rangle$. The results of these measurements imply that, if both photons are detected, we can identify the state $|\Psi^+\rangle$ with a reliability of 95% and the state $|\Psi^-\rangle$ with 93%.

The performance of the dense coding transmission is influenced not only by the quality of the interference

TABLE I. Overview of possible manipulations and detection events of the quantum dense coding experiment with correlated photons (we use h to denote the state of a photon in the mode towards detector D_H, etc.).

Bob's setting $\lambda/2$	Bob's setting $\lambda/4$	State sent	State at output of Bell-state analyzer	Alice's registration events
0°	0°	$\lvert\Psi^+\rangle$	$\{hv + h'v' + vh + v'h'\}/2$	Coincidence between D_H *and* D_V or $D_{H'}$ *and* $D_{V'}$
0°	90°	$\lvert\Psi^-\rangle$	$\{hv' - h'v' + v'h - vh'\}/2$	Coincidence between D_H *and* $D_{V'}$ or $D_{H'}$ *and* D_V
45°	0°	$\lvert\Phi^+\rangle$	$\{hh + vv + h'h' + v'v'\}/2$	2 photons in either D_H, D_V, $D_{H'}$, or $D_{V'}$
45°	90°	$\lvert\Phi^-\rangle$	$\{hh - vv + h'h' + v'v'\}/2$	2 photons in either D_H, D_V, $D_{H'}$, or $D_{V'}$

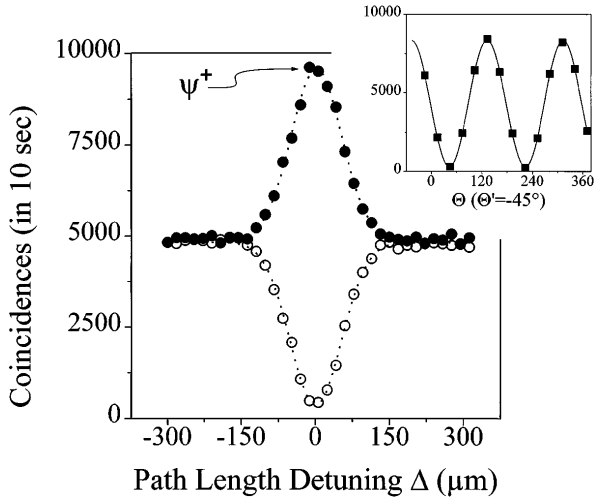


FIG. 2. Coincidence rates C_{HV} (●) and $C_{HV'}$ (○) as functions of the path length difference Δ when the state $|\Psi^+\rangle$ is transmitted. For perfect tuning ($\Delta = 0$), constructive interference occurs for C_{HV}, allowing identification of the state sent. The inset shows a correlation measurement with the beam splitter of the Bell-state analyzer removed to check the quality of the transmitted state. (θ, θ' are the orientations of half-wave plates, not shown in Fig. 1, in front of the polarizers POL or POL′.)

alignment, but also by the quality of the states sent by Bob. In order to evaluate the latter the beam splitter was translated out of the beams. Then an Einstein-Podolsky-Rosen-Bell–type correlation measurement (using additional half-wave plates with orientation θ and θ', not shown in Fig. 1, in front of the polarizers) analyzed the degree of entanglement of the source as well as the quality of Bob's transformations (typical scans of the half-wave plate orientation θ relative to V are shown in the insets of Figs. 2 and 3 for $\theta' = 45°$). The correlations were only (1−2)% higher than the visibilities

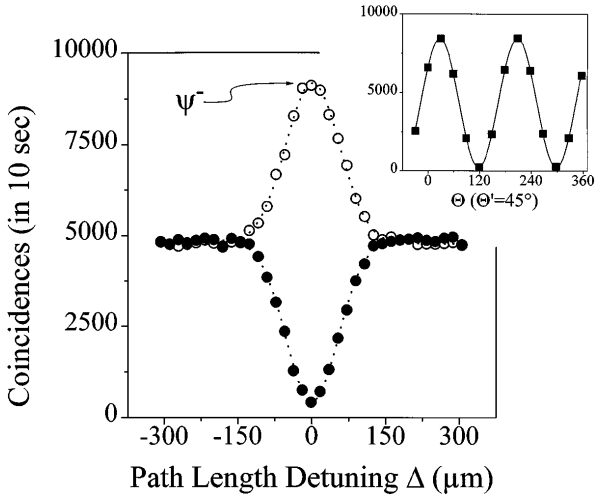


FIG. 3. Coincidence rates C_{HV} (●) and $C_{HV'}$ (○) depending on the path length difference Δ, for transmission of the state $|\Psi^-\rangle$. The constructive interference for the rate $C_{HV'}$ enables one to read the information associated with that state.

with the beam splitter in place, which means that the quality of this experiment is limited more by the quality of the entanglement of the two beams than by that of the achieved interference.

When using Si-avalanche diodes in the Geiger mode for single-photon detection, a modification of the Bell-state analyzer is necessary, since then one also has to register the two photons leaving the Bell-state analyzer for the states $|\Phi^+\rangle$ or $|\Phi^-\rangle$ via a coincidence detection [13]. One possibility is to avoid interference for these states by introducing polarization-dependent delays $\gg \ell_c$ before Alice's beam splitter, e.g., using thick quartz plates, retarding $|H\rangle$ in one beam and $|V\rangle$ in the other (the analog technique for momentum-entangled photon pairs is described in [9]). Another approach is to split the incoming two-photon state at an additional beam splitter and to detect it (with 50% likelihood) by a coincidence count between detectors in each output (inset of Fig. 4). For the purpose of this proof-of-principle demonstration we put such a configuration only in place of detector D_H. Figure 4 shows the increase of the coincidence rate $C_{H\overline{H}}$ (□) at path length difference $\Delta = 0$, with the rates C_{HV} and $C_{HV'}$ at the background level, when Bob sends the state $|\Phi^-\rangle$. Note, however, that for both methods half of the time both photons still are absorbed by one detector; therefore, and since we inserted only one such configuration, the maximum rate for $C_{H\overline{H}}$ is about a quarter of that of C_{HV} or $C_{HV'}$ in Figs. 2 and 3.

Since we now can distinguish the three different messages, the stage is set for the quantum dense coding transmission. Figure 5 shows the various coincidence rates (normalized to the respective maximum rate of the transmitted state) when sending the ASCII codes of "KM°" (i.e., codes 75, 77, 179) in only 15 trits instead of

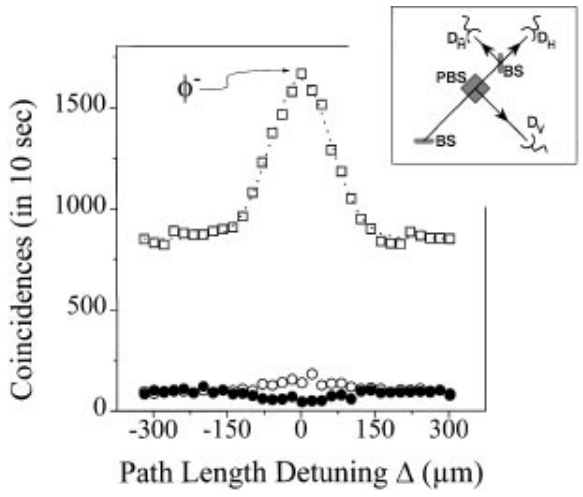


FIG. 4. Coincidence rates $C_{H\overline{H}}$ (□), C_{HV} (●), and $C_{HV'}$ (○) as functions of the path-length detuning Δ. The maximum in the rate $C_{H\overline{H}}$ signifies the transmission of a third state $|\Phi^-\rangle$ encoded in a two-state particle. The addition to the Bell-state analyzer is shown in the inset. $C_{H\overline{H}}$ is smaller by a factor of 4 compared to the rates of Figs. 2 and 3 due to a still reduced registration probability of $|\Phi^-\rangle$, see text.

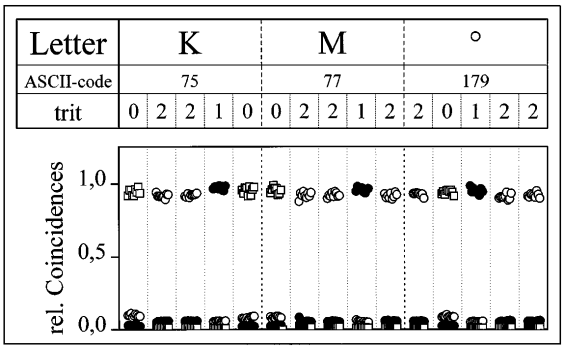


FIG. 5. "1.58 bit per photon" quantum dense coding: The ASCII codes for the letters "KM°" (i.e., 75, 77, 179) are encoded in 15 trits (with "0" $\equiv |\Phi^-\rangle \mathrel{\hat{=}} \square$, "1" $\equiv |\Psi^+\rangle \mathrel{\hat{=}} \bullet$, and "2" $\equiv |\Psi^-\rangle \mathrel{\hat{=}} \bigcirc$) instead of the 24 bits usually necessary. The data for each type of encoded state are normalized to the maximum coincidence rate for that state.

24 classical bits. From this measurement, one also obtains a signal-to-noise ratio by comparing the rates signifying the actual state with the sum of the two other registered rates. The ratios for the transmission of the three states varied due to the different visibilities of the respective interferences and were $S/N_{|\Psi^+\rangle} = 14.8$, $S/N_{|\Psi^-\rangle} = 13.0$, and $S/N_{|\Phi^-\rangle} = 8.5$.

In this Letter we have reported the realization of a quantum dense coding transmission using polarization-entangled photons. The transmission of three messages per two-state photon becomes possible by utilizing interferometric Bell-state analysis and enables an increase of the channel capacity by a factor of 1.58 [14]. The high quality of the observed interference encourages us to proceed to other quantum communication methods, such as the teleportation of quantum states, or the transfer and manipulation of entanglement in many-particle systems.

This work was supported by the Austrian Fonds zur Förderung der wissenschaftl. Forschung (S6502 and M077-PHY) and the Jubiläumsfond der österr. Nationalbank (5299).

[1] D. M. Greenberger, M. A. Horne, and A. Zeilinger, Phys. Today **46**, No. 8, 22 (1993).

[2] C. H. Bennett, Phys. Today **48**, No. 10, 24 (1995).

[3] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[4] While it is clear that this scheme enhances the information capacity of the transmission channel accessed by Bob to 2 bits, we have to notice that the channel carrying the other photon transmits 0 bits of information, thus the total transmitted information does not exceed 2 bits.

[5] M. Brune, P. Nussenzveig, F. Schmidt-Kaler, F. Bernadot, A. Maali, J. M. Raimond, and S. Haroche, Phys. Rev. Lett. **72**, 3339 (1994); Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble, Phys. Rev. Lett. **75**, 4710 (1995).

[6] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, Phys. Rev. Lett. **75**, 4714 (1995); J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).

[7] H. Weinfurter, Europhys. Lett. **25**, 559 (1994); S. L. Braunstein and A. Mann, Phys. Rev. A **51**, R1727 (1995).

[8] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. H. Shih, Phys. Rev. Lett. **75**, 4337 (1995).

[9] M. Michler, K. Mattle, H. Weinfurter, and A. Zeilinger, Phys. Rev. A **53**, R1209 (1996).

[10] The interference effects at the Bell-state analyzer showed a high sensitivity on the size and position of the irises. The reason might be that the irises still are within the Rayleigh length of the source. Fresnel diffraction has therefore to be considered [R. Chiao (private communication)].

[11] The component polarized along the axis of the quarter-wave plate is advanced only by $\pi/2$ relative to the other. Reorienting the optical axis from vertical to horizontal causes a net phase change of π between $|H\rangle$ and $|V\rangle$.

[12] A photon state has to be bosonic, i.e., symmetric upon exchange of the particles. Thus the symmetry of the spatial part of the wave function will be changed together with the spin part. This is the case when switching to and from $|\Psi^-\rangle$. For changing between the other three Bell states the spatial part of the wave function remains unchanged, giving the characteristic interference effects [C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987); A. Zeilinger, H. J. Bernstein, and M. A. Horne, J. Mod. Opt. **41**, 2375 (1994)].

[13] Because of our limited detection efficiency (≈30%), a special identification of the two-photon state is necessary. However, Si-avalanche photodiodes give the same output pulse for one or more photons, thus only a coincidence detection allows the registration of the two-photon state. Special photomultipliers can distinguish between one- and two-photon absorption, but are too inefficient at present.

[14] The achieved signal-to-noise ratio results in an actual channel capacity of 1.13 bit. This value is, of course, further reduced when using Si-avalanche single photon detectors due to their mentioned deficiencies and the limited efficiency.

Chapter 10

The Hong-Ou-Mandel effect, the quantum eraser and Wheeler's delayed choice

10.1 The beam splitter

A beam splitter has two input ports and two output ports, it can be realized in different ways. A glass plate with the right thickness of metal can act as a beam splitter, two prisms can be coupled to make a beam splitter or two waveguides (optical fibers) can be coupled over a given length to form a beam splitter. The splitting ratio is not necessarily 50-50, it can just as well be 90-10 or any other ratio.

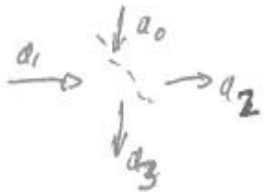


Figure 10.1: A beam splitter has two inputs and two outputs.

There is always a phase shift between the transmitted and reflected beam, this is imposed by energy conservation, see the article *Derivation of reciprocity relations for a beam splitter from energy balance* by Ou and Mandel in the annex. We consider a 50:50 beam splitter where the reflected beam undergoes a $\pi/2$ phase shift as this is the most common and relevant case.

- If there is no photon impinging the beam splitter:

$$|0\rangle_0 |0\rangle_1 \rightarrow |0\rangle_2 |0\rangle_3$$

this is rather obvious, nothing goes in and nothing goes out.

- With one photon at one input port, we have:

$$|0\rangle_0 |1\rangle_1 \rightarrow \frac{1}{\sqrt{2}}(ia_2^+ + a_3^+) |0\rangle_2 |0\rangle_3 = \frac{1}{\sqrt{2}}(i |1\rangle_2 |0\rangle_3 + |0\rangle_2 |1\rangle_3)$$

The photon comes out in both arms and is in a superposition of being in both arms until it is detected. The detection process will then randomly take place in one of the two output ports, this effect can be used to generate random numbers, provided the beam splitter is perfectly balanced or post-measurements can correct for the effects of an unbalanced beam splitter.

It is also very interesting to note that the output of the beam splitter when one single photon impinges is an entangled state: we have entanglement between one photon and the vacuum. This is harder to measure than when we have two photons entangled in polarization.

10.2 The Hong Ou Mandel effect

We now consider the case where two identical photons are simultaneously impinging on the beam splitter at each input.

$$|1\rangle_0 |1\rangle_1 = a_0^+ a_1^+ |0\rangle_0 |0\rangle_1$$

$$|1\rangle_0 |1\rangle_1 \rightarrow \frac{1}{2}(a_2^+ + ia_3^+)(ia_2^+ + a_3^+) |0\rangle_2 |0\rangle_3$$

$$= \frac{i}{2}(a_2^+ a_2^+ - a_3^+ a_2^+ + a_2^+ a_3^+ + a_3^+ a_3^+) |0\rangle_2 |0\rangle_3$$

$$= \frac{i}{2}(a_2^+ a_2^+ + a_3^+ a_3^+) |0\rangle_2 |0\rangle_3$$

$$= \frac{i}{2}(|2\rangle_2 |0\rangle_3 + |0\rangle_2 |2\rangle_3)$$

The two photons always emerge together, the case where they come out alone in each output interfere.

Figure 10.2: When two indentical photons impinge on a beam splitter, there are four possible outcomes. Only two take place: the two photons always emerge together, this is the Hong Ou Mandel effect.

The output of a beam splitter when fed with two identical and simultaneous photons is therefore in stark contrast when analysed with quantum mechanics compared with classical physics: the two photons always emerge together in the same mode. This is a useful tool to test for indistinguishability of two photons and can constitute a quantum gate (an AND gate) which could prove crucial for photonic quantum computing. Testing the indistinguishabilty of two photons is therefore done easily with the Hong Ou Mandel effect.

10.3 The quantum eraser

The Hong Ou Mandel effect is based on the indistinguishability of the two incoming photons: they have the same polarization, frequency and arrival time. If we now control the polarization in one arm:

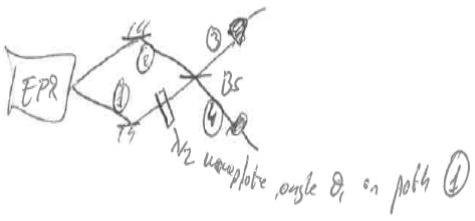


Figure 10.3: Controling the polarization of one photon compared to the other enables us to control their distinguishability.

We now have:

$$|\theta\rangle_1 = |H\rangle_1 cos\theta_1 + |V\rangle_1 sin\theta_1$$

And the input at the beam splitter is now:

$$|H\rangle_2 |\theta\rangle_1 = cos\theta_1 |H\rangle_2 |H\rangle_1 + sin\theta_1 |H\rangle_2 |V\rangle_1$$

This implies that the output of the beam splitter will be:

$$|\Psi_{out}(\theta)\rangle = \frac{i}{\sqrt{2}} cos\theta_1 (|2H\rangle_3 |0\rangle_4 + |0\rangle_3 |2H\rangle_4) + \frac{1}{\sqrt{2}} sin\theta_1 (|H\rangle_3 |V\rangle_4 - |V\rangle_3 |H\rangle_4)$$

The terms containing the single photon states no longer cancel each other because of the different polarization. In the extreme case, for: $\theta_1 = \frac{\pi}{2}$ we get:

$$|\Psi_{out}(\frac{\pi}{2})\rangle = \frac{1}{\sqrt{2}}(|H\rangle_3 |V\rangle_4 - |V\rangle_3 |H\rangle_4)$$

Rotating one photon's polarization by 90 degrees is like 'marking' it: it gives a which path information, even if it is not known/measured by the experimenter, just like for the famous double slit experiment.

We now only act after the beam splitter where we place a polarizer with angle on path (3).

$$|\theta\rangle_3 = |H\rangle_3 cos\theta_3 + |V\rangle_3 sin\theta_3$$

Only photons with polarization θ_3 are detected. We get

$$|\Psi_1 \theta_3\rangle = \frac{|\theta_3\rangle\langle\theta_3|\Psi_{out}(\frac{\pi}{2})\rangle}{\langle\Psi_{out}(\frac{\pi}{2})|\theta_3\rangle\langle\theta_3|\Psi_{out}(\frac{\pi}{2})\rangle)^{1/2}} = |\theta_3\rangle(|V_4\rangle cos\theta_3 - |H_4\rangle sin\theta_3)$$

Where the photon of mode (4) has perpendicular polarization to the detected photon. We place a similar polarizer at angle θ_4 on beam 4 and calculate the probability to get coincident detections at angles θ_3 and θ_4.

$$P_{coinc} = |\langle\theta_3|\theta_4|\Psi_{out}(\frac{\pi}{2})\rangle|^2 = \frac{1}{2} sin^2(\theta_2 - \theta_1)$$

The dip in coincidence is recovered! Polarizers (3) and (4) erase the information encoded on one of the beams by the waveplate. A question we can now ask ourselves is where does the Hong Ou Mandel effect take place?

10.4 Wheeler's delayed choice

In experiments, photons can manifest properties of particle or wave, but not both at the same time. Which property is observed depends on the type of experiment carried out. John Wheeler came up with experiments addressing the question: *when does the photon decide it is going to travel as a wave or as a particle?* In the experiment below, we test the particle nature of light: photons from the source on the left will take either of both arms and will be detected with single photon detectors in one of the two arms, just like in the Hanbury-Brown Twiss interferometer we use to demonstrate the generation of single photons.

Figure 10.4: In Wheeler's choice experiment, when the photon enters the interferometer the choice has not been made whether the wave or particle nature of the photon will be measured.

In the second experiment below, we will observe intereferences: we are now testing the wave nature of light, the photons travel along both paths and interfere with themselves at the second beam splitter.

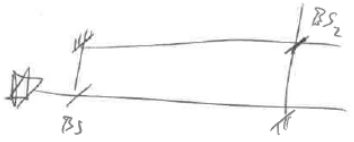


Figure 10.5: Beam splitter 2 can be introduced after the photon has entered the interferometer.

John Wheeler proposed the delayed choice: we place beam splitter BS2 after the photon crossed the first beam splitter so that the photon has to 'decide' whether it will behave as a particle or a wave after traveling through the first beam splitter. When the experiment is carried out and the second beam splitter is placed after the photon has crossed the first beamsplitter we see that the presence or absence of the second beam splitter

always determines the wave or particle demonstration. 'The past has no existence except as recorded in the present'.

Measurement of Subpicosecond Time Intervals between Two Photons by Interference

C. K. Hong, Z. Y. Ou, and L. Mandel
Department of Physics and Astronomy, University of Rochester, Rochester, New York 14627
(Received 10 July 1987)

A fourth-order interference technique has been used to measure the time intervals between two photons, and by implication the length of the photon wave packet, produced in the process of parametric down-conversion. The width of the time-interval distribution, which is largely determined by an interference filter, is found to be about 100 fs, with an accuracy that could, in principle, be less than 1 fs.

PACS numbers: 42.50.Bs, 42.65.Re

The usual way to determine the duration of a short pulse of light is to superpose two similar pulses and to measure the overlap with a device having a nonlinear response.[1] The latter might, for example, make use of the process of harmonic generation in a nonlinear medium. Indeed, such a technique was recently used[2] to determine the coherence length of the light generated in the process of parametric down-conversion.[3] The coherence time was found to be of subpicosecond duration, as predicted theoretically.[4] It is, however, in the nature of the technique that it requires very intense light pulses and would be of no use for the measurement of single photons. On the other hand, if we are dealing with two photons and wish to determine the time interval between them, which has a dispersion governed by the length of the photon wave packet, we are usually limited by the resolving time of the photodetector to intervals of order 100 ps or longer.[5]

We wish to report an experiment in which the time interval between signal and idler photons, and by implication the length of a subpicosecond photon wave packet, produced in parametric down-conversion was measured. The technique is based on the interference of two two-photon probability amplitudes in two-photon detection, and is easily able to measure a time interval of 50 fs, with an accuracy that could be 1 fs or better.

An outline of the experiment is shown in Fig. 1. A coherent beam of light of frequency ω_0 from an argon-ion laser oscillating on the 351.1-nm line falls on an 8-cm-long nonlinear crystal of potassium dihydrogen phosphate, where some of the incident photons split into two lower-frequency signal and idler photons of frequencies ω_1 and ω_2, such that

$$\omega_0 = \omega_1 + \omega_2. \tag{1}$$

The two signal and idler photons are directed by mirrors M1 and M2 to pass through a beam splitter BS as shown, and the superposed beams interfere and are detected by photodetectors D1 and D2. We measure the rate at which photons are detected in coincidence, when the beam splitter is displaced from its symmetry position by various small distances $\pm c\,\delta\tau$. It should be emphasized that the signal and idler photons have no definite phase, and are therefore mutually incoherent, in the sense that they exhibit no second-order interference when brought together at detector D1 or D2. However, fourth-order interference effects occur, as demonstrated by the coincidence counting rate between D1 and D2.[6-8] The experiment has some similarities to another, recently reported, two-photon interference experiment in which fringes were observed and measured, but without the use of a beam splitter.[6]

Although the sum frequency $\omega_1+\omega_2$ is very well defined in the experiment, the individual down-shifted frequencies ω_1,ω_2 have large uncertainties, that, in practice, are largely determined by the pass bands of the interference filters IF inserted in the down-shifted beams, as shown in Fig. 1. These pass bands are of order 5×10^{12} Hz, corresponding to a coherence time for each photon of order 100 fs. Needless to say, the two-photon probability amplitudes at the detectors D1,D2 are expected to interfere only if they overlap to this accuracy or better. We start by examining how this interference arises.

Let us label the field modes on the input sides of the beam splitter by 01,02 and on the output sides by 1,2 and suppose first that the light is monochromatic. If we take the state at the input resulting from one degenerate down-conversion to be the two-photon Fock state $|1_{01},1_{02}\rangle$, then one can show from general arguments[7] that the state on the output side of the beam splitter is

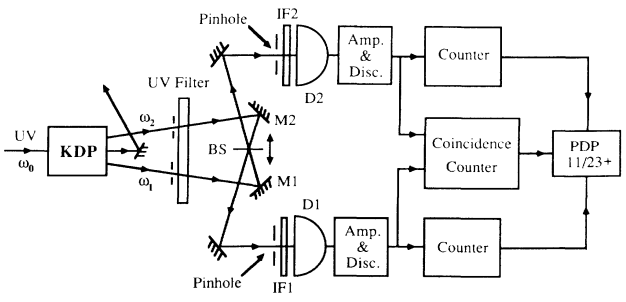


FIG. 1. Outline of the experimental setup.

given by

$$|\psi_{\text{out}}\rangle=(R-T)|1_1,1_2\rangle+i(2RT)^{1/2}|2_1,0_2\rangle+i(2RT)^{1/2}|0_1,2_2\rangle, \tag{2}$$

where R and T are the reflectivity and transmissivity of the beam splitter, with $R+T=1$. It follows that for a 50%:50% beam splitter with $R=\frac{1}{2}=T$, the first term is zero by virtue of the destructive interference of the corresponding two-photon probability amplitudes. No coincidences (other than accidentals) should therefore be registered by detectors D1 and D2.

In practice the down-shifted photons are never monochromatic. Let us represent the two-photon state produced by the potassium-dihydrogen-phosphate crystal by the linear superposition

$$|\psi\rangle=\int d\omega\,\phi(\omega_1,\omega_0-\omega_1)|\omega_1,\omega_0-\omega_1\rangle, \tag{3}$$

where $\phi(\omega_1,\omega_2)$ is some weight function which is peaked at $\omega_1=\frac{1}{2}\omega_0=\omega_2$. (A plausible example is given in Ref. 8.) We assume here that the directions of signal and idler photons are reasonably well defined by apertures, but the frequency spreads are substantial; in practice they are largely determined by the interference filters IF. Then the joint probability of the detection of photons at both detectors D1 and D2 at times t and $t+\tau$, respectively, is given by[9]

$$P_{12}(\tau)=K\langle\hat{E}_1^{(-)}(t)\hat{E}_2^{(-)}(t+\tau)\hat{E}_2^{(+)}(t+\tau)\hat{E}_1^{(+)}(t)\rangle, \tag{4}$$

where $\hat{E}_1^{(+)}(t)$ and $\hat{E}_2^{(+)}(t)$ are the positive-frequency parts of the fields at detectors D1 and D2, and K is a constant characteristic of the detectors. $\hat{E}_1^{(+)}(t)$ and $\hat{E}_2^{(+)}(t)$ are related to the fields $\hat{E}_{01}^{(+)}(t)$ and $\hat{E}_{02}^{(+)}(t)$ at the two mirrors M1 and M2 shown in Fig. 1. If $R+T=1$, then

$$\hat{E}_1^{(+)}(t)=\sqrt{T}\hat{E}_{01}^{(+)}(t-\tau_1)+i\sqrt{R}\hat{E}_{02}^{(+)}(t-\tau_1+\delta\tau), \tag{5}$$

$$\hat{E}_2^{(+)}(t)=\sqrt{T}\hat{E}_{02}^{(+)}(t-\tau_1)+i\sqrt{R}\hat{E}_{01}^{(+)}(t-\tau_1-\delta\tau). \tag{6}$$

Here τ_1 is the propagation time from mirror to detector, and $\pm c\,\delta\tau$ represents the small displacement of the beam splitter BS towards one or the other detector.

By combining Eqs. (3) to (6) we may readily show that the joint probability is

$$P_{12}(\tau)=K|G(0)|^2\{T^2|g(\tau)|^2+R^2|g(2\delta\tau-\tau)|^2-RT[g^*(\tau)g(2\delta\tau-\tau)+\text{c.c.}]\}, \tag{7}$$

where $G(\tau)$ is the Fourier transform of the weight function $\phi(\omega_0/2+\omega,\omega_0/2-\omega)$ with respect to ω,

$$G(\tau)=\int\phi(\omega_0/2+\omega,\omega_0/2-\omega)e^{-i\omega\tau}d\omega, \tag{8}$$

and $g(\tau)\equiv G(\tau)/G(0)$. This shows how $P_{12}(\tau)$ varies with the time interval τ. If $\phi(\omega_0/2+\omega,\omega_0/2-\omega)$ is real and symmetric in ω, as we assume, then $G(\tau)$ and $g(\tau)$ are both real and symmetric in τ.

In practice the coincidence measurement corresponds to an integration of the probability $P_{12}(\tau)$ with respect to τ over the coincidence resolving time of a few nanoseconds, but as this time is so much longer than the correlation time of $g(\tau)$ in the experiment, we may effectively integrate $P_{12}(\tau)$ over all τ. From Eq. (7) the expected number N_c of observed photon coincidences is then given by

$$N_c=C\left[R^2+T^2-2RT\frac{\int_{-\infty}^{\infty}g(\tau)g(\tau-2\delta\tau)d\tau}{\int_{-\infty}^{\infty}g^2(\tau)d\tau}\right], \tag{9}$$

where C is another constant. It follows from this relation that $N_c=C(R-T)^2$ when $\delta\tau=0$, which vanishes when $R=\frac{1}{2}=T$, whereas $N_c=C(T^2+R^2)$ when $\delta\tau$ appreciably exceeds the correlation time of $g(\tau)$. A plot of the number of coincidences N_c versus the displacement $\delta\tau$ therefore should exhibit a sharp dip near $\delta\tau=0$, of width determined by the length of the wave packet, or coherence time, of the down-shifted photons. The vanishing of the photon coincidence rate is a purely quantum-mechanical feature of the fourth-order interference, as has been shown.[6,8]

In the special case when $g(\omega_0/2+\omega,\omega_0/2-\omega)$ is Gaussian in ω with bandwidth $\Delta\omega$, then $g(\tau)$ has the Gaussian form

$$g(\tau)=e^{-(\Delta\omega\tau)^2/2}, \tag{10}$$

and Eq. (9) yields

$$N_c=C(T^2+R^2)\left[1-\frac{2RT}{R^2+T^2}e^{-(\Delta\omega\delta\tau)^2}\right]. \tag{11}$$

In the experiment the path difference $c\,\delta\tau$ was varied by our mounting the beam splitter on a translator and making very small displacements with a precisely calibrated micrometer. Still finer adjustments can be made with a piezoelectric transducer. The coincidence counting rate was measured by our feeding the amplified and standardized photomultiplier pulses to the start and the stop inputs of a time-to-digital converter, and recording the time interval distribution. Because of the transit-

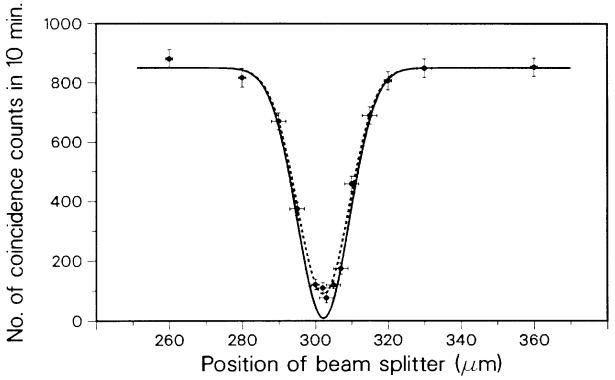


FIG. 2. The measured number of coincidences as a function of beam-splitter displacement $c\,\delta\tau$, superimposed on the solid theoretical curve derived from Eq. (11) with $R/T=0.95$, $\Delta\omega=3\times10^{13}$ rad s^{-1}. For the dashed curve the factor $2RT/(R^2+T^2)$ in Eq. (11) was multiplied by 0.9. The vertical error bars correspond to one standard deviation, whereas horizontal error bars are based on estimates of the measurement accuracy.

time spread of the photoelectric pulses and the slewing of the discriminator pulses, a range of time intervals centered on zero delay was obtained with a spread of several nanoseconds. For the purpose of the measurement, pulse pairs received within a 7.5-ns interval were treated as "coincident." Pulse pairs received within an interval of 35 to 80 ns were regarded as accidentals, and when scaled by the factor 7.5/45 provided a measure of the number of accidental coincidences that occur within any 7.5-ns interval.

The results of the experiment are presented in Fig. 2, which is a plot of the number of observed photon coincidences, after subtraction of accidentals, as a function of the displacement of the beam splitter. It will be seen that for a certain symmetric position of the beam splitter, the two-photon coincidence rate falls to a few percent of its value in the wings, by virtue of the destructive interference of the two two-photon probability amplitudes. The width of the dip in the coincidence rate provides a measure of the length of the photon wave packet. It is found to be about 16 μm at half height, corresponding to a time of about 50 fs, which should really be doubled to allow for the greater movement of the mirror image. This time is about what is expected from the passband of the interference filters.

Direct measurements of the beam-splitter reflectivity and transmissivity show that $R/T\approx0.95$, which makes the combination $2RT/(R^2+T^2)\approx0.999$, and implies that N_c should fall close to zero when $\delta\tau=0$. That it does not fall quite that far is probably due to a slight lack of overlap of the signal and idler fields admitted by the two pinholes, causing less than perfect destructive interference. The solid curve in Fig. 2 is based on Eq. (11) with $R/T=0.95$ and $\Delta\omega=3\times10^{13}$ rad/s $\approx5\times10^{12}$ Hz, if we identify $c\,\delta\tau$ with the beam-splitter displacement $(x-302.5)$ in micrometers. For the dashed curve the factor $2RT/(R^2+T^2)$ was multiplied by 0.9 to allow for less than perfect overlap of the signal and idler photons. It will be seen that, except for the minimum, Eq. (11) is obeyed quite well, corresponding to a coherence time of about 100 fs.

We have therefore succeeded in measuring subpicosecond time intervals between two photons, and by implication the length of the photon wave packet, by a fourth-order interference technique. Unlike second-order interference, this method does not require that path differences be kept constant to within a fraction of a wavelength. The method is applicable to other situations in which pairs of single photons are produced, but becomes less efficient for more intense pulses of light, because the "visibility" of the interference is then reduced and cannot exceed 50% at high intensities.[6] In principle, the resolution could be better than 1 μm in length or 1 fs in time.

This work was supported by the National Science Foundation and by the U.S. Office of Naval Research.

[1]See, for example, E. P. Ippen and C. V. Shank, in *Ultrashort Light Pulses,* edited by S. L. Shapiro (Springer-Verlag, Berlin, 1984), 2nd ed., p. 83.

[2]I. Abram, R. K. Raj, J. L. Oudar, and G. Dolique, Phys. Rev. Lett. **57**, 2516 (1986).

[3]D. C. Burnham and D. L. Weinberg, Phys. Rev. Lett. **25**, 84 (1970).

[4]C. K. Hong and L. Mandel, Phys. Rev. A **31**, 2409 (1985).

[5]S. Friberg, C. K. Hong, and L. Mandel, Phys. Rev. Lett. **54**, 2011 (1985).

[6]R. Ghosh and L. Mandel, Phys. Rev. Lett. **59**, 1903 (1987).

[7]Z. Y. Ou, C. K. Hong, and L. Mandel, to be published.

[8]R. Ghosh, C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. A **34**, 3962 (1986).

[9]R. J. Glauber, Phys. Rev. **130**, 2529 (1983), and **131**, 2766 (1963).

version of amplitudes between first and second extremes. The measured value of the rise time Δt_r is (16 ± 4) ns and through Eq. (8) one gets a fall time for the corresponding $V_s(t)$ of (20 ± 6) ns, which is in good agreement with the value measured from Fig. 2.

FINAL REMARKS

The effect of the switching action of a real electrical switch on simple circuits can be predicted, with moderate computational effort, yielding a good description of the measured behavior.

The subject can be presented to the students not only theoretically but also experimentally, using low voltages and semiconductor devices as switches. However, care must be taken in the design of these experiments because of the large percentage of energy that may be dissipated in the switch.

[a] Member of the Carrera del Investigador, CONICET.
[b] Fellowship of Buenos Aires University.

[1] G. P. Harnwell, *Principles of Electricity and Electromagnetism* (McGraw-Hill, New York, 1949), Chap. XIII, p. 457.
[2] E. M. Purcell, *Electricity and Magnetism, Berkeley Physics Course* (McGraw-Hill, New York, 1963), Vol. II, Chap. 8, p. 274.
[3] B. Kurrelmeyer and W. H. Mais, *Electricity and Magnetism* (Van Nostrand, Princeton, NJ, 1967), Chap. 13, p. 298.
[4] F. Reif, *Fundamentals of Statistical and Thermal Physics* (McGraw-Hill, New York, 1965), Chap. 9, p. 389.
[5] B. Carnahan, H. A. Luther, and J. O. Wilkes, *Applied Numerical Methods* (Wiley, New York, 1969), Chap. 6, p. 361.

Derivation of reciprocity relations for a beam splitter from energy balance

Z. Y. Ou and L. Mandel
Department of Physics and Astronomy, University of Rochester, Rochester, New York 14627

(Received 8 January 1988; accepted for publication 16 March 1988)

It is shown that the usual amplitude and phase relations connecting the reflectance and transmittance of a stratified or continuous, nonabsorbing beam splitter can be derived by a simple energy balance argument relating to a Michelson interferometer.

I. INTRODUCTION

Reciprocity relations connecting the complex reflectance r and transmittance t of a nonabsorbing beam splitter with the corresponding quantities r',t' for light incident from the opposite direction have been well known in optics for a long time.[1,2] The subject has nevertheless received renewed attention in recent years, as the original reciprocity relations of Stokes were generalized.[3–5] In particular, for a beam splitter in the form of a stratified multilayer, where the information about r,t,r',t' is contained in the so-called characteristic matrix,[1,2] the expressions for r,t,r',t' become quite complicated. However, the following relations have been derived for an arbitrary angle of incidence,

$$|r| = |r'|, \quad |t| = |t'|, \tag{1}$$

$$|r|^2 + |t|^2 = 1 = |r'|^2 + |t'|^2, \tag{2}$$

$$r^*t' + t^*r' = 0, \tag{3}$$

in some cases after "lengthy...calculation."[3] Equation (2) obviously expresses the conservation of energy at the beam splitter, but Eq. (3) has not usually been interpreted in the same way. The relations have been derived by use of the principle of time reversal invariance.[4]

We would like to draw attention to the fact that the three relations (1)–(3) can all be derived by a simple energy balance argument relating to a Michelson interferometer. It applies to any beam splitter in which a plane wave incident from one side emerges from the other side as a plane wave traveling in the same direction. This article contains no new results, but only a simplified derivation of some previously derived results that holds under rather general conditions and provides some additional insight.

II. DERIVATION

We consider the Michelson type of interferometer system illustrated in Fig. 1, containing a parallel-sided beam splitter whose refractive index is a function only of the coordinate perpendicular to the face, either discrete or continuous. The beam splitter may therefore be a stratified or a continuous medium. To ensure that a plane wave incident from one side emerges as a plane wave traveling in the same direction, we shall suppose that the same medium (e.g., air) is in contact with both sides. Let a linearly polarized (TE or TM) monochromatic plane wave, of unit complex amplitude referred to point A, be incident from the left at some arbitrary angle, as shown, and let ϕ_0 be the phase shft suffered by this wave in propagating from A to P. The beam splitter then gives rise to reflected and transmitted waves of complex amplitudes r and t referred to points P and Q, respectively, which travel to two perfect mirrors $M1$ and $M2$, where they are reflected straight back. Let ϕ_1 and ϕ_2 be the (arbitrary) phase shifts experienced by these waves along the paths PC + CP and QB + BQ, respectively. The two returning waves both give rise to further reflected and transmitted components, and we shall use r',t' to denote the complex reflectance and transmittance of the beam splitter for waves incident from the right. As a result, outgoing waves with complex amplitudes E_A,E_D emerge at A and D. Let ϕ_3 be the phase shift corresponding to the path from Q to D.

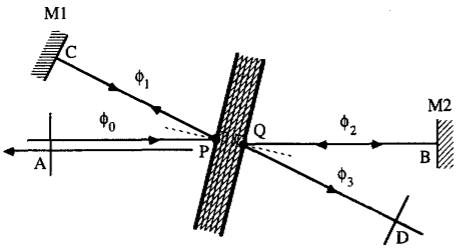


Fig. 1. Outline of the geometry for the Michelson interferometer.

Reference to Fig. 1 shows that we may represent E_A and E_D by the combinations

$$E_A = e^{i\phi_0} r e^{i\phi_1} r e^{i\phi_0} + e^{i\phi_0} t e^{i\phi_2} t' e^{i\phi_0}$$
$$= e^{2i\phi_0}(r^2 e^{i\phi_1} + tt' e^{i\phi_2}), \tag{4}$$
$$E_D = e^{i\phi_0} r e^{i\phi_1} t e^{i\phi_3} + e^{i\phi_0} t e^{i\phi_2} r' e^{i\phi_3}$$
$$= e^{i(\phi_0+\phi_3)}(rte^{i\phi_1} + tr' e^{i\phi_2}). \tag{5}$$

From Eqs. (4) and (5) we immediately find for the corresponding light intensities,

$$I_A = |E_A|^2 = |r|^4 + |t|^2|t'|^2 + 2|r^2 tt'|\cos(\theta_t + \theta_t' - 2\theta_r + \phi_2 - \phi_1), \tag{6}$$

$$I_D = |E_D|^2 = |rt|^2 + |r't|^2 + 2|rr't^2| \times \cos(\theta_r' - \theta_r + \phi_2 - \phi_1), \tag{7}$$

where we have written

$$r = |r|e^{i\theta_r}, \quad r' = |r'|e^{i\theta_r'}, \quad t = |t|e^{i\theta_t}, \quad t' = |t'|e^{i\theta_t'}. \tag{8}$$

Now, if energy is to be conserved, the sum of the outgoing light intensities I_A, I_D must equal unity, which is the incoming light intensity. Hence,

$$1 = |r|^2(|r|^2 + |t|^2) + |t|^2(|t'|^2 + |r'|^2) + 2|r^2 tt'|\cos(\theta_t + \theta_t' - 2\theta_r + \phi_2 - \phi_1) + 2|rr't^2|\cos(\theta_r' - \theta_r + \phi_2 - \phi_1). \tag{9}$$

Now the third and fourth terms on the right contain the arbitrary phase shift $\phi_2 - \phi_1$. As the right-hand side must equal unity and these two terms cannot be made separately equal to zero, they must sum to zero, while the first two terms sum to unity. This requires the amplitudes of the two cosine terms to be made equal, so that

$$|r||t'| = |r'||t|, \tag{10}$$

while

$$|r|^2 + |t|^2 = 1 = |r'|^2 + |t'|^2. \tag{11}$$

From Eqs. (10) and (11),

$$|r|/|t| = |r'|/|t'|$$

or

$$|r|/\sqrt{1-|r|^2} = |r'|/\sqrt{1-|r'|^2}$$

or

$$|r| = |r'|, \quad |t| = |t'|. \tag{12}$$

Hence, on combining the two cosine terms in Eq. (9), we obtain

$$1 = 1 + 4|r|^2|t|^2 \cos\left(-\frac{3\theta_r}{2} + \frac{\theta_r'}{2} + \frac{\theta_t}{2} + \frac{\theta_t'}{2} + \phi_2 - \phi_1\right)\cos\left(\frac{\theta_t - \theta_r + \theta_t' - \theta_r'}{2}\right). \tag{13}$$

Now the second term has to vanish. But, because the first cosine factor in this term contains the arbitrary phase difference $\phi_2 - \phi_1$, it is the second cosine factor that must vanish in general. Hence, we conclude that

$$\theta_t - \theta_r + \theta_t' - \theta_r' = \pm\pi \tag{14}$$

in all cases. For a symmetric beam splitter, this would, of course, imply that $\theta_t - \theta_r = \pm\pi/2$. From Eq. (14),

$$e^{i(\theta_r' - \theta_r)} + e^{i(\theta_t' - \theta_t)} = 0, \tag{15}$$

and on multiplying both sides of this equation by $|r||t|$ and using Eq. (12) we obtain

$$r^* t' + t^* r' = 0. \tag{16}$$

III. CONCLUSION

We have derived the three reciprocity relations (1)–(3), and we see that all three of them follow from considerations of energy balance alone. Moreover, it makes no difference if the medium is stratified in several layers or continuous, so long as the index of refraction depends on only one coordinate. That the phase relationship (14) is required by energy balance just as the more obvious energy relations (11) appears not to have been generally recognized.

ACKNOWLEDGMENTS

This work was supported by the National Science Foundation and by the Office of Naval Research.

[1]See, for example, M. Born and E. Wolf, *Principles of Optics* (Pergamon, Oxford, 1980), 6th ed., Sec. 1.6.
[2]A. Vasicek, *Optics of Thin Films* (North-Holland, Amsterdam, 1960).
[3]A. T. Friberg and P. D. Drummond, J. Opt. Soc. Am. **73**, 1216 (1983).
[4]P. D. Drummond and A. T. Friberg, J. Appl. Phys. **54**, 5618 (1983).
[5]M. Nieto-Vesperinas and E. Wolf, J. Opt. Soc. Am. A **3**, 2038 (1986).

Chapter 11

Quantum Repeaters and Quantum Memories

Long-distance quantum communication between a large number of network nodes, often called the 'Quantum Internet', is envisioned to enable applications out of reach for the classical internet, e.g. secure communication (via quantum key distribution), secure access to quantum computers, more accurate clock synchronization and scientific applications in astronomy (see Science 362, eaam9288, 2018; development stages for a quantum internet are proposed). In contrast to classical bits of information, qubits cannot be copied (cf. no-cloning theorem), which prevents signal amplification as employed in conventional telecommunication systems relying on classical information. The loss in quantum bit transmission in standard telecom fibers (considered here as physical implementation of the quantum channel) scales exponentially with distance, which severely limits the achievable rates for entanglement and quantum key distribution.

Let us consider some practical examples: The entanglement generation rate scales linearly with optical fiber transmittivity $\eta = \exp -\frac{L}{L_0}$, where the attenuation length of standard fibers at telecommunication wavelengths (around 1550 nm) is around 22 km (loss 0.2 dB/km). Further, we assume a photon generation rate of 1 GHz (optimistic, can be much lower in experimental implementations). For a distance of 70 km (Stockholm - Uppsala), we would end up with a rate around 40 MHz; for a distance of 210 km (Stockholm - Linköping), we would end up with a rate around 70 kHz; for a distance of 470 km (Stockholm - Gothenburg), we would end up with a rate around 50 mHz. For a more detailed discussion on secret key rates see e.g. Nat. Comm. 5, 5235, 2014 or Nat. Comm. 8, 15043, 2016. It is evident that such transmission rates do not compare favorably with classical telecommunication signals and are not suitable for high-speed, long-distance communication. To mitigate this problem, quantum repeaters have been proposed, which will be discussed in the following.

11.1 Quantum Repeaters

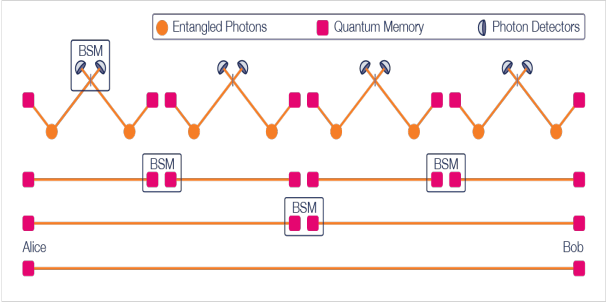


Figure 11.1: Quantum repeaters enable sharing entanglement over long distances.

Quantum repeaters were initially proposed by Briegel, Dür, Cirac and Zoller in 1998 (Phys. Rev. Lett. 81, 5932, 1998). The general idea entails to divide the long-distance communication link into shorter segments with acceptable losses. Three basic operations are needed: 1) Entanglement generation and distribution between adjacent network nodes (e.g. via spontaneous parametric down-conversion); 2) Entanglement purification (distillation), i.e. creating a highly entangled state from multiple states with lower fidelity; 3) Entanglement swapping (cf. quantum teleportation), where a Bell-state measurement is performed within a node on two qubits that are originating from separate Bell states.

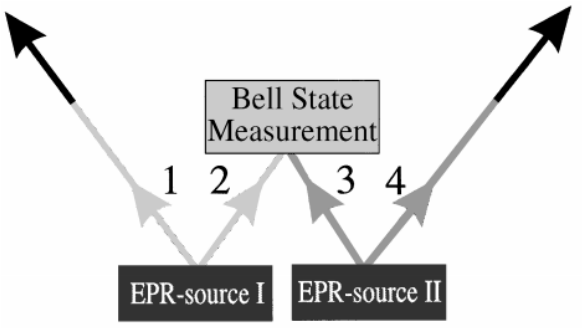


Figure 11.2: Entanglement swapping using two sources of entangled photon pairs and performing a Bell state measurement (Taken from Phys. Rev. Lett. 80, 3891, 1998).

After successfully repeating entanglement swapping n times, quantum entanglement is established between the outermost nodes of the long-distance communication link between Alice and Bob. As multiple steps have to be performed subsequently in this scheme, the reliable storage of photonic quantum states becomes important. Hence, the implementation of quantum memories (see following section) in each intermediate repeater node is required. The major advantage of such a scheme is that the entanglement distribution time scales polynomially with communication distance (at least when considering only loss in the quantum channel) as opposed to exponentially in the absence of a quantum repeater. A schematic of this fundamental quantum repeater scheme is shown below, whereas a proposal for implementing quantum repeaters with atomic gases and linear optics can be found in Nature 414, 413, 2001.

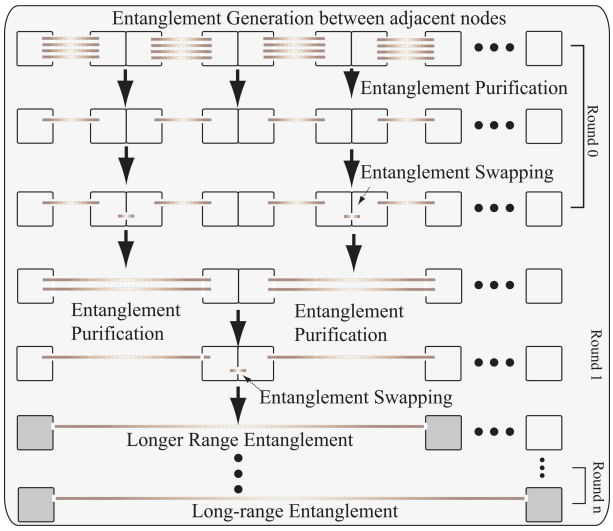


Figure 11.3: Quantum repeater scheme for generating long-distance quantum entanglement (Taken from IEEE J. Sel. Top. Quantum Electron. 21, 6400813, 2015).

A few words regarding entanglement purification (distillation): While this step has been considered in the initial quantum repeater proposal, it has to be noted that its implementation is linked with significant overheads (linked with lower entanglement distribution rates) as the number of entangled photon pairs that need to be generated is at least doubled. Thus it is often omitted in simple architectures employing only few communication nodes where error probablities are still acceptable.

The development of quantum repeater schemes and their experimental implementation remains an active field of research. For realistic scenarios a large number of additional factors have to be considered, e.g. non-ideal Bell state generation (fidelity below unity) and measurement, finite storage and coherence times of quantum memories, photon detection probability below unity, overheads resulting from classical communication (heralding of successful photon detection and entanglement distribution) etc. Several improvements to the described quantum repeater scheme have been proposed, the interested reader is referred to e.g. Rev. Mod. Phys. 83, 33, 2011 and IEEE J. Sel. Top. Quantum Electron. 21, 6400813, 2015. Despite significant progress over the last decades, the experimental implementation of quantum repeaters outperforming quantum state distribution rates achievable with direct transmission remains extremely challenging.

11.2 Quantum Memories

Quantum memories are an essential building block of quantum repeaters and, more general, for implementing certain quantum information processing operations. A review of quantum memory performance parameters as well as physical implementations can be found in Eur. Phys. J. D 58, 1-22, 2010. One use case of quantum memories is the realization of a deterministic single-photon source from a probabilistic photon pair source. Considering a photon pair from a spontaneous parametric down-conversion source, one photon of the pair can be detected when it is emitted, while the other photon is stored in a quantum memory. Relying on the photon detection event as indicator for a photon being stored in the quantum memory, the latter can be employed as deterministic single-photon source assuming high efficiency of photon storage and retrieval. In a similar way, quantum memories can be employed in entanglement-based quantum sensing approaches - a topic that will be discussed in a later lecture.

Physical implementations of photonic quantum memories need to provide sufficient light-matter coupling, often given by the probability of light absorbtion / collection. Furthermore, the coherence properties of the physical system are decisive for achieving high-performance quantum memories. In particular, fluctuating electro-magnetic fields are a major source for decoherence, for instance externally applied fields or fields intrinsic to the solid-state host material (e.g. resulting from nuclear spins).

Considering the quantum repeater application described above in the context of long-distance quantum communication, the properties and performance parameters of quantum memories need to fulfil several requirements. First, the fidelity and efficiency should be high, which means that there is a large overlap between the quantum state that is stored and subsequently read-out and that the storage and read-out can be performed with a high probability. The latter is linked with efficient light-matter coupling, which can be for instance engineered by employing optical cavities. Moreover, the quantum memory storage time has to exceed the communication time between distant nodes of the quantum network, i.e. average entanglement creation times, which can be on second timescales for realistic parameters. It is also important that the quantum memory can be interfaced at optical wavelengths suitable for long-distance communication (telecommunication bands for optical fibers; free-space communication via satellites), or efficient wavelength conversion schemes would need to be implemented. Examples of quantum memory implementations include:

- Single atoms in optical traps
- Atomic ensembles (room temperature or ultracold gases)
- Rare-earth ions in the solid state
- Defect centers in diamond
- Semiconductor quantum dots

Chapter 12

Quantum Computation

Developments in quantum computation is now widely covered by popular media and funding agencies are eagerly funding research and development efforts in quantum computation in a large number of countries: The USA, China, Australia, the UK, the European Union, Germany, the Netherlands, France, Sweden all have large programs to support the development of quantum technologies with an important part for quantum computers. The EU for instance has a 1 billion Euro quantum flagship program. The idea of quantum computation, to take advantage of quantum effects in computers, can be traced back to a presentation by Feynman where he suggested to simulate quantum systems with quantum computers.

12.1 What can quantum computers do?

Computers have reshaped our lives and there is a general belief that quantum computers could again deeply impact society by providing far more computation power and more importantly have the ability to solve problems that are currently beyond the reach of the most powerful computers. One issue is however that after two decades of intense research, very few quantum algorithms have been developed, factorizing numbers (Shors's algorithm) and searching (Grover's alorithm) are the main reasons to build a quantum computer. One might wonder whether such a limited range of applications would justify the effort. Governments and large corporations are however afraid of falling behind others and are making lavish funding available to develop quantum computers. The prospect of quickly factorizing large numbers poses a threat to widespread encryption protocols such as RSA encryption. One parade would be to rely on quantum cryptogrpahy such as BB84, or other encryption schemes known as post quantum cryptography.

The physical implementation of a quantum computer could be done with a wide range of physical systems to encode and process qubits. We require a stable qubit system, that does not decohere too quickly so that operations can be performed before the qubit has decohered. Other requirements include the initialization of the qubit, readout schemes and most important: controlled interactions among qubits to build quantum gates. The hardest requirement so far has been scalability: while one or very few qubits can be studied with great precision in the lab, a quantum computer requires the operation of many thousands of qubits, possibly millions to solve any relevant problem. The required conditions to build a quantum computer were listed in an important publication by DiVicenzo in 2000.

12.2 The CNOT gate

While many gates are required to operate a computer, the CNOT gate is essential and would allow for the construction of other complex gates. The CNOT gate (controlled NOT gate) can entangle and distentangle qubits. It has the following truth table: the target bit is flipped if the control bit has value 1 and of course when using photons and their polarization, 1 can be encoded as a vertically polarized photon and 0 as a horizontally polarized photon.

If we feed the control input $A = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and the target input $B = |0\rangle$ to a CNOT gate, we get out the state.

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Which is an entangled state! This can be realized with simple optical elements: beam splitters and phase shifters.

Before		After	
Control	Target	Control	Target
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

Figure 12.1: Truth table for a CNOT gate: if the control is 1, the target qubit is flipped.

Early implementations of quantum gates were performed with superconducting based systems, trapped ions and electron spins that enabled some key experiments over the past twenty years. In superconducting quantum computing (the implementation used by IBM, Google and Rigetti), the qubit is the current flowing in a Josephson junction. In trapped ions, qubits are implemented as the internal states of ions trapped in lattices. In electron spins implementations, the spin of single electrons are manipulated in semiconductor nanostructures. These implementations usually require extremely low temperatures, which has made dilution cryostats able to operate at mK temperatures very usual equipment. Some associated problems are how to send massive amounts of information in and out of a system at very low temperatures, the thermal conductivity of metals limits the use of coaxial cables.

Because quantum computation is proving very hard to implement, other easier goals have emerged in the community such as quantum simulations and quantum supremacy. In quantum simulations, the goal is not to realize a general purpose quantum computer but to simulate one particular system such as a molecule. In quantum supremacy, the goal is to beat a classical computer at solving one particular problem. A first important claim at quantum supremacy with made in 2019 by Google's Santa Barbara lab where a 53 qubit processor based on superconducting qubits was used to solve a problem that was thought to take 10000 years on a supercomputer, it was however later shown by IBM that it could be solved in 2 days.

It came as a surprise to many when the strongest claim for quantum supremacy was reported in 2020 by the USTC group in China headed by Prof. Jianwei Pang using a photonic implementation where 76 qubits were used to compute the Torontonian of a matrix far faster than a supercomputer. While the Torontonian of a matrix still has to find a use, this demonstration has put photonics in the leading position in the field of quantum computation and more advances are on their way with Xanadu in Canada developing quantum computation based on non-linear optics and PsiQuantum in California developing a quantum computer based on integrated quantum optics.

Quantum photonics offers a very strong path to the realization of quantum computers. Integrated photonics where single photon detectors, circuits and sources are massively scaled down and all integrated on silicon. It is also important to note that in addition to scalability, photonics implementations do not require low temperatures. It is only the high-performance photon detectors that require cooling to a few Kelvins, but not mK. LOQC (Linear Optical Quantum Computer) was proposed in 2001 by Knill, Laflamme and Milburn (KLM scheme), with only single photon sources, detectors and linear elements such as beam splitters, mirrors and phase shifters a quantum computer could be operated. The challenge here is that photon generation and detection must be performed with near-unity efficiency.

To realize large scale quantum computers, quantum error correction must be implemented to protect from decoherence as well as from non-ideal quantum gates, memories and limited fidelity in qubit preparation. This represents an important challenge as the number of qubits involved explodes when quantum error correction is implemented. One scheme relies on storing the information of one qubit onto nine entangled qubits, a measurement can then identify which type of error took place and a corrective operation can then be applied.

While the technological challenges lying ahead to realize a quantum computer may seem overwhelming, a working system might be a few decades away only. The main question is whether the investment will be worth the result. One important impact of the development of quantum computation is that we are learning to process information encoded on single photons, this represents the lowest possible amount of energy and could result in computation system dissipating far less energy than current implementations, even when no quantum protocol is implemented.

Boson sampling has gained popularity as it is an easy to implement technique that yields results that are very hard to predict with a classical computer. A simple example is a cascade of beamsplitters where some single photons are inserted. The output, even with a limited number of photons and beamsplitters is very hard to predict. The only issue is that this does not solve any useful problem.

It should also be mentioned that D-wave has been selling quantum computers since 2015 that had 1000 qubits, the latest model will have 5000 qubits, based on superconducting qubits. These are however not general purpose quantum computers but quantum annealers where the system evolves to find the lowest energy configuration.

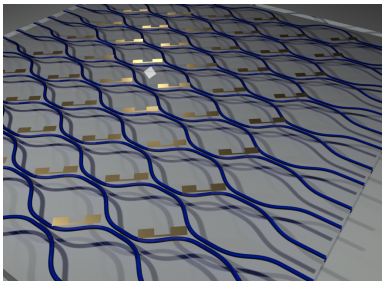


Figure 12.2: Cascading beam splitters allows for Boson sampling experiments that are computationally hard to simulate, image from the group of Fabio Sciarrino.

An issue that is often overlooked is energy consumption, while the human brain can solve incredibly complex problems dissipating only 100 Watts. Neural networks inspired by biological systems can excel at some tasks such as pattern recognition. En emerging field with tremendous potentials is the confluence of quantum technology and neural networks to develop quantum neural networks where operation at the single photon level and exploiting entanglement would result in 'quantum brains'.

QUANTUM COMPUTING

Quantum computational advantage using photons

Han-Sen Zhong[1,2]*, Hui Wang[1,2]*, Yu-Hao Deng[1,2]*, Ming-Cheng Chen[1,2]*, Li-Chao Peng[1,2], Yi-Han Luo[1,2], Jian Qin[1,2], Dian Wu[1,2], Xing Ding[1,2], Yi Hu[1,2], Peng Hu[3], Xiao-Yan Yang[3], Wei-Jun Zhang[3], Hao Li[3], Yuxuan Li[4], Xiao Jiang[1,2], Lin Gan[4], Guangwen Yang[4], Lixing You[3], Zhen Wang[3], Li Li[1,2], Nai-Le Liu[1,2], Chao-Yang Lu[1,2]†, Jian-Wei Pan[1,2]†

Quantum computers promise to perform certain tasks that are believed to be intractable to classical computers. Boson sampling is such a task and is considered a strong candidate to demonstrate the quantum computational advantage. We performed Gaussian boson sampling by sending 50 indistinguishable single-mode squeezed states into a 100-mode ultralow-loss interferometer with full connectivity and random matrix—the whole optical setup is phase-locked—and sampling the output using 100 high-efficiency single-photon detectors. The obtained samples were validated against plausible hypotheses exploiting thermal states, distinguishable photons, and uniform distribution. The photonic quantum computer, *Jiuzhang*, generates up to 76 output photon clicks, which yields an output state-space dimension of 10^{30} and a sampling rate that is faster than using the state-of-the-art simulation strategy and supercomputers by a factor of ~10^{14}.

The extended Church-Turing thesis is a foundational tenet in computer science, which states that a probabilistic Turing machine can efficiently simulate any process on a realistic physical device (*1*). In the 1980s, Feynman observed that many-body quantum problems seemed difficult for classical computers because of the exponentially growing size of the quantum-state Hilbert space. He proposed that a quantum computer would be a natural solution.

A number of quantum algorithms have since been devised to efficiently solve problems believed to be classically hard, such as Shor's factoring algorithm (*2*). Building a fault-tolerant quantum computer to run Shor's algorithm, however, still requires long-term efforts. Quantum sampling algorithms (*3*–*6*) based on plausible computational complexity arguments were proposed for near-term demonstrations of quantum computational speed-up, relative to current supercomputers, in solving certain well-defined tasks. If the speed-up appears overwhelming, such that no classical computer can perform the same task in a reasonable amount of time and this differential is unlikely to be overturned by classical algorithmic or hardware improvements, it is called quantum computational advantage or quantum supremacy (*7*, *8*). Here, we use the first term.

A recent experiment on a 53-qubit processor generated a million noisy (~0.2% fidelity) samples in 200 s (*8*), whereas a supercomputer would take 10,000 years. It was soon argued that the classical algorithm can be improved so that it would cost only a few days to compute all the 2^{53} quantum probability amplitudes and generate ideal samples (*9*). Thus, if the competition were to generate a much larger number of samples (for example, ~10^{10}), the quantum advantage would be reversed if there were sufficient storage. This sample size dependence of the comparison—an analog to loopholes in Bell tests (*10*)—suggests that quantum advantage would require long-term competitions between faster classical simulations and improved quantum devices.

Boson sampling, proposed by Aaronson and Arkhipov (*4*), was the first feasible protocol for quantum computational advantage. In boson sampling and its variants (*11*, *12*), nonclassical light is injected into a linear optical network, and the highly random, photon number– and path-entangled output state is measured by single-photon detectors. The dimension of the entangled state grows exponentially with both the number of photons and the modes, which quickly renders the storage of the quantum probability amplitudes impossible. The state-of-the-art classical simulation algorithm calculates one probability amplitude (Permanent of the submatrix) at a time. The Permanent is classically hard, and because at least one Permanent is evaluated for each sample (*13*, *14*), the sample size loophole can be avoided. In

[1]Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, China. [2]CAS Centre for Excellence and Synergetic Innovation Centre in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China. [3]State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, China. [4]Department of Computer Science and Technology and Beijing National Research Center for Information Science and Technology, Tsinghua University, Beijing 100084, China.
*These authors contributed equally to this work.
†Corresponding author. Email: cylu@ustc.edu.cn (C.-Y.L.); pan@ustc.edu.cn (J.-W.P.)

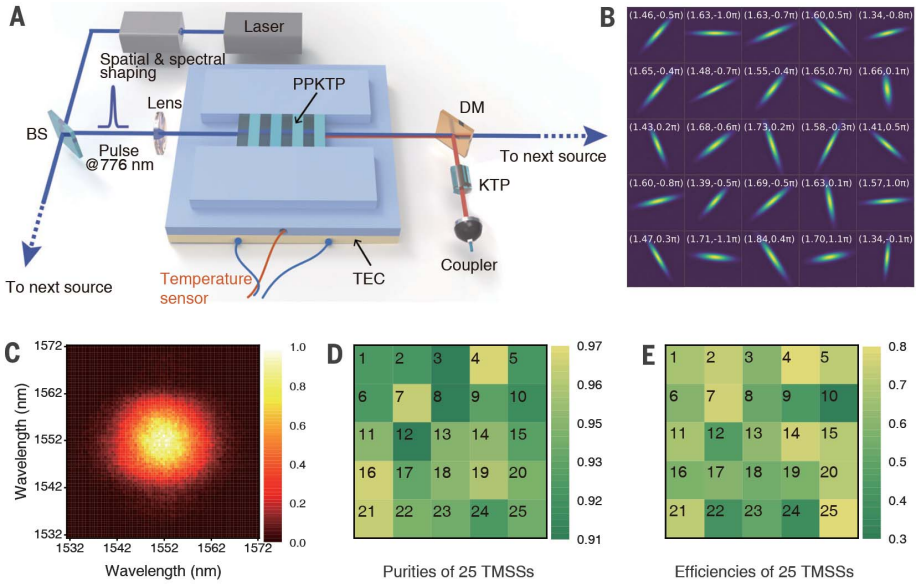


Fig. 1. Quantum light sources for Gaussian boson sampling (GBS). (**A**) An illustration of the experimental setup for generating squeezed states. A custom-designed laser system—consisting of a Coherent Mira 900, a pulse shaper, and a Coherent RegA 9000—generates the pump laser, which is spectrally and spatially shaped to reach transform limit (figs. S1 and S2). The pulsed laser is split by beamsplitters (BSs) into 13 paths (figs. S3 and S4) and focused onto 25 PPKTP crystals. Each crystal is placed on a thermoelectric cooler (TEC) for wavelength tuning. The downconverted photons are separated from the pumping laser by a dichromic mirror (DM); the time walk between different polarizations is compensated by a KTP crystal. (**B**) Wigner functions of all the 25 sources, showing the squeezing parameter r and phase ϕ of each source. In each subplot, the color encoding from purple to yellow represents a Wigner function from zero to its maximum. (**C**) The measured joint spectrum of the photon pairs indicates that the two photons are frequency-uncorrelated. (**D**) The purity of the 25 photon sources. The measured average purity is 0.938, obtained by unheralded second-order correlation measurement. (**E**) The measured collection efficiencies, with an average of 0.628.

addition, boson samplers use photons that can be operated at room temperature and are robust to decoherence.

Early proof-of-principle demonstrations of boson sampling (*15*, *16*) used probabilistic, post-selected pseudo–single photons from parametric downconversion (PDC) (*17*). Improved single-photon sources based on quantum dots were developed and were used to increase the multiphoton count rates, which culminated at 14-photon detection (*18*). However, scaling up boson sampling to a computationally interesting regime remained an outstanding experimental challenge.

Recently, Gaussian boson sampling (GBS) (*11*, *12*) has emerged as a new paradigm that not only can provide a highly efficient approach to large-scale implementations but also can offer potential applications in graph-based problems (*19*) and quantum chemistry (*20*). Instead of using single photons, GBS makes full use of the Gaussian nature of the PDC sources and uses single-mode squeezed states (SMSSs) as input nonclassical light sources, which can be deterministically prepared. Sending k SMSSs through an m-mode interferometer and sampling the output scattering events using threshold detectors (fig. S1), Quesada *et al.* showed that the output distribution is related to a matrix function called Torontonian (*12*), which is related to Permanent. Computing the Torontonian appears to be a computationally hard problem in the complexity class #P-hard. Li *et al*. recently showed that it takes about 2 days to evaluate a Torontonian function for a 50-photon click pattern (*21*).

Although small-scale demonstrations of GBS with up to five photons have been reported (*22*, *23*), implementing a large-scale GBS incurs technological challenges: (i) It requires arrays of SMSSs with sufficiently high squeezing parameters, photon indistinguishability, and collection efficiency. (ii) Large interferometers are needed with full connectivity, matrix randomness, near-perfect wave-packet overlap and phase stability, and near-unity transmission rate. (iii) In contrast to the Aaronson-Arkhipov boson sampling, where there is no phase relation between single photons, GBS requires phase control of all the photon number states in the SMSSs. (iv) High-efficiency detectors are needed to sample the output distribution. (v) The obtained sparse samples from a huge output state space should be validated, and the performance of the GBS should be benchmarked and compared with a supercomputer.

We start by describing the quantum light source arrays. Transform-limited laser pulses, with an average power of 1.4 W at a repetition rate of 250 kHz (figs. S1 and S2), are split into 13 paths and focused on 25 periodically poled potassium titanyl phosphate (PPKTP) crystals (Fig. 1A and figs. S3 and S4) to produce 25 two-mode squeezed states (TMSSs), which is equivalent to 50 SMSSs with a hybrid encoding (see below). The relative phase and squeezing parameter for each pair are shown in Fig. 1B. The PPKTP crystals are designed and temperature-controlled (fig. S5) to generate degenerate and frequency-uncorrelated photon pairs, as confirmed by the joint spectrum in Fig. 1C, which predicts a spectral purity of 0.98. The purity is increased to 0.99 by 12-nm filtering (figs. S6 and S7). A second estimation of the pairwise purity is by unheralded second-order correlation measurements (*24*). The measured purities are plotted in Fig. 1D, with an average of 0.938. The decrease of purity relative to the prediction from the joint spectra is mainly due to self–phase modulation. Figure 1E shows that the average collection efficiency is 0.628.

The whole optical setup—from the 25 PPKTPs to the 100-mode interferometer—must be locked to a fixed phase in the presence of various environmental perturbations. To achieve this aim, we developed an active phase-locking system (Fig. 2A) that covers the whole optical path, in combination with passive stabilization inside the interferometer (Fig. 2B) (*25*). For the active locking, the phase of the 776-nm laser is locked with a standard deviation of 0.04 rad [~5 nm (*25*)] (Fig. 2B, top). For the passive stabilization, the drift is controlled to be within λ/180 in 3.5 hours (Fig. 2B, bottom). For the whole system (Fig. 2D), the high-frequency noise standard deviation is λ/350 and the low-frequency drift is λ/63 within 1 hour, a time sufficient for completing the sampling and characterizations. We estimate that the drop in photon interference visibility as a result of the phase instability is less than 1%.

We made use of the photons' spatial and polarization degrees of freedom to realize a 100 × 100 unitary transformation (*15*, *26*). Here, the mode mapping is {1, 2, ... 100} = $\{|H\rangle_1|V\rangle_1|H\rangle_2|V\rangle_2 \ldots |H\rangle_{50}|V\rangle_{50}\}$, where H and V denote horizontal and vertical polarization, respectively, and the subscripts denote the spatial mode in the interferometer. We developed a compact three-dimensional design for the 50–spatial mode interferometer, which

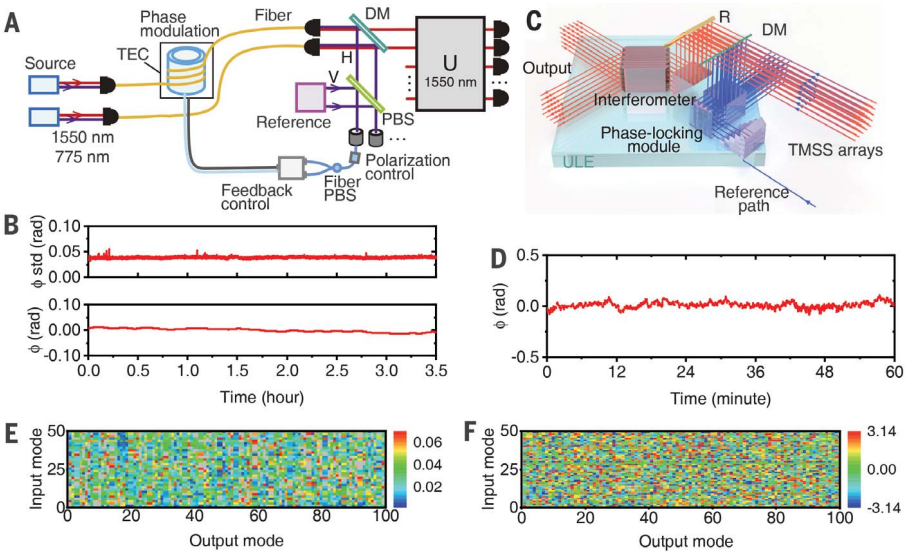


Fig. 2. Phase locking from the photon sources to the interferometer. (**A**) Schematic diagram of the active phase-locking system. A pump laser beam is used as a reference for all the squeezed states. After propagating through a ~2-m free space and 20-m optical fiber, a ~10-μW pump laser that shares the same propagation path as the downconverted photons is separated by a dichromatic mirror; The pump laser pulses are then combined on a beamsplitter with the reference laser pulse. A balanced detection scheme, which is insensitive to laser power fluctuation, is used to read out the phase information. To overcome the path length fluctuation, we wind optical fiber (length 5 m) around a piezoelectric cylinder with sensitivity of 1.5 rad/V, resonance frequency of 18.3 KHz, and dynamical range of 300 rad. (**B**) Phase stability tests. The top and bottom panels respectively show a typical monitoring of phase fluctuation of active and passive phase locking over 3.5 hours. The measured standard deviation of the phase is as small as 0.02 rad (λ/150) for active phase locking and 0.017 rad (λ/180) for passive phase locking. (**C**) We apply passive phase stabilization to the interferometer by adhering the devices onto an ultralow-expansion glass plate that is temperature-stabilized within 0.02°C. The blue light paths are for the interference of the 25 pumping lasers with the reference laser. The red light paths are the input and output of the photonic network. R denotes a reflective mirror. (**D**) A typical phase stability measurement of the whole system in 1 hour. (**E**) Diagram of the measured 5000 amplitudes of the matrix. (**F**) Diagram of the measured 5000 phases of the matrix.

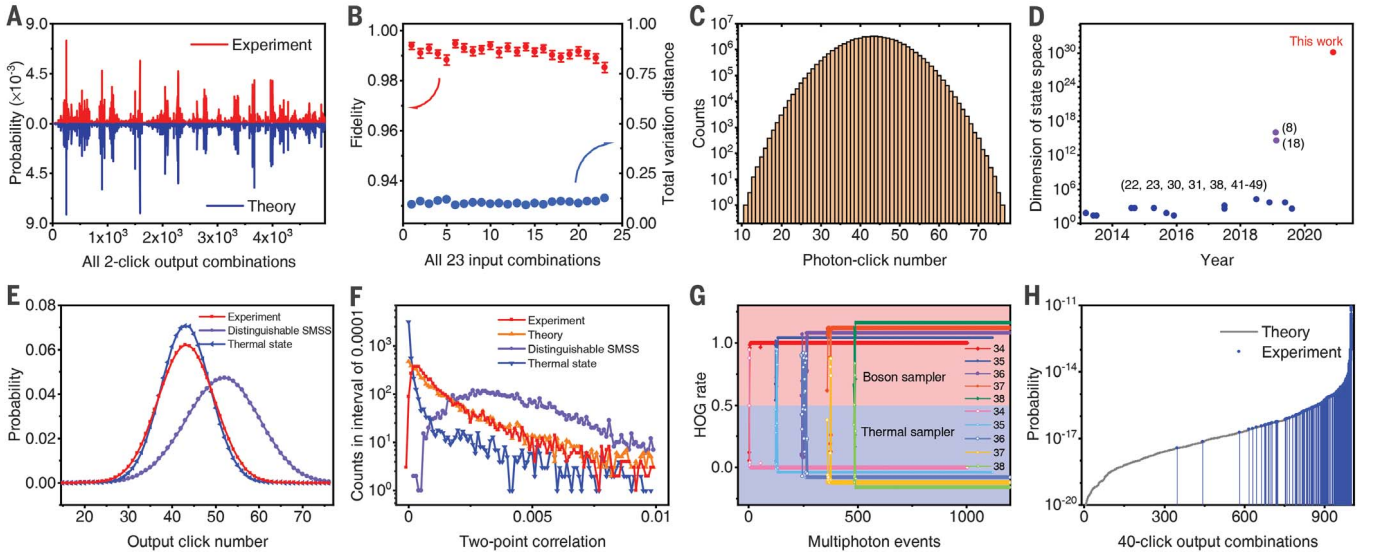


Fig. 3. Experimental validation of the GBS setup. (**A**) Experimental (red) and theoretical (blue) two-photon distribution with three TMSSs input. (**B**) Summary of statistical fidelity and total variation distance of two-photon distribution for 23 different input sets. (**C**) Output photon number distribution with all 25 TMSSs input. The average detected photon number is 43; the maximal detected photon number is 76. (**D**) Summary of the output state-space dimension. (**E**) Photon number distributions of the experimental result (red) and from the thermal state (blue) and distinguishable SMSS (purple) hypotheses. The deviations of the line shape and peak positions indicate that our experiment is far from these two hypotheses. (**F**) Two-photon correlation statistics for all two-mode combinations. The statistic of the experimental results (red) highly overlap with the theoretical predictions (orange) and deviate from the thermal state hypothesis (blue) and the distinguishable SMSS hypothesis (purple). (**G**) Validation against thermal state hypothesis with detected photon number ranging from 34 to 38. (**H**) Validation against uniform distribution.

simultaneously fulfills near-perfect phase stability and wave-packet overlap, full connectivity, random matrix, and near-unity transmission rate (Fig. 2C) (*25*). This optical network effectively consists of 300 beamsplitters and 75 mirrors (see fig. S9). The transmission rate of the interferometer is measured to be 97.7%, and the average coupling efficiency in all the output ports is ~90%. We estimate that the mode mismatch causes a ~0.2% drop of the interference visibility between independent photons.

Contrary to the Aaronson-Arkhipov boson sampling, where the sampling matrix is given solely by the interferometer, the GBS matrix absorbs both the unitary transformation of the interferometer and the squeezing parameters and phases of the Gaussian input state. We reconstructed the corresponding unitary matrix of the spatial polarization hybrid-encoded 100 × 100 interferometer, as plotted in Fig. 2, E and F, for the elements of amplitudes and phases, respectively. Further analysis shows that the obtained matrix is unitary (fig. S14) and Haar-random (fig. S15).

We named our GBS machine *Jiuzhang*. We first describe the experimental results from the easy regime, where we can obtain the full output distribution. We tested with three pairs of input TMSSs and two-photon click in the output. The obtained distribution is plotted in Fig. 3A. We use fidelity (F) and total variation distance (D) to characterize the obtained distribution, defined by $F = \sum_i \sqrt{p_i q_i}$, and $D = \sum_i |p_i - q_i|/2$ (p_i and q_i denote the theoretical and experimental probability of the ith basis, respectively). For a perfect boson sampler, the fidelity should equal 1 and the distance should be 0. The measured average fidelity is 0.990 ± 0.001, and the measured average distance is 0.103 ± 0.001. The data for all 23 different input configurations are shown in Fig. 3B, which confirms that the GBS works properly.

We next consider the sparse and intractable regime. Using 25 TMSSs as input, the output photon number distribution using threshold detectors is plotted in Fig. 3C. The average click number is 43. Within 200 s, we obtained 3,097,810 events of 43-photon coincidence, and one 76-photon coincidence. The state-space dimension of our experiment is plotted in Fig. 3D, reaching up to 10^{30}, which is 14 and 16 orders of magnitude larger than the dimension achieved in previous experiments using superconducting qubits (*8*) and single photons (*18*), respectively.

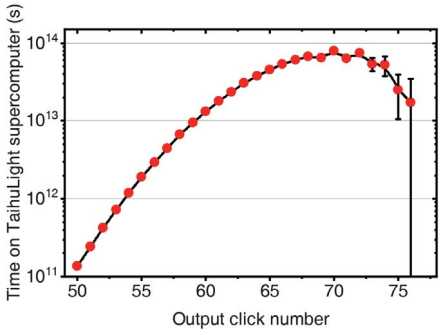


Fig. 4. Classical computational cost. The estimated time cost on a Sunway TaihuLight supercomputer is plotted as a function of the output photon click number. The error bar is calculated from Poissonian counting statistics of the raw detected events.

Although a full verification of the results in the large–photon number regime is unlikely because of the nature of the sampling problem, we hope to provide strong evidence that the large-scale GBS continues to be governed by quantum mechanics when it reaches the quantum advantage regime. The credibility of the certification processes (*27*–*32*) relies on gathering circumstantial evidence while ruling out alternative hypotheses that might be plausible in this experiment. We validated the desired input TMSSs against input photons that are thermal states (which would result from excessive photon loss) and are distinguishable (which would be caused by mode mismatch).

We began by comparing the obtained output distribution with the hypotheses using thermal light and distinguishable SMSSs. Figure 3E shows evidently strong deviations in line shapes and peak positions, which imply that the obtained distribution indeed arises from genuine multiphoton quantum interference. We then investigated two-point correlation (*32*), which is derived from the Hanbury-Brown-Twiss experiment, to reveal the nonclassical

properties of the output light field. Here, the two-point correlation between mode i and mode j is defined as $C_{i,j} = \langle \Pi_1^i \Pi_1^j \rangle - \langle \Pi_1^i \rangle \langle \Pi_1^j \rangle$, where $\Pi_1^i = \mathbf{I} - |0\rangle_i\langle 0|_i$ represents a click in mode i. We calculated the distribution of all values of $C_{i,j}$ for the experimentally obtained samples, and then compared the result with those from theoretical predictions, the thermal-states hypothesis, and the distinguishable-SMSSs hypothesis. As shown in Fig. 3F, the statistics of experimental samples diverge from the two hypotheses and agree with the theoretical prediction.

Having studied the whole distribution, we closely looked into each subspace with a specific photon click number. We developed a method called the heavy output generation (HOG) ratio test (*25*). Figure 3G and fig. S26 show typical examples of HOG analysis for photon clicks from 26 to 38, which show a stark difference between TMSSs with thermal states. We emphasize that the tested 26- to 38-click regime—which shares the same setup as higher photon number—is in the post-selected subspace that effectively suffers from more photon loss than in the regime with a larger number of clicks, which we deduce can be validated against the thermal-states hypothesis with higher confidence.

We continue to rule out another important hypothesis that boson sampling output would be operationally indistinguishable from a uniform random outcome, one of the earliest criticisms (*27*) of boson sampling. In stark contrast, because of constructive and destructive interference, an ideal boson sampler is expected to generate samples with lognormal-like distribution (*4*, *27*). We developed a method (*25*) to reconstruct the theoretical probability distribution curve for the 40-photon case (Fig. 3H). We can match each obtained sample to the theoretical curve, as illustrated by the blue data points and vertical blue lines in Fig. 3H (see fig. S27 for more data). The frequency of occurrence of the blue lines is in good agreement with the probability curve, which intuitively indicates that our results cannot be reproduced by a uniform sampler.

Finally, we estimated the classical computational cost to simulate an ideal GBS device. We have benchmarked the GBS on the Sunway TaihuLight supercomputer (*21*) using a highly optimized algorithm (*33*). The time cost to calculate one Torontonian scales exponentially as a function of output photon clicks. Moreover, to obtain one sample usually requires the calculation of ~100 Torontonians of the candidate samples (*13*). The GBS simultaneously generates samples of different photon-number coincidences (Fig. 3C), which can be seen as a high-throughput sampling machine. For each output channel and the registered counts in Fig. 3C, we calculated the corresponding time cost for the supercomputer (Fig. 4). Summing over the data points in Fig. 4, we estimate that the required time cost for the TaihuLight to generate the same number of samples in 200 s with the GBS device would be 8×10^{16} s, or 2.5 billion years. For the Fugaku supercomputer, the time cost would be 2×10^{16} s, or 0.6 billion years. We hope that this work will inspire new theoretical efforts to quantitatively characterize large-scale GBS, improve the classical simulation strategies optimized for the realistic parameters (*33*, *34*), and challenge the observed quantum computational advantage of ~10^{14}.

REFERENCES AND NOTES

1. E. Bernstein, U. Vazirani, in *Proceedings of the 25th Annual ACM Symposium on Theory of Computing* (1993).
2. P. W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (1994).
3. B. M. Terhal, D. P. DiVincenzo, arXiv 0205133 [quant-ph] (11 March 2004).
4. S. Aaronson, A. Arkhipov, in *Proceedings of the 43rd Annual ACM Symposium on Theory of Computing* (2011).
5. S. Aaronson, L. Chen, in *Proceedings of the 32nd Computational Complexity Conference* (2017).
6. M. J. Bremner, A. Montanaro, D. J. Shepherd, *Phys. Rev. Lett.* **117**, 080501 (2016).
7. J. Preskill, Rapporteur talk at the 25th Solvay Conference on Physics, Brussels (2012).
8. F. Arute *et al*., *Nature* **574**, 505–510 (2019).
9. E. Pednault, J. A. Gunnels, G. Nannicini, L. Horesh, R. Wisnieff, arXiv 1910.09534 [quant-ph] (22 October 2019).
10. A. W. Harrow, A. Montanaro, *Nature* **549**, 203–209 (2017).
11. C. S. Hamilton *et al*., *Phys. Rev. Lett.* **119**, 170501 (2017).
12. N. Quesada, J. M. Arrazola, N. Killoran, *Phys. Rev. A* **98**, 062322 (2018).
13. A. Neville *et al*., *Nat. Phys.* **13**, 1153–1157 (2017).
14. P. Clifford, R. Clifford, in *Proceedings of the 29th Annual ACM-SIAM Symposium on Discrete Algorithms* (2018).
15. M. A. Broome *et al*., *Science* **339**, 794–798 (2013).
16. J. B. Spring *et al*., *Science* **339**, 798–801 (2013).
17. P. G. Kwiat *et al*., *Phys. Rev. Lett.* **75**, 4337–4341 (1995).
18. H. Wang *et al*., *Phys. Rev. Lett.* **123**, 250503 (2019).
19. J. M. Arrazola, T. R. Bromley, *Phys. Rev. Lett.* **121**, 030503 (2018).
20. J. Huh, G. G. Guerreschi, B. Peropadre, J. R. McClean, A. Aspuru-Guzik, *Nat. Photonics* **9**, 615–620 (2015).
21. X. Li *et al*., arXiv 2009.01177 [cs.DC] (2 September 2020).
22. H.-S. Zhong *et al*., *Sci. Bull.* **64**, 511–515 (2019).
23. S. Paesani *et al*., *Nat. Phys.* **15**, 925–929 (2019).
24. A. Christ, K. Laiho, A. Eckstein, K. N. Cassemiro, C. Silberhorn, *New J. Phys.* **13**, 033027 (2011).
25. See supplementary materials.
26. I. Dhand, S. K. Goyal, *Phys. Rev. A* **92**, 043813 (2015).
27. S. Aaronson, A. Arkhipov, *Quantum Inf. Comput.* **14**, 1383 (2014).
28. M. C. Tichy, K. Mayer, A. Buchleitner, K. Mølmer, *Phys. Rev. Lett.* **113**, 020502 (2014).
29. M. Walschaers *et al*., *New J. Phys.* **18**, 032001 (2016).
30. N. Spagnolo *et al*., *Nat. Photonics* **8**, 615–620 (2014).
31. J. Carolan *et al*., *Nat. Photonics* **8**, 621–626 (2014).
32. D. S. Phillips *et al*., *Phys. Rev. A* **99**, 023836 (2019).
33. N. Quesada, J. M. Arrazola, *Phys. Rev. Res.* **2**, 023005 (2020).
34. H. Qi, D. J. Brod, N. Quesada, R. García-Patrón, *Phys. Rev. Lett.* **124**, 100502 (2020).

ACKNOWLEDGMENTS

This work is dedicated to the people in the fight against the COVID-19 outbreak, during which the final stage of this experiment was carried out. We thank J. Renema, J. P. Dowling, C. Weedbrook, N. Quesada, Y. Jiang, J.-W. Jiang, S.-Q. Gong, B.-B. Wang, Y.-H. Li, H.-W. Cheng, Q. Shen, Y. Cao, Y. Chen, H. Lu, H. Fu, and T.-Y. Chen for very helpful discussions and assistance. **Funding:** Supported by the National Natural Science Foundation of China, the National Key R&D Program of China, the Chinese Academy of Sciences, the Anhui Initiative in Quantum Information Technologies, and the Science and Technology Commission of Shanghai Municipality. **Author contributions:** C.-Y.L. and J.-W.P. designed and supervised the research. H.-S.Z., M.-C.C., and J.Q. developed the theory. H.-S.Z., H.W., Y.-H.D., L.-C.P., Y.-H.L., J.Q., D.W., X.D., L.L., N.-L.L., and C.-Y.L. carried out the optical experiment and collected the data. Y.H. and X.J. designed the 100-channel counter. M.-C.C., Y.L., P.H., L.G., and G.Y. performed data analysis and validation on a supercomputer. P.H., X.-Y.Y., W.-J.Z., H.L., L.Y., and Z.W. developed single-photon detectors. H.-S.Z., M.-C.C., C.-Y.L., and J.-W.P. analyzed the data and prepared the manuscript. All authors discussed the results and reviewed the manuscript. **Competing interests:** The authors declare no competing interests. **Data and materials availability:** All data are available in the manuscript or the supplementary materials.

SUPPLEMENTARY MATERIALS

science.sciencemag.org/content/370/6523/1460/suppl/DC1
Materials and Methods
Supplementary Text
Figs. S1 to S28
Tables S1 to S3
References (*35*–*50*)

19 September 2020; accepted 19 November 2020
Published online 3 December 2020
10.1126/science.abe8770

Chapter 13

Quantum Sensing

There are other uses of entanglement beyond communication and computation: making better measurements by increasing resolution, known as quantum sensing.

The concept can be traced back to the 1956 publication by Hanbury Brown and Twiss who showed in 1956 that a very high angular resolution could be achieved by measuring correlations between two telescopes. They could measure the angular size of the star Sirius with two small telescopes coupled to single photon detectors (photomultiplier tubes). Each telescope was far too small to resolve the size of Sirius, it was only the correlations between the two telescopes that gave enough resolution to resolve the size of Sirius. Michelson showed that higher spatial resolution can be obtained by increasing a telescope aperture with additional mirrors, Hanbury Brown and Twiss showed that correlations among photon detection events from two independent telescopes can also yield increased angular resolution.

Figure 13.1: Two telescopes focus incoming light from a distant star. Correlation measurements between the two detectors yields the angular size of the star. The resolution is equivalent to a telescope with an aperture equal to the distance between the two telescopes.

Michelson showed that higher spatial resolution can be obtained by increasing a telescope aperture with additional mirrors, Hanbury Brown and Twiss showed that correlations among photon detection events from two independent telescopes can also yield increased angular resolution.

13.1 NOON states

Non-classical states of light can yield more precise measurements than classical states of light composed of the same number of photons. There could be applications for these effects in phase measurements or lithography.

We use NOON states where all photons are in one mode or the other: $|N0\rangle + |0N\rangle$ are interesting, they are maximally entangled states (MES).

$$|\Psi_N\rangle_{MES} = \frac{1}{\sqrt{2}}(|N0\rangle + e^{i\phi_N}\,|0N\rangle)$$

Generating a state with $N = 2$ is rather easy, it is for instance the output of a Hong-Ou-Mandel experiment. But generating NOON states with $N > 2$ is tricky.

We can use a NOON state for a phase measurement:

With classical light, we have $\Delta\theta = \frac{1}{\sqrt{n}}$ where n is the mean number of photons.

For N=2 NOON state, we have:

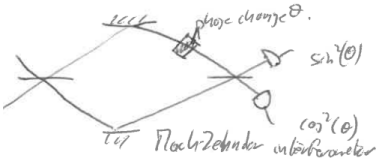


Figure 13.2: A Mach Zehnder intereferometer can be used to measure phase changes in one arm.

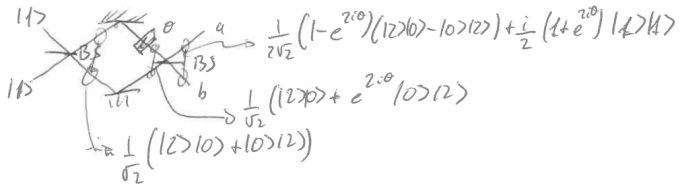


Figure 13.3: A NOON state with N=2 gives a more precise measurement of the phase difference in a Mach Zehnder intereferometer.

For a NOON state, we have a phase shift of $e^{N\theta}$ whereas for a classical state we get a $\sqrt{N}$ increase. This is clearly a quantum advantage but is only interesting for high N and this scheme is sensitive to photon losses: the NOON state must be preserved through the interferometer and be detected.

Interpretation of this experiment: the momentum of the photon wave packet is N times larger than for a single photon, one could say that the effective wavelength is reduced by 1/N.

Any intereference pattern will be shortened by a factor 1/N, this is very interesting for quantum photolithography.

13.2 Quantum Imaging

Quantum imaging can be performed with pairs of photon that have correlated momentum. The two photons can be non-degenerate, we could direct infrared photons on the object to be imaged and use a visible or blue photon for direct detection on a fast imaging detector. The fast imaging detector records precisely the photon direction. The detector placed behind the object is a bucket detector: it is a large, single pixel detector that only measures whether the photon was transmitted by the object or not. The measurements performed on one of the two arms clearly do not yield any interesting data, only random events. However, when correlations are measured, we can obtain a very sharp image of the object under study. For every photon that was transmitted through the object, by correlating with the imaging detector we obtain the corresponding momentum of the transmitted photon. Because infrared light can be shone on the object, a very sensitive object that could not be imaged with visible light can be studied. This technique can also be applied to microscopy, in the European project FastGhost we are building a ghost imaging microscope.

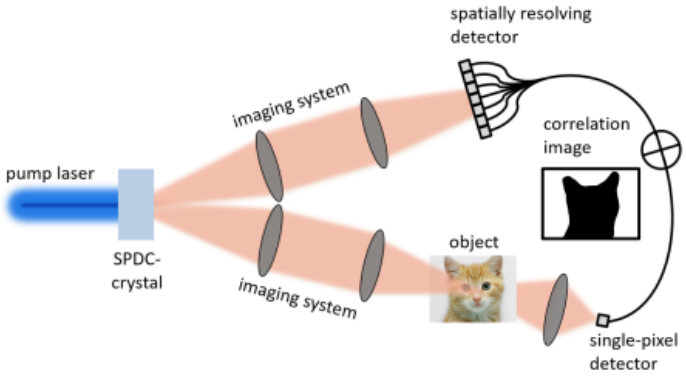


Figure 13.4: In quantum imaging, pairs of photons are generated, one photon is imaged directly, the other is transmitted through an object. Correlations between the two events yield a sharp image of the object.

One question is what is quantum and what is not? For instance, performing Lidar measurements with a single photon detector, that is building 3D images one photon at a time can be quantum sensing to some and not to others.

13.3 Quantum Microscopy

We can also make use of quantum measurements in an optical microscope to increase spatial resolution and beat the diffraction limit. When observing a single photon source, we can build an image of the photon intensity, a very usual and straightforward task. But we can also measure and plot two photon correlation events, this gives a higher resolution and we can proceed to higher order correlation events and obtain even higher resolution. There is in principle no limit to this technique, just that acquiring very high order correlations takes a very long time because it requires unlikely detection events to occur.

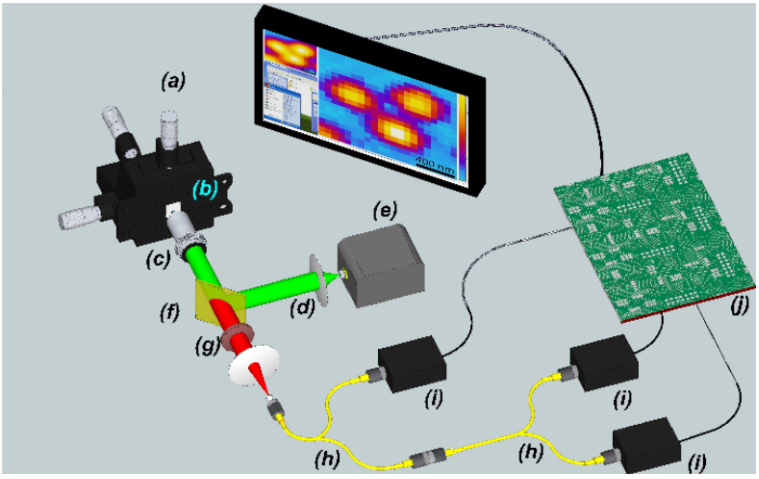


Figure 13.5: An optical microscope is used to image single defects in diamond. The light intensity is plotted as a function of position. Taken from Phys. Rev. Lett. 113, 143602 (2014)

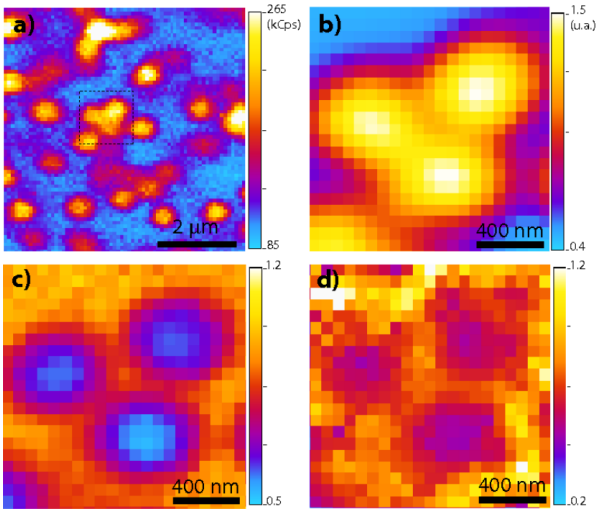


Figure 13.6: (a) microscopy image of single photon emitters. (b) magnification of the area of interest. (c)plot of the second order correlation function. (d)plot of the third order correlation function. Taken from Phys. Rev. Lett. 113, 143602 (2014)

13.4 Quantum Lidar

Lidar is radar with light: a pulse of light is sent out and the time taken for some of the pulse is measured as a function of direction to build an image. Because very short light pulses of the order of picoseconds can be propagated over long distances and because detectors with 10 picosecond of time resolution are available, very precise three dimenstional images can be obtained.

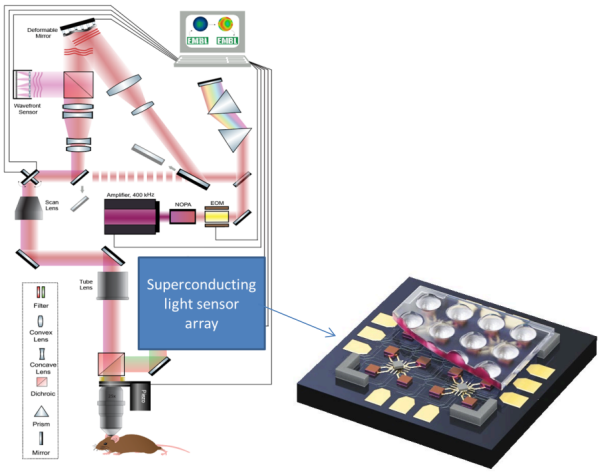


Figure 13.7: In the European project Brainiaqs, a single photon infrared microscope is being built to image in live brains.

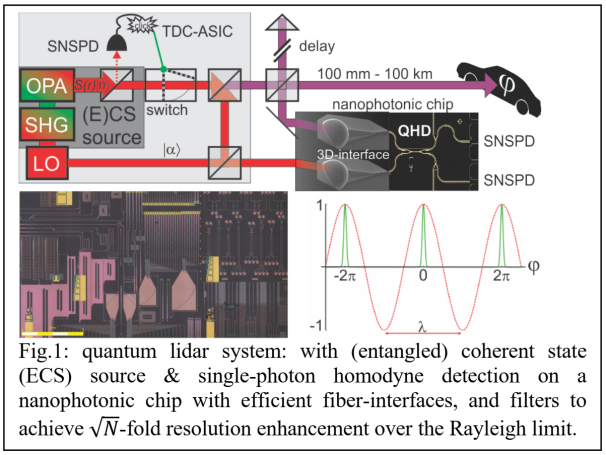


Fig.1: quantum lidar system: with (entangled) coherent state (ECS) source & single-photon homodyne detection on a nanophotonic chip with efficient fiber-interfaces, and filters to achieve $\sqrt{N}$-fold resolution enhancement over the Rayleigh limit.

Figure 13.8: In the European project Surquid, we are building a quantum lidar.

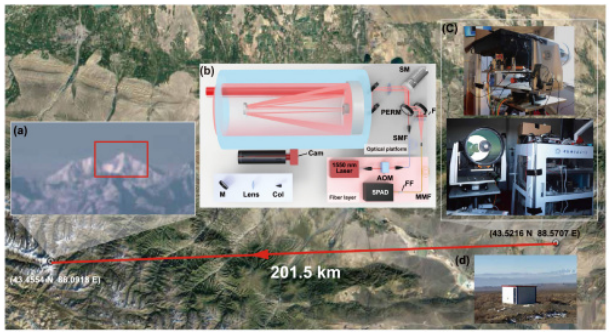


Figure 13.9: Very long distance lidar: a laser pulse is sent towards a mountain 200 km away and the reflected light is detected to build a 3D image. Taken from Optica Vol. 8, Issue 3, pp. 344-349 (2021).

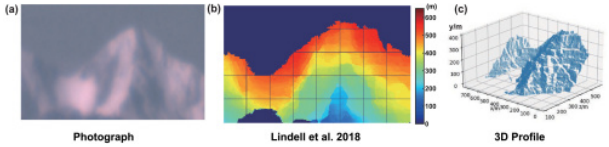


Figure 13.10: Lidar image of a mountain 200 km away obtained with single photon detectors. Taken from Optica Vol. 8, Issue 3, pp. 344-349 (2021).

LETTER

doi:10.1038/nature13586

Quantum imaging with undetected photons

Gabriela Barreto Lemos[1,2], Victoria Borish[1,3], Garrett D. Cole[2,3], Sven Ramelow[1,3]†, Radek Lapkiewicz[1,3] & Anton Zeilinger[1,2,3]

Information is central to quantum mechanics. In particular, quantum interference occurs only if there exists no information to distinguish between the superposed states. The mere possibility of obtaining information that could distinguish between overlapping states inhibits quantum interference[1,2]. Here we introduce and experimentally demonstrate a quantum imaging concept based on induced coherence without induced emission[3,4]. Our experiment uses two separate down-conversion nonlinear crystals (numbered NL1 and NL2), each illuminated by the same pump laser, creating one pair of photons (denoted idler and signal). If the photon pair is created in NL1, one photon (the idler) passes through the object to be imaged and is overlapped with the idler amplitude created in NL2, its source thus being undefined. Interference of the signal amplitudes coming from the two crystals then reveals the image of the object. The photons that pass through the imaged object (idler photons from NL1) are never detected, while we obtain images exclusively with the signal photons (from NL1 and NL2), which do not interact with the object. Our experiment is fundamentally different from previous quantum imaging techniques, such as interaction-free imaging[5] or ghost imaging[6–9], because now the photons used to illuminate the object do not have to be detected at all and no coincidence detection is necessary. This enables the probe wavelength to be chosen in a range for which suitable detectors are not available. To illustrate this, we show images of objects that are either opaque or invisible to the detected photons. Our experiment is a prototype in quantum information—knowledge can be extracted by, and about, a photon that is never detected.

The conceptual arrangement of our imaging technique, based on a quantum interference experiment[3,4] by Zou, Wang and Mandel, is illustrated in Fig. 1. A pump beam (green) divided by a 50:50 beam splitter (BS1) coherently illuminates two identical nonlinear crystals, NL1 and NL2, where pairs of collinear photons called signal (yellow) and idler (red) can be created ($|c\rangle|d\rangle$ in NL1 and $|e\rangle|f\rangle$ in NL2). The idler amplitude created in NL1 reflects at the dichroic mirror D1 into spatial mode d, and signal amplitude passes into spatial mode c. The idler passes through the object O of real transmittance coefficient T and phase shift γ: $|c\rangle_s|d\rangle_i \rightarrow Te^{i\gamma}|c\rangle_s|d\rangle_i + \sqrt{1-T^2}|c\rangle_s|w\rangle_i$, where for simplicity we lump all lost idler amplitude into a single state $|w\rangle_i$ (here subscripts s and i represent signal and idler). By reflection at dichroic mirror D2, the idler from NL1 aligns perfectly with idler amplitude produced at NL2, $|d\rangle_i \rightarrow |f\rangle_i$. The state at the grey dotted line is thus

$$\frac{1}{\sqrt{2}}\left[\left(Te^{i\gamma}|c\rangle_s + |e\rangle_s\right)|f\rangle_i + \sqrt{1-T^2}|c\rangle_s|w\rangle_i\right] \quad (1)$$

The idler is now reflected at the dichroic mirror D3 and discarded. The signal states $|c\rangle_s$ and $|e\rangle_s$ are combined at the 50:50 beam splitter BS2. The detection probabilities at the outputs $|g\rangle_s$ and $|h\rangle_s$, obtained by ignoring (tracing out) the idler modes, are

$$P_{g/h} = \frac{1}{2}\left[1 \pm T\cos\gamma\right] \quad (2)$$

Thus, fringes with visibility T can be seen at either output, even though the signals combined at BS2 have different sources[4,10]. These fringes appear in the signal single photon counts; the idlers are not detected. No coincidence detection is required.

The peculiar feature of this interferometer is that no detected photon has taken path d. Yet, in our experiment, it is precisely here where we put the object to be imaged. The key to this experiment is how the signal-source information carried by the undetected idler photon depends on T. For, if $T = 0$, an idler detected after D3, coincident with a signal count at $|g\rangle_s$ or $|h\rangle_s$, would imply the signal source was NL2. Detection of a signal photon without a coincident idler would imply the signal source was NL1. This which-source information destroys interference because it makes the quantum states overlapping at BS2 distinguishable. If $T = 1$, the idler photon carries no which-source information. The signal states overlapped at each output of BS2 are then indistinguishable; thus the interference term in equation (2) appears. The above arguments are valid even though the idler photons are not detected, for it is only the possibility of obtaining which-source information that matters in this experiment.

Our experiment has a connection to interaction-free measurements[11,12]. Note that $P_h = 0$ if no object is placed in the set-up ($T = 1$ and $\gamma = 0$). Now insert an opaque object ($T = 0$) so that $P_h > 0$, and monitor the idler reflection from D3. Coincident counts in $|h\rangle_s$ and the idler detector reveal that the object is present even though no photon interacted with the object. With our set-up it is thus possible to realize non-degenerate interaction-free imaging.

With O and D2 removed, equation (1) would be an ordinary two-particle entanglement[13], $|c\rangle_s|d\rangle_i + |e\rangle_s|f\rangle_i$. With them in, $|d\rangle_i \rightarrow Te^{i\gamma}|f\rangle_i$, which creates equation (1). A normal two-particle entanglement has changed into an interesting single-particle superposition, which is especially rich when T and γ are transverse-position dependent.

We expand the conceptual arrangement of Fig. 1 into an imaging system (Fig. 2). We replace the photon counters with cameras sensitive to single photons and the uniform object with one bearing features, that is, $T = T(x, y)$ and $\gamma = \gamma(x, y)$ depend on transverse position (x, y). Our source produces spatially entangled photon pairs[14,15]. Sharp spatial correlations between signal and idler in the object plane and confocal lens systems[16] (see Methods) guarantee a point-by-point correspondence between the object plane and the detector surface on the camera.

The intensity image (non-constant transmittance) is due to transverse-position-dependent which-source information carried by the undetected idler photons. The phase image is of a different nature: it is due to the fact that the position-dependent phase shift on the idler photons in path d is actually passed to the signal; that is[17], $|c\rangle_s\left(Te^{i\gamma}|f\rangle_i\right) + |e\rangle_s|f\rangle_i = \left(Te^{i\gamma}|c\rangle_s + |e\rangle_s\right)|f\rangle_i$. Remarkably, the idler beam $|f\rangle_i$ alone does not even carry the phase pattern, and without detection in coincidence it could not be used to obtain the phase image[18,19].

We will now show images obtained by detecting 810-nm photons with a camera capable of single-photon sensitivity at this wavelength, when three different objects are illuminated by 1,550-nm photons, to which our camera is blind (see Methods). First, a cardboard cut-out placed into the path D1–D2 is imaged. Next, we show that a position-dependent phase shift produces an image even when the object is opaque (an etched silicon plate) or invisible (etched silica plate) at the detection

[1]Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanngasse 3, Vienna A-1090, Austria. [2]Vienna Center for Quantum Science and Technology (VCQ), Faculty of Physics, University of Vienna, A-1090 Vienna, Austria. [3]Quantum Optics, Quantum Nanophysics, Quantum Information, University of Vienna, Boltzmanngasse 5, Vienna A-1090, Austria. †Present address: Cornell University, 159 Clark Hall, 142 Science Drive, Ithaca, New York 14853, USA.

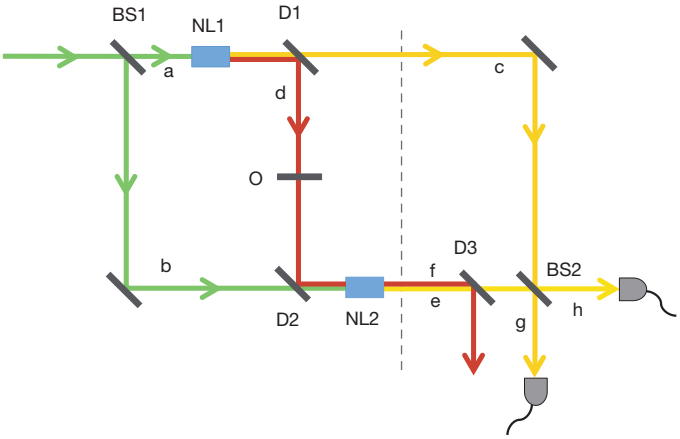


Figure 1 | Schematic of the experiment. Laser light (green) splits at beam splitter BS1 into modes a and b. Beam *a* pumps nonlinear crystal NL1, where collinear down-conversion may produce a pair of photons of different wavelengths called signal (yellow) and idler (red). After passing through the object O, the idler reflects at dichroic mirror D2 to align with the idler produced in NL2, such that the final emerging idler $|f\rangle_i$ does not contain any information about which crystal produced the photon pair. Therefore, signals $|c\rangle_s$ and $|e\rangle_s$ combined at beam splitter BS2 interfere. Consequently, signal beams $|g\rangle_s$ and $|h\rangle_s$ reveal idler transmission properties of object O.

wavelength. The images obtained with an electron multiplying charge coupled device (EMCCD) camera show single (non-heralded) counts per pixel (16 μm × 16 μm) obtained in an exposure time of 0.5 s with an electron multiplying gain factor of 20. The visibility achieved in the experiment is 77% (see Methods for details).

Figure 3a shows the beamsplitter output when a cardboard cut-out (illustrated in Fig. 3b) is inserted in the path D1–D2. Constructive interference is seen at one output of the beam splitter and destructive interference is observed in the other output. Interference only occurs in the region corresponding to the idler beam transmitted through the shape cut out of the cardboard, as seen in the sum and difference of the complementary images, shown in Fig. 3c and d, respectively. The sum of the two outputs of the beamsplitter gives the featureless intensity profile of the signal beams, demonstrating that the signal beams, while carrying the intensity information, are not absorbed at all by the mask.

In Fig. 4a, we show the image of an etched 500-μm-thick silicon plate; the plate is shown in Fig. 4b (see Methods section for details of the silicon plate and the etching process). Silicon is opaque to illumination at 810 nm,

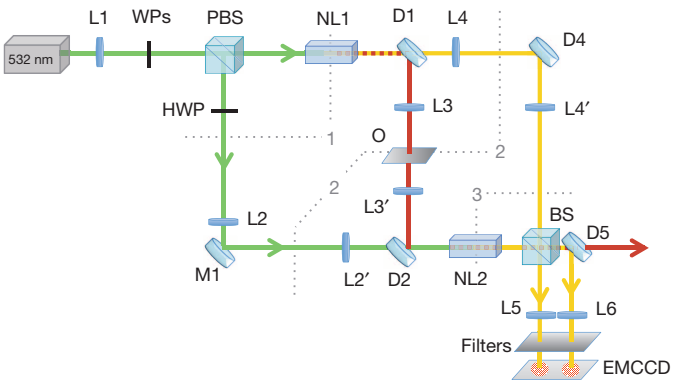


Figure 2 | Experimental set-up. A continuous-wave 532-nm laser (green) illuminates crystals NL1 and NL2. Wave plates (WPs) adjust the relative phase and intensity of the outputs of the polarizing beam splitter (PBS). The dichroic mirror D1 separates down-converted 810-nm (yellow) and 1,550-nm (red) photons. The 1,550-nm photons are transmitted through the object O and sent through NL2 by dichroic mirror D2. Lenses image plane 1 onto plane 3, and plane 2 onto the EMCCD camera. A 50:50 beam splitter (BS) combines the 810-nm beams. Dichroic mirrors D1, D2, D4 and D5 transmit the pump.

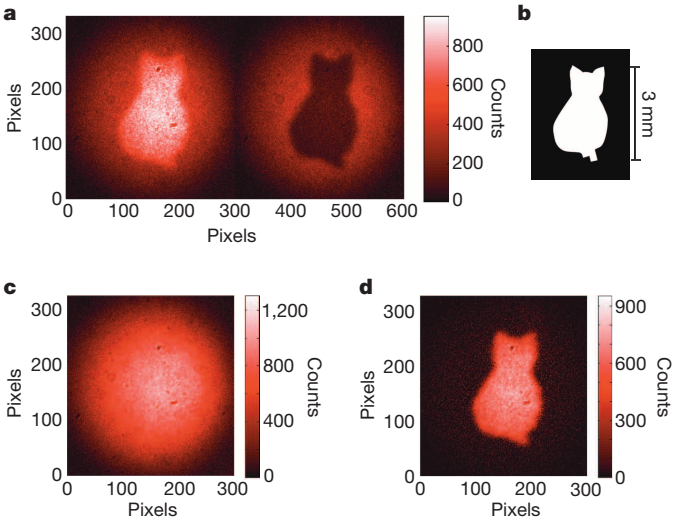


Figure 3 | Intensity imaging. **a**, Inside the cat, constructive and destructive interference are observed at the outputs of BS when we placed the cardboard cut-out shown in **b** in the path D1–D2. Outside the cat, idler photons from NL1 are blocked and therefore the signals do not interfere. **c**, The sum of the outputs gives the intensity profile of the signal beams. **d**, The subtraction of the outputs leads to an enhancement of the interference contrast, as it highlights the difference between constructive and destructive interference.

thus it is impossible to realize transmission imaging by illuminating the silicon with 810-nm photons. However, silicon is highly transparent at 1,550 nm and when we place the object in path D1–D2, the difference in optical path length for the etched and non-etched regions corresponds to a relative phase shift of π. Even though our camera is blind to 1,550-nm light, the image is seen by detecting 810-nm photons at the output of BS2 (Fig. 4a).

Finally, Fig. 5a shows the image of a fused silica (SiO_2) plate etched with a pattern that is invisible at the detection wavelength (details are given in the Methods section). We take advantage of the flexibility of our source to obtain collinear non-degenerate down-conversion at 820 nm

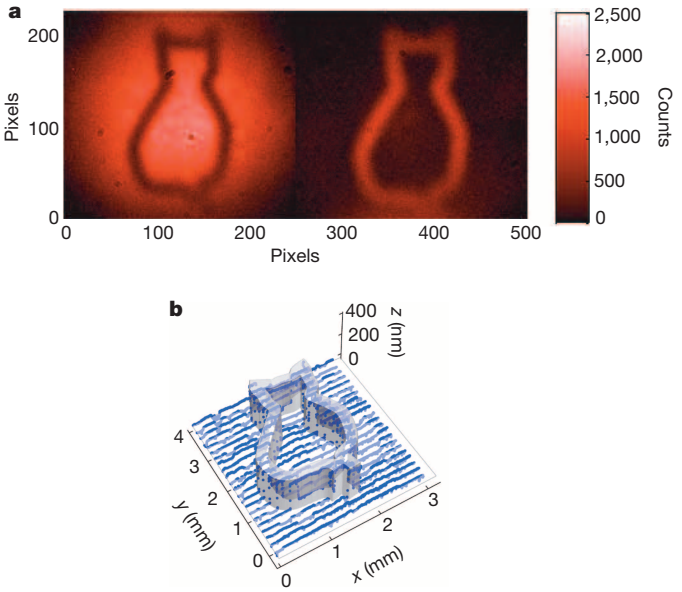


Figure 4 | Phase image of an object opaque to 810-nm light. **a**, Detection of 810-nm photons at both outputs of BS when a silicon plate (opaque to 810-nm light) with a 3-mm-tall etched cat (**b**) was introduced in path D1–D2. **b**, Three-dimensional rendering of the etch design overlaid with stylus profilometer scans (blue points) of the actual etch depth.

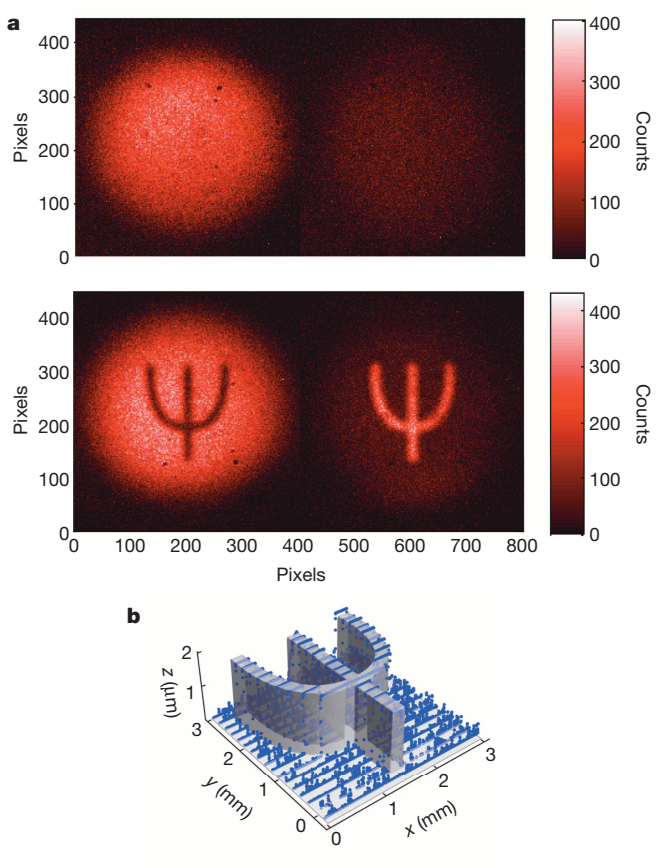


Figure 5 | Phase imaging of a 2π step at 820 nm. a, The top picture was taken with the object (shown in **b**) placed in the 820-nm beam between L4 and L4′; in the bottom picture, the object was placed in the 1,515-nm beam in path D1–D2. **b**, Three-dimensional rendering of the design overlaid with stylus profilometer scans (blue dots) of the actual etch depth.

and 1,515 nm (see Methods). The object (Fig. 5b) has an etch depth of 1,803 nm, imparting a relative phase shift of ~2π for 820-nm light. Thus the object is invisible when placed in the path of the detected photons between L4 and L4′ (top of Fig. 5a). This same etch depth gives an ~π phase step for 1,515-nm light, so when this same object is placed in the path D1–D2 of undetected photons, an image seen in the contrast of constructive to destructive interference is retrieved in the 820-nm outputs (bottom of Fig. 5a).

In summary, we have presented a quantum system for intensity and phase imaging where the photons that illuminate the object are not detected and the photons that are detected do not illuminate the object. We image objects that are either opaque or invisible at the detection wavelength (near-infrared) by illuminating three different objects with a wavelength to which our detector is blind. This experiment is fundamentally different to ghost imaging[6–9] as it relies on single-photon interference and does not require coincidence detection. Furthermore, our technique could be used for non-degenerate interaction-free imaging, with potential applications spanning biological imaging to the inspection of integrated circuits. Our system can realize grey-scale intensity or phase imaging, and it can be modified in order to measure spectral features (spectral imaging)[20].

We have demonstrated that our technique does not require the laser or the detector to function at the same wavelength as that of the light probing the object. Additionally, any nonlinear process can be used as a source, and this provides flexibility in the wavelength range for both detection and illumination of the object. In particular, in spontaneous parametric down-conversion (as used here), the only absolute restriction is that the sum of the two photon energies equals that of the pump photons. We have shown that information can be obtained about an object without detecting the photons that interacted with the object. Knowing the two-photon state, one can obtain information about an object. It has not escaped our attention that, on the other hand, by knowing the object, one could obtain information about the quantum state without detecting it.

METHODS SUMMARY

A detailed schematic of our imaging set-up is shown in Fig. 2. A 532-nm linearly polarized Gaussian pump laser beam focused by lens L1 on plane 1 is divided at a polarizing beam splitter (PBS) and coherently illuminates two identical periodically poled potassium titanyl phosphate (ppKTP) crystals, NL1 and NL2. The PBS plus wave plates (WPs) are used to control the relative amplitudes and phases between the reflected and transmitted pump beams. With an extra half-wave plate (HWP) in the reflected beam, both beams have the same polarization. The 1,550-nm idler amplitude produced at NL1 is reflected by dichroic mirror D1, through which the 810-nm signal and the pump are transmitted. Dichroic mirror D4 transmits 532-nm light and reflects 810-nm light. A long-pass filter (not shown in the figure) placed directly before the object O blocks any residual 532-nm or 810-nm light. The 1,550-nm amplitude from NL1 illuminates the object O and is then overlapped with the pump beam at dichroic mirror D2 that transmits 532-nm light and reflects 1,550-nm light.

Lens pairs L2–L2′, L3–L3′, and L4–L4′ image plane 1 onto plane 3, thereby ensuring that pump, idler and signal, respectively, are identical in these planes, thus contributing to obtain high interference visibility[21] (see Methods). Lenses L5 and L6 together with L3′ and L4′ image object plane 2 onto the camera surface.

The 810 ± 1.5 nm photons are detected (without heralding) in both outputs of the BS using an EMCCD camera that exhibits single-photon sensitivity at 810 nm, but has a negligible response at 1,550 nm.

Online Content Methods, along with any additional Extended Data display items and Source Data, are available in the online version of the paper; references unique to these sections appear only in the online paper.

Received 26 January; accepted 11 June 2014.

1. Feynman, R. P., Leighton, R. B. & Sands, M. *The Feynman Lectures on Physics* Vol. III, Chs 1 and 3 (Addison-Wesley, 1964).
2. Mandel, L. Coherence and indistinguishability. *Opt. Lett.* **16,** 1882–1883 (1991).
3. Zou, X. Y., Wang, L. J. & Mandel, L. Induced coherence and indistinguishability in optical interference. *Phys. Rev. Lett.* **67,** 318–321 (1991).
4. Wang, L. J., Zou, X. Y. & Mandel, L. Induced coherence without induced emission. *Phys. Rev. A* **44,** 4614–4622 (1991).
5. White, A. G., Mitchell, J. R., Nairz, O. & Kwiat, P. G. "Interaction-free" imaging. *Phys. Rev. A* **58,** 605–613 (1998).
6. Abouraddy, A. F., Stone, P. R., Sergienko, A. V., Saleh, B. E. A. & Teich, M. C. Entangled-photon imaging of a pure phase object. *Phys. Rev. Lett.* **93,** 213903 (2004).
7. Gatti, A., Brambilla, E. & Lugiato, L. Quantum imaging. *Prog. Opt.* **51,** 251–348 (2008).
8. Pittman, T. B. *et al.* Two-photon geometric optics. *Phys. Rev. A* **53,** 2804–2815 (1996).
9. Aspden, R. S., Tasca, D. S., Boyd, R. W. & Padgett, M. J. EPR-based ghost imaging using a single-photon-sensitive camera. *New J. Phys.* **15,** 073032 (2013).
10. Wiseman, H. M. & Mølmer, K. Induced coherence with and without induced emission. *Phys. Lett. A* **270,** 245–248 (2000).
11. Elitzur, A. C. & Vaidman, L. Quantum mechanical interaction-free measurements. *Found. Phys.* **23,** 987–997 (1993).
12. Kwiat, P., Weinfurter, H., Herzog, T., Zeilinger, A. & Kasevich, M. A. Interaction-free measurement. *Phys. Rev. Lett.* **74,** 4763–4766 (1995).
13. Horne, M. in *Experimental Metaphysics* Vol. 1. (eds Cohen, R. S., Horne, M. & Stachel, J.) 109–119 (Kluwer Academic, 1997).
14. Howell, J. C., Bennink, R. S., Bentley, S. J. & Boyd, R. W. Realization of the Einstein-Podolsky-Rosen paradox using momentum-and position-entangled photons from spontaneous parametric down conversion. *Phys. Rev. Lett.* **92,** 210403 (2004).
15. Walborn, S. P., Monken, C. H., Pádua, S. & Souto Ribeiro, P. H. Spatial correlations in parametric down-conversion. *Phys. Rep.* **495,** 87–139 (2010).
16. Tasca, D. S., Walborn, S. P., Souto Ribeiro, P. H., Toscano, F. & Pellat-Finet, P. Propagation of transverse intensity correlations of a two-photon state. *Phys. Rev. A* **79,** 033801 (2009).
17. Horne, M. A., Shimony, A. & Zeilinger, A. Two particle interferometry. *Phys. Rev. Lett.* **62,** 2209–2212 (1989); Two particle interferometry. *Nature* **347,** 429–430 (1990).
18. Ribeiro, P. H. S., Pádua, S., Machado da Silva, J. C. & Barbosa, G. A. Controlling the degree of visibility of Young's fringes with photon coincidence measurements. *Phys. Rev. A* **49,** 4176–4179 (1994).
19. Abouraddy, A. F., Stone, P. R., Sergienko, A. V., Saleh, B. E. A. & Teich, M. C. Entangled-photon imaging of a pure phase object. *Phys. Rev. Lett.* **93,** 213903 (2004).
20. Zou, X. Y., Grayson, T. P. & Mandel, L. Observation of quantum interference effects in the frequency domain. *Phys. Rev. Lett.* **69,** 3041–3044 (1992).

21. Grayson, T. P. & Barbosa, G. A. Spatial properties of spontaneous parametric down-conversion and their effect on induced coherence without induced emission. *Phys. Rev. A* **49,** 2948–2961 (1994).

Acknowledgements We thank M. Horne for reading the manuscript, clarifying suggestions and many discussions, P. Enigl for designing the figures for the objects, D. Greenberger and S. von Egan-Krieger for discussions, and C. Schaeff for equipment loans. Microfabrication was carried out at the Center for Micro- and Nanostructures (ZMNS) of the Vienna University of Technology. We acknowledge D. Ristanic for assistance with cryogenic Si etching and M. Schinnerl for contact mask production. G.B.L. was funded by the Austrian Academy of Sciences (ÖAW) through a fellowship from the Vienna Center for Science and Technology (VCQ). S.R. is funded by an EU Marie Curie Fellowship (PIOF-GA-2012-329851). This project was supported by ÖAW, the European Research Council (ERC Advanced grant no. 227844 'QIT4QAD', and SIQS grant no. 600645 EU-FP7-ICT), and the Austrian Science Fund (FWF) with SFB F40 (FOQUS) and W1210-2 (CoQus).

Author Contributions A.Z. initiated this research. G.B.L., V.B., R.L., S.R. and A.Z. designed the experiment. G.B.L., V.B. and R.L. carried out the experiment. G.D.C. fabricated the silicon and silica phase masks. All authors contributed to the writing of the manuscript.

Author Information Reprints and permissions information is available at www.nature.com/reprints. The authors declare no competing financial interests. Readers are welcome to comment on the online version of the paper. Correspondence and requests for materials should be addressed to G.B.L. (gabriela.barreto.lemos@univie.ac.at) and A.Z. (anton.zeilinger@univie.ac.at).

METHODS

Down-conversion sources. The 532-nm pump beam is generated by a frequency-doubled diode-pumped solid-state laser (Coherent Sapphire SF) and is focused onto the two periodically poled potassium titanyl phosphate (ppKTP) crystals with dimension 1 mm × 2 mm × 2 mm and poling period 9.675 μm for type-0 phase matching. The crystals are spatially oriented so down-conversion occurs when the CW pump beam is horizontally polarized (both the signal and idler produced are also horizontally polarized). In order to conform to the phase-matching conditions for 810-nm and 1,550-nm photons, NL1 (NL2) is heated to 83.7 °C (84.7 °C). When the set-up is adjusted to produce 820-nm and 1,515-nm photons (to be used with the fused silica phase object), NL1 (NL2) is heated to 39.2 °C (39.7 °C). All images were obtained with 150-mW pump power.

Wavelength filtering. Inside the interferometer, D1 is used to separate the 810-nm photons from the 1,550-nm photons. Mirror D1 (and also D2) reflects about 93% of 1,550-nm light and transmits about 99% of 810-nm light. Most of the pump beam going through NL1 is transmitted through both D1 and D4 (each with a transmittance of around 97% at 532 nm) and therefore almost never reaches BS. The dichroic mirror D5 additionally transmits some 532-nm light (around 25%), so some of the pump beam that goes through NL2 as well as some of the remaining pump beam from NL1 are discarded there. All remaining pump beam light is eliminated with either filters or the imaging object itself. The silicon sample is opaque to both 532-nm and 810-nm light, thus completely blocking these wavelengths along the path D1–D2. When the other samples are used, a long-pass filter is placed just before the object to cut out these lower wavelengths. The remaining 532-nm light that is not separated out through the dichroic mirrors or object is blocked in front of the camera by three filters. A 3-nm narrowband filter centred at 810 nm and two long pass filters were attached directly to the front of the camera. As it utilizes a silicon-based detector, the camera (Andor Luca-R EMCCD) does not detect 1,550-nm photons. Nonetheless, a combination of spectral filters guarantees that neither 1,550-nm photons nor 532-nm pump photons reach the camera.

Imaging lens systems. As it is crucial that the down-converted photons be identical, we use confocal lens systems to image plane 1 onto plane 3 (see Fig. 2), thus ensuring that the pump beams at NL1 and NL2 are identical, the 810-nm photons when they combine at the BS are identical, and the 1,550-nm photons are identical from NL2 onward. Lenses L2 and L2′ image plane 1 of the pump onto plane 3, and similarly L3 (L4) and L3′ (L4′) image plane 1 onto plane 3 for the 1,550-nm (810-nm) photons. Lenses L5 and L6 in combination with L4′ image plane 2 onto the EMCCD camera. Lenses L2, L2′, L3, L3′, L4, L4′ have a focal length of $F_1 = 75$ mm. The distance from plane 1 to each of L2, L3 and L4 is 75 mm; from those lenses to plane 2 is another 75 mm; from plane 2 to L2′, L3′ and L4′ is also 75 mm; and from those lenses to plane 3 is yet another 75 mm. This ensures that the photons produced in both crystals have the same waist and divergence when they reach the BS. Lenses L5 and L6 have a focal length of $F_2 = 150$ mm. They are placed 150 mm after plane 3 and 150 mm before the camera. The total imaging magnification from the object to the camera is given by $\frac{F_2\lambda_s}{F_1\lambda_i}$, where λ_s and λ_i are the wavelengths of the signal and idler photons, respectively.

Optical path lengths. In our single photon interferometer the paths D1–D4–BS and D1–D2–BS need to be equal, even though no detected photons actually follow the entire path D1–D2–BS. To assure indistinguishability of the emission in the two crystals (NL1 and NL2) the time delay between the arrival of the signal and idler for each of the two crystals must be the same. The path length difference between the signal and idler for the pair from NL1 is the distance NL1–D1–D2–BS subtracted from the distance NL1–D1–D4–BS. The path length difference between the signal and idler for the pair from NL2 is zero since the down-conversion is collinear. Thus, we see that the optical path lengths between D1–D4–BS and D1–D2–BS must be equal to within the coherence length of the photons. The coherence length of the photons is in our case determined by the filtering (3 nm), so we approximate the coherence length to be 0.2 mm. The other relevant optical path lengths are the paths PBS–D1–D2–NL2 and PBS–M1–NL2. The differential distance between these paths must be within the coherence length of the laser, which in our case is approximately 200 m.

Intensity object. Our intensity object is constructed from 0.33-mm-thick card stock with images defined by laser cutting. The images on the object were each 3 mm high.

Microfabricated silicon phase sample. The first custom phase sample consists of 500-μm-thick double-side polished (100)-oriented single-crystal silicon with imaging targets defined on one face using standard microfabrication techniques. The absorption coefficient of silicon is ~1,000 cm^{-1} at 810 nm (ref. 22), and it is ~10^{-4} cm^{-1} at 1,550 nm (ref. 23). Processing begins by cleaving a 75-mm-diameter silicon wafer to obtain chips with lateral dimensions of 25 mm × 25 mm. The cleaved chips are patterned using conventional optical contact lithography followed by plasma etching. In order to generate a relative π-phase shift at 1,550 nm, features are etched to a depth of approximately 310 nm (nominal height of 321 nm using a refractive index of silicon of 3.48; ref. 24) into the exposed Si surface using a cryogenic (−108 °C) SF_6/O_2 reactive-ion etching (RIE) process protected with a positive photoresist mask. To improve thermal transfer, the silicon chips are mounted on a carrier wafer using a thin layer of vacuum grease. Additionally, in order to minimize variations in the overall etch depth and thus resulting phase shift from the imaging targets, the feature linewidth is kept constant over the lithographic pattern to mitigate the effects of aspect-ratio dependent etching (or 'RIE lag'). After etching, the chips are removed from the carrier wafer and the masking resist and mounting film are stripped using a combination of organic solvents and oxygen plasma ashing. In order to eliminate spurious reflections from the polished surfaces, a dual-sided silicon nitride anti-reflection (AR) coating is deposited via plasma-enhanced chemical vapour deposition (PECVD) using He-diluted SiH_4 and NH_3 as reactive process gases. The deposition process yields quarter-wave optical thickness layers at a target film thickness of 2,040 Å (with a refractive index of 1.9 at the imaging wavelength of 1,550 nm).

In order to achieve the highest contrast, the relative path-length difference between the etched and non-etched regions should be equal to a half wavelength of 1,550-nm light adjusted for the difference in the indices of refraction of silicon and air. This gives a target thickness difference of 321 nm (for a refractive index of silicon of 3.48). Given the slight error in etch depth, the actual thickness difference is 310 nm, which is still sufficient to obtain high contrast images.

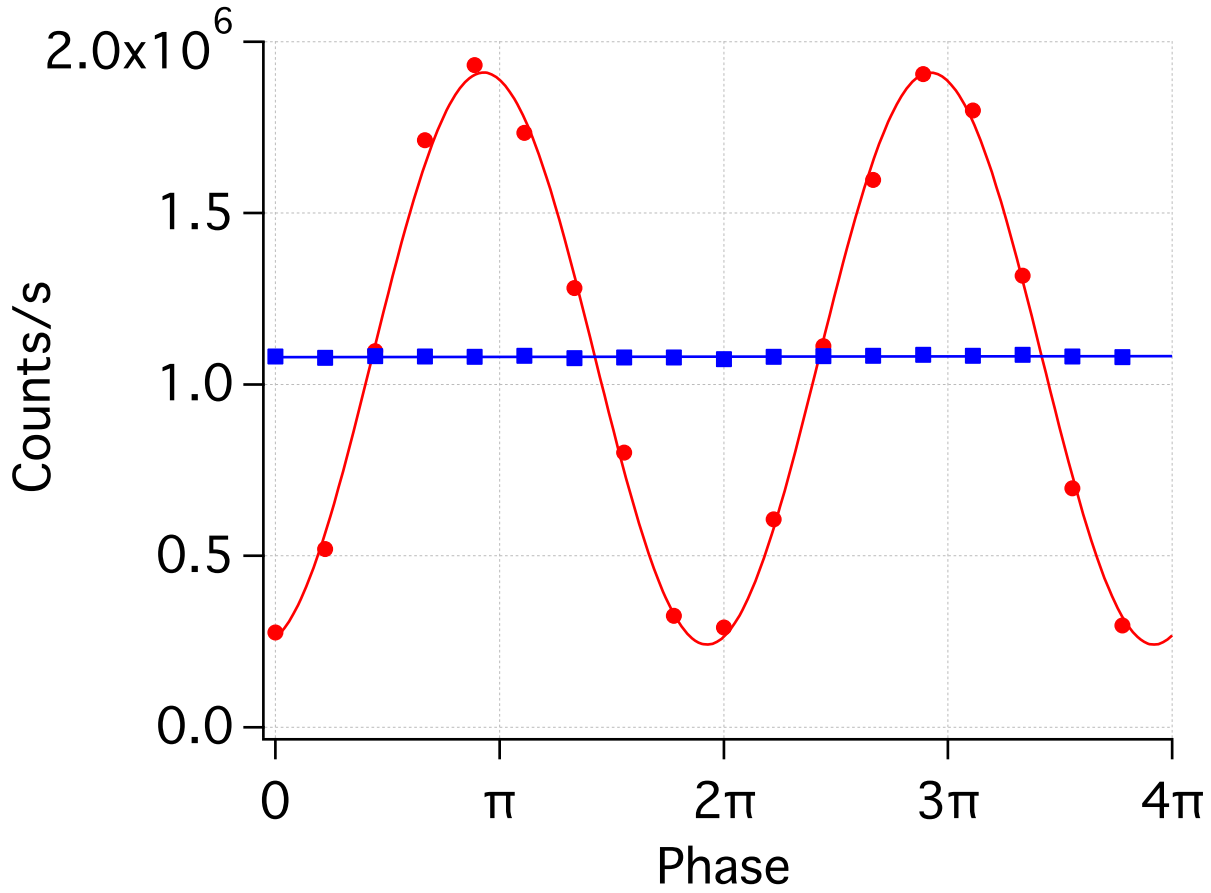
Microfabricated fused silica phase sample. Similar to the silicon phase object described above, the fused silica phase sample, cleaved from a 500-μm-thick glass wafer, is constructed via a standard lithographic and reactive ion etching process. In this case the same mask pattern is once again defined with contact lithography. In order to transfer the features into the fused silica, a high-power inductively coupled plasma (ICP) RIE process is required (150 W ICP, 250 W RF powers) with an etch chemistry consisting of SF_6 and Ar. Given the poor selectivity to the masking resist, a thick (10 μm) coating of AZP4620 photoresist is required. The target etch depth of 1,788 nm is achieved within roughly 10 min at room temperature. Given the high plasma energy, thermalization with the cooled carrier wafer is key. Due to non-uniformities in thermal contact with the carrier, we observe significant variation in etch depth (±200 nm) across the surface of the 25 mm × 25 mm pattern. No AR coating is employed given the small Fresnel reflection (4%) from the low-index silica substrate.

For 820-nm light, an exact 2π phase shift is given by a thickness difference of 1,811 nm (using an index of refraction of 1.45)[25]; after processing, the average etch depth recorded for the fused silica sample is 1,803 nm.

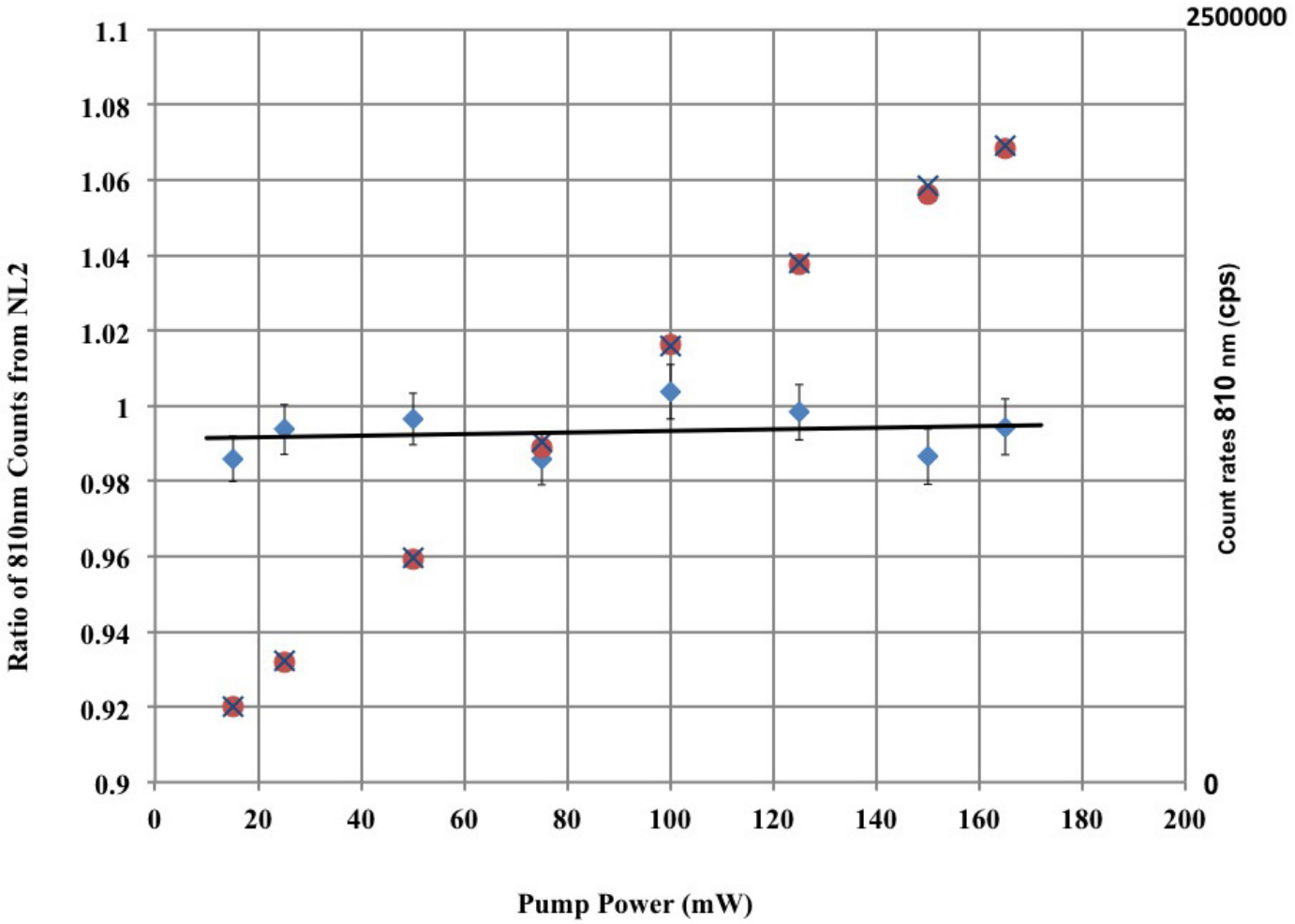
Interference visibility. In order to quantify the visibility in our imaging experiment, we detect the total intensity of 810-nm photons at one output of BS as a function of the relative phase between the pump beams that illuminate each crystal. Extended Data Fig. 1 shows a plot of the count rate measured with an avalanche photodiode when no object is present. The red circles show the experimental points, and the best fitting sinusoidal function (red line) gives a visibility of (77 ± 1)%. The visibility for our experiment is given not only by losses in both the 1,550-nm and 810-nm arms of the interferometer, but also by residual imperfections in the alignment for the two idler beams. The blue squares correspond to data obtained when the path NL1–NL2 is completely blocked, which results in zero interference visibility. Interference only arises if the idler between the two crystals is unblocked, for only then is its source, and therefore also the source of its signal sister, unknowable.

Showing that induced emission is negligible in the experiment. In order to demonstrate in our experiment that the 1,550-nm photons from NL1 do not induce down-conversion in NL2, we show in Extended Data Fig. 2 the count rates for 810-nm photons originating at NL2 when the 1,550-nm beam between D1 and D2 was blocked (blue crosses) and unblocked (red dots). The mean count rate and the standard deviation were obtained by analysing data obtained over 40 s. The blue diamonds show that the ratio of the count rates for the blocked and unblocked configuration is very close to 1 irrespective of the pump power.

22. Jellison, G. E. Jr. & Modine, F. A. Optical absorption of silicon between 1.6 and 4.7 eV at elevated temperatures. *Appl. Phys. Lett.* **41,** 180 (1982).
23. Khalaidovski, A., Steinlechner, J. & Schnabel, R. Indication for dominating surface absorption in crystalline silicon test masses at 1550 nm. *Class. Quantum Grav.* **30,** 165001 (2013).
24. Malitson, I. H. Interspecimen comparison of the refractive index of fused silica. *J. Opt. Soc. Am.* **55,** 1250 (1965).
25. Bass, M. *Handbook of Optics* Vol. 2, 2nd edn (Optical Society of America, 1995).



Extended Data Figure 1 | Visibility of the experiment. The count rates were recorded with the path D1–D2 both unblocked (red dots) and blocked (blue squares) as the relative phase between the transmitted and reflected beams of the PBS was varied. The red line is a sine curve fit for the experimental data giving (77 ± 1)% visibility. The error bars are smaller than the size of the data points.



Extended Data Figure 2 | Excluding induced emission. Shown are the count rates for 810-nm photons produced in NL2 when the path between D1 and D2 was blocked (blue crosses) and unblocked (red dots). The blue diamonds show the ratio of the count rates for the blocked and unblocked configuration. The linear fit for this data (black line) gives an angular coefficient of $(2 \pm 4) \times 10^{-5}$ $(\mathrm{mW})^{-1}$.

REVIEW ARTICLE
https://doi.org/10.1038/s41566-018-0301-6

nature photonics

Advances in photonic quantum sensing

S. Pirandola[1,2*], B. R. Bardhan[3], T. Gehring[4], C. Weedbrook[5] and S. Lloyd[2,6]

Quantum sensing has become a broad field. It is generally related with the idea of using quantum resources to boost the performance of a number of practical tasks, including the radar-like detection of faint objects, the readout of information from optical memories, and the optical resolution of extremely close point-like sources. Here, we first focus on the basic tools behind quantum sensing, discussing the most recent and general formulations for the problems of quantum parameter estimation and hypothesis testing. With this basic background in hand, we then review emerging applications of quantum sensing in the photonic regime both from a theoretical and experimental point of view. Besides the state of the art, we also discuss open problems and potential next steps.

Quantum technologies are today developing at unprecedented pace. As a matter of fact, the technological applications of the field of quantum information[1–8] are many and promising. One of the most advanced areas is certainly quantum sensing. This is a broad term encompassing all those quantum protocols of estimation and discrimination able to outperform any classical strategy. One can leverage important quantum characteristics such as entanglement, single photons and squeezed states[5] to achieve orders-of-magnitude improvements in precision. In this scenario, the photonic regime is certainly the best setting thanks to the relative simplicity in the generation, manipulation and detection of such quantum features.

This Review aims to provide a survey of some recent advances in photonic quantum sensing. We refer the reader to ref. [9] for an overview of quantum sensing in non-photonic areas (spin qubits, trapped ions, for example). We also stress that we adopt a quantum information approach to quantum sensing, which clearly does not encompass all the possible methods known in the literature. We start with theoretical background in quantum parameter estimation[10–14] and hypothesis testing[15–18], presenting the most general adaptive formulation of these problems[19–28] and methods of channel simulation, based on programmability[29–31] and teleportation stretching[32–34]. This background will allow us to identify the goals, the structure, and the classical benchmarks for the following protocols of quantum sensing that we will discuss theoretically and experimentally.

Quantum hypothesis testing is at the very basis of quantum reading[35–53], where the information stored in an optical memory is efficiently retrieved by using just a few photons of quantum light. This light better senses the difference between the reflectivities of a memory cell, greatly improving the readout of information. Quantum hypothesis testing is also at the basis of quantum illumination[54–71], where the radar-like detection of remote and faint targets is boosted by the use of quantum correlations, even though entanglement may be destroyed in the process. Then, quantum parameter estimation is the core idea for the most recent advances in quantum imaging and optical resolution[72–88], where the 'Rayleigh's curse' may be dispelled by means of quantum metrological detection schemes[72–74].

Estimation and discrimination protocols

Consider a parameter θ encoded in a quantum channel $\mathcal{E}_\theta$, which is in turn stored in a black box, of which Alice may prepare the input and Bob may detect the output. In an estimation problem, θ is a continuous parameter, whereas in a discrimination problem, θ takes a discrete finite number of values with some prior probabilities. In particular, in a basic problem of binary symmetric discrimination, θ only takes two values, θ_0 (null hypothesis) or θ_1 (alternative hypothesis), with the same Bayesian cost and prior probability. In other words, there is a classical bit u encoded in the parameter θ_u.

Let us analyse the problem with an increasing level of complexity. In a 'block' protocol, Alice sends an input state ρ through the unknown channel $\mathcal{E}_\theta$ whose output $\mathcal{E}_\theta(\rho)$ is received by Bob. This process is identically performed n times, so that Alice sends n copies $\rho^{\otimes n}$ and Bob receives $\mathcal{E}_\theta(\rho)^{\otimes n}$. To retrieve θ, Bob applies a measurement on his n-copy output state. In channel estimation, the measurement is performed locally and identically on each single-copy output state. This measurement has a continuous outcome from which Bob constructs an unbiased estimator $\tilde{\theta}$ of θ, affected by some error variance $\delta\theta^2 := \langle(\tilde{\theta}-\theta)^2\rangle$. In channel discrimination, Bob uses a dichotomic measurement that provides the bit u with some mean error probability p_{err}. This measurement is optimal only if non-local, that is, jointly applied to all output copies.

In a sequential protocol, the approach is different. Instead of preparing a tensor product of n-copy input states (each one sent through an instance $\mathcal{E}_\theta$ of the unknown channel), Alice transmits an input state ρ through the sequence of channels $\mathcal{E}_\theta^n := \mathcal{E}_\theta \circ \cdots \circ \mathcal{E}_\theta$ whose output $\mathcal{E}_\theta^n(\rho)$ is then detected by Bob. The sequential protocol can also be seen as a scheme where the output state received by Bob in each transmission through the channel is teleported back as input. This happens n times, after which Bob performs his measurement.

More generally, the previously described protocols may be 'assisted'. This means that the parties may use additional reference systems, or idlers, that help the output measurement. In particular, there may be entanglement between these reference systems and the signal systems used to probe the box. For a block protocol, this means that Alice prepares n copies of a bipartite input state ρ_{sr} where the signal system s is transmitted through the channel $\mathcal{E}_\theta$, while the reference system r is subject to the identity map $\mathcal{I}$. Therefore, Bob receives $[\mathcal{E}_\theta \otimes \mathcal{I}(\rho_{sr})]^{\otimes n}$. For a sequential protocol, this means that the signal system is subject to the sequence $\mathcal{E}_\theta^n$ while the reference is subject to the identity. Therefore, Bob receives $\mathcal{E}_\theta^n \otimes \mathcal{I}(\rho_{sr})$.

[1]Computer Science and York Centre for Quantum Technologies, University of York, York, UK. [2]Research Laboratory of Electronics, MIT, Cambridge, MA, USA. [3]Department of Physics and Astronomy, State University of New York at Geneseo, Geneseo, NY, USA. [4]Department of Physics, Technical University of Denmark, Fysikvej, Kongens, Lyngby, Denmark. [5]Xanadu, Toronto, Ontario, Canada. [6]Department of Mechanical Engineering, MIT, Cambridge, MA, USA. *e-mail: stefano.pirandola@york.ac.uk

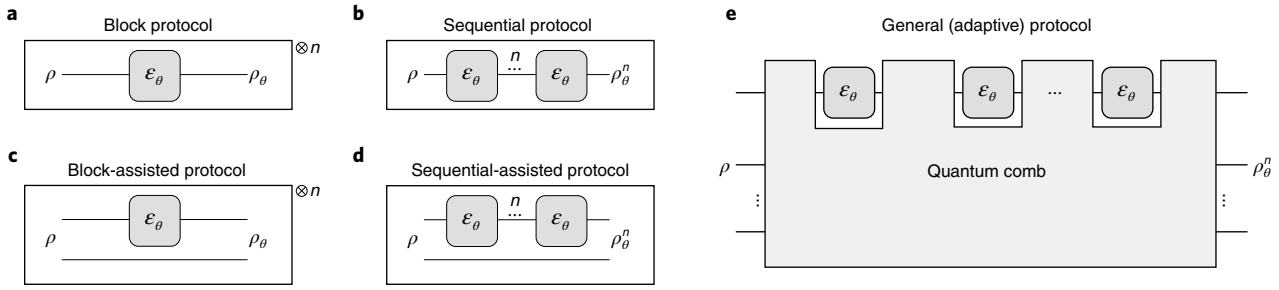


Fig. 1 | Protocols for quantum estimation and discrimination. a, Block protocol where channel $\mathcal{E}_\theta$ is probed n times in an identical and independent way. **b**, Sequential protocol where the input is transmitted through n consecutive instances of the channel. **c**, Block-assisted protocol where channel $\mathcal{E}_\theta$ is probed by a signal system coupled to a reference system. **d**, Sequential-assisted protocol where the input is bipartite and partially transmitted through n consecutive instances of $\mathcal{E}_\theta$. **e**, General (adaptive) protocol represented as a quantum comb. An input register with an arbitrary number of systems (wires) is prepared in a fundamental initial state ρ. Each probing of the unknown channel $\mathcal{E}_\theta$ is performed by inputting a system from the register and storing the output back in the register. Probings are interleaved by arbitrary QOs performed over the entire register. After n probings, the total output state ρ_θ^n is subject to a joint quantum measurement.

The most general protocol is based on unlimited entanglement and adaptive quantum operations (QOs), which are applied jointly by Alice and Bob[19–28]. As also discussed in ref. [34], this protocol can be represented as a quantum comb[89]. This is a quantum circuit board whose slots are filled with the unknown channel $\mathcal{E}_\theta$. The comb is based on a register with an arbitrary number of systems and prepared in a fundamental state ρ. The entire register undergoes arbitrary QOs before and after each probing of the channel, as depicted in Fig. 1. The QOs can always be assumed to be trace-preserving by adding extra systems and deferring measurements[1]. At the output of the comb, the state ρ_θ^n is detected by an optimal (non-local) quantum measurement whose outcome is classically processed. The quantum comb includes all the previous protocols as specific cases.

Performance of channel estimation

Assume that the quantum comb in Fig. 1 is used for quantum channel estimation. The ultimate performance is limited by the quantum Cramér–Rao bound (QCRB)

$$\delta\theta^2 \geq \frac{1}{\mathrm{QFI}(\rho_\theta^n)} \tag{1}$$

where QFI is the quantum Fisher information[10]

$$\mathrm{QFI}(\rho_\theta^n) = \frac{8[1-F(\rho_\theta^n, \rho_{\theta+\mathrm{d}\theta}^n)]}{\mathrm{d}\theta^2} \tag{2}$$

and $F(\rho,\sigma) := \mathrm{Tr}\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}$ is the Bures fidelity between ρ and σ. We are interested in the 'scaling' of the QCRB, that is, how $\delta\theta^2$ behaves for large n. There are two main behaviours[14]: the standard quantum limit (SQL), which is the typical scaling $\delta\theta^2 \gtrsim n^{-1}$ achievable in classical strategies, and the Heisenberg limit $\delta\theta^2 \gtrsim n^{-2}$, which is the ultimate scaling allowed by quantum mechanics. These have energetic analogues when we consider parameter estimation with bosonic channels. Assuming a single use of the comb ($n=1$) but allowing for N mean number of photons at the channel input, we have that $\delta\theta^2 \gtrsim N^{-1}$ corresponds to the SQL and $\delta\theta^2 \gtrsim N^{-2}$ to the Heisenberg limit.

As shown in refs [23,28], quantum teleportation[90] and port-based quantum teleportation[91,92] can be used as basic tools in quantum metrology. In particular, ref. [23] showed that teleportation covariance implies the SQL. Recall that a channel $\mathcal{E}$ is teleportation-covariant if, for any teleportation unitary U (Pauli or displacement operator), we can write[32]

$$\mathcal{E}(U\rho U^\dagger) = V\,\mathcal{E}(\rho)\,V^\dagger \tag{3}$$

with unitary V (here † means Hermitian conjugate). Then, a parametrized channel $\mathcal{E}_\theta$ is jointly teleportation-covariant[23,34] if equation (3) holds for any θ, that is, $\mathcal{E}_\theta(U\rho U^\dagger) = V\,\mathcal{E}_\theta(\rho)\,V^\dagger$ where V does not depend on θ. Because of this property, we may write the channel simulation[23,34]

$$\mathcal{E}_\theta(\rho) = \mathcal{T}(\rho \otimes \rho_{\mathcal{E}_\theta}) \tag{4}$$

where $\mathcal{T}$ is teleportation and $\rho_{\mathcal{E}} := \mathcal{E}\otimes\mathcal{I}(\Phi_{sr})$ is the Choi matrix of the channel (this is the state that is obtained by propagating part of a maximally entangled state Φ_{sr} through the quantum channel). Therefore, $\mathcal{E}_\theta$ is a specific type of programmable channel[29,30]. If $\mathcal{E}_\theta$ is bosonic, the simulation is asymptotic[34] with Choi matrix $\rho_{\mathcal{E}_\theta} := \lim_\mu \rho_{\mathcal{E}_\theta}^\mu$, where $\rho_{\mathcal{E}_\theta}^\mu := \mathcal{E}_\theta\otimes\mathcal{I}(\Phi_{sr}^\mu)$ is computed on a two-mode squeezed vacuum (TMSV) state[5] Φ_{sr}^μ with variance μ.

Replacing the simulation of equation (4) in each slot of the comb in Fig. 1 and stretching[32] the adaptive protocol, the output state becomes[23]

$$\rho_\theta^n = \Lambda(\rho_{\mathcal{E}_\theta}^{\otimes n}) \tag{5}$$

where Λ is a global quantum channel. Because the QFI is monotonic under channels and multiplicative over tensor products, equation (5) implies $\mathrm{QFI}(\rho_\theta^n) \leq n\mathrm{QFI}(\rho_{\mathcal{E}_\theta})$, so that the QCRB must satisfy the SQL[23]

$$\delta\theta^2 \geq [n\mathrm{QFI}(\rho_{\mathcal{E}_\theta})]^{-1} \tag{6}$$

where $\mathrm{QFI}(\rho_{\mathcal{E}_\theta}) := \lim_\mu \mathrm{QFI}(\rho_{\mathcal{E}_\theta}^\mu)$ for a bosonic channel. Thus, the general adaptive protocol is reduced to a block-assisted protocol, where n maximally entangled states $\Phi_{sr}^{\otimes n}$ probe $\mathcal{E}_\theta$.

Because the class of teleportation-covariant channels is wide, channel estimation is limited to the SQL in many situations. For instance, the estimation of the probability parameter p in depolarizing, dephasing or erasure channels is limited to[23] $\delta p^2 \geq p(1-p)n^{-1}$. The estimation of thermal noise $\bar{n}$ in a thermal-loss channel $\mathcal{E}_{\eta,\bar{n}}$ with fixed transmissivity η is limited to[23,24] $\delta\bar{n}^2 \geq \bar{n}(\bar{n}+1)n^{-1}$. By contrast, the ultimate estimation limit of the transmissivity η is not known, because $\mathcal{E}_{\eta,\bar{n}}$ is not jointly teleportation-covariant in η and equation (6) does not apply.

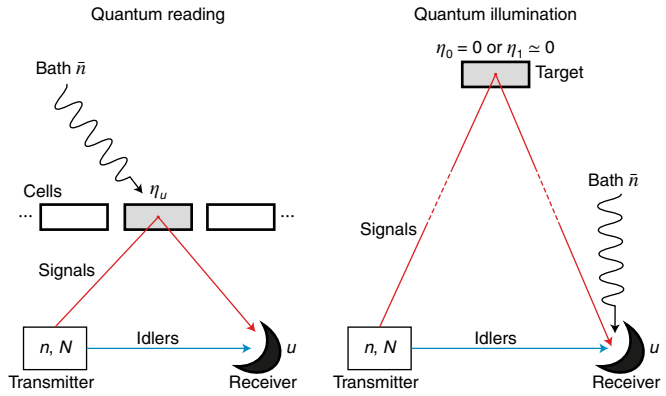


Fig. 2 | Technological applications of quantum channel discrimination. Quantum reading[35] (left) and Gaussian quantum illuminantion[55] (right). In the basic formulation, these are both based on an EPR transmitter, so that n two-mode squeezed vacuum (TMSV) states[5] irradiate N mean photons per mode over the cell (quantum reading) or target (quantum illumination) (where N is typically low). The reflected signals are combined with the retained idler (reference) modes in a joint detection, whose output u discriminates between two hypotheses. In quantum reading, the task is specifically the readout of data from an optical memory. In the simple single-cell model shown here, an information bit $u = 0,1$ is encoded in a cell with typically-high reflectivities, η_0 and η_1, and subject to (relatively low) thermal noise $\bar{n}$. Quantum features such as entanglement are typically preserved at the output receiver. In quantum illumination, the task is specifically target detection, where u is related with the absence ($\eta_0 = 0$) or the presence ($\eta_1 \simeq 0$) of a low-reflectivity object. Furthermore, the reflection is mixed with bright thermal noise $\bar{n} \gg 1$, so that entanglement is lost at the output receiver. These schemes are examples of block-assisted protocols for quantum channel discrimination. In the regimes considered, they largely outperform classical strategies, that is, corresponding schemes based on classical transmitters that are not entangled but composed of mixtures of coherent states.

The optimal adaptive estimation of bosonic loss is still an open problem. Solving it is of paramount importance because the transmissivity η of a quantum channel sets the ultimate limit of any point-to-point protocol of quantum or private communication. This limit is equal to $-\log_2(1-\eta)$ bits per use and known as the Pirandola–Laurenza–Ottaviani–Banchi bound[32]. The best performance in estimating η of a pure-loss channel $\mathcal{E}_\eta := \mathcal{E}_{\eta,0}$ is currently[93] $\delta\eta^2 \geq \eta(1-\eta)N^{-1}$ for N mean photons. This is a SQL in terms of the input mean number of photons N. However, note that the pre-factor $\eta(1-\eta)$ improves the performance that is achievable by using coherent states with the same input energy, that is, the scaling[94] $\delta\eta^2 \geq \eta N^{-1}$. The optimal performance of coherent states is also known as the shot-noise limit[14].

On the experimental side, the performance of absorption spectroscopy has been demonstrated to operate beyond the shot-noise limit in entanglement-assisted block protocols. In ref. [95], it was reported that photon pairs were generated with one of the photons being transmitted through an absorptive sample. At the output, coincidence counts were measured and post-processed. Quantum advantage over the shot-noise limit was also reported in refs [96,97], where the detection was based on intensity correlation measurements of signal and idler twin beams from a parametric downconversion source. Other multi-pixel experiments have also been performed where twin beams are used to enhance absorption microscopy[98,99].

Besides the estimation of bosonic loss, there is the complementary problem of phase estimation. Because phase shifts are unitary operations, they are not teleportation-covariant, so that their estimation is not necessarily limited to the SQL and, indeed, the Heisenberg scaling is achievable. The most famous phase estimation experiments are certainly the interferometer-based gravitational wave detectors. These kilometre-sized interferometers measure tiny phase shifts around a known phase and have recently been demonstrated to show an improved sensitivity beyond the SQL by injecting squeezed light[100,101].

Apart from squeezed light, the SQL has been surpassed in smaller-scale interferometric experiments using a variety of optical systems[102], in particular, with entangled states such as N00N states (a quantum superposition of N photons in one interferometer arm with no photons in the other and vice versa). While N00N states promise Heisenberg scaling, they are very fragile with respect to optical loss. For this reason, early experiments have surpassed the SQL only by conditioning on detected photons[103], while more recent experiments have been able to beat the SQL using photon sources and detectors with very high efficiency[104]. Other quantum states beyond N00N states have been engineered to be more loss-tolerant while still beating the SQL[105,106].

It is also important to remark that, in phase estimation, the SQL can be surpassed without using entanglement[14]. For instance, this is possible by applying the phase shift multiple times, that is, in a sequential protocol[107]. Using squeezed light, real-time phase tracking has been implemented using a feedback algorithm on the phase[108]. Ab initio phase estimation, that is, the estimation of the phase in a range without prior knowledge, has also been implemented to surpass the SQL, conditionally, with N00N states[109] and unconditionally, with squeezed states and using adaptive measurements[110].

Performance of channel discrimination

Assume that the comb in Fig. 1 is used for binary discrimination, so that parameter θ takes two values $\{\theta_0,\theta_1\}$ with the same probability. This is now a problem of channel discrimination between $\mathcal{E}_0 = \mathcal{E}_{\theta_0}$ and $\mathcal{E}_1 = \mathcal{E}_{\theta_1}$, where we aim to retrieve the classical bit $u = 0$, 1 encoded in $\mathcal{E}_u$. For a given comb with output state ρ_u^n, the minimum error probability affecting the channel discrimination is the Helstrom bound[15]

$$p_{\text{err}} = [1 - D(\rho_0^n, \rho_1^n)]/2 \tag{7}$$

where $D(\rho,\sigma) := ||\rho-\sigma||/2$ is the trace distance[1]. Equivalently, the maximum classical information J retrieved is

$$J = 1 - H_2(p_{\text{err}}) \tag{8}$$

where H_2 is the binary Shannon entropy.

The difficult part is the optimization of p_{err} over all possible adaptive protocols (combs). Remarkably, the problem can be solved if $\mathcal{E}_0$ and $\mathcal{E}_1$ are jointly teleportation-covariant, so that $\mathcal{E}_u(U\rho U^\dagger) = V\mathcal{E}_u(\rho)V^\dagger$ for any u. This allows us to use the teleportation simulation $\mathcal{E}_u(\rho) = \mathcal{T}(\rho \otimes \rho_{\mathcal{E}_u})$ over the Choi matrix $\rho_{\mathcal{E}_u}$. We may then stretch the comb and write its output as $\rho_u^n = \Lambda(\rho_{\mathcal{E}_u}^{\otimes n})$ for a global channel Λ. Because the trace distance is monotonic under Λ, we have $p_{\text{err}} \geq [1 - D(\rho_{\mathcal{E}_0}^{\otimes n}, \rho_{\mathcal{E}_1}^{\otimes n})]/2$ that holds for any comb. Then, we note that this bound is achievable by using maximally entangled states at the input, so that the minimum error probability in the adaptive discrimination of these types of channel is[23]

$$p_{\text{err}}(\mathcal{E}_0,\mathcal{E}_1) = [1 - D(\rho_{\mathcal{E}_0}^{\otimes n}, \rho_{\mathcal{E}_1}^{\otimes n})]/2 \tag{9}$$

where $D = \lim_\mu D(\rho_{\mathcal{E}_0}^{\mu\otimes n}, \rho_{\mathcal{E}_1}^{\mu\otimes n})$ in the bosonic case. In finite dimension, equation (9) establishes the diamond distance between jointly teleportation-covariant channels as $||\mathcal{E}_0 - \mathcal{E}_1||_\diamond = ||\rho_{\mathcal{E}_0} - \rho_{\mathcal{E}_1}||$. (Recall that the diamond distance between two arbitrary channels,

$\mathcal{E}_0$ and $\mathcal{E}_1$, is defined by the maximization of the trace distance $||\mathcal{I}_A \otimes \mathcal{E}_0(\rho_{AB}) - \mathcal{I}_A \otimes \mathcal{E}_1(\rho_{AB})||$ over all possible bipartite input states ρ_{AB}.)

Starting from equation (9), we write lower and upper bounds using the Fuchs–van de Graaf relations[111] and the quantum Chernoff bound (QCB)[17]. Recall that, in discriminating a pair of multicopy states $\rho_0^{\otimes n}$ and $\rho_1^{\otimes n}$, the minimum error probability $p_{\rm err} = [1 - D(\rho_0^{\otimes n}, \rho_1^{\otimes n})]/2$ satisfies the fidelity lower bound[111] and the QCB[17]

$$p_{\rm err} \geq \frac{1-\sqrt{1-F(\rho_0,\rho_1)^{2n}}}{2} := F_-^{(n)}(\rho_0,\rho_1) \tag{10}$$

$$p_{\rm err} \leq \frac{Q(\rho_0,\rho_1)^n}{2}, Q := \inf_{s\in[0,1]} {\rm Tr}(\rho_0^s \rho_1^{1-s}) \tag{11}$$

In particular, for arbitrary Gaussian states[5] ρ_0 and ρ_1, we know formulas for computing the fidelity[112] and the QCB[18]. These inequalities can be extended to the adaptive error probability of equation (9) valid for jointly teleportation-covariant channels, so that we may write[23]

$$F_-^{(n)}(\rho_{\mathcal{E}_0},\rho_{\mathcal{E}_1}) \leq p_{\rm err}(\mathcal{E}_0,\mathcal{E}_1) \leq \frac{Q(\rho_{\mathcal{E}_0},\rho_{\mathcal{E}_1})^n}{2} \tag{12}$$

with asymptotic functionals over bosonic Choi matrices.

The results from equations (9) and (12) apply to many cases, including the adaptive discrimination of Pauli channels, erasure channels, and noise parameters in bosonic Gaussian channels, such as the thermal number $\bar{n}$ of two thermal-loss channels $\mathcal{E}_{\eta,\bar{n}_0}$ and $\mathcal{E}_{\eta,\bar{n}_1}$. Unfortunately, they do not apply to the discrimination of transmissivity η, because $\mathcal{E}_{\eta_0,\bar{n}}$ and $\mathcal{E}_{\eta_1,\bar{n}}$ are not jointly teleportation-covariant. Thus, the optimal discrimination of bosonic loss is still unknown. What we currently know is that block-assisted strategies based on entangled states may greatly outperform block strategies without assistance, especially at the low-photon-number regime. This observation is at the basis of quantum reading and quantum illumination.

Quantum reading of classical data

In 2011, Pirandola[35] showed how the readout of classical data from an optical digital memory can be modelled as a problem of quantum channel discrimination. In the most basic description, an optical classical memory can be seen as an array of cells described as microscopic beamsplitters with different reflectivities. Each cell stores an information bit $u = 0,1$ in two equiprobable and typically-high reflectivities, the pit reflectivity $\eta_0 \in (0,1)$ and the land reflectivity $\eta_1 > \eta_0$ (Fig. 2). This single-cell model is equivalent to a black-box model read in reflection so that the reflectivity plays the role of the transmissivity parameter. The readout may also be affected by (relatively low) thermal noise, for example, due to stray photons generated by the source. Thus the readout corresponds to discriminating between two thermal-loss channels, $\mathcal{E}_0 := \mathcal{E}_{\eta_0,\bar{n}}$ and $\mathcal{E}_1 := \mathcal{E}_{\eta_1,\bar{n}}$, with different reflectivity, η_0 and η_1, but fixed thermal number $\bar{n}$. Other decoherence effects may be included[35], for example, optical diffraction, memory effects and inter-bit interference[36].

We may consider different 'transmitters' composed of signal modes probing the cell and reference modes assisting detection. The coherent-state transmitter only uses n signal modes in identical coherent states $|\alpha\rangle_s\langle\alpha|^{\otimes n}$. More powerfully, we may define a 'classical' transmitter in the quantum-optical sense. This is a block-assisted protocol employing mixtures of coherent states $\int {\rm d}^{2n}\boldsymbol{\alpha}\mathcal{P}(\boldsymbol{\alpha})|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|$, where $\mathcal{P}(\boldsymbol{\alpha})$ is a probability distribution of amplitudes $\boldsymbol{\alpha}$, and $|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|$ is a multimode coherent state with n signal modes and n reference modes. The optimal classical transmitter has to be compared with an Einstein–Podolsky–Rosen (EPR) transmitter. This is a block entanglement-assisted protocol where we send part of n TMSV states $\Phi_{sr}^{\mu\otimes n}$, so that each signal mode is entangled with a reference or 'idler' mode. For both classical and EPR transmitters, the input $2n$-mode state ρ_{sr} is transformed by the cell into an output state $\sigma_u := \mathcal{E}_u^{\otimes n} \otimes \mathcal{I}^{\otimes n}(\rho_{sr})$ for the n reflected signal modes and the n kept reference modes. This output is detected by an optimal quantum measurement[15] with some error probability. We then compare the information retrieved by the classical transmitter $J_{\rm class}$ and the EPR transmitter $J_{\rm EPR}$ in terms of gain $\Delta := J_{\rm EPR} - J_{\rm class}$. Positive values $\Delta > 0$ means quantum advantage.

A fair comparison between these transmitters involves fixing the mean number of signal photons probing the cell. One type of constraint is 'local', meaning that we fix the mean number of photons N in each probing, so that the total energy scales as nN. We may write the following bound for the error probability $p_{\rm class}$ achievable by any classical transmitter[35]

$$p_{\rm class} \geq \mathcal{C}(n,N) := \frac{1-\sqrt{1-F(N)^{2n}}}{2} \tag{13}$$

where $F(N)$ is the fidelity between $\mathcal{E}_0(|\sqrt{N}\rangle\langle\sqrt{N}|)$ and $\mathcal{E}_1(|\sqrt{N}\rangle\langle\sqrt{N}|)$ generated by an input coherent state with N mean photons. This leads to $J_{\rm class}(n,N) \leq 1 - H_2[\mathcal{C}(n,N)]$. For the EPR transmitter, the QCB provides $J_{\rm EPR} \geq 1 - H_2[Q(\rho_{\mathcal{E}_0}^{\mu},\rho_{\mathcal{E}_1}^{\mu})^n/2]$, where $\rho_{\mathcal{E}_u}^{\mu}$ is generated by a TMSV state Φ_{sr}^{μ} with $\mu = 2N+1$. These bounds provide a sufficient condition for proving $\Delta > 0$.

Positive values of Δ are typical at low signal photon numbers. When the land reflectivity is high $\eta_1 \to 1$ (ideal cell), one finds analytical expressions[37] and regimes where $\Delta \to 1$ bit per cell. This extremal value means that the EPR transmitter fully reads the cell, while classical transmitters do not retrieve information, an advantage that might be used to design cryptographic memories[38]. Another type of energy constraint is 'global', meaning that we fix the mean total number of photons $N_{\rm T}$, so that we employ an average of $N_{\rm T}/n$ photons per use. Let us call n the 'bandwidth' of the transmitter. One can show that, at sufficiently low photons $N_{\rm T} \lesssim 10$, a narrowband EPR transmitter (for example, monochromatic $n_{\rm EPR} = 1$) is able to beat arbitrary classical transmitters, even with extremely large bandwidths. Because a few entangled photons can retrieve more information than any classical source of light, one may work at very low energies, a regime that may potentially be mapped into faster optical readers and denser memories[35].

Quantum reading has been extensively studied[35–53] and the term is today unambiguously associated with the quantum-enhanced readout of classical information from optical memories (therefore it should not to be confused with other applications of channel discrimination, such as communication via control-unitaries between registers of a quantum computer[113]). Already in 2011, a follow-up work[39] extended the model to multi-cell error correction and introduced the notion of quantum reading capacity[36,39], later shown to be super-additive[40]. Another work[41] studied the error exponent for quantum reading and defined a similar notion of reading capacity[42], a quantity that has been recently reconsidered[43]. Note that a two-way notion of quantum reading capacity is immediately given by extending the original definition[39] to adaptive channel discrimination[23], with adaptive-to-block simplification[32] for jointly teleportation-covariant channels[23,34]. Then, ref. [44] showed that Fock states are optimal for (non-adaptive) reading of an ideal cell in noiseless conditions and that suitable entangled states (with the signal beam in a number-diagonal reduced state) may also provide a positive quantum advantage. This latter class of states was also found to be optimal for non-adaptive discrimination of single-mode and multi-mode pure-loss channels[45].

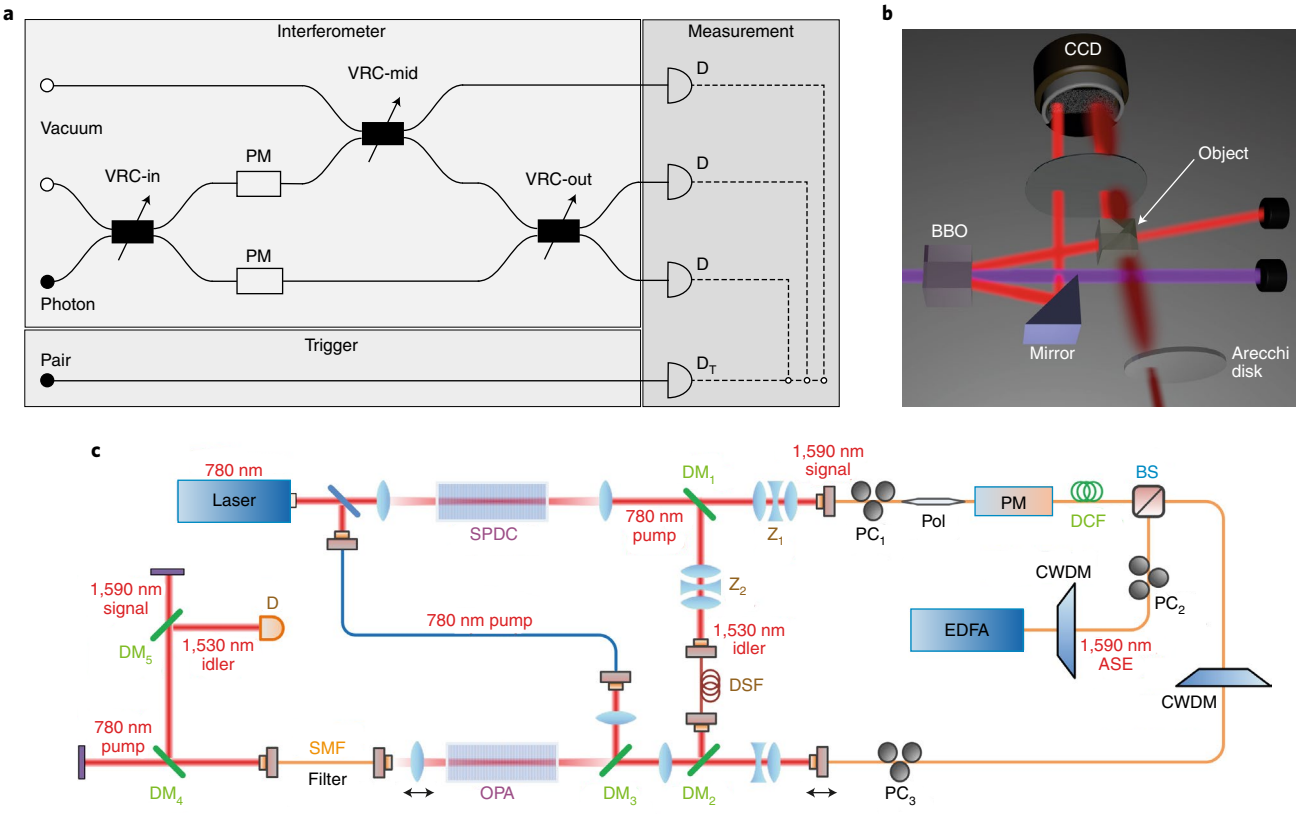


Fig. 3 | Experimental demonstrations of quantum reading and quantum illumination. a, Experimental set-up of perfect quantum reading[49]. A photon-pair source is used to generate a heralded single photon using a trigger detector (D_T). The heralded single photon is fed into a Mach–Zehnder interferometer with variable ratio couplers (VRCs) and phase modulators (PMs) to add additional phase shifts. Coincidence detection of the outputs are used to discriminate between two possible splitting ratios of VRC-mid. With the perfect beamsplitter under test ($\eta_1 = 1$), only one of the detectors (D) at the output of the interferometer would detect the photon (Hong–Ou–Mandel effect). For the non-perfect beamsplitter ($\eta_0 < 1$), any of the two other detectors would detect the photon (due to the additional phase shift). **b**, Quantum illumination experiment of Lopaeva et al.[67] (see also ref. [68]). Both beams of a photon-pair source are detected by a photon-counting CCD camera. In the experiment the target object is a 50:50 beamsplitter placed in one of the beams. The beamsplitter is simulated to be in a thermal environment by illuminating it with scattered light from an Arecchi disk. **c**, In the quantum illumination experiment of Zhang et al.[70], photon pairs are generated by spontaneous parametric downconversion (SPDC) at two different wavelengths and split using a dichroic mirror (DM). One of the photons is stored in a delay line using a dispersion-shifted LEAF fibre (DSF). The other photon is phase modulated (PM). A lossy and noisy environment is simulated by a beamsplitter (BS) and amplified spontaneous emission (ASE) from an erbium-doped fibre amplifier (EDFA). The joint detection is implemented using an optical parameteric amplifier (OPA) whose output is detected by a p–i–n photodetector (D). DCF, dispersion-compensating fibre; POL, polarizer; CWDM, coarse wavelength-division multiplexer; PC, polarization controller; Z, zoom lens. Thin lines are optical fibre, thick lines are unguided propagation. Figure adapted from: **a**, ref. [49], APS; **b**, ref. [67], APS; **c**, ref. [70], APS.

Reference [46] proposed an alternative model based on a binary phase encoding and showed how entangled coherent states may achieve error-free quantum reading. Non-Gaussian entangled states were also considered in other literature[47]. Reference [48] studied a noise-free unitary model of quantum reading where both the inputs of the unknown beamsplitter are accessible for probing and both its outputs for detection. Assuming a single probe per cell ($n = 1$), it was found that the optimal (non-adaptive) two-mode input is the superposition of a N00N state and the vacuum $|00\rangle$. This approach was extended[50] to unambiguous quantum reading, where the statistical error is replaced by an inconclusive result.

Similar to ref. [46], another work[49] also considered a version of perfect quantum reading with zero discrimination error. This is possible by designing an ideal cell that is either a beamsplitter with perfect reflectivity ($\eta_1 = 1$) or a beamsplitter with lower reflectivity $\eta_0 < 1$ and suitable $\pm\pi/2$ phase shifters at the input and output ports. This scheme was experimentally implemented[49]. The set-up consisted of a Mach–Zehnder interferometer with the variable beamsplitter situated in one arm. A single photon from a heralded single-photon source was injected into the interferometer and detected by one of the three detectors located at the two outputs of the interferometer and at the second output port of the beamsplitter under test. Coincidence counts with the heralding detector were measured. Due to the Hong–Ou–Mandel effect only coincidence counts with one of the detectors at the output were observed for the beamsplitter with perfect reflectivity. For the beamsplitters with lower reflectivity however, reduced coincidence counts were measured. See Fig. 3a for more details.

Quantum illumination of targets

Quantum sensing can be used not only to enhance the readout of information from classical systems, but also to boost the standoff detection of remote objects. This idea was first pushed forward by the efforts of Lloyd, Shapiro and collaborators[54–56]. In 2008, Lloyd[54] designed a qubit-based protocol of quantum illumination, showing how the detection of a low-reflectivity target object can be enhanced by quantum entanglement. The advantage of the entangled transmitter over non-entangled ones is achieved even if the entanglement

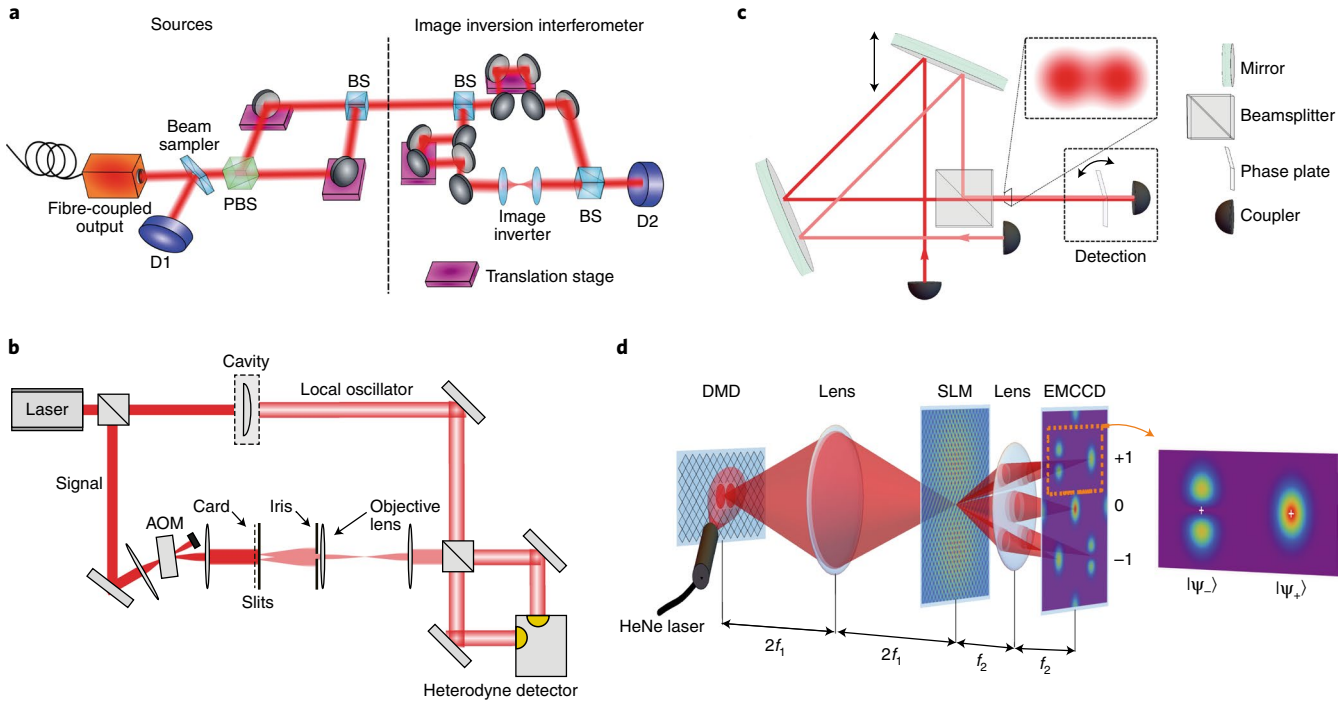


Fig. 4 | Proof-of-principle experiments demonstrating a quantum detection scheme able to measure a distance of two incoherent point-like sources better than the Rayleigh limit. a, In the experiment of Tang et al.[79], a HeNe laser with fibre-coupled output is split at a polarizing beamsplitter (PBS) into two beams of orthogonal polarization. They are recombined at a beamsplitter (BS) with a slight lateral displacement to simulate two incoherent light sources. The light sources are imaged using an image inversion interferometer, a Mach–Zehnder interferometer with an image inverter consisting of two lenses in one arm. One output of the interferometer is detected by a photodetector (D2). **b**, In the experiment of Yang et al.[81], the signal beam is frequency shifted by an acousto-optical modulator (AOM) and illuminates slits. A paper card is placed in front of the slits to make the illumination incoherent. The signal beam is measured by heterodyne detection using a local oscillator prepared in TEM_{01} mode by means of an optical cavity. **c**, In the experiment of Tham et al.[82], two partially overlapping beams (as shown in the upper inset) are generated by coupling laser light out of a fibre and combining them on a beamsplitter. The distance between the beams can be controlled by the position of the upper mirror. The separation of the two beams is detected by projecting the beams onto a mode orthogonal to TEM_{00}, in this case a spatially antisymmetric field mode. This is performed by passing the two beams through a phase plate that is built in such a way that it introduces different phase shifts between opposite halves of the beam and aligned such that coupling into a well-aligned fibre coupler is minimized. The coupling into a single-mode fibre corresponds to a projection onto the TEM_{00} mode, thus together with the phase plate the beams are projected onto a mode orthogonal to TEM_{00}. **d**, In the experiment of Paúr et al.[83], two closely spaced incoherent beams are generated by using a high-frequency switched digital micromirror chip (DMD) illuminated by a HeNe laser. The beam is projected onto different modes by an amplitude spatial light modulator (SLM) generating a digital hologram. The first-order diffraction spectrum is detected by an electron-multiplying CCD (EMCCD) camera. *f*, focal length; $|\psi_+\rangle$, symmetric state; $|\psi_-\rangle$, antisymmetric state. Figure adapted from: **a**, ref. [79], OSA; **b**, ref. [81], OSA; **c**, ref. [82], APS; **d**, ref. [83], OSA.

itself is completely lost after reflection from the target. In fact, the initial signal–idler entanglement is mapped into residual but yet quantum correlations between the reflected signal and the kept idler that a suitably designed quantum detector may 'amplify' with respect to the thermal background.

In the same year, a team led by Shapiro[55] proposed a practical version of quantum illumination based on continuous-variable systems[5,6]. In ref. [55], a Gaussian protocol is described where bosonic modes are prepared in Gaussian states and sent to detect an object with low reflectivity $\eta \simeq 0$ in a region with bright thermal noise, that is, with $\bar{n} \gg 1$ mean thermal photons. The detection process can be modelled as the discrimination between a zero-reflectivity thermal-loss channel $\mathcal{E}_{\eta=0,\bar{n}}$ (target absent) and a low-reflectivity thermal-loss channel $\mathcal{E}_{\eta,\bar{n}'}$ with $\eta \simeq 0$ and $\bar{n}' = \bar{n}/(1-\eta)$ (target present). Here the factor $(1-\eta)^{-1}$ excludes a 'passive signature' that is the possibility of detecting the target by just measuring a lower received background level. As also depicted in Fig. 2, one can assume that the detector's noise does not depend on the presence of the target.

In this set-up, we assume a local energy constraint, so that N mean photons are irradiated by each of the n bosonic modes sent over the target. Under this assumption, we compute the error probability associated with the various transmitters. In particular, we exploit the bounds in equations (10) and (11) to compare the performance of the EPR transmitter (based on TMSV states) with that of the classical transmitter. In the regime of low-energy signals ($N \ll 1$) and many modes ($n \gg 1$), the EPR transmitter has the scaling[55] $p_{\mathrm{EPR}}^{\mathrm{err}} \simeq \exp(-n\eta N/\bar{n})/2$, which clearly outperforms the classical transmitter $p_{\mathrm{class}}^{\mathrm{err}} \geq \exp(-n\eta N/2\bar{n})/4$. In particular, $p_{\mathrm{EPR}}^{\mathrm{err}}$ realizes a 6 dB advantage in the error-probability exponent over the coherent-state transmitter $p_{\mathrm{CS}}^{\mathrm{err}} \simeq \exp(-n\eta N/4\bar{n})/2$. Zhuang et al.[57] proved that the theoretical limit $p_{\mathrm{EPR}}^{\mathrm{err}}$ can be achieved by an explicit quantum receiver based on feed-forward sum-frequency generation. This receiver has also been used to show the quantum illumination advantage in terms of detection probability versus false-alarm probability[58].

In 2015, Gaussian quantum illumination was extended to the microwave regime, thus providing a prototype of quantum radar[59]. In this scheme, an electro-optomechanical converter[114,115] transforms an optical mode into microwave. If this transducer has high quantum efficiency, then optical–optical entanglement is translated into microwave–optical entanglement. The microwave signal is sent to probe the target region, while the optical idler is retained.

The microwave radiation collected from the target region is then phase conjugated and upconverted into an optical field by a second use of the transducer. The optical output is finally combined with the retained idler in a joint detection based on a practical receiver design[60]. In this way, ref. [59] reports that the error probability of microwave quantum illumination is superior to that of any classical radar of equal transmitted energy. A follow-up analysis has been recently carried out[61].

More recently, another study[62] considered the protocol of quantum illumination using the tools of quantum metrology so as to measure the reflectivity of the target. They employed the QFI to bound the error probability showing a 3-dB enhancement of the signal-to-noise ratio with respect to the use of local measurements. They also considered non-Gaussian Schrödinger's cat states. Other studies have quantified the quantum illumination advantage in terms of 'consumption' of discord associated with the target[63], and in terms of mutual information[64]. Finally note that quantum illumination has been also studied as an asymmetric Gaussian discrimination problem[65,66,116,117]. In this asymmetric setting, TMSV states have been identified as optimal probes for asymptotic discrimination, also in the adaptive case[66,117]. However, in the standard symmetric setting, finding the ultimate adaptive performance achievable by Gaussian quantum illumination remains an open question, while this problem has been recently solved for the discrete-variable version[28].

Several experiments of quantum illumination have been reported[67–70]. As depicted in Fig. 3b, Lopaeva et al.[67] exploited a parametric downconversion source using a beta-barium borate (BBO) crystal to generate two intensity-correlated light beams in orthogonal polarizations at 710 nm. Both beams were detected by a photon-counting high-quantum-efficiency charge-coupled device (CCD) camera. The target object, a 50:50 beamsplitter in the experiment, was placed in one of the two entangled beams before detection. The beamsplitter object was illuminated by photons scattered on an Arecchi's rotating ground glass to simulate a thermal environment. A single captured image was used to measure the second-order correlations between the two beams. The implementation shows robustness against noise and losses; it also demonstrates a quantum enhancement in target detection in thermal environments even when non-classicality is lost. However, coincidence detection of spontaneous parametric downconversion is not the optimal detection method to extract the most information from the signal–idler entangled modes, and the implemented classical scheme using weakly thermal states is also non-optimal.

Adopting a different approach, in 2013 Zhang et al.[69] reported a secure communication experiment based on quantum illumination, in a set-up of two-way quantum key distribution[118]. More recently, Zhang et al.[70] demonstrated the advantage of quantum illumination over coherent states by using broadband entangled Gaussian states, as produced by continuous-wave spontaneous parametric downconversion. In the experiment shown in Fig. 3c, the signal modes were phase modulated before probing the weakly reflecting target, while the idler modes were stored in a delay line. The joint measurement was performed by combining the reflected signal modes and the idler modes with a pump in another optical parametric amplifier. The output on the order of nanowatts was then detected by a p–i–n photodetector with high gain and low noise. They showed a 20% improvement of the signal-to-noise ratio in comparison to the optimal classical scheme in an environment exhibiting 14 dB loss and a thermal background 75 dB above the returned probe light.

Optical resolution beyond the Rayleigh limit

The Rayleigh criterion is a well-known result in classical imaging. Two point-like sources cannot be optically resolved (in the far field) if they are closer than the Rayleigh length $\simeq \lambda/a$, where λ is the wavelength of the emitted light and a is the numerical aperture of the observing lens. For this reason, if we use a converging optical system to focus light on a screen and an array of detectors to measure the intensity, the Rayleigh's criterion together with the presence of photon shot noise, can lead to severe limitations in resolving point-like sources.

Various approaches have been implemented to beat the Rayleigh limit in both the near field[119–122] and the far field[123–126]. Achieving sub-diffraction resolution is clearly a well-desired result in microscopy, otherwise limited to features no closer than 0.2 μm. In the far field, the most notable breakthroughs have been achieved in fluorescence microscopy where diffraction has been overcome by stimulated emission depletion (STED)[123]. In STED, the idea is to use a light pulse to excite a volume of fluorescent molecules, followed by another pulse quenching fluorescence from all molecules but a middle nanometre-sized volume. While scanning the sample, only the light levels from the central volumes are registered, so that an image is reconstructed with nanometre resolution[124]. In general, far-field super-resolved microscopy[124,125] is based on switchable fluorophores and localization algorithms, with the positions of the fluorophores being inferred from the images[126]. Point sources may be imaged via direct photon-counting, with the Cramér–Rao bound setting the limit for any unbiased estimator[127–129].

The quantum-metrology-inspired measurements can achieve much higher Fisher information and a much lower error than the limits derived in the previous classical techniques. Furthermore, there is no need for switchable fluorophores so that the quantum approach is suitable for both microscopy and telescopy. By considering a fully quantum description of the light and the measurement apparatus, Tsang et al.[72] showed the existence of a quantum detection scheme able to measure the distance between two point-like sources with a constant accuracy, even when the sources have sub-wavelength separation. This ground-breaking result was achieved by addressing the resolution of two incoherent point-like sources with the tools of quantum estimation theory.

The theory behind these results was extended from incoherent sources emitting faint pulses to thermal sources of arbitrary brightness[73,74]. In general, ref. [73] established a connection between optical resolution and bosonic channel estimation, so that measuring the separation between two point-like sources is equivalent to estimating the loss parameters of two lossy channels. In this way, the authors of ref. [73] developed a theory of super-resolution for point-like sources emitting light in a generic state, that is, attenuated or bright, classical, coherent, incoherent, as well as entangled (for example, in a microscope set-up). The ultimate resolution was found as a function of the optical properties of the two sources and their separation[73] (see also the adaptive lower bound in ref. [28]). In particular, super-resolution can be enhanced when the sources emit entangled or quantum-correlated (discordant) light[73].

More recently, ref. [75] extended Tsang and colleagues' analysis from a Gaussian point spread function to a hard-aperture pupil, proving the information optimality of image-plane sinc-Bessel modes. They also generalized the result to an arbitrary point spread function. Another work[76] investigated the optimal measurements for beating the Rayleigh limit, while ref. [77] explored the use of homodyne or heterodyne detection. Finally, ref. [78] reported the quantum-optimal detection of one-versus-two incoherent optical sources.

Shortly after the idea of Tsang et al.[72] was presented, it was experimentally verified in several proof-of-principle experiments. The first experiment by Tang et al.[79] was based on super-localization by image inversion interferometry[80]. As shown in Fig. 4a, they used an image inversion interferometer to determine the separation of two incoherent point sources, generated by two laser beams in orthogonal polarizations stemming from the same HeNe laser. Using the light from the simulated sources as input, the interferometer was implemented as a Mach–Zehnder interferometer with image inversion generated by a lens system in one arm. The other arm was

delayed so that the detector at the output of the interferometer ideally showed no response for zero separation due to destructive interference. With growing separation of the two sources the destructive interference becomes more and more imperfect, yielding an optical resolution beyond the Abbe–Rayleigh limit.

Yang et al.[81] used heterodyne detection with a local oscillator in TEM_{01} mode to detect the separation of the two slits in a double-slit configuration beyond the classical resolution limit. As depicted in Fig. 4b, they used paper to achieve incoherence and diffuse transmission. Measuring at a frequency of some MHz to avoid noise at lower frequencies, the beat between the local oscillator and the beam illuminating the slits becomes zero if the separation is zero. Separating the two slits yields a measurement beyond the Abbe limit. While the scheme requires the two sources to be exactly aligned to the centre of the TEM_{01} mode, using higher-order TEM modes will provide general sub-Rayleigh imaging. Other experiments by Tham et al.[82] and Paúr et al.[83] are reported in Fig. 4c,d. Let us conclude that super-resolving quantum imaging is a hot topic and other experiments could be mentioned[84–86].

Discussion and outlook

Quantum sensing is a rapidly evolving field with many potential implications. Despite the great advances that have been achieved in recent years, a number of problems and experimental challenges remain open. From the point of view of the basic theoretical models of quantum metrology and hypothesis testing, we may often compute the ultimate performances allowed by quantum mechanics. However, we do not know in general how to implement the optimal measurements achieving these performances and/or what optimal states we need to prepare at the input of the unknown quantum channel. Then, do we need to consider feedback and perform adaptive protocols? For instance, this is an open question for both estimation and discrimination of bosonic loss, which is at the basis of quantum reading, Gaussian quantum illumination and quantum-enhanced optical super-resolution.

From a more practical and experimental point of view, there are non-trivial challenges as well. Despite a first proof-of-principle demonstration[49] based on the unitary discrimination of beamsplitters, we do not have yet a truly quantum reading experiment where a single output of the cells is effectively accessed for the readout. A full demonstration would involve an actual (one- or two-dimensional) array of optical cells, where information is stored with classical codes and the quantum readout is performed on blocks of cells. This idea may be further developed into an experiment of bosonic quantum pattern recognition where the use of entanglement across an array may boost the resolution of problems of data clustering.

Quantum illumination has had various experimental demonstrations[67–70]. Challenges become non-trivial when we consider the microwave regime[59]. Here the development of highly efficient microwave–optical converters could mitigate experimental issues related with the generation of microwave entanglement and the detection of microwave fields at the single-photon level. Furthermore these converters are highly desired for other applications, in particular as interfaces between superconducting quantum chips and optical fibres in a potential hybrid quantum Internet[92].

Other designs of quantum radar are possible. For instance, as already suggested in ref. [59], a fully microwave implementation of quantum illumination (without converters) may be achieved using a superconducting Josephson parametric amplifier to generate signal–idler microwave entanglement. Reflected signals could then be phase conjugated via another parametric amplifier, recombined with the idlers, and finally measured, for example, by using a transmon qubit as a single-photon detector. The idea of using Josephson mixers and photocounters was later studied [71] with the aim of using microwave quantum illumination to reveal phase shift induced by cloaking.

Other experimental challenges need to be addressed in order to build an actual quantum radar. An important aspect is the preservation of the idler modes while the signals are being propagated forward and back from the target. The idlers should be kept in a low-loss delay line or stored in quantum registers with sufficiently long coherence times, until the final joint detection. Then, unlike classical radars, whose performance improves as the signal power is increased at constant bandwidth, for the quantum counterpart the bandwidth needs to be increased at constant signal brightness. The challenge is therefore to generate microwave pulses with a time–bandwidth product of 10^6 modes or more. Furthemore, classical radars can interrogate many potential target bins with a single pulse, while present models of quantum radar may only query a single polarization, azimuth, elevation, range, Doppler bin at a time. This is an area that needs development with very promising steps forward[130].

On the basis of current and next-available quantum technology, it is foreseen that the main application of quantum radar will be at relatively short ranges, where it may achieve the same detection performance of classical radars but using orders-of-magnitude fewer numbers of photons. In general, low-power radars are interesting not only for stealthy short-range target detection but also for proximity sensing and environmental scanning in robotic applications. The principles of quantum radar may also be developed into a non-invasive form of quantum microwave spectroscopy, with direct applications to condensed-matter physics (solid or atomic spins) and rotational spectroscopy (molecular rotors, organic molecules).

Regarding the experimental challenges for super-resolution[79], most of the current schemes, from spatial-mode demultiplexing to super-localization by image inversion and heterodyne, rely on the assumption that we need to know the location of the centroid of the sources in order to get full quantum-optimal resolution. In general, this location is not exactly known[79,81–83], so that achieving maximum alignment before estimating the separation becomes an important step to optimize the performance in a realistic implementation. On the theoretical side, it would be interesting to quantify the performance of adaptive quantum schemes, for instance in microscope-like set-ups.

Received: 21 February 2018; Accepted: 18 October 2018;
Published online: 28 November 2018

References

1. Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
2. Hayashi, M. *Quantum Information Theory: Mathematical Foundation* (Springer-Verlag, Berlin, Heidelberg, 2017).
3. Watrous, J. *The Theory of Quantum Information* (Cambridge University Press, Cambridge, 2018).
4. Andersen, U. L., Neergaard-Nielsen, J. S., van Loock, P. & Furusawa, A. Hybrid discrete- and continuous-variable quantum information. *Nat. Phys.* **11**, 713–719 (2015).
5. Weedbrook, C. et al. Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621–669 (2012).
6. Braunstein, S. L. & Van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* **77**, 513–577 (2005).
7. Adesso, G., Ragy, S. & Lee, A. R. Continuous variable quantum information: Gaussian states and beyond. *Open Syst. Inf. Dyn.* **21**, 1440001 (2014).
8. Serafini, A. *Quantum Continuous Variables: A Primer of Theoretical Methods* (Taylor & Francis, Oxford, 2017).
9. Degen, C. L., Reinhard, F. & Cappellaro, P. Quantum sensing. *Rev. Mod. Phys.* **89**, 035002 (2017).
10. Braunstein, S. L. & Caves, C. M. Statistical distance and the geometry of quantum states. *Phys. Rev. Lett.* **72**, 3439–3443 (1994).
11. Braunstein, S. L., Caves, C. M. & Milburn, G. J. Generalized uncertainty relations: theory, examples, and Lorentz invariance. *Ann. Phys.* **247**, 135–173 (1996).
12. Giovannetti, V., Lloyd, S. & Maccone, L. Quantum-enhanced measurements: beating the standard quantum limit. *Science* **306**, 1330–1336 (2004).

13. Giovannetti, V., Lloyd, S. & Maccone, L. Advances in quantum metrology. *Nat. Photon.* **5**, 222–229 (2011).
14. Braun, D. et al. Quantum enhanced measurements without entanglement. *Rev. Mod. Phys.* **90**, 035006 (2018).
15. Helstrom, C. W. *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
16. Barnett, S. M. & Croke, S. Quantum state discrimination. *Adv. Opt. Photon.* **1**, 238–278 (2009).
17. Audenaert, K. M. R. et al. Discriminating states: the quantum Chernoff bound. *Phys. Rev. Lett.* **98**, 160501 (2007).
18. Pirandola, S. & Lloyd, S. Computable bounds for the discrimination of Gaussian states. *Phys. Rev. A* **78**, 012331 (2008).
19. Hayashi, M. Discrimination of two channels by adaptive methods and its application to quantum system. *IEEE Trans. Inf. Theory* **55**, 3807–3802 (2009).
20. Harrow, A. W., Hassidim, A., Leung, D. W. & Watrous, J. Adaptive versus nonadaptive strategies for quantum channel discrimination. *Phys. Rev. A* **81**, 032339 (2010).
21. Cooney, T., Mosonyi, M. & Wilde, M. M. Strong converse exponents for a quantum channel discrimination problem and quantum-feedback-assisted communication. *Commun. Math. Phys.* **344**, 797–829 (2016).
22. Giovannetti, V., Lloyd, S. & Maccone, L. Quantum metrology. *Phys. Rev. Lett.* **96**, 010401 (2006).
23. Pirandola, S. & Lupo, C. Ultimate precision of adaptive noise estimation. *Phys. Rev. Lett.* **118**, 100502 (2017).
24. Takeoka, M. & Wilde, M. M. Optimal estimation and discrimination of excess noise in thermal and amplifier channels. Preprint at https://arxiv.org/abs/arXiv:1611.09165 (2016).
25. Zhou, S., Zhang, M., Preskill, J. & Jiang, L. Achieving the Heisenberg limit in quantum metrology using quantum error correction. *Nat. Commun.* **9**, 78 (2018).
26. Demkowicz-Dobrzanski, R., Czajkowski, J. & Sekatski, P. Adaptive quantum metrology under general Markovian noise. *Phys. Rev. X* **7**, 041009 (2017).
27. Cope, T. P. W. & Pirandola, S. Adaptive estimation and discrimination of Holevo-Werner channels. *Quantum Meas. Quantum Metrol.* **4**, 44–52 (2017).
28. Pirandola, S., Laurenza, R. & Lupo, C. Fundamental limits to quantum channel discrimination. Preprint at https://arxiv.org/abs/arXiv:1803.02834 (2018).
29. Nielsen, M. A. & Chuang, I. L. Programmable quantum gate arrays. *Phys. Rev. Lett.* **79**, 321–324 (1997).
30. Ji, Z., Wang, G., Duan, R., Feng, Y. & Ying, M. Parameter estimation of quantum channels. *IEEE Trans. Inf. Theory* **54**, 5172–5185 (2008).
31. Demkowicz-Dobrzański, R. & Maccone, L. Using entanglement against noise in quantum metrology. *Phys. Rev. Lett.* **113**, 250801 (2014).
32. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017).
33. Pirandola, S. et al. Theory of channel simulation and bounds for private communication. *Quantum Sci. Technol.* **3**, 035009 (2018).
34. Laurenza, R., Lupo, C., Spedalieri, G., Braunstein, S. L. & Pirandola, S. Channel simulation in quantum metrology. *Quantum Meas. Quantum Metrol.* **5**, 1–12 (2018).
35. Pirandola, S. Quantum reading of a classical digital memory. *Phys. Rev. Lett.* **106**, 090504 (2011).
36. Lupo, C., Pirandola, S., Giovannetti, V. & Mancini, S. Quantum reading capacity under thermal and correlated noise. *Phys. Rev. A* **87**, 062310 (2013).
37. Spedalieri, G., Lupo, C., Mancini, S., Braunstein, S. L. & Pirandola, S. Quantum reading under a local energy constraint. *Phys. Rev. A* **86**, 012315 (2012).
38. Spedalieri, G. Cryptographic aspects of quantum reading. *Entropy* **17**, 2218–2227 (2015).
39. Pirandola, S., Lupo, C., Giovannetti, V., Mancini, S. & Braunstein, S. L. Quantum reading capacity. *New J. Phys.* **13**, 113012 (2011).
40. Lupo, C. & Pirandola, S. Super-additivity and entanglement assistance in quantum reading. *Quantum Inf. Comput.* **17**, 0611–0622 (2017).
41. Guha, S. & Shapiro, J. H. Reading boundless error-free bits using a single photon. *Phys. Rev. A* **87**, 062306 (2013).
42. Guha, S., Dutton, Z., Nair, R., Shapiro, J. H. & Yen, B. Information capacity of quantum reading. In *Conference on Laser Science XXVII* Paper LTuF2 (OSA, 2011).
43. Das, S. & Wilde, M. M. Quantum reading capacity: general definition and bounds. Preprint at https://arxiv.org/abs/arXiv:1703.03706 (2017).
44. Nair, R. Discriminating quantum-optical beam-splitter channels with number-diagonal signal states: applications to quantum reading and target detection. *Phys. Rev. A* **84**, 032312 (2011).
45. Nair, R. & Yen, B. J. Optimal quantum states for image sensing in loss. *Phys. Rev. Lett.* **107**, 193602 (2011).
46. Hirota, O. Error free quantum reading by quasi Bell state of entangled coherent states. *Quantum Meas. Quantum Metrol.* **4**, 70–73 (2017).
47. Prabhu Tej, J., Usha Devi, A. R. & Rajagopal, A. K. Quantum reading of digital memory with non-Gaussian entangled light. *Phys. Rev. A* **87**, 052308 (2013).
48. Bisio, A., Dall'Arno, M. & D'Ariano, G. M. Tradeoff between energy and error in the discrimination of quantum-optical devices. *Phys. Rev. A* **84**, 012310 (2011).
49. Dall'Arno, M. et al. Experimental implementation of unambiguous quantum reading. *Phys. Rev. A* **85**, 012308 (2012).
50. Invernizzi, C., Paris, M. G. A. & Pirandola, S. Optimal detection of losses by thermal probes. *Phys. Rev. A* **84**, 022334 (2011).
51. Dall'Arno, M., Bisio, A. & D'Ariano, G. M. Ideal quantum reading of optical memories. *Int. J. Quantum Inf.* **10**, 1241010 (2012).
52. Wilde, M. M., Guha, S., Tan, S.-H., & Lloyd, S. Explicit capacity-achieving receivers for optical communication and quantum reading. In *Proc. 2012 IEEE Int. Symposium on Information Theory* 551–555 (IEEE, 2012).
53. Roga, W. & Buono, D. & Illuminati, F. Device-independent quantum reading and noise-assisted quantum transmitters. *New J. Phys.* **17**, 013031 (2015).
54. Lloyd, S. Enhanced sensitivity of photodetection via quantum illumination. *Science* **321**, 1463–1465 (2008).
55. Tan, S.-H. et al. Quantum illumination with Gaussian states. *Phys. Rev. Lett.* **101**, 253601 (2008).
56. Shapiro, J. H. & Lloyd, S. Quantum illumination versus coherent-state target detection. *New J. Phys.* **11**, 063045 (2009).
57. Zhuang, Q., Zhang, Z. & Shapiro, J. H. Optimum mixed-state discrimination for noisy entanglement-enhanced sensing. *Phys. Rev. Lett.* **118**, 040801 (2017).
58. Zhuang, Z., Zhang, Z. & Shapiro, J. H. Entanglement-enhanced Neyman–Pearson target detection using quantum illumination. *J. Opt. Soc. Am. B* **34**, 1567–1572 (2017).
59. Barzanjeh, Sh. et al. Microwave quantum illumination. *Phys. Rev. Lett.* **114**, 080503 (2015).
60. Guha, S. & Erkmen, B. I. Gaussian-state quantum-illumination receivers for target detection. *Phys. Rev. A* **80**, 052310 (2009).
61. Xiong, B., Li, X., Wang, X.-Y. & Zhou, L. Improve microwave quantum illumination via optical parametric amplifier. *Ann. Phys.* **385**, 757–768 (2017).
62. Sanz, M., Las Heras, U., Garca-Ripoll, J. J., Solano, E. & Di Candia, R. Quantum estimation methods for quantum illumination. *Phys. Rev. Lett.* **118**, 070803 (2017).
63. Weedbrook, C., Pirandola, S., Thompson, J., Vedral, V. & Gu, M. How discord underlies the noise resilience of quantum illumination. *New J. Phys.* **18**, 043027 (2016).
64. Ragy, S. et al. Quantifying the source of enhancement in experimental continuous variable quantum illumination. *J. Opt. Soc. Am. B* **31**, 2045–2050 (2014).
65. Wilde, M. M., Tomamichel, M., Lloyd, S. & Berta, M. Gaussian hypothesis testing and quantum illumination. *Phys. Rev. Lett.* **119**, 120501 (2017).
66. De Palma, G. & Borregaard, J. The minimum error probability of quantum illumination. *Phys. Rev. A* **98**, 012101 (2018).
67. Lopaeva, E. D. et al. Experimental realization of quantum illumination. *Phys. Rev. Lett.* **110**, 153603 (2013).
68. Meda, A. et al. Photon-number correlation for quantum enhanced imaging and sensing. *J. Opt.* **19**, 094002 (2017).
69. Zhang, Z., Tengner, M., Zhong, T., Wong, F. N. C. & Shapiro, J. H. Entanglement's benefit survives an entanglement-breaking channel. *Phys. Rev. Lett.* **111**, 010501 (2013).
70. Zhang, Z., Mouradian, S., Wong, F. N. C. & Shapiro, J. H. Entanglement-enhanced sensing in a lossy and noisy environment. *Phys. Rev. Lett.* **114**, 110506 (2015).
71. Las Heras, U. et al. Quantum illumination reveals phase-shift inducing cloaking. *Sci. Rep.* **7**, 9333 (2017).
72. Tsang, M., Nair, R. & Lu, X.-M. Quantum theory of superresolution for two incoherent optical point sources. *Phys. Rev. X* **6**, 031033 (2016).
73. Lupo, C. & Pirandola, S. Ultimate precision bound of quantum and subwavelength imaging. *Phys. Rev. Lett.* **117**, 190802 (2016).
74. Nair, R. & Tsang, M. Far-field superresolution of thermal electromagnetic sources at the quantum limit. *Phys. Rev. Lett.* **117**, 190801 (2016).
75. Kerviche, R., Guha, S. & Ashok, A. Fundamental limit of resolving two point sources limited by an arbitrary point spread function. Preprint at https://arxiv.org/abs/1701.04913 (2017).
76. Rehacek, J., Paúr, M., Stoklasa, B., Hradil, Z. & Sánchez-Soto, L. L. Optimal measurements for resolution beyond the Rayleigh limit. *Opt. Lett.* **42**, 231–234 (2017).
77. Yang, F., Nair, R., Tsang, M., Simon, C. & Lvovsky, A. I. Fisher information for far-field linear optical superresolution via homodyne or heterodyne detection in a higher-order local oscillator mode. *Phys. Rev. A* **96**, 063829 (2017).

78. Lu, X.-M., Krovi, H., Nair, R., Guha, S. & Shapiro, J. H. Quantum-optimal detection of one-versus-two incoherent optical sources with arbitrary separation. Preprint at https://arxiv.org/abs/1802.02300 (2018).
79. Tang, Z. S., Durak, K. & Ling, A. Fault-tolerant and finite-error localization for point emitters within the diffraction limit. *Opt. Express* **24**, 22004–22012 (2016).
80. Nair, R. & Tsang, M. Interferometric superlocalization of two incoherent optical point sources. *Opt. Express* **24**, 3684–3701 (2016).
81. Yang, F., Taschilina, A., Moiseev, E. S., Simon, C. & Lvovsky, A. I. Far-field linear optical superresolution via heterodyne detection in a higher-order local oscillator mode. *Optica* **3**, 1148–1152 (2016).
82. Tham, W. K., Ferretti, H. & Steinberg, A. M. Beating Rayleigh's curse by imaging using phase information. *Phys. Rev. Lett.* **118**, 070801 (2017).
83. Paúr, M., Stoklasa, B., Hradil, Z., Sánchez-Soto, L. L. & Rehacek, J. Achieving the ultimate optical resolution. *Optica* **3**, 1144–1147 (2016).
84. Gatto Monticone, D. et al. Beating the Abbe diffraction limit in confocal microscopy via nonclassical photon statistics. *Phys. Rev. Lett.* **113**, 143602 (2014).
85. Treps, N. et al. Surpassing the standard quantum limit for optical imaging using nonclassical multimode light. *Phys. Rev. Lett.* **88**, 203601 (2014).
86. Classen, A. et al. Superresolving imaging of arbitrary one-dimensional arrays of thermal light sources using multiphoton interference. *Phys. Rev. Lett.* **117**, 253601 (2016).
87. Tsang, M. Quantum imaging beyond the diffraction limit by optical centroid measurements. *Phys. Rev. Lett.* **102**, 253601 (2009).
88. Rozema, L. A. et al. Scalable spatial superresolution using entangled photons. *Phys. Rev. Lett.* **112**, 223602 (2014).
89. Chiribella, G., D'Ariano, G. M. & Perinotti, P. Quantum circuit architecture. *Phys. Rev. Lett.* **101**, 060401 (2008).
90. Bennett, C. H. et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70**, 1895–1899 (1993).
91. Ishizaka, S. & Hiroshima, T. Asymptotic teleportation scheme as a universal programmable quantum processor. *Phys. Rev. Lett.* **101**, 240501 (2008).
92. Pirandola, S., Eisert, J., Weedbrook, C., Furusawa, A. & Braunstein, S. L. Advances in quantum teleportation. *Nat. Photon.* **9**, 641–652 (2015).
93. Adesso, G., Dell'Anno, F., Siena, S. D., Illuminati, F. & Souza, L. A. M. Optimal estimation of losses at the ultimate quantum limit with non-Gaussian states. *Phys. Rev. A* **79**, 040305(R) (2009).
94. Monras, A. & Paris, M. G. A. Optimal quantum estimation of loss in bosonic channels. *Phys. Rev. Lett.* **98**, 160401 (2007).
95. Whittaker, R. et al. Absorption spectroscopy at the ultimate quantum limit from single-photon states. *New J. Phys.* **19**, 023013 (2017).
96. Moreau, P.-A. et al. Demonstrating an absolute quantum advantage in direct absorption measurement. *Sci. Rep.* **7**, 6256 (2017).
97. Losero, E., Berchera, I. R., Meda, A., Avella, A. & Genovese, M. Unbiased estimation of an optical loss at the ultimate quantum limit with twin-beams. *Sci. Rep.* **8**, 7431 (2018).
98. Samantaray, N., Berchera, I. R., Meda, M. & Genovese, M. Realization of the first sub-shot-noise wide field microscope. *Light Sci. Appl.* **6**, e17005 (2017).
99. Brida, G., Genovese, M. & Berchera, I. R. Experimental realization of sub-shot-noise quantum imaging. *Nat. Photon.* **4**, 227–230 (2010).
100. Abadie, J. et al. A gravitational wave observatory operating beyond the quantum shot-noise limit. *Nat. Phys.* **7**, 962–965 (2011).
101. Schnabel, R., Mavalvala, N., McClelland, D. E. & Lam, P. K. Quantum metrology for gravitational wave astronomy. *Nat. Commun.* **1**, 121 (2010).
102. Banaszek, K., Demkowicz-Dobrzański, R. & Walmsley, I. A. Quantum states made to measure. *Nat. Photon.* **3**, 673–676 (2009).
103. Nagata, T., Okamoto, R., O'Brien, J. L., Sasaki, K. & Takeuchi, S. Beating the standard quantum limit with four-entangled photons. *Science* **316**, 726–729 (2007).
104. Slussarenko, S. et al. Unconditional violation of the shot-noise limit in photonic quantum metrology. *Nat. Photon.* **11**, 700–703 (2017).
105. Dorner, U. et al. Optimal quantum phase estimation. *Phys. Rev. Lett.* **102**, 040403 (2009).
106. Kacprowicz, M., Demkowicz-Dobrzański, R., Wasilewski, W., Banaszek, K. & Walmsley, I. A. Experimental quantum-enhanced estimation of a lossy phase shift. *Nat. Photon* **4**, 357–360 (2010).
107. Higgins, B. L., Berry, D. W., Bartlett, S. D., Wiseman, H. M. & Pryde, G. J. Entanglement-free Heisenberg-limited phase estimation. *Nature* **450**, 393–396 (2007).
108. Yonezawa, H. et al. Quantum-enhanced optical phase tracking. *Science* **337**, 1514–1517 (2012).
109. Xiang, G. Y., Higgins, B. L., Berry, D. W., Wiseman, H. M. & Pryde, G. J. Entanglement-enhanced measurement of a completely unknown optical phase. *Nat. Photon.* **5**, 43–47 (2011).
110. Berni, A. A. et al. Ab initio quantum-enhanced optical phase estimation using real-time feedback control. *Nat. Photon.* **9**, 577–581 (2015).
111. Fuchs, C. A. & van de Graaf, J. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Trans. Inf. Theory* **45**, 1216–1227 (1999).
112. Banchi, L., Braunstein, S. L. & Pirandola, S. Quantum fidelity for arbitrary Gaussian states. *Phys. Rev. Lett.* **115**, 260501 (2015).
113. Bose, S., Rallan, L. & Vedral, V. Communication capacity of quantum computation. *Phys. Rev. Lett.* **85**, 5448–5451 (2000).
114. Barzanjeh, Sh., Abdi, M., Milburn, G. J., Tombesi, P. & Vitali, D. Reversible optical-to-microwave quantum interface. *Phys. Rev. Lett.* **109**, 130503 (2012).
115. Barzanjeh, Sh., Vitali, D., Tombesi, P. & Milburn, G. J. Entangling optical and microwave cavity modes by means of a nanomechanical resonator. *Phys. Rev. A* **84**, 042342 (2011).
116. Spedalieri, G. & Braunstein, S. L. Asymmetric quantum hypothesis testing with Gaussian states. *Phys. Rev. A* **90**, 052307 (2014).
117. Berta, M., Hirche, C., Kaur, E. & Wilde, M. M. Amortized channel divergence for asymptotic quantum channel discrimination. Preprint at https://arxiv.org/abs/arXiv:1808.01498 (2018).
118. Pirandola, S., Mancini, S., Lloyd, S. & Braunstein, S. L. Continuous-variable quantum cryptography using two-way quantum communication. *Nat. Phys.* **4**, 726–730 (2008).
119. Novotny, L. & Hecht, B. *Principles of Nano-Optics* (Cambridge University Press, Cambridge, 2006).
120. Pendry, J. B. Negative refraction makes a perfect lens. *Phys. Rev. Lett.* **85**, 3966–3969 (2000).
121. Liu, Z., Lee, H., Yi, X., Sun, C. & Zhang, X. Far-field optical hyperlens magnifying sub-diffraction-limited objects. *Science* **315**, 1686 (2007).
122. Smolyaninov, I. I., Hung, Y.-J. & Davis, C. C. Magnifying superlens in the visible frequency range. *Science* **315**, 1699–1701 (2007).
123. Hell, S. W. & Wichmann, J. Breaking the diffraction resolution limit by stimulated emission: stimulated-emission-depletion fluorescence microscopy. *Opt. Lett.* **19**, 780–782 (1994).
124. Hell, S. W. Far-field optical nanoscopy. *Science* **316**, 1153–1158 (2007).
125. Betzig, E. et al. Imaging intracellular fluorescent proteins at nanometer resolution. *Science* **313**, 1642–1645 (2006).
126. Small, A. & Stahlheber, S. Fluorophore localization algorithms for super-resolution microscopy. *Nat. Methods* **11**, 267–279 (2014).
127. Tsai, M. J. & Dunn, K. P. *Performance Limitations on Parameter Estimation of Closely Spaced Optical Targets Using Shot-Noise Detector Model* Technical Report ADA073462 (Lincoln Laboratory, MIT, 1979).
128. Bettens, E. et al. Model-based two-object resolution from observations having counting statistics. *Ultramicroscopy* **77**, 37–48 (1999).
129. Ram, S., Ward, E. S. & Ober, R. J. Beyond Rayleigh's criterion: a resolution measure with application to single-molecule microscopy. *Proc. Natl Acad. Sci. USA* **103**, 4457–4462 (2006).
130. Zhuang, Q., Zhang, Z. & Shapiro, J. H. Entanglement-enhanced lidars for simultaneous range and velocity measurements. *Phys. Rev. A* **96**, 040304(R) (2017).

Acknowledgements

The authors would like to thank U. L. Andersen, L. Banchi, Sh. Barzanjeh, J. Borregaard, S. L. Braunstein, V. Giovannetti, S. Guha, C. Lupo, A. Lvovsky, M. Miková, M. Tsang and Z. Zhang for feedback. S.P. would like to specifically thank J. H. Shapiro and A. Farina for discussions on the experimental challenges related with a quantum radar, and R. Nair for the feedback on the experimental challenges in optical super-resolution. S.P. thanks support from the EPSRC via the 'UK Quantum Communications Hub' (EP/M013472/1). T.G. would like to acknowledge support from the Danish Research Council for Independent Research (Sapere Aude 4184-00338B) as well as the Innovation Fund Denmark (Qubiz) and the Danish National Research Foundation (Center for Macroscopic Quantum States, bigQ DNRF142).

Competing interests

The authors declare no competing interests.

Additional information

Reprints and permissions information is available at www.nature.com/reprints.

Correspondence should be addressed to S.P.

Chapter 14

Integrated Quantum Photonics

14.1 Motivation

While table-top optical setups are flexible, modular and can be realized in a rather straight-forward manner, it is often desirable to implement quantum optics experiments on-chip, i.e. in a photonic integrated circuit. For this purpose, technologies for on-chip generation, manipulation and detection of light at the single-photon level are needed. The use of photonic integrated circuits is linked with several advantages compared to bulk setups:

- Miniaturization / scalability: Complex photonic circuits can be realized with a footprint in the *mm* or *cm* range; the fabrication of photonic chips can be performed in an industrial manner allowing for cost-efficient mass production.
- Stability: Photonic integrated circuits are robust against external influencing factors and misalignment.
- Co-integration: Photonic integrated circuits can be interfaced with electronic integrated circuits, allowing for additional functionality and signal processing.

14.2 Basic Building Blocks

To realize photonic integrated circuits, it is clear that structures for on-chip guiding and routing of light are needed. The former can be achieved with photonic waveguides (Fig. 14.1 a-c), which share similarities with optical fibers and are based on refractive index differences leading to total internal reflection. Different material platforms are available and waveguide structures with low propagation loss down to below 1 dB / cm have been developed. The involved nanofabrication steps are crucial in terms of ensuring minimum surface roughness and imperfections to allow for such low propagation loss values. As an alternative, photonic crystal structures exhibiting a photonic band gap can also be used for on-chip guiding of light.

It is often needed to distribute the photons between different circuit components, for instance via symmetric 50% - 50% beam splitter structures (Fig. 14.1 d) or at other ratios that can potentially be dynamically adjusted. Another important building block are wavelength-selective filters, which can be for instance realized as ring resonator structures.

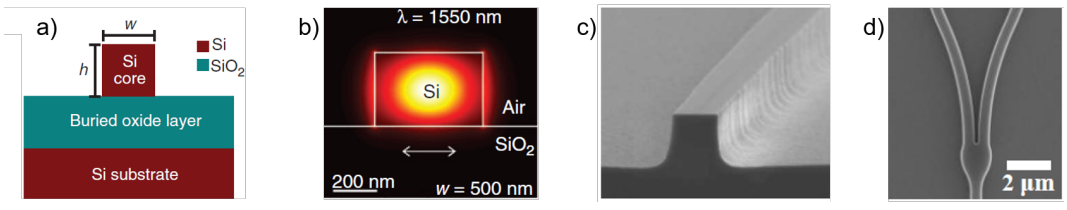


Figure 14.1: On-chip guiding and routing of light. a) Schematic of photonic waveguide structure using a silicon-on-insulator platform. b) Simulated electric field distribution inside a photonic waveguide. c) Exemplary scanning electron microscopy image of photonic waveguide. d) Beam splitter structure for on-chip routing of light. Adapted from Nanophotonics 6, 235 (2017); Advances in Optics and Photonics 6, 156 (2014); Optics Express 27, 14341, 2019.

An important feature of photonic integrated circuits is tunability, which means that key parts of the circuits such as beam splitters and filters can be re-configured by means of an external control parameter (e.g. by

applying a voltage at certain circuit elements). Most commonly, tunable elements rely on externally induced changes of refractive index, e.g. by thermo-optic effects, by electro-optic effects, or by means of free carrier injection. Another option is to achieve tunable photonic integrated circuits by relying on mechanical motion in micro-electro-mechanical systems (MEMS).

Significant advances have been made in integrating single-photon or entangled photon pair sources into photonic integrated circuits. For quantum dots and atom-like defects two different approaches have been followed: - monolithic integration, where the circuits components are realized on the chip where the quantum light source was realized / grown (e.g. quantum dots in III/V semiconductors, Applied Physics Letters 106, 221101, 2015). Alternatively, the quantum light sources can be mechanically transferred onto waveguide structures realized on a different chip, which is commonly referred to as hybrid or heterogeneous integration (e.g. Nature Communications 8, 889, 2017). For the case of entangled photon pair generation, probabilistic four-wave mixing processes relying on optical non-linearities in resonator structures have been developed (PRX Quantum 2, 010337, 2021).

For on-chip light detection, it is required to couple light guided on-chip to integrated photodetector devices. Single-photon detector devices commonly used in quantum optics have been successfully integrated with photonic waveguide structures, in particular superconducting nanowire detectors (Nature Communications 3, 1325, 2012) and avalanche photodiodes (Optics Express 25, 16130, 2017). While the latter case can be technologically challenging, superconducting nanowire detectors can be placed on top of photonic waveguides (Fig. 14.2), coupling to the evanescent field. In this traveling wave geometry photons are efficiently absorbed along the direction of light propagation over distances of several tens of micrometers.

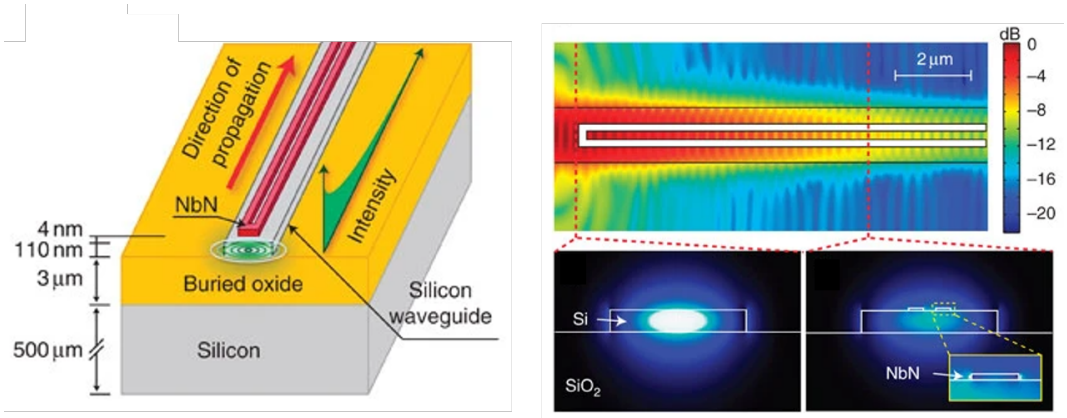


Figure 14.2: Single-photon detection with superconducting nanowires in traveling wave geometry. Adapted from Nature Communications 3, 1325, 2012.

Article

Quantum circuits with many photons on a programmable nanophotonic chip

https://doi.org/10.1038/s41586-021-03202-1

Received: 14 June 2020

Accepted: 4 January 2021

Published online: 3 March 2021

Check for updates

J. M. Arrazola[1]✉, V. Bergholm[1], K. Brádler[1], T. R. Bromley[1], M. J. Collins[1], I. Dhand[1], A. Fumagalli[1], T. Gerrits[2], A. Goussev[1], L. G. Helt[1], J. Hundal[1], T. Isacsson[1], R. B. Israel[1], J. Izaac[1], S. Jahangiri[1], R. Janik[1], N. Killoran[1], S. P. Kumar[1], J. Lavoie[1], A. E. Lita[2], D. H. Mahler[1], M. Menotti[1], B. Morrison[1], S. W. Nam[2], L. Neuhaus[1], H. Y. Qi[1], N. Quesada[1], A. Repingon[1], K. K. Sabapathy[1], M. Schuld[1], D. Su[1], J. Swinarton[1], A. Száva[1], K. Tan[1], P. Tan[1], V. D. Vaidya[1], Z. Vernon[1]✉, Z. Zabaneh[1] & Y. Zhang[1]

Growing interest in quantum computing for practical applications has led to a surge in the availability of programmable machines for executing quantum algorithms[1,2]. Present-day photonic quantum computers[3–7] have been limited either to non-deterministic operation, low photon numbers and rates, or fixed random gate sequences. Here we introduce a full-stack hardware–software system for executing many-photon quantum circuit operations using integrated nanophotonics: a programmable chip, operating at room temperature and interfaced with a fully automated control system. The system enables remote users to execute quantum algorithms that require up to eight modes of strongly squeezed vacuum initialized as two-mode squeezed states in single temporal modes, a fully general and programmable four-mode interferometer, and photon number-resolving readout on all outputs. Detection of multi-photon events with photon numbers and rates exceeding any previous programmable quantum optical demonstration is made possible by strong squeezing and high sampling rates. We verify the non-classicality of the device output, and use the platform to carry out proof-of-principle demonstrations of three quantum algorithms: Gaussian boson sampling, molecular vibronic spectra and graph similarity[8]. These demonstrations validate the platform as a launchpad for scaling photonic technologies for quantum information processing.

The past decade has seen remarkable progress in quantum computation and simulation. Breakthroughs across a range of platforms have enabled the construction of programmable machines delivering the automation, stability and repeatability demanded by increasingly sophisticated quantum algorithms. Rigorous benchmarks have been carried out on an 11-qubit trapped ion system[1,9], and a 53-qubit superconducting system has been used to generate random samples from a probability distribution at a rate exceeding what is reasonably achievable using classical hardware[2,10]. Similar machines can now be remotely accessed and loaded with algorithms written in high-level programming languages by users having little knowledge of the low-level quantum hardware details of the apparatus. These capabilities have accelerated application development for near-term quantum computers[11–13].

Such hardware has primarily been designed to access problems in the qubit model, where computation is carried out by initializing a quantum state in a space spanned by a product of binary-valued basis states, followed by a sequence of gates selected from a typically discrete set of operations[14]. Present-day machines are limited to dozens of noisy qubits, restricting their applicability to quantum algorithms compatible with this scale[15]. Other algorithms are more efficiently expressed in a model where each independent quantum system is described by a state in an infinite-dimensional Hilbert space. Examples include those implementing bosonic error correction codes[16,17], a wide class of Gaussian boson sampling (GBS) applications[8,18–23], and bespoke algorithms exploiting the structure of infinite-dimensional Hilbert spaces[24,25].

A promising platform for the large-scale implementation of bosonic quantum algorithms is offered by photonic hardware. A number of groundbreaking demonstrations of photonic quantum information processing have recently been completed. Two-dimensional cluster states with tens of thousands of entangled nodes have been deterministically generated using bulk-optical components[3,4], and photonic experiments have been constructed to sample from the photon number distribution of multi-mode Gaussian states[6,7]. Combined with advances in photonic chip fabrication[26], such demonstrations coincide with new optimism towards photonics as a platform for quantum computation[27].

Despite these advances, much work remains in developing photonic systems for practical use in quantum computation. Photonic cluster state demonstrations[3,4] were limited to all-Gaussian states, gates and measurements, rendering them efficiently simulatable at any scale by classical computers. Single-photon-based experiments on integrated platforms[5] suffer from non-deterministic state preparation and gate implementation, hindering their scalability. This deficit can be evaded in photonic experiments by using deterministically prepared squeezed states and linear optics, with non-Gaussian operations provided by

[1]Xanadu, Toronto, Ontario, Canada. [2]National Institute of Standards and Technology, Boulder, CO, USA. ✉e-mail: juanmiguel@xanadu.ai; zach@xanadu.ai

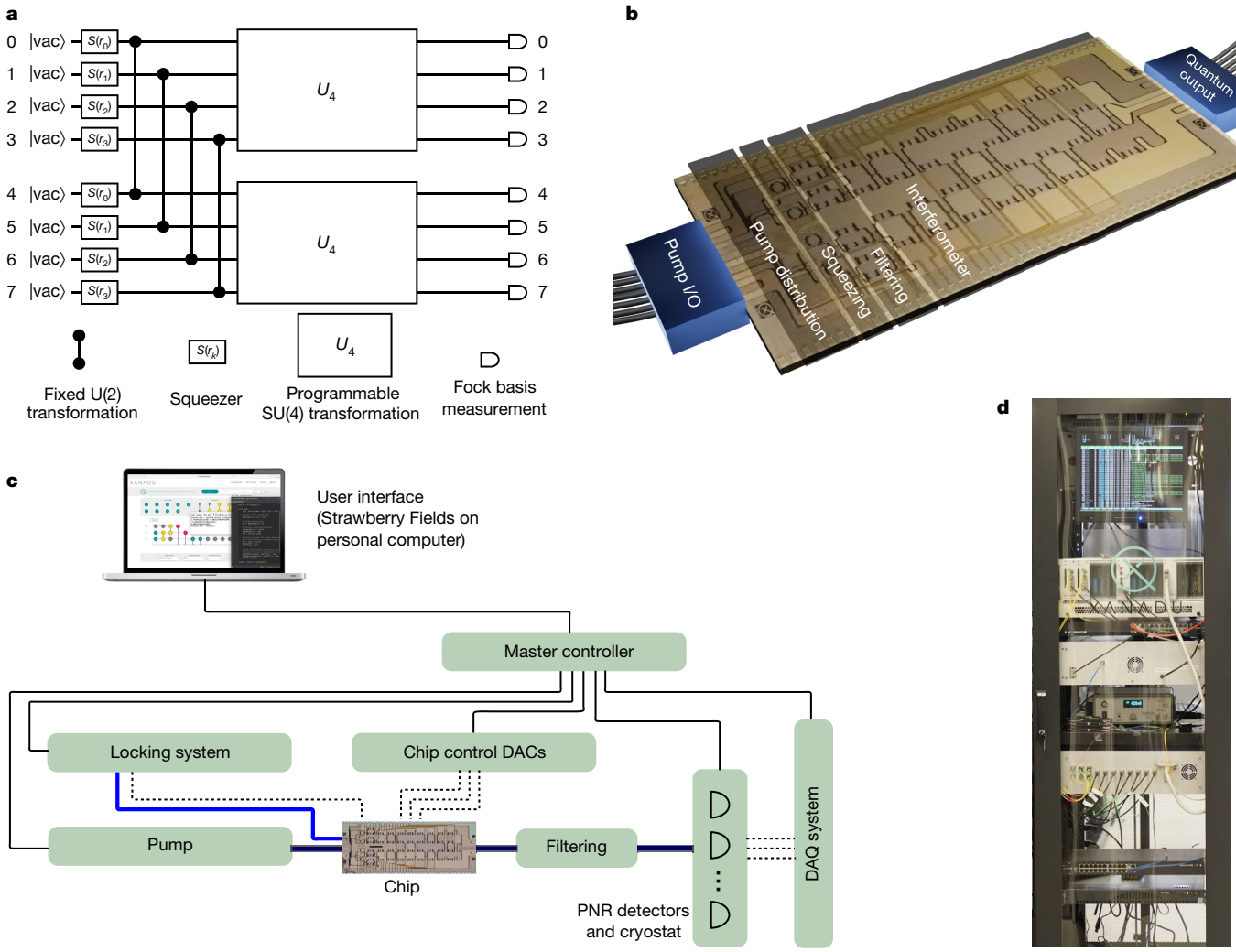


Fig. 1 | Overview of apparatus. a, Equivalent quantum circuit diagram illustrating the functionality of the photonic hardware. Up to eight modes initialized as vacuum are squeezed with squeezing parameters r_k and entangled (via the fixed two-mode unitary transformation U(2) equivalent to a 50/50 beam splitter with the relative input phase set to produce two-mode squeezing at the output) to form two-mode squeezed vacuum states. Programmable four-mode rotation gates (SU(4) transformation, represented by the large boxes labelled U_4) are applied to each four-mode subspace. All eight modes are individually read out by measurements in the Fock basis. **b**, Rendering of the chip (based on a micrograph of the actual device) showing fibre optical inputs and outputs, and on-chip modules for coherent pump power distribution, squeezing, pump filtering and programmable linear optical transformations. **c**, Schematic of full apparatus and control system. Solid (dashed) black lines indicate digital (analogue) electronic signals; blue lines indicate optical signals. DAC, digital-to-analogue converter; DAQ, data acquisition; PNR, photon number resolving. **d**, Photograph of entire system (except for photon-number-resolving detector hardware), which has been fitted into a standard server rack.

photon-counting detectors. In such experiments, and in the machine we present, squeezed state inputs have the role of qubits as the basic independently accessible quantum systems. But demonstrations of such squeezing-based photonic machines[6,7] lacked programmability, with each accessing only a fixed, randomized quantum state. Furthermore, these demonstrations were limited to small numbers of detected photons.

To date, no photonic machine has been demonstrated that is simultaneously (1) dynamically programmable, (2) readily scalable to hundreds of modes and photons, and (3) able to access a class of quantum circuits that could not, when the system size is scaled, be efficiently simulated by classical hardware. Here we report results from a device based on a programmable nanophotonic chip that includes all of these capabilities in a single scalable and unified machine. We describe the performance of the components designed for initial state preparation, gate sequence implementation, and readout, and verify the non-classicality of the device output. We then use the machine to carry out proof-of-principle demonstrations of the execution of three types of quantum algorithms: GBS[28], molecular vibronic spectra[18] and graph similarity[22]. Although our device, at its current scale, can readily be simulated by a classical computer, the architecture and platform developed can potentially enable future generations of such machines to exit this regime and perform tasks that are not practically simulatable by classical systems.

The core of our device is a 10 mm × 4 mm photonic chip. It generates squeezed light[29] in up to eight optical modes, with a fixed initialization into four independent two-mode squeezed vacuum states. The squeezing is generated between bichromatic mode pairs, with each such pair populating one of four spatially separated waveguide modes. An interferometer, based on a network of beam splitters and phase shifters, implements a user-programmable gate sequence corresponding to an SU(4) transformation (with SU(n) the special unitary group of degree n) applied to the spatial modes. The resulting eight-mode Gaussian state synthesized by the chip is then measured in the Fock basis using eight independent photon-number-resolving detectors. An equivalent quantum circuit diagram for the machine is illustrated in Fig. 1a.

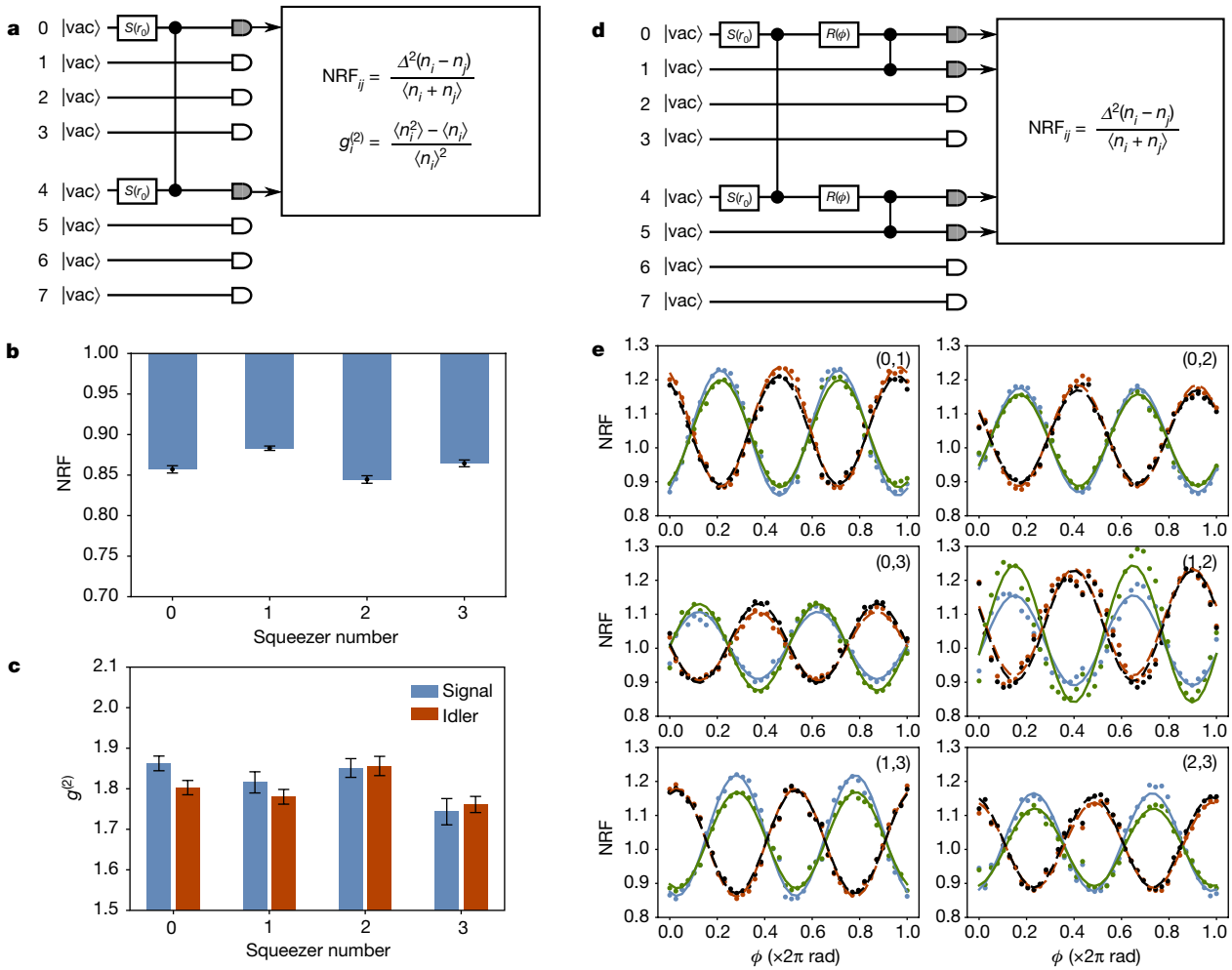


Fig. 2 | Component statistics. a, Schematic of the circuit used to measure NRFs and second-order correlation statistics for individual squeezers, here illustrated for squeezer 0. The unitary is set to the identity transformation, and each squeezer is turned on individually. Photon samples collected from the corresponding signal and idler outputs are collected and used to calculate the relevant quantities. **b**, Raw NRF for each of the squeezers. Each is well below unity, indicating non-classicality. Error bars represent one standard deviation over eight batches of 10^5 samples. **c**, Raw measured unheralded second-order correlation statistic $g^{(2)}$ of the signal and idler for each squeezer. Each is close to $g^{(2)} = 2$, indicating nearly single-temporal-mode operation. Error bars represent one standard deviation over eight batches of 10^5 samples. **d**, Schematic of the circuit used to measure quantum interference between pairs of squeezers. Here the circuit for the (0,1) pair is illustrated: two squeezers are turned on, and the interferometer is used to interfere their outputs on an effective 50/50 beam splitter with relative input phase ϕ, implemented by the single-mode rotation $R(\phi)$. The NRFs are then calculated from the photon-number samples. **e**, Interference traces between pairs of squeezers. The six panels each correspond to a different squeezer pair (k, l). Within each panel, four NRFs are plotted as function of the relative phase ϕ: [signal 1 – idler 1] (blue), [signal 2 – idler 2] (green), [signal 1 – idler 2] (red), [signal 2 – idler 1] (black). Points correspond to raw, uncorrected measured data; solid and dashed lines are best fits (least squares) to a model that incorporates no imperfections except photon loss.

The chip itself (Fig. 1b) is based on silicon nitride waveguides and thermo-optic phase shifters, fabricated using a commercially available service offered by Ligentec SA. The die contains modules for coherent distribution of pump light, generation of squeezed states, filters to separate pump light from generated quantum signals, and programmable linear-optical transformations. Four squeezers based on microring resonators[30] are integrated, each generating a bichromatic two-mode squeezed state in a nearly single temporal mode when pumped with a pulsed laser; that is, each squeezer generates an entangled-mode pair in its respective waveguide output. The modes in these pairs are distinguished by wavelength; we refer to them as the 'signal' and 'idler'. Four wavelength filters separate the pump light from the generated squeezed states, directing the squeezed light into the programmable interferometer and the pump light out of the chip. The interferometer implements an arbitrary programmable four-mode linear optical transformation on both the signal and idler subspaces of the squeezed light. The use of two-mode squeezers doubles the total number of modes available for detection per spatial mode, at the cost of restricting the space of eight-mode Gaussian states accessible from the chip. The synthesized Gaussian state is then coupled out of the chip for photon counting. More detail is provided in Methods.

To operate the apparatus, a control system was developed to autonomously actuate all required control signals, monitor system status and acquire data. An overview diagram of the full system is shown in Fig. 1c. A master controller (conventional server computer) running custom-developed control software coordinates the operation of the chip and all other hardware required. The system is accessed by a high-level application programming interface: a classical computer providing the quantum programs for the photonic chip, using the Strawberry Fields Python library[31]. This enables users with no knowledge of the hardware details to run quantum algorithms remotely on the device. Apart from the photon-counting system, the entire machine

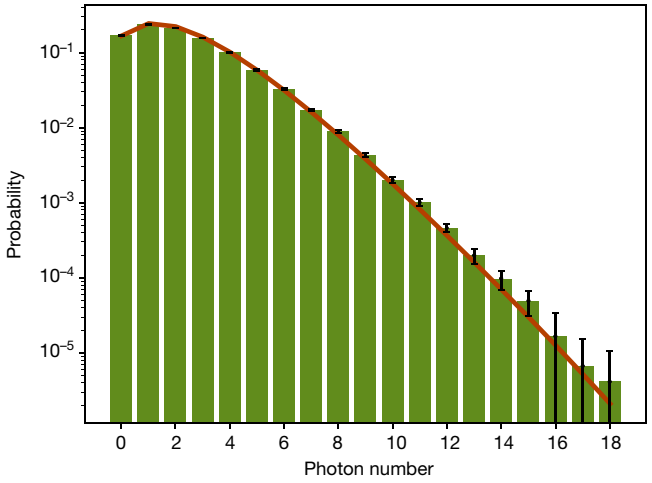


Fig. 3 | Total photon-number distribution. All squeezers are turned on and the interferometer is set to the identity. Estimates of the probabilities obtained from experimental samples are shown as bars. The theoretical prediction appears as a continuous line. Error bars denote one standard deviation taken over 12 runs of 10^5 samples. For large photon numbers, error bars are comparable to the probabilities.

is contained in a standard server rack (Fig. 1d); the chip itself is optically and electronically packaged, forming a mechanically stable solid-state system. The full apparatus is alignment-free and indefinitely stable for continuous operation, except for the cryogenic detection system, which requires 2 h of downtime every 24 h for its automated cycling process to complete.

In contrast with demonstrations of earlier photonic devices[6,7], our machine features non-classical light sources designed to generate squeezed light in single temporal modes with high average photon number (squeezing parameter $r \approx 1$, mean photon number $\bar{n} = \sinh^2 r \approx 1.4$ at the sources). In addition, detection is carried out using transition-edge sensors, yielding true photon-number resolution at the readout stage[32]. This enables execution of quantum algorithms involving multi-photon contributions, a key requirement for implementing many squeezing-based photonic quantum applications. For example, large-photon-number contributions are essential for accessing higher-energy transitions when using a photonic device for vibronic spectrum simulations[18]. Large $\bar{n}$ is also crucial for achieving a quantum advantage[33]. Our device readily achieves large-photon-number event rates exceeding all previous demonstrations of programmable photonic devices: with all squeezers activated, four-photon detection events occur at an average rate of 10,000 events per second, ten-photon events at an average rate of 270 events per second, and nineteen-photon events at an average rate of 0.3 events per second.

We characterize the component-level system performance by operating the interferometer in fixed simple configurations and computing relevant statistics on the event data acquired. As shown in Fig. 2a, the interferometer is first set to the identity transformation and each squeezer individually turned on. The two-mode cross-correlation $V^{(i)}_{\Delta n}/n^{(i)}_{\mathrm{tot}}$ is then measured, where $n^{(i)}_{\mathrm{tot}}$ is the combined total mean photon number in the ith signal/idler mode pair and $V^{(i)}_{\Delta n}$ is the variance of the photon number difference between the ith signal/idler mode pair. This quantity is termed the noise reduction factor (NRF) and is a measure of non-classicality[34]. For two-mode Gaussian states $V_{\Delta n_i}/n_{\mathrm{tot,i}} = 0$ indicates an ideal two-mode squeezed state, and $V_{\Delta n_i}/n_{\mathrm{tot},i} = 1$indicates a classical coherent state. As evident in Fig. 2b, the measured NRF for each signal/idler mode pair is well below unity, averaging 0.86(1). This value is limited primarily by losses, which degrade the measurable correlations in an otherwise ideal two-mode squeezed state as $V^{(i)}_{\Delta n}/n^{(i)}_{\mathrm{tot}} = 1 - \eta_i$, with η_i the total transmission efficiency experienced by mode pair i (assuming balanced losses between the signal and idler pair). Our estimated system efficiency of approximately 15%, inferred both from direct measurements of components using classical light and from fitting the photon-number statistics to a general theoretical model, is consistent with measured NRFs. From this, we estimate the effective input squeezing in each mode (that is, the squeezing produced by each squeezer in the circuit representation of Fig. 1a, in the absence of losses) to be approximately 8 dB.

Next, we characterize the temporal mode structure of the squeezers. This can be quantified by the Schmidt numbers K_i (refs. [30,35]) of our sources, or, equivalently, the unheralded second-order correlation statistic $g^{(2)}_{S(I),i} = (\langle n^2_{S(I),i}\rangle - \langle n_{S(I),i}\rangle)/\langle n_{S(I),i}\rangle^2$, where $n_{S(I),i}$ is the photon number measured in the signal (idler) from the ith squeezer. This statistic is independent of the NRF of the sources, as it pertains not to the degree of photon-number correlation between the mode pairs, but to the temporal mode structure of each generated squeezed state. Ideally, $g^{(2)}_{S(I),i} = 2$ for all squeezers, indicating a single-mode thermal state populating a single temporal mode, as is expected from each half of a two-mode squeezed state. The raw measured second-order correlation statistics for each of the eight measured modes is plotted in Fig. 2c; the average $g^{(2)}$ over all eight modes is 1.81(4), indicating that our squeezers are working close to single-temporal-mode operation. From this and the inferred level of background noise, we estimate that over 85% of detected photons come from squeezing in the dominant Schmidt mode across all squeezers.

An even more stringent requirement than single-temporal-mode operation is uniformity of the squeezed light sources: for high-visibility quantum interference to occur, the temporal modes populated by each squeezer must be nearly identical. To verify that genuine multi-source quantum interference is accessible in our device, we configure the interferometer to selectively interfere pairs of squeezed sources, and measure the phase-dependent response of four NRFs between all six possible pairs of squeezers. A representative quantum circuit is shown in Fig. 2e. The 24 resulting traces are plotted in Fig. 2e alongside fits to a theoretical model of this interference that includes only optical loss as an imperfection. The pronounced phase-dependent response of the photon statistics, consistent with the theoretical model, demonstrates multi-photon quantum interference between all four sources. We emphasize that, in contrast to the typical presentation of data from experiments based on heralded single-photon sources, no post-selection or other post-processing was applied to the data exhibited in Fig. 2e.

Finally, we show that the output distribution of the device cannot be efficiently simulated with small error by approximating the output state with a classical Gaussian state, that is, a state with a positive Glauber–Sudarshan P-function[36,37]. This condition is necessary but not sufficient to demonstrate the inability to classically simulate the device.

We characterize the chip using a model with a single Schmidt mode per squeezer, non-uniform loss, and excess noise from residual photons not blocked by the filtering system[38]. Using P_0 to denote the experimental photon number distribution, and P for the fitted model distribution, we find the sampling error, defined as $d_0 := \delta(P_0, P)$, where $\delta(P, Q) = \frac{1}{2}\|P - Q\|_1$ is the total variation distance, to be $d_0 = 0.10(1)$.

A device is deemed classical, meaning it can be efficiently simulated up to error ε by sampling from classical states, if the following condition is satisfied[33]:

$$\sum_{i=1}^{M} \ln\left(\frac{x_i + x_i^{-1}}{2}\right) < \frac{\varepsilon^2}{4}, \tag{1}$$

where $x_i = \sqrt{(\eta_i e^{-2r_i} + 1 - \eta_i)/(1 - 2p_i^{\mathrm{D}})}$, η_i is the transmission efficiency of mode i, r_i is the single-mode squeezing level, p_i^{D} is the probability of detecting one excess photon and M is the number of modes. Setting ε equal to the modelling error d_0 and substituting the model parameters, we obtain 2.5×10^{-3} for the right-hand side and 1.0×10^{-2} for the left-hand

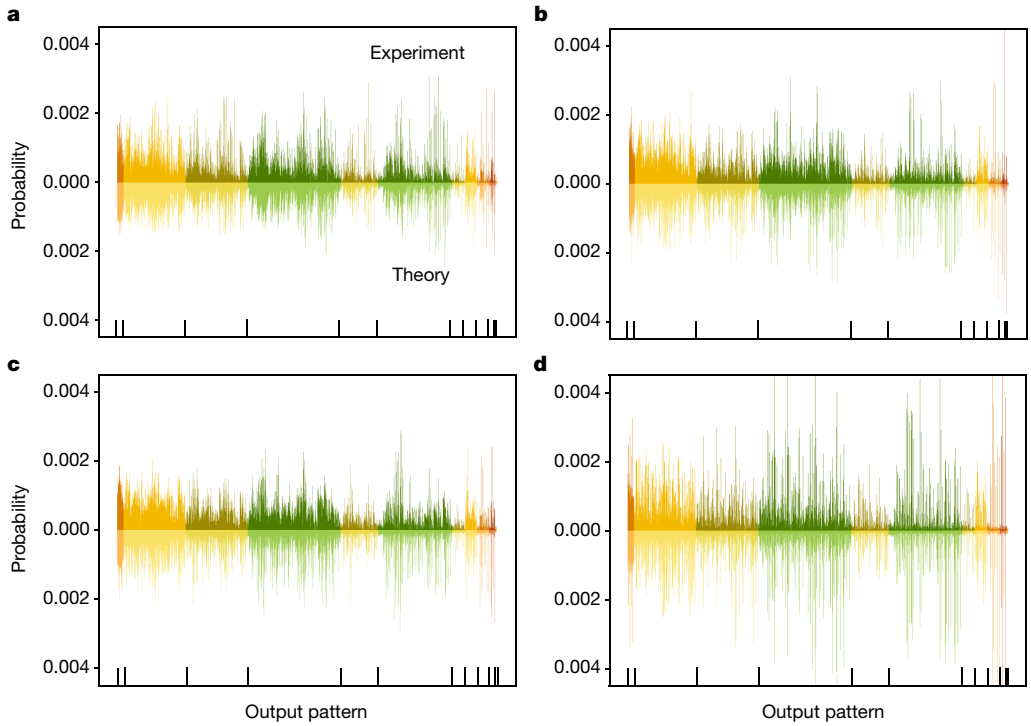


Fig. 4 | GBS experiment. In each figure, the top bar plot depicts experimental probabilities estimated from chip samples and the bottom plots show the theoretical values. Output patterns are organized by orbits, separated by different colours as well as vertical bars in the bottom of the plots. Starting from the left, the orbits are [1,1,1,1,1,1], [2,1,1,1,1], [3,1,1,1], [2,2,1,1], [4,1,1], [3,2,1], [5,1], [2,2,2], [4,2], [3,3] and [6]. Panels **a** to **c** show the distributions for Haar-random interferometers, and panel **d** is the identity.

side in equation (1), meaning that the inequality is not satisfied and the device passes the non-classicality test. The minimum error ε_0 satisfying the inequality can be interpreted as a measure of non-classicality; large ε_0 indicates a highly non-classical device. We find $\varepsilon_0 \approx 0.20$. This can be compared to previous four-mode experimental results[6] for which $\varepsilon_0 \approx 0.017$ can be inferred[33]. Thus our device samples from a distribution that is quantifiably more non-classical, which originates from the improved level of squeezing and transmission efficiency.

We now showcase the programmability, high sampling rate and photon-number-resolving capabilities of the machine by demonstrating proof-of-principle implementations of photonic quantum algorithms. The device is programmed remotely using Strawberry Fields[31]. Theoretical predictions are performed with respect to a model of the device involving two Schmidt modes per squeezer, non-uniform loss and excess noise.

GBS

Sampling from the distribution induced by a Fock basis measurement on Gaussian states is believed to require exponential time using classical computers[28,39]. This model is known as GBS and it is a leading platform for demonstrating a quantum advantage using photonic hardware.

Owing to strong on-chip squeezing in the device, a large number of photons can be generated. This is illustrated in Fig. 3, which shows the probability distribution for the total number of photons measured. In the implementation, the device is configured according to three different interferometers randomly selected from the Haar measure,

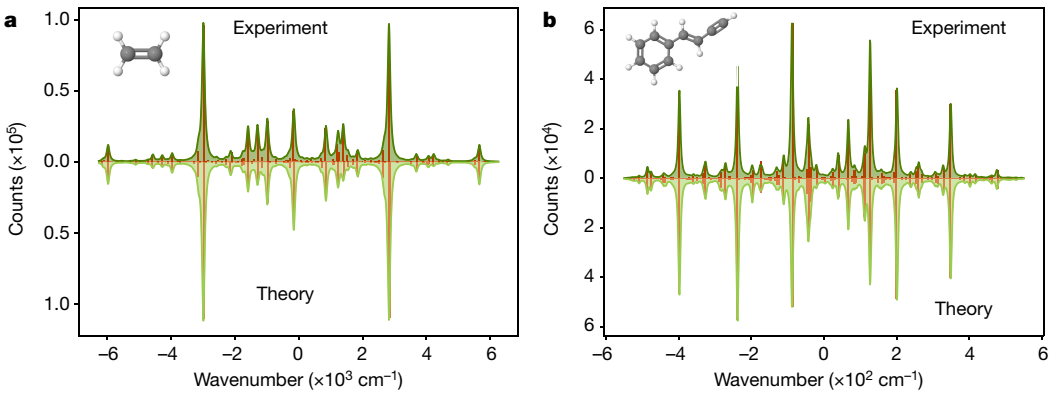


Fig. 5 | Vibronic spectra experiment. Franck–Condon profiles are obtained from chip distributions programmed according to the vibronic transitions of ethylene (**a**, with structure shown in the inset) and (*E*)-phenylvinylacetylene (**b**, with structure shown in the inset). The red bar graphs depict the histogram of energies, whereas green continuous lines show a Lorentzian broadening of the bars. Counts refer to the number of times the corresponding energy was observed. Wavenumbers correspond to the energy differences between initial and final energy levels. Vacuum outputs are omitted.

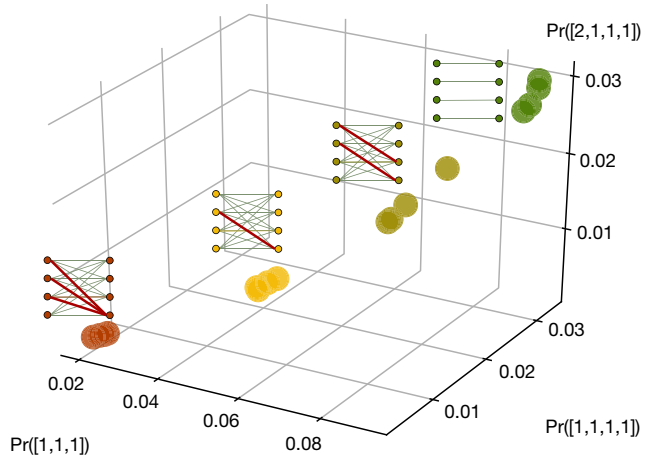


Fig. 6 | Graph similarity experiment. Feature vectors corresponding to four different graphs, which are drawn next to their corresponding feature vectors. Negative-weighted edges are highlighted by thick red lines. The components of the vectors are probabilities for the orbits [1,1,1], [1,1,1,1] and [2,1,1,1], respectively. Feature vectors are also calculated for three random permutations of the graph. These appear as clusters of permutationally invariant graphs.

generating 1.2×10^6 samples for each. Sampling is repeated for an interferometer set to the identity. The results are shown in Fig. 4, where we plot the full distribution of six-photon output patterns compared to their theoretical predictions based on the detailed model described above. The average total variation distance between experimental and theoretical distributions is 0.09(1).

Vibronic spectra

The vibronic spectrum of a molecule specifies the frequencies and intensities of light absorbed when the molecule undergoes a transition between different vibrational and electronic states. In the photonic algorithm, optical modes represent the vibrational normal modes and the device is programmed in terms of squeezing, displacement and linear interferometers to generate Franck–Condon profiles efficiently[18,40]. We program the chip interferometer according to the Duschinsky matrices that represent mixing between four normal coordinates in ethylene (C_2H_4) and (*E*)-phenylvinylacetylene ($C_{10}H_8$). Displacements are not included and squeezing is only present in the first mode, so the resulting profiles do not correspond to the true vibronic spectra of these molecules. Nevertheless they can be used as proof-of-principle benchmarks with respect to the theoretical model of the device[6]. Results are shown in Fig. 5, obtained by generating 1.2×10^6 samples for each molecule.

Graph similarity

A graph can be encoded in a photonic circuit through a correspondence between the graph's adjacency matrix and the combination of a linear optical interferometer with squeezed light[21]. The statistics of detected photon patterns can be used to estimate orbit probabilities and collect them in *m*-tuples called feature vectors[22,41]. The distance between feature vectors is used to quantify the similarity of the corresponding graphs. We demonstrate this algorithm by encoding bipartite graphs on eight vertices. Four graphs are considered, with their corresponding adjacency matrices shown in the Supplementary Information. Feature vectors are estimated using 20 million samples for each graph. The results are illustrated in Fig. 6, showing that these graphs result in separate feature vectors, which are invariant to mode permutations. To showcase this property, three random permutations were selected and each of the four graphs was permuted accordingly, resulting in clusters of isomorphic graphs. These results are the first demonstration of graph similarity on a quantum device.

Discussion

We have presented a nanophotonic device pioneering several record capabilities: high sampling rates, large on-chip squeezing, nearly ideal second-order correlation statistics, and considerably more detected photons than previously reported in similar devices. The hardware is programmable and can be remotely configured via a custom application programming interface, which enables deployment for cloud access. We have further showcased the capabilities of the nanophotonic chip with example demonstrations.

As the first of its generation, our device constitutes an initial step in scaling nanophotonic chips to a larger number of modes, eventually reaching the regime of quantum advantage. The greatest challenge in scaling is maintaining acceptably low losses. Designs for integrated beamsplitters and phase shifters, requiring more precise (but available) chip fabrication tools, could achieve an order-of-magnitude improvement in the loss per layer. This would enable a 100-mode device to be realized with less than 3 dB of loss in the interferometer. The inclusion of tunable single-mode squeezing[42] and displacement will constitute a substantial upgrade, permitting the generation of arbitrary Gaussian states and unlocking the capability of implementing quantum algorithms. Such scaling and upgrades are natural next steps for near-term photonic quantum information processing demonstrations.

Online content

Any methods, additional references, Nature Research reporting summaries, source data, extended data, supplementary information, acknowledgements, peer review information; details of author contributions and competing interests; and statements of data and code availability are available at https://doi.org/10.1038/s41586-021-03202-1.

1. Wright, K. et al. Benchmarking an 11-qubit quantum computer. *Nat. Commun.* **10**, 5464 (2019).
2. Arute, F. et al. Quantum supremacy using a programmable superconducting processor. *Nature* **574**, 505–510 (2019).
3. Larsen, M. V., Guo, X., Breum, C. R., Neergaard-Nielsen, J. S. & Andersen, U. L. Deterministic generation of a two-dimensional cluster state. *Science* **366**, 369–372 (2019).
4. Asavanant, W. et al. Generation of time-domain-multiplexed two-dimensional cluster state. *Science* **366**, 373–376 (2019).
5. Qiang, X. et al. Large-scale silicon quantum photonics implementing arbitrary two-qubit processing. *Nat. Photon.* **12**, 534–539 (2018).
6. Paesani, S. et al. Generation and sampling of quantum states of light in a silicon chip. *Nat. Phys.* **15**, 925–929 (2019).
7. Zhong, H.-S. et al. Experimental Gaussian boson sampling. *Sci. Bull.* **64**, 511–515 (2019).
8. Bromley, T. R. et al. Applications of near-term photonic quantum computers: Software and algorithms. *Quant. Sci. Technol.* **5**, 034010 (2020).
9. Kielpinski, D., Monroe, C. & Wineland, D. J. Architecture for a large-scale ion-trap quantum computer. *Nature* **417**, 709–711 (2002).
10. Clarke, J. & Wilhelm, F. K. Superconducting quantum bits. *Nature* **453**, 1031–1042 (2008).
11. Wootton, J. R. & Loss, D. Repetition code of 15 qubits. *Phys. Rev. A* **97**, 052313 (2018).
12. Dumitrescu, E. F. et al. Cloud quantum computing of an atomic nucleus. *Phys. Rev. Lett.* **120**, 210501 (2018).
13. Anschuetz, E., Olson, J., Aspuru-Guzik, A. & Cao, Y. Variational quantum factoring. In *Int. Worksh. on Quantum Technology and Optimization Problems* 74–85 (Springer, 2019).
14. Nielsen, M. A. & Chuang, I. *Quantum Computation And Quantum Information* (Cambridge Univ. Press, 2010).
15. Preskill, J. Quantum computing in the NISQ era and beyond. *Quantum* **2**, 79 (2018).
16. Gottesman, D., Kitaev, A. & Preskill, J. Encoding a qubit in an oscillator. *Phys. Rev. A* **64**, 012310 (2001).
17. Flühmann, C. et al. Encoding a qubit in a trapped-ion mechanical oscillator. *Nature* **566**, 513–517 (2019).
18. Huh, J., Guerreschi, G. G., Peropadre, B., McClean, J. R. & Aspuru-Guzik, A. Boson sampling for molecular vibronic spectra. *Nat. Photon.* **9**, 615 (2015).
19. Arrazola, J. M. & Bromley, T. R. Using Gaussian boson sampling to find dense subgraphs. *Phys. Rev. Lett.* **121**, 030503 (2018).

20. Brádler, K., Friedland, S., Izaac, J., Killoran, N. & Su, D. Graph isomorphism and gaussian boson sampling. Preprint at https://arxiv.org/abs/1810.10644 (2018).
21. Brádler, K., Dallaire-Demers, P.-L., Rebentrost, P., Su, D. & Weedbrook, C. Gaussian boson sampling for perfect matchings of arbitrary graphs. *Phys. Rev. A* **98**, 032310 (2018).
22. Schuld, M., Brádler, K., Israel, R., Su, D. & Gupt, B. Measuring the similarity of graphs with a Gaussian boson sampler. *Phys. Rev. A* **101**, 032314 (2020).
23. Banchi, L., Fingerhuth, M., Babej, T., Ing, C. & Arrazola, J. M. Molecular docking with Gaussian boson sampling. *Sci. Adv.* **6**, eaax1950 (2020).
24. Killoran, N. et al. Continuous-variable quantum neural networks. *Phys. Rev. Res.* **1**, 033063 (2019).
25. Arrazola, J. M., Kalajdzievski, T., Weedbrook, C. & Lloyd, S. Quantum algorithm for nonhomogeneous linear partial differential equations. *Phys. Rev. A* **100**, 032306 (2019).
26. Wang, J., Sciarrino, F., Laing, A. & Thompson, M. G. Integrated photonic quantum technologies. *Nat. Photon.* **14**, 273–284 (2019).
27. Rudolph, T. Why I am optimistic about the silicon-photonic route to quantum computing. *APL Photon.* **2**, 030901 (2017).
28. Hamilton, C. S. et al. Gaussian boson sampling. *Phys. Rev. Lett.* **119**, 170501 (2017).
29. Lvovsky, A. Squeezed light. In *Photonics* Vol. 1 *Fundamentals of Photonics and Physics* 121–164 (Wiley, 2015)
30. Vaidya, V. D. et al. Broadband quadrature-squeezed vacuum and nonclassical photon number correlations from a nanophotonic device. *Sci. Adv.* **6**, eaba9186 (2020).
31. Killoran, N. et al. Strawberry Fields: a software platform for photonic quantum computing. *Quantum* **3**, 129 (2019).
32. Rosenberg, D., Lita, A. E., Miller, A. J. & Nam, S. W. Noise-free high-efficiency photon-number-resolving detectors. *Phys. Rev. A* **71**, 061803 (2005).
33. Qi, H., Brod, D. J., Quesada, N. & García-Patrón, R. Regimes of classical simulability for noisy Gaussian boson sampling. *Phys. Rev. Lett.* **124**, 100502 (2020).
34. Aytür, O. & Kumar, P. Pulsed twin beams of light. *Phys. Rev. Lett.* **65**, 1551 (1990).
35. Christ, A., Laiho, K., Eckstein, A., Cassemiro, K. N. & Silberhorn, C. Probing multimode squeezing with correlation functions. *New J. Phys.* **13**, 033027 (2011).
36. Glauber, R. J. Coherent and incoherent states of the radiation field. *Phys. Rev.* **131**, 2766 (1963).
37. Sudarshan, E. Equivalence of semiclassical and quantum mechanical descriptions of statistical light beams. *Phys. Rev. Lett.* **10**, 277 (1963).
38. Burenkov, I. A. et al. Full statistical mode reconstruction of a light field via a photon-number-resolved measurement. *Phys. Rev. A* **95**, 053806 (2017).
39. Aaronson, S. & Arkhipov, A. The computational complexity of linear optics. *Theor. Comput.* **9**, 143–252 (2013).
40. Quesada, N. Franck-Condon factors by counting perfect matchings of graphs with loops. *J. Chem. Phys.* **150**, 164113 (2019).
41. Brádler, K., Israel, R., Schuld, M. & Su, D. A duality at the heart of gaussian boson sampling. Preprint at https://arxiv.org/abs/1910.04022 (2019).
42. Vernon, Z. et al. Scalable squeezed-light source for continuous-variable quantum sampling. *Phys. Rev. Appl.* **12**, 064024 (2019).

Methods

Programming a nanophotonic chip

The device can be programmed remotely using the Strawberry Fields Python library[31]. A user with valid credentials can specify the settings of the device using a few lines of code and subsequently request samples. The example Python code shown in the Supplementary Information, from version 0.14.0 of Strawberry Fields, shows a typical workflow where 4×10^5 samples are requested from a device. All squeezers are turned on and the interferometer is programmed according to a unitary transformation drawn randomly from the Haar measure.

Apparatus details

As described in the main text and in Fig. 1, the full apparatus consists of:

- A custom modulated pump laser source producing a regular pulse train (100 kHz repetition rate) of 1.5-ns-duration rectangular pulses,
- An electrically and optically packaged chip that synthesizes a programmable eight-mode Gaussian state with temporal-mode characteristics appropriate for photon-number resolving readout,
- A locking system which serves to align and stabilize the resonance wavelengths of the on-chip squeezer resonators,
- An array of DACs for programming phase shifter voltages on the chip,
- An array of low-loss (off-chip) wavelength filters to suppress unwanted light, passing only wavelengths close to the signal and idler for detection,
- A detection system, which consists of an array of eight transition-edge sensor detectors for photon-number-resolving readout, and the auxiliary equipment, including an adiabatic demagnetization refrigerator, required to operate and acquire data from them, and
- A master controller consisting of a conventional server computer running custom software to coordinate the continuous and automated operation of all subsystems, and receive and process jobs sent to the machine.

In the following sections we provide more detail on these subsystems and the techniques used to characterize them.

Pump system

The pump laser is a compact continuous-wave tunable laser assembly, tuned to a wavelength of 1,554.9 nm. The laser is connected to a 10-GHz-bandwidth fibre-integrated intensity modulator which is used to define a regular train of 1.5-ns-wide optical pulses with a 100 kHz repetition rate. The output of the modulator is coupled to a 99/1 fibre splitter, with the 1% tap directed to a photodiode used to lock the modulator bias voltage. Bias voltage locking in continuous operation is performed by a modular field programmable gate array (FPGA)/DAC board. The other 99% is directed to a fibre polarizer, before being sent to an erbium doped fibre amplifier (EDFA). After the EDFA, the pump is spectrally filtered using low-loss fibre bandpass filters and directed to the chip subsystem. All of the components of the pump are controlled remotely and do not require human intervention for operation.

Integrated components

The chip layout is illustrated in Fig. 1b. Pump light is edge-coupled from fibre to the chip through a single waveguide input. This waveguide enters a binary tree of 50/50 beam splitters based on multimode interferometer (MMI) devices, which distributes the pump light equally among four spatial modes. Each of these four waveguides is coupled to a separate squeezer. The chip was fabricated using a photolithographic process on a dedicated wafer run through a commercial service offered by Ligentec SA.

The squeezers are based on a microring resonator design that uses strongly pumped spontaneous four-wave mixing to generate bichromatic two-mode squeezing. This design is described in full detail by ref. [30]; here we summarize the operation and details specific to the squeezers on the eight-mode chip. The waveguide cross-section of the rings is 1,500 nm × 800 nm, and their radius is chosen to be 113 μm, corresponding to a free spectral range of 200 GHz. The loaded quality factors of the resonances used were approximately 7×10^5, corresponding to a full-width at half-maximum linewidth of 275 MHz, and varying less than 5% across all four rings. The escape efficiencies for these resonances are approximately 75%, that is, the probability of a photon generated in a ring being lost before it can be collected by the bus waveguide is approximately 25%. This makes up 1.2 dB of the loss within the overall 8 dB system efficiency.

To produce single-temporal-mode squeezed light, it is sufficient to employ pump pulses with duration comparable to the resonator dwelling time; the exact pulse shape is unimportant. In our case, 1.5-ns square pulses yielded nearly single-temporal-mode operation, as quantified by the second-order correlation data exhibited in Fig. 2c. Shorter pulses can be used, but they do not appreciably improve the temporal-mode structure, and they compromise the generation efficiency as the pulse bandwidth exceeds the resonator linewidth. The exact pulse energy used is difficult to measure precisely, owing to the extremely low duty cycle of the pulse train, but we estimate this quantity to be of the order of 0.5 nJ. This was chosen to yield a mean photon number of about one per mode at the sources, and could be increased by using more pump power or designing better resonators with higher escape efficiencies and quality factors. This value of 8 dB for effective input squeezing cannot easily be directly measured, but serves as a guideline for theoretical modelling of our device.

No excess noise from unwanted processes occurring within the ring was measured. As discussed below, the dominant source of photon noise in the squeezing band is from Raman scattering in the fibre components carrying pump power to the chip. This can be managed in future versions by better pump filtering before the squeezers.

Each resonator output mode is directed to a separate asymmetric Mach–Zehnder interferometer (AMZI) device, which acts as a pump rejection filter. This ensures that very little nonlinear light generation occurs in the interferometer portion of the chip, and also allows the rejected pump to be collected and used as a signal for locking the ring resonances to the pump laser wavelength. The bright outputs of the AMZI filters are directed back to the input facet and coupled out of the chip for detection. The free spectral ranges of the AMZIs and rings are carefully matched to be compatible with the standard telecom dense wavelength division multiplexing spacing of 100 GHz, and to allow the signal and idler to pass to the interferometer when the AMZI is tuned to reject the pump. The signal and idler resonances are each separated in frequency from the pump by three ring free spectral ranges (approximately 600 GHz).

The interferometer is composed of a network of MMIs and phase shifters in a rectangular configuration[43]. The user must specify twelve independent real parameters to program this transformation, with the remaining three free parameters of the SU(4) transformation corresponding to irrelevant output phases. This transformation implements the gate sequence on both four-mode subspaces distinguished by their optical wavelength. This configuration contains a sequence of six SU(2) transformations that enable arbitrary programmability of the interferometer by controlling the thermo-optic phase shifters integrated within the chip. The splitting ratio of the MMIs is constant to within 1% over the range of wavelengths used. This control is accomplished using a multi-channel DAC system. Light is coupled out of the chip via edge couplers to a fibre array, and then directed to a fibre-based low-loss filter stack that separates the signal and idler photons and directs them to separate photon-number-resolving detectors. The total pump rejection ratio is well in excess of 100 dB. In addition, the filter stack rejects photons from unwanted resonator modes, and any residual pump light and broadband generated photons from in-fibre Raman scattering. The total remaining number of noise photons per pulse from all sources (pump leakage and Raman scattering) incident

on the transition-edge sensor detectors is approximately 0.02 or lower for each channel. Overall, about 5% of the photons detected in our experiments arise from noise photons generated by Raman scattering in fibre components before the chip, and 10% from unwanted temporal modes populated by the squeezers. These figures can be improved by implementing better wavelength filtering on the pump input to the chip to eliminate noise, and by engineering the squeezers to permit more broadband pump pulses to be used. The residual pump light rejected by the filter stack is directed to a photodiode array, and was used for the calibration of the interferometer. The filter stack comprises approximately 2 dB of the overall 8 dB of loss in the system.

The chip is both electrically and optically packaged to ensure stable operation. The chip is glued to a copper sub-mount using a thermally conductive die adhesive. The submount is mounted on top of a thermo-electric cooler used to actively stabilize the temperature of the chip. Connectorized printed circuit boards are affixed to the sub-mount and the chip is wirebonded to these boards. Cables carry the electronic signals responsible for programming the unitary transformation and locking the rings to a secondary printed circuit board that interfaces with custom control circuitry and the interferometer DAC. V-groove arrays of ultrahigh numerical aperture (UHNA7) fibre are aligned to each edge facet of the chip using loop-back waveguide structures placed on the chip. These fibre arrays are fixed in place using an optical adhesive, resulting in an average coupling efficiency of approximately 70%.

Operating procedure

Quantum programs are written by users with the Strawberry Fields Python library[31]. These programs are sent to the master controller as 'jobs', that is, scripts specifying squeezing parameters and interferometer phases. Upon receipt of a job, the information is compiled into a set of hardware instructions. The control system then implements the following control sequence:

- Voltages of the interferometer that correspond to the requested unitary operation are set,
- The chip is allowed to equilibrate thermally,
- The ring resonance wavelengths are swept to calibrate the squeezer control circuitry, followed by locking of the rings to the pump wavelength,
- Checks are performed to ensure that the interferometer and squeezers are in the desired state,
- The requested number of samples are acquired from the detectors,
- Checks are performed to ensure the interferometer and squeezers are still in their desired state, that is, that the chip has not drifted out of the specified state during data acquisition,
- The sample and job data are returned to the user, and finally
- The chip is re-initialized to its default state.

Chip calibration

To set the interferometer to a user-specified state, the on-chip thermo-optic phase shifters must first be calibrated to determine the voltage-to-phase relationship for each phase shifter. The thermal nature of the phase shifter implies (and tests confirm) that to a high degree of accuracy, the relationship between phase and voltage can be described by

$$\phi = \phi_0 + \alpha V^2. \tag{2}$$

The goal of the calibration process is to determine ϕ_0 and α. Then, when a specific phase is requested, the phase-to-voltage can be inverted to produce the required voltage. The calibration is accomplished by injecting classical light into a single mode of the interferometer at a time by injecting pump light into the second input of the filter AMZI for that mode. A standard telecom fibre switch enables control of which mode the calibration light is injected into. The transmission of the interferometer is detected using classical light detectors connected to the pump rejection channel of the output filter stack. Employing optimization algorithms, it is possible to learn the voltage-to-phase relationship for each thermo-optic phase shifter in sequence.

It is challenging, however, to learn the input phases of the interferometer using classical light, since these phases will depend on properties of the squeezers themselves. Instead, to calibrate these three relevant phases, two-squeezer interference is used. Each pair of neighbouring squeezers is locked to the pump laser, and the input phase shifters in modes 0, 1 and 2 are swept. Mode 3 has no input phase shifter because only the relative phase between the inputs is physically relevant. The NRF is monitored between the pair of interfering modes and the relevant phase-to-voltage relationship is extracted.

Photon detection system

Each of our transition-edge-sensor-based detectors has quantum efficiency above 95% and produces an analogue voltage pulse every 10 μs, synchronized with the incident optical pulse train, with a shape that depends on the number of incident photons. These voltage signals are digitized by analogue-to-digital converters, resulting in time series referred to here as voltage traces. Thus, determining photon numbers amounts to being able to associate a photon number n to each trace. This is typically accomplished for sets of a few hundred thousand traces, by first ordering them according to a feature such as their maximum or their overlap with some reference trace. Reasonable points are then determined, in terms of this feature, by which to organize the traces into photon-number bins[44,45]. In previous work on measuring photon-number difference squeezing from nanophotonic sources[30], a principal component analysis was performed on sets of 8×10^5 traces. These traces were then ordered with respect to their overlap with their first principal component, and a sum of Gaussians fitted to the resulting histogram, solving for the points of intersection between adjacent Gaussians to determine photon-number bin edges.

That approach suffers from two drawbacks, which make it less appropriate for a more complex system like the one described in this work. The first is that it relies on a global comparison of each trace to the full set of traces acquired during the corresponding experimental run, and so cannot associate a photon number with a single trace in real time after it is generated given that the principal component analysis depends on all traces in the dataset. This limits the speed of the trace-to-photon number discrimination in our system. Second, and of more concern, the maximum assignable photon number $n_{\max}$—that is, the n value at which actual $(n + m)$-photon events (with $m > 0$) will be identified as n-photon events—could be different for each dataset, because each dataset may identify a different number of photon-number bins. Both of these drawbacks were eliminated in our system.

Before activating the full system, we first calibrate each detector, allowing each subsequent voltage trace to immediately be assigned, in real time, to a photon number up to the $n_{\max}$ determined by the calibration. This calibration involves two steps: (1) identification of a standard trace for calculating overlaps, and (2) determination of photon-number bin edges associated with the standard trace. Each calibration uses a set of 10^7 voltage traces. To obtain a standard trace, we perform principal component analysis and histogram fitting to identify all of the two-photon traces in the set, and calculate the resulting average trace. We use the set of two-photon traces as opposed to one-, three- or four- photon traces in an effort to balance the tradeoff between capturing some detector nonlinearity and having enough events to obtain a representative average trace. Using sets of higher-photon-number traces in principle allows us to extend $n_{\max}$. However, as we calibrate using one arm of a two-mode squeezed vacuum state we always expect to have more n- than $(n + 1)$-photon traces. Next, we calculate the overlap of each trace in the full set of 10^7 traces with the standard trace, generate a histogram, fit to it a sum of Gaussians, and determine photon-number bin edges. The resultant $n_{\max}$ for each of our eight detectors ranges between five and seven.

NRF

To assess the degree of photon number correlations between the signal and idler for each individual squeezer, the NRF was measured. For a single two-mode squeezed vacuum source, we define this as

$$\mathrm{NRF} = \frac{\Delta^2(n_\mathrm{s} - n_\mathrm{i})}{\langle n_\mathrm{s} + n_\mathrm{i}\rangle}, \tag{3}$$

where n_s and n_i are the photon number observables for the signal and idler, respectively, and $\Delta^2(n_\mathrm{s} - n_\mathrm{i})$ refers to the variance of the photon number difference. An ideal measurement of a perfect source would yield NRF = 0, since the photon number of the signal and idler are perfectly correlated for a two-mode squeezed vacuum state. On the other hand, a pair of coherent states would yield NRF = 1. In our system, the dominant imperfection that degrades the correlation is loss: a total photon transmission efficiency of η yields an NRF of

$$\mathrm{NRF} = 1 - \eta \tag{4}$$

for two-mode squeezed vacuum[30].

The NRF values reported in Fig. 2b were obtained by setting the interferometer to the identity transformation, activating only one squeezer at a time, and collecting 8×10^5 samples. These samples were divided into eight batches of 1×10^5, and the NRF was calculated for each batch. The mean and standard deviation of these eight NRF values correspond respectively to the data points and uncertainties ($\pm 1\sigma$) reported.

Second-order correlation

For faithful execution of quantum circuits according to the idealized functionality illustrated in Fig. 1a, it is important that no additional co-propagating modes are substantially populated with photons apart from those that carry the desired Gaussian state; because the photon detectors cannot distinguish between overlapping temporal modes, they would show up as an effective noise contribution to the collected samples. It is therefore vital to assess the temporal-mode structure of the individual squeezer outputs: the squeezed states should as closely as possible populate only a single temporal mode.

To verify that each squeezer is substantially populating only one temporal mode, the unheralded second-order correlation statistic $g^{(2)}$ was measured for the signal and idler of each squeezer[30]. For any output channel of the device described by photon number operator n, this statistic is defined as

$$g^{(2)} = \frac{\langle n^2\rangle - \langle n\rangle}{\langle n\rangle^2}. \tag{5}$$

This statistic provides a loss-insensitive measure of the temporal-mode structure of a two-mode squeezed vacuum source. In the absence of noise, the Schmidt number K is related to $g^{(2)}$ via[35]

$$g^{(2)} = 1 + \frac{1}{K}. \tag{6}$$

An ideal single-temporal-mode two-mode squeezed vacuum source would yield $g^{(2)} = 2$ for the signal and idler, whereas coherent states or highly multi-mode squeezed light would yield $g^{(2)} = 1$.

The $g^{(2)}$ values reported in Fig. 2c were obtained, like the NRF values, by setting the interferometer to the identity transformation, activating only one squeezer at a time, and collecting 8×10^5 samples. These samples were divided into eight batches of 1×10^5, and the $g^{(2)}$ was calculated for each batch. The mean and standard deviation of these eight $g^{(2)}$ values correspond respectively to the data points and uncertainties ($\pm 1\sigma$) reported. The values reported are raw and uncorrected for noise, which tends to lower the measured $g^{(2)}$ towards unity. Noise from unwanted Raman scattering is the dominant factor affecting the measured $g^{(2)}$ in our system, and therefore the values reported are in fact lower bounds for this quantity.

Two-squeezer interference

Here we provide a simple model to explain the behaviour of the NRF as a function of the phases of the interferometer used in our chip. We consider two identical squeezing sources, labelled 1 and 2, that each produce photons in their idler arms a_1, a_2 and in their signal arms b_1 and b_2. We write the NRF between an arbitrary pair of modes c, d as

$$\begin{aligned}\mathrm{NRF}_{cd} &= \frac{\Delta^2(n_c - n_d)}{\langle n_c + n_d\rangle} \\ &= \frac{\Delta^2 n_c + \Delta^2 n_d - 2(\langle n_c n_d\rangle - \langle n_c\rangle\langle n_d\rangle)}{\langle n_c + n_d\rangle}.\end{aligned} \tag{7}$$

Since we are considering Gaussian states (two-mode squeezed states with squeezing parameter r) undergoing Gaussian operations (a beam splitter with unitary matrix U and loss quantified by transmission efficiency η), and assuming the losses to be homogeneous and the squeezing identical in both sources, it can be shown that the variance and mean photon number of all the modes are the same and given by

$$\Delta^2 n = \bar{n}(\bar{n} + 1),\ \langle n\rangle = \bar{n} = \eta \sinh^2 r. \tag{8}$$

Now we need to evaluate only

$$\langle n_c n_d\rangle = \langle c^\dagger c d^\dagger d\rangle = \langle c^\dagger c\rangle\langle d^\dagger d\rangle + \langle c^\dagger d^\dagger\rangle\langle cd\rangle, \tag{9}$$

where Wick's theorem[46] was used to write the fourth-order expectation values in terms of second-order ones. For our system, the same interferometer acts on both the signal modes and the idler modes (as in Fig. 1a), and that interferometer transformation can be expressed according to $a_i \to \sum_j U_{ji} a_j$. With this, we find that

$$\begin{aligned}\mathrm{NRF}_{a_1,b_1} = \mathrm{NRF}_{a_2,b_2} &= 1 - \eta + (\eta + n)\sin^2\theta \sin^2\phi, \\ \mathrm{NRF}_{a_1,b_2} = \mathrm{NRF}_{a_2,b_1} &= 1 + n - (\eta + n)\sin^2\theta \sin^2\phi,\end{aligned} \tag{10}$$

where we parameterized the interferometer in terms of the unitary matrix

$$U = \begin{pmatrix} \cos(\theta/2) & e^{i\phi}\sin(\theta/2) \\ -e^{-i\phi}\sin(\theta/2) & \cos(\theta/2) \end{pmatrix}. \tag{11}$$

The data exhibited in each panel of Fig. 2e were obtained as follows: the corresponding pair (k, l) of squeezers were activated, with the others turned off. The unitary transformation U was set to interfere the two squeezers with $\theta = \pi/2$, corresponding to an effective 50/50 beam splitter with relative input phase ϕ. A batch of 4×10^5 photon number samples was then acquired for each of 40 different settings of ϕ between 0 and 2π. The four NRF combinations (signal 1 – idler 1, signal 2 – idler 2, signal 1 – idler 2, signal 2 – idler 1) were then computed from these samples, and the results plotted alongside least-squares fits to the model of equation (10) (with a free offset phase included to account for calibration offsets in ϕ).

The interference can be quantified by the amplitude of the oscillations in these traces. The NRFs between modes from separate squeezers, made to interfere according to the circuit of Fig. 2d, obey an oscillatory dependence on the relative phase ϕ, with an amplitude proportional to the sum of the mean photon number (after losses) and total system transmissivity. The amplitudes extracted from the fits in Fig. 2e are consistent to within 40% of the independently estimated values for these quantities; imperfections apart from loss, including

squeezer distinguishability, need to be accounted for in the model to obtain better agreement. In future, more general modelling of the device can be used to extract an estimate for the overlap between the temporal modes populated by different squeezers, informing the path to optimizing two-source interference of these devices.

We note that if the sources were completely distinguishable, that is, if the temporal modes populated by different squeezers were very different, then the visibility of the interference would be zero: interferometer would not be able to interfere the modes and there would be no oscillating phase dependence with amplitude $n + \eta$ in equation (10). The extracted fit parameters for the curves, averaged over all traces, are $n = 0.18(4)$ and $\eta = 0.11(1)$. The extracted transmission efficiency is consistent with independent estimates, whereas the extracted mean photon number is about 40% smaller than independent estimates. The interference visibility is thus measurably affected by imperfections other than loss, including unitary transformation infidelity (the effective 50/50 beam splitter has approximately 18 dB extinction), noise, temporal multi-modedness, and potentially some squeezer distinguishability.

Scalability

An important factor in assessing the viability of the platform presented is the scalability of this approach. What improvements to the platform and design are required in order to scale the system size to a level where quantum advantage could potentially be achieved? To answer this, we fix a target of 100 modes, which in our architecture would require: 50 squeezers operating with squeezing factors of $r \approx 1$, a universal 50-spatial-mode interferometer, and 100 photon-number-resolving detector channels. We also stipulate, as a rough estimate, that such a machine should incur no more than 3 dB of loss in the interferometer; this criterion is especially demanding, since the interferometer loss scales with the number of modes. Events with hundreds of photons would be detectable with such a machine.

At present, the total system loss is approximately 8 dB, of which about 3 dB is incurred in the four-spatial-mode interferometer. This is dominated by losses in the MMI-based beam splitters (0.2 to 0.4 dB per layer) and in the bent segments of the waveguide coils used in the interferometer phase shifters (0.35 to 0.55 dB per layer). MMIs are employed for their fabrication tolerance, as they reliably achieve close to 50:50 splitting ratio across large chip areas even with imperfect lithography and wafer uniformity. The waveguide coils are designed to achieve a longer phase shifter propagation length, increasing thermal efficiency. For both of these components, the dominant source of loss is not directly related to the fundamental straight-waveguide propagation loss of 0.2 dB cm^{-1} associated with their lengths.

Optimization of the design and fabrication process can greatly reduce these losses. By moving to a fabrication line offering more precise lithography, less fabrication-tolerant directional couplers can replace MMIs as the beam splitting element. These can achieve length-limited loss, contributing approximately 200 μm of length per layer, which would correspond to about 0.008 dB of loss per layer. Upgrading the microheaters used in the phase shifters to a more specialized material can lower the required number of bends and shorten the propagation length of the two waveguide coils to 3 mm per layer, contributing 0.06 dB per layer. These coils can also achieve length-limited performance by designing more adiabatic transitions between straight and bent segments. Combined, these changes would yield an interferometer loss of approximately 0.068 dB per layer. For a 50-spatial-mode interferometer, this would result in a total of 3.4 dB of loss. A modest improvement in waveguide propagation loss to 0.17 dB cm^{-1} would then suppress interferometer losses to below 3 dB. Considering silicon nitride waveguides have been demonstrated in a similar platform with losses as low as 0.055 dB cm^{-1} (ref. [47]), we believe this is a demanding but realistic pathway to controlling losses as the system size scales.

Other challenges associated with scaling the interferometer arise from the power dissipated by the thermo-optic phase shifters. Currently, the interferometer in our device dissipates approximately 1 W of power for a typical unitary setting, in a chip area of 0.4 cm^2. A 50-spatial-mode interferometer would require 2,450 phase shifters, dissipating a total of about 120 W across a chip area of about 21 cm^2 (corresponding to three reticle write-fields of a standard lithography tool), when each is tuned to achieve a π phase shift. The thermal load density (power dissipated per unit chip area) would therefore approximately double, despite the number of phase shifters increasing by two orders of magnitude. For comparison, a modern microprocessor dissipates between 100 W and 200 W under full load in a die area of about 1 cm^2. With proper thermal management, we do not anticipate power dissipation posing a barrier to scaling.

Model parameters

A theoretical model of the chip distribution is used for benchmarking purposes in the experimental demonstrations. To estimate the model parameters quoted in the tables below, we construct a two-dimensional photon-number histogram for each signal and idler mode in a two-mode squeezed vacuum state generated by a single squeezer, keeping all other squeezers off. We model this data as a pair of two-mode squeezed vacua (two Schmidt modes each with squeezing parameter r_i) hitting the detectors after undergoing loss (with transmissivity η). The squeezing parameter is related to the two-mode squeezing operator by $S_2(r) = \exp[r(a^\dagger b^\dagger - ab)]$. To represent noise in the detectors, we add an extra model with Poisson statistics (mean value $\bar{n}$) that accounts for the measured counts when all the squeezers are off. With these physical parameters it is possible to calculate a two-dimensional histogram using the methods from ref. [38]. After this we simply use the well known Levenberg–Marquardt algorithm to solve the inverse problem and retrieve the physical parameters from the measured photon number histograms. It is important to note that these parameters are not the directly measured values of squeezing and losses; they are the values that best approximate the behaviour of the chip given the simplified model we consider. All parameter values are reported in the Supplementary Information.

Sampling from non-classical light

A non-classicality test for photonic devices has been formulated by ref. [33]. The results there presented are valid for a simple noise model that includes uniform single Schmidt mode squeezers, uniform loss and threshold detectors with dark counts. Therefore, we also consider a model with a single Schmidt mode and coarse-grain the output distribution as if obtained with threshold detectors. We furthermore generalize the formula in ref. [33] to include non-uniform squeezing and losses. Numerically, we find a modelling error of $d_0 = 0.10(1)$ averaged over 15 random unitary transformations and calculations are made by considering a cutoff of 14 photons per mode. Since the coarse-graining procedure can only decrease the total variation distance, we can use the value of d_0 quoted above.

We briefly present the derivation of equation (1), which generalizes the results of ref. [33]. Assuming the aforementioned noise model, the output quantum state of the device is given by $\rho = U\left(\prod_{i=1}^{M} \sigma_i\right)U^\dagger$, where $\sigma_i = L_{\eta_i}(|r_i\rangle\langle r_i|)$ are the lossy squeezed states in each mode. In ref. [48], the authors studied the problem of exact sampling from an M-mode quantum state of the form $\tilde{\rho} = U\left(\prod_{i=1}^{M} \tau_i\right)U^\dagger$, where τ_i is an arbitrary (t_i)-classical Gaussian state, that is, a state with positive s_i-ordered phase-space quasiprobability distribution[48]. We denote the distribution obtained by sampling from this classical state by $\tilde{P}$, which is calculated using The Walrus[49]. It can be shown that sampling from $\tilde{\rho}$ by using noisy threshold detector with excess photon rate p_i^{D} can be simulated exactly in classical polynomial time if $t_i > 1 - 2p_i^{\mathrm{D}}$ (ref. [48]).

Therefore, when the mixed input state σ_i is close to some classical Gaussian state τ_i, the corresponding noisy GBS experiment can be efficiently simulated with small error. Since any such state τ_i leads to an efficient classical simulation, it is necessary to minimize the distance

to σ_i over all possible choices of τ_i. This intuition is made precise in ref. [33]. Following a similar procedure, it is straightforward to derive that we have $\delta(P, \bar{P}) < \varepsilon$ whenever $\sum_{i=1}^{K} - \ln(F(\sigma_i, \tau_i)) \leq \varepsilon^2/4$. Here $F(\sigma, \tau)$ is the quantum fidelity between σ and τ. From ref. [33], the maximal fidelity optimized over all possible τ_i is given by $\operatorname{sech}\left[-\frac{1}{2}\ln\left(\frac{1-2p_i^{\mathrm{p}}}{\eta_i e^{2r_1}+1-\eta_i}\right)\right]$. By setting $x_i = \frac{\eta_i e^{-2r_i}+1-\eta_i}{1-2p_i^{\mathrm{p}}}$, we obtain the sufficient condition of the efficient simulation of noisy GBS given in equation (1).

GBS

It has been shown[28] that for a Gaussian state prepared using only squeezing followed by linear interferometry, the probability $\Pr(S)$ of observing an output $S = (s_1, s_2, \ldots, s_m)$, where s_i denotes the number of photons detected in the ith mode, is given by

$$\Pr(S) = \frac{1}{\sqrt{\det(Q)}} \frac{\mathrm{Haf}(\mathcal{A}_S)}{s_1!\, s_2! \cdots s_m!}, \tag{12}$$

where $Q := \Sigma + 1/2$, $\mathcal{A} := X(\mathbb{1} - Q^{-1})$, $X := \begin{bmatrix} 0 & \mathbb{1} \\ \mathbb{1} & 0 \end{bmatrix}$, and Σ is the covariance matrix of the state in the creation/annihilation operator basis. The submatrix $\mathcal{A}_S$ is specified by the output pattern (sample) S of detected photons: if $s_i = 0$, the rows and columns i and $i + m$ are deleted from $\mathcal{A}$ and, if $s_i > 0$, the corresponding rows and columns are repeated s_i times. When the Gaussian state is pure, the matrix $\mathcal{A}$ can be written as $\mathcal{A} = A \oplus A^*$, with A an $m \times m$ symmetric matrix. In this case, the output probability distribution is given by

$$\Pr(S) = \frac{1}{\sqrt{\det(Q)}} \frac{|\mathrm{Haf}(A_S)|^2}{s_1!\, s_2! \cdots s_m!}, \tag{13}$$

where the submatrix is defined with respect to rows and columns i, not $(i, i + m)$. The matrix function $\mathrm{Haf}(\cdot)$ is the Hafnian[50], defined as

$$\mathrm{Haf}(\mathcal{A}) = \sum_{\pi \in \mathrm{PMP}} \prod_{(i,j)\in\pi} \mathcal{A}_{ij}, \tag{14}$$

where $\mathcal{A}_{ij}$ are the entries of $\mathcal{A}$ and PMP is the set of perfect matching permutations. Computing the Hafnian is a #P-hard problem, a fact that has been leveraged to argue that, unless the polynomial hierarchy collapses to third level, it is not possible to efficiently simulate GBS using classical computers[28,39]. These complexity proofs are valid when the squeezing levels are equal in all modes and the interferometer unitary transformation is chosen randomly from the Haar measure.

In the architecture of our device, a Gaussian state is prepared using two-mode squeezing operations and an interferometer U acts equally on both halves of the modes. This is similar to the scattershot boson sampling proposal of ref. [51], with a notable difference: both pairs of modes are affected by the interferometer and no post-selection is necessary. The GBS distribution is also given by equation (14), but in this case the A matrix satisfies

$$A = \begin{pmatrix} 0 & C \\ C^{\mathrm{T}} & 0 \end{pmatrix}, \tag{15}$$

$$C = U\, \mathrm{diag}(\tanh r_i) U^{\mathrm{T}}, \tag{16}$$

where r_i is the squeezing parameter on the ith pair of modes. The resulting distribution can be expressed directly in terms of the matrix C. Using the identity

$$\mathrm{Haf}\left[\begin{pmatrix} 0 & C \\ C^{\mathrm{T}} & 0 \end{pmatrix}\right] = \mathrm{Per}[C], \tag{17}$$

we can express the GBS distribution as:

$$\Pr(S) = \frac{1}{\sqrt{\det(Q)}} \frac{|\mathrm{Per}(C_{s,t})|^2}{s_1! \cdots s_m!\, t_1! \cdots t_m!}, \tag{18}$$

where Per denotes the permanent of a matrix and where we use $S = (s;t) = (s_1, \ldots, s_m; t_1, \ldots, t_m)$ to denote a sample across $2m$ modes. The notation $C_{s,t}$ corresponds to a submatrix obtained as follows: if $s_i = 0$, the ith row of C is removed. If $s_i > 0$, it is instead repeated s_i times. Similarly, if $t_i = 0$, the ith column of C is removed and if $t_i > 0$, it is repeated t_i times. This architecture can be interpreted as a combination of boson sampling and GBS: the number of photons is not fixed and probabilities are given by permanents, but of a symmetric matrix C. This suggests that hardness proofs for boson sampling may be readily ported to this setting.

These hardness proofs show that ideal boson sampling cannot be efficiently simulated classically, even approximately, unless the polynomial hierarchy collapses, modulo the validity of two well established conjectures[39]. Because these proofs apply to approximate classical sampling, they imply that imperfect GBS is also hard to simulate classically, provided the imperfections are sufficiently small. This raises the question of how much loss can be tolerated to ensure hardness.

Ideally, a sufficient condition would be formulated. This remains a challenge. Several studies have been performed providing necessary conditions for hardness, for example ref. [52]. in the context of boson sampling. For GBS, ref. [33] provides the condition that is used in this work as a benchmark of non-classicality. These studies place stringent restrictions on the amount of tolerable loss, which set a bar for experiments. Conversely, any experiment that is able to satisfy all known necessary conditions while also outperforming the best known classical simulation algorithms will provide strong evidence for having achieved a quantum advantage. It is possible this will require detection of 100 photons in 100 modes.

In the demonstration described in the main text, three unitary transformations were generated and implemented in the device, which are reported in the Supplementary Information.

Vibronic spectra

According to the Franck–Condon approximation[53], the probability of a given vibronic transition is given by the Franck–Condon factor, defined as

$$F(m) = |\langle m|\hat{U}_{\mathrm{Dok}}|\mathbf{0}\rangle|^2, \tag{19}$$

where $\hat{U}_{\mathrm{Dok}}$ is the Doktorov operator, $|\mathbf{0}\rangle$ is the vacuum state of all modes in the initial electronic state, and $|m\rangle = |m_1, m_2, \ldots, m_M\rangle$ is the state with m_i phonons in the ith vibrational mode of the excited electronic state. The Franck–Condon profile FCP_T determines the probability of generating a transition at a given vibrational frequency ω_{vib}. For finite-temperature vibronic transitions it is defined as

$$\mathrm{FCP}_T(\omega_{\mathrm{vib}}) = \sum_{n,m} P_{T(n)} |\langle m|\hat{U}_{\mathrm{Dok}}|n\rangle|^2 \delta(\omega_{\mathrm{vib}} - \Delta\omega), \tag{20}$$

$$\Delta\omega := \sum_{k=1}^{M} \omega'_k m_k + \sum_{k=1}^{M} \omega_k n_k, \tag{21}$$

where $|n\rangle$ is the vibrational Fock state of the electronic ground state, $P_{T(n)}$ is its initial thermal distribution at temperature T, ω_k is the frequency of the kth vibrational mode of the initial electronic state, and ω'_k is the frequency of the kth vibrational mode of the final electronic state.

A photonic algorithm for computing Franck–Condon profiles was introduced by ref. [18]. The main insight of this algorithm is that a quantum device can be programmed to sample from a distribution that naturally assigns high probability to outputs with large Franck–Condon factors,

without actually having to compute these factors. Sampling from the distribution can then be used to generate outputs with large Franck–Condon factors, which show up as peaks in the spectra.

In the algorithm, optical photons correspond to vibrational phonons, and the Doktorov operator can be decomposed in terms of multi-mode displacement, squeezing and linear interferometer operations, each determined by the transformation between the normal coordinates of the initial and final electronic states. In particular, the interferometer is configured as follows. The diagonal matrices Ω and Ω' are constructed respectively from the ground and excited electronic state frequencies:

$$\Omega = \mathrm{diag}(\sqrt{\omega_1}, \ldots, \sqrt{\omega_k}), \tag{22}$$

$$\Omega' = \mathrm{diag}(\sqrt{\omega_1'}, \ldots, \sqrt{\omega_k'}). \tag{23}$$

The Duschinsky matrix U_D is obtained from the normal mode coordinates of the ground and excited electronic states, q and q' respectively, as $q' = U_D q + d$, where d is a displacement vector related to the structural changes of the molecule upon vibronic excitation. From the matrix $J = \Omega' U_D \Omega^{-1}$, a singular value decomposition is performed: $J = U_L \Sigma U_R$, where U_L and U_R are the left and right unitary matrices. For the specific case of zero-temperature vibronic spectra, it is sufficient to set the interferometer according to the unitary transformation U_R. This is done in the experiments reported in the main text.

When sampling from the resulting distribution, each output photon pattern (n,m) is assigned a frequency

$$\omega(n,m) = \sum_{k=1}^{M} \omega_k' m_k - \sum_{k=1}^{M} \omega_k n_k, \tag{24}$$

and the collection of output frequencies is used to create a histogram that represents the Franck–Condon profile.

There is no known efficient classical algorithm for computing molecular vibronic spectra. Methods for computing approximate spectra exist, but these can still be challenging to employ for large molecules. Therefore, the quantum algorithm tackles a problem that is known to be hard, but it faces the challenge of providing better approximations than classical methods, even in the presence of imperfections. Additionally, the algorithm requires tunable squeezing and displacements, which are additional technological challenges in the construction of photonic devices. There is optimism that a quantum advantage can be obtained for this problem, for example as expressed in ref. [54], but more work remains to further support this.

In the proof-of-principle demonstration, a single mode is squeezed and there are no displacements. The interferometer is configured as described above according to the Duschinksy rotations U_D and normal-mode frequencies of two molecules: ethylene (C_2H_4) (ref. [55]) and (*E*)-phenylvinylacetylene ($C_{10}H_8$) (ref. [56]). This chemical information is reported in the Supplementary Information.

Graph similarity

An undirected weighted graph G can be represented in terms of its symmetric adjacency matrix A. The entries $A_{ij} = A_{ji}$ denote the weight of the edge connecting nodes i and j. Symmetric matrices can be encoded in a GBS distribution following equation (13). For the nanophotonic chip implementing the class of quantum circuits illustrated in Fig. 1a, it is possible to encode bipartite graphs on eight vertices that are compatible with the architecture of the device. For a given bipartite graph with adjacency matrix A, the circuit is constructed by finding the eigendecomposition of A: the eigenvectors determine the unitary transformation of the linear interferometer and the eigenvalues are used to set the squeezing parameters[8].

Once the graph is encoded in the device, feature vectors are constructed by estimating orbit probabilities. An orbit is a set of click patterns that are equivalent under permutation. It can be represented as a sorting of a pattern in non-increasing order with the trailing zeros removed. For example, a click pattern $S = (1, 0, 0, 0, 2, 0, 1, 0)$ belongs to the orbit [2,1,1]. Similarly, the orbit [2,1,1] consists of all patterns with four photons where two photons are detected in only one mode, and a single photon is observed in exactly two modes. For a given orbit O_n, the probability of observing a sample belonging to the orbit is given by

$$p(O_n) = \sum_{S \in O_n} \Pr(S). \tag{25}$$

Since there is a combinatorially large number of samples in an orbit, the probability $p(O_n)$ is sufficiently high that it can be estimated without the need for a prohibitive number of samples. By choosing m suitable orbits, a feature vector is defined as $f = (p(O_1), p(O_2), \ldots, p(O_m))$.

It is currently unclear whether this GBS algorithm can provide a quantum advantage for graph similarity problems. The strongest evidence is the study performed in ref. [22], where an exact computation of GBS feature vectors outperformed existing classical methods for some graph classification tasks. However, there are several challenges. No study of the effect of losses has been conducted, so there is a possibility that there is insufficient loss tolerance for this approach. Additionally, graph similarity problems are amenable to a wide array of heuristic approaches that work very well in practice and are therefore challenging to outperform.

For the demonstration reported in the main text, these orbits were chosen to be $O_1 = [111]$, $O_2 = [1111]$ and $O_3 = [211]$, which allows the feature vectors to be displayed in a three-dimensional plot. We focus on these orbits because they strike a balance between a sufficiently large number of photons and a high probability of observing outputs in the orbit. Four bipartite weighted graphs were encoded into the device. Their adjacency matrices A_1 through A_4 are reported in the Supplementary Information. Each graph was then permuted three times to create clusters of isomorphic graphs. Using one-line notation, the permutations are $\pi_1 = (3, 1, 2, 4)$, $\pi_2 = (4, 3, 2, 1)$, $\pi_3 = (2, 3, 4, 1)$.

Data availability

All data underlying the findings of this work are available upon request from the authors.

Code availability

Codes used for data analysis in this work are available upon request from the authors. The Supplementary Information contains example Strawberry Fields code, parameters of the theoretical model, and interferometer unitaries used in the demonstrations.

43. Clements, W. R., Humphreys, P. C., Metcalf, B. J., Kolthammer, W. S. & Walmsley, I. A. Optimal design for universal multiport interferometers. *Optica* **3**, 1460–1465 (2016).
44. Levine, Z. H. et al. Algorithm for finding clusters with a known distribution and its application to photon-number resolution using a superconducting transition-edge sensor. *J. Opt. Soc. Am. B* **29**, 2066–2073 (2012).
45. Humphreys, P. C. et al. Tomography of photon-number resolving continuous-output detectors. *New J. Phys.* **17**, 103044 (2015).
46. Vignat, C. A generalized Isserlis theorem for location mixtures of Gaussian random vectors. *Stat. Probab. Lett.* **82**, 67–71 (2012).
47. Pfeiffer, M. H. P. et al. Photonic damascene process for low-loss, high-confinement silicon nitride waveguides. *IEEE J. Sel. Top. Quant. Electron.* **24**, 1–11 (2018).
48. Rahimi-Keshari, S., Ralph, T. C. & Caves, C. M. Sufficient conditions for efficient classical simulation of quantum optics. *Phys. Rev. X* **6**, 021039 (2016).
49. Gupt, B., Izaac, J. & Quesada, N. The Walrus: a library for the calculation of hafnians, Hermite polynomials and Gaussian boson sampling. *J. Open Source Softw.* **4**, 1705 (2019).
50. Caianiello, E. R. On quantum field theory–I: explicit solution of Dyson's equation in electrodynamics without use of Feynman graphs. *Il Nuovo Cimento* **10**, 1634–1652, (1953).
51. Lund, A. P. et al. Boson sampling from a gaussian state. *Phys. Rev. Lett.* **113**, 100502 (2014).
52. Brod, D. J. & Oszmaniec, M. Classical simulation of linear optics subject to nonuniform losses. *Quantum* **4**, 267 (2020).
53. Sharp, T. & Rosenstock, H. Franck–Condon factors for polyatomic molecules. *J. Chem. Phys.* **41**, 3453–3463 (1964).

54. Sawaya, N. P., Paesani, F. & Tabor, D. P. Near-and long-term quantum algorithmic approaches for vibrational spectroscopy. Preprint at https://arxiv.org/abs/2009.05066 (2020).
55. Mebel, A., Hayashi, M., Liang, K. & Lin, S. Ab initio calculations of vibronic spectra and dynamics for small polyatomic molecules: Role of duschinsky effect. *J. Phys. Chem. A* **103**, 10674–10690 (1999).
56. Müller, C. W., Newby, J. J., Liu, C.-P., Rodrigo, C. P. & Zwier, T. S. Duschinsky mixing between four non-totally symmetric normal coordinates in the s 1–s 0 vibronic structure of (*E*)-phenylvinylacetylene: a quantitative analysis. *Phys. Chem. Chem. Phys*. **12**, 2331–2343 (2010).

Acknowledgements Certain commercial equipment, instruments, or materials are identified in this paper to foster understanding. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

Author contributions B.M., D.H.M., A.G., J.L., M.M., K.T., Z.V. and Y.Z. designed and tested the chip, and developed its components. D.H.M. also led the development of the control hardware system, designing and building the machine alongside A.R. and V.D.V. M.J.C., T.G., A.E.L. and S.W.N. developed the photon detection system. L.N., L.G.H. and J.H. developed the control and data acquisition software. V.B., A.F., T.I., J.I., R.J., N.K., N.Q., J.S., A.S., P.T. and Z.Z. designed and deployed the platform for remote programming of the device. J.M.A., K.B., T.B., R.I., S.J., K.K.S., M.S. and D.S. designed, and implemented the demonstrations. I.D., S.P.K., H.Y.Q. and N.Q. designed and implemented the non-classicality test. Z.V. and J.M.A. led the project and wrote the manuscript with input from all authors.

Competing interests The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41586-021-03202-1.

Correspondence and requests for materials should be addressed to J.M.A. or Z.V.

Peer review information *Nature* thanks the anonymous reviewer(s) for their contribution to the peer review of this work.

Imaging with quantum states of light

Paul-Antoine Moreau *, *Ermes Toninelli, Thomas Gregory and Miles J. Padgett* *

Abstract | The production of pairs of entangled photons simply by focusing a laser beam onto a crystal with a nonlinear optical response was used to test quantum mechanics and to open new approaches in imaging. The development of the latter was enabled by the emergence of single-photon-sensitive cameras that are able to characterize spatial correlations and high-dimensional entanglement. Thereby, new techniques emerged, such as ghost imaging of objects — in which the quantum correlations between photons reveal the image from photons that have never interacted with the object — or imaging with undetected photons by using nonlinear interferometers. In addition, quantum approaches in imaging can also lead to an improvement in the performance of conventional imaging systems. These improvements can be obtained by means of image contrast, resolution enhancement that exceeds the classical limit and acquisition of sub-shot-noise phase or amplitude images. In this Review, we discuss the application of quantum states of light for advanced imaging techniques.

Quantum decoherence
The loss of quantum coherence of a quantum system through its interaction with the environment. This loss of coherence leads to the collapse of the system wavefunction, which leads to loose quantum superposition or entanglement.

With the emergence of modern nonlinear optics in the second half of the twentieth century[1–3], physicists found the source of choice to conduct the desired tests of quantum mechanics. Light, unlike other physical systems, remains well isolated from its environment and is, therefore, by its nature not very sensitive to the effects of quantum decoherence. This good insulation of photons from their environment and from each other is highly desirable to study or harness the quantum properties of a system; however, it is also a drawback when it comes to the production of entangled particles because it is difficult to make two photons interact with each other to create entanglement. In early tests of quantum mechanics principles, the photons were generated through a cascaded two-photon emission process from single atoms[4–6]. Such techniques are difficult to implement. They were quickly superseded by the use of nonlinear optics, which allow the creation of twin photons within a medium with a nonlinear response, such as a nonlinear crystal. It was shown theoretically[7–9] and experimentally[10–12] that it is possible to generate photon pairs through the interaction of a single pump photon with a nonlinear medium. Such a three-wave interaction process between a pump photon and two lower-frequency — signal and idler — photons is called spontaneous parametric down-conversion (SPDC). It was shown that SPDC allows the generation of quantum states of light[13,14]. In particular, it is possible to generate entanglement in polarization[15] using such a nonlinear process[16,17]. SPDC has since been widely used as a source for various fundamental demonstrations of quantum mechanics and quantum information protocols. Notably, the parametric down-conversion process has been used in the demonstration of Hong–Ou–Mandel two-photon interference[18], implementation of delayed-choice experiments[19,20], quantum teleportation[21], and elaboration of optical quantum gates and information protocols[22,23], as well as in entanglement based on quantum key distribution[24]. It has also been used in two realizations of the loophole-free Bell test experiment[25,26].

Interestingly, as demonstrated for imaging applications, the light emitted through the SPDC process (FIG. 1) exhibits quantum correlations in both position and momentum[27]. The existence of momentum correlations between the photons created and annihilated in the SPDC process was highlighted experimentally as early as 1970 (REF.[12]) together with the first demonstration of the existence of temporal photon correlations in the light emitted in this process. These correlations were perfectly expected as they are a result of momentum conservation between the annihilated pump photon and the two photons emitted in the SPDC process. Even more interestingly, it was recognized that the state produced through the SPDC process is in fact a good approximation of the original Einstein–Podolsky–Rosen (EPR) state of entanglement[28] because it presents both position and momentum correlations[29]. The availability of such a state and the simplicity of its generation — which requires only a nonlinear crystal to be pumped with a laser — initiated the development of new types of imaging experiments. Through these experiments emerged the field of quantum imaging. Below, we give an overview of how the quantum behaviour of light can be detected through imaging and how it can be harnessed advantageously in imaging protocols. In particular, we describe why SPDC sources play an essential role in these realizations.

SUPA, School of Physics and Astronomy, University of Glasgow, Glasgow, UK.

**e-mail: paul-antoine.moreau@glasgow.ac.uk; miles.padgett@glasgow.ac.uk*

https://doi.org/10.1038/s42254-019-0056-0

Key points

- Improvements in available camera technologies have enabled the efficient detection and characterization of quantum behaviours in continuous spatial variables.
- The use of cameras in the context of quantum optics allows the detection and use of high-dimensional quantum states.
- Quantum states of light can be harnessed to implement quantum imaging protocols that allow improved imaging over classical techniques; such protocols can lead to improved estimation of the transmission, reflectance and phase of an imaged object, in addition to offering improved resolution images of the object.
- Quantum imaging techniques allow new types of imaging, such as ghost imaging, quantum imaging with undetected photons or the implementation of interaction-free measurements in the context of imaging.
- Sources of pairs of photons with different wavelengths allow the lack of high-fidelity detectors at exotic wavelengths to be overcome through ghost imaging techniques and quantum nonlinear interferometric imaging techniques.

Cameras to detect quantum behaviour

The widespread use of SPDC as a source of quantum states rapidly generated interest in the study of correlations and entanglement in the spatial domain. Not only did it promise the development of new types of imaging but also it allowed very high-dimensional quantum states to be engineered. The concurrent development of new types of camera technologies enabled the detection of single photons with cameras[30,31]. The new types of quantum optical demonstrations no longer relied on scanning point-like avalanche photodiodes but rather on spatially resolved detectors. This development in detection techniques enabled highly parallel correlation measurements, and ultimately led to time-efficient detection of quantum signatures that may be exploited in the context of quantum information protocols. In this section, we describe different camera technologies that have led to quantum imaging demonstrations of fundamental nature, highlight different regimes in which these cameras can perform and discuss the respective advantages and disadvantages of the current technology.

Detection of quantum correlations. Following the early detection of spatial photon correlations[12], further work was performed throughout the 1990s to both characterize and exploit the quantum correlations emitted through SPDC[32–34]. However, these techniques were inherently inefficient because they used avalanche photodiodes to detect single photons and a scanning pinhole to detect the spatial features of the correlations. Such a pinhole-filtering technique leads to the loss of the vast majority of the photons, and, therefore, the experiment requires a long time to measure the spatial form of the correlation. Since then, researchers have tried to detect spatial correlations between photon pairs with cameras, thereby removing the necessity to filter at one particular position. The first attempt at detecting spatial correlations of quantum origin with a camera was performed in 1998 (REF.[30]) using a photon-counting intensified charge-coupled device (ICCD) camera. The results of this study — despite the relatively noisy images of photon detection — inspired many experiments with more technologically advanced cameras.

Sub-shot-noise
A variable exhibits sub-shot-noise statistics if the noise on that variable is smaller than the shot noise. The shot noise is due to the discrete and independent arrival of photons, which exhibits Poisson statistics.

However, because of the technological limitations, including the dark count, the noise and low quantum efficiencies of available cameras, subsequent tests had to be performed under a different regime. In 2000, a conventional single-frame camera was used to detect intensity correlations in the spatial spectrum of SPDC beams[35]. A lithium triborate crystal was used to generate a down-converted beam in a high-gain regime. To ensure efficient emission of the signal and idler waves through parametric fluorescence, the idler and the signal phases must match throughout the propagation of the waves inside the nonlinear material. This phase matching ensures that the waves emitted at some point of the crystal do not interfere destructively with the upstream emissions. There are two main types of phase matching that exist in the context of parametric fluorescence: type I and type II. In type I phase matching, both signal and idler waves are emitted with the same polarization and therefore propagate along the same birefringent axis of the nonlinear crystal[36,37]. In type II phase matching, however, the two waves that are emitted have orthogonal polarizations and propagate along two distinct birefringent axes, which permits, under non-collinear phase-matching conditions, the generation of two distinct beams propagating in different directions. Under the conditions used in REF.[35], the relatively bright beam intensity is able to exceed the noise floor of the camera. In this study, the correlated intensity fluctuations were detected within different parts of the beam (FIG. 1b).

In the aforementioned demonstration, the correlations were simply observed and spatially characterized. However, it is also possible to demonstrate sub-shot-noise behaviour with such correlations, thus establishing their quantum nature. Within two correlated regions of interest of the beam, the detected intensities are indeed expected to follow the same temporal fluctuations. If these joint fluctuations are due to the arrival of correlated photons rather than a result of classical intensity fluctuations, then, for an ideal system, one would expect to detect in both regions of interest exactly the same number of emitted photons. As a consequence, by subtracting the two signal intensities, one may obtain zero and the fluctuation of this intensity difference will also tend to zero. By contrast, classically correlated intensities when subtracted cannot go below a certain limit. This limit, called shot noise, is due to the quantum nature of light and the fact that the number of photons in a light beam is subject to a fundamental standard deviation that is equal to the square root of the average number according to Poisson statistics. The shot-noise limit corresponds to the intensity fluctuations of the lowest-noise classical state: a coherent state, which is that of an ideal laser. If by subtracting two intensity signals one obtains a quantity that fluctuates less than that of the shot noise, then the underlying statistics is said to be sub-shot noise and one can conclude that the two beams exhibit quantum correlations[38,39]. This was achieved in parametric down-conversion in the context of correlated single-mode beams[40–46] before being demonstrated in the context of imaging. Indeed, a few years after the aforementioned demonstration[35],

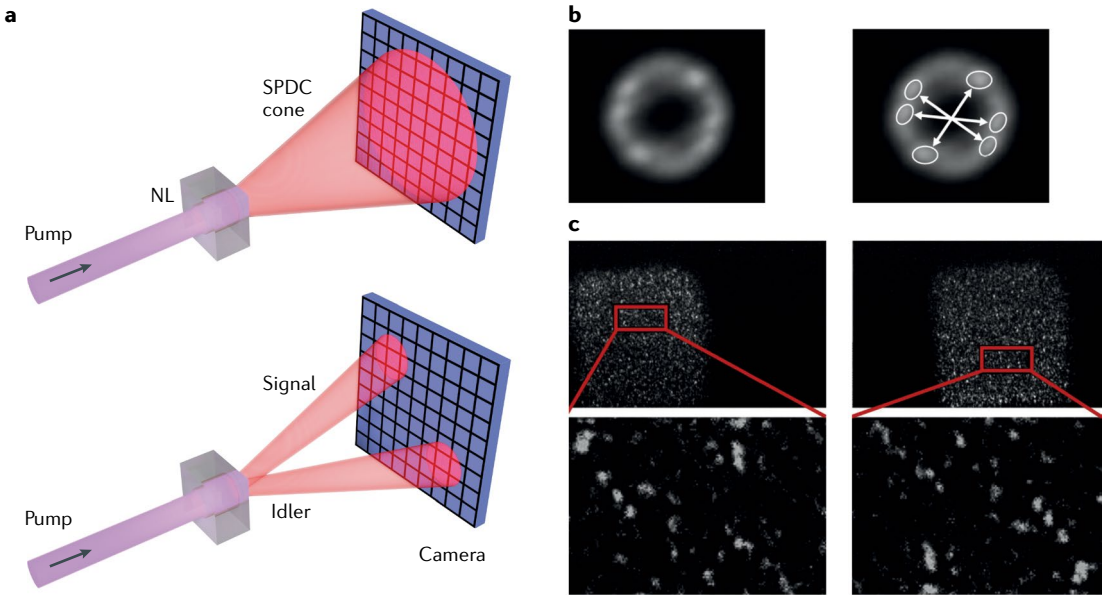


Fig. 1 | **Generation and detection of quantum correlations in spontaneous parametric down-conversion.** **a** | Spontaneous parametric down-conversion (SPDC) generation in a nonlinear crystal (NL). The process is depicted here for type I (top) and type II (bottom) phase matching, leading to the emission of one and two SPDC beams, respectively. Inside these beams, spatial photon correlations can be detected. **b** | Observation of correlations within a type I SPDC beam in a high-gain regime. The image on the left is reproduced on the right, with white arrows highlighting the correspondence between similar intensity features that are due to intensity correlations within diametrically opposed portions of the beam. **c** | Observation of correlations between type II SPDC beams in a high-gain regime. The left and right images correspond to the two beams (signal and idler, respectively) imaged on different regions of a camera. One can also observe similar patterns within the two beams with a 180° rotation, which is a signature of momentum anticorrelations. Panel **b** is reproduced from REF.[35], Springer Nature Limited. Panel **c** is reproduced with permission from REF.[47], APS.

such a quantum signature of correlations in images was observed under a similar regime[47,48]. It was done using parametric fluorescence generated in a barium borate crystal with type II phase matching. By acquiring images of the bright fluorescence beams, the authors showed the sub-shot-noise nature of the detected spatial correlations (FIG. 1c).

As mentioned above, although it is true that these results demonstrated genuine photon quantum correlations, they were performed in a high-gain regime of the down-converted emission. This means that such correlations were composed not only of pure twin-photon correlations but also of higher-order photon correlations generated through the stimulated emission. Such higher-order terms can introduce excess noise when the imaging system is subject to losses, that is, in non-ideal conditions. A few years later, the sub-shot-noise behaviour of SPDC light in images captured with an electron-multiplying CCD (EMCCD) camera was demonstrated[49]. Moreover, in another study[50], a scheme was proposed to use photon correlations to achieve sub-shot-noise imaging, that is, the acquisition of images in a scheme that outperforms classical imaging schemes in terms of noise. It was suggested that an optimal regime to use for such a realization is a bright light low-gain regime, which prevents the introduction of excess noise. Following these suggestions, a similar regime was later used to detect twin photons[51] on the way to realizing sub-shot-noise imaging of a low-transmission sample[52]. To access this particular regime, a pump laser with a pulse duration much longer than the coherence time of the SPDC was used to ensure that the number of photons emitted per spatiotemporal mode of fluorescence emission was low enough to make the stimulated emission negligible. Hence, a very low contribution from the higher-order photon number correlations was ensured, thus limiting the impact of the excess noise. This low emission rate led to a demonstration of sub-shot-noise spatial correlations without background subtraction using a conventional CCD camera[52].

Efficient characterization with cameras. The aforementioned demonstrations were focused on simply detecting a signature of quantum correlations. As we have seen, this can be done in a bright light regime with conventional scientific cameras. However, such cameras are not sensitive enough to detect single photons. Indeed, the noise floor of such cameras is typically of several electrons even when the sensor is cooled. Under such conditions, the detection of a single photon leading to a photoelectron trapped in the CCD well would not be observable in the image, which would be largely dominated by the technical noise of the camera. This considerably limits the range of quantum behaviour that can be observed with such cameras. To detect more subtle quantum characteristics that require the detection of single photons, one needs to use a different camera, for example, an EMCCD camera. In contrast to conventional CCDs, EMCCD cameras incorporate

on-chip gain placed before the charge reading stage[53]. The gain register generates a multiplicative avalanche effect that occurs in around 500 stages. At each stage, the electrons contained in accelerated potential wells have a small probability of generating a secondary electron through impact ionization with the chip substrate. This amplification before reading has the potential to make single-photon events emerge from the camera readout noise.

With such cameras, it is possible to develop photon-counting strategies[31]. As mentioned before, these strategies led to the detection of sub-shot-noise features in SPDC light[49,54]. It was followed by several other demonstrations aimed at detecting and using quantum correlations with EMCCD cameras[55–59].

With single-photon cameras, one can also demonstrate more fundamental quantum phenomena, such as an EPR paradox[28]. Correlations demonstrating the EPR paradox were performed in a series of experiments[60–63] (FIG. 2).

In these experiments, SPDC light is used to produce EPR-type spatial correlations. The correlated beams are then detected with an EMCCD camera and correlations are recorded between different regions of the camera. These correlations are measured in two different configurations: the first configuration in which the camera acquires images of the crystal plane thus recording correlations between the positions of the down-converted photons and the second configuration in which a Fourier plane of the crystal is imaged onto the camera thus leading to the detection of correlations between the transverse momenta of the photons. The existence of such correlations in both position and momentum is demonstrative of the EPR paradox. In contrast to the previous manifestation of the EPR paradox[27], cameras enable an inherently more efficient demonstration: scanning a point-like single-photon detector is inefficient as it leads to the loss of most of the photons.

Two synchronized cameras were also used in REF.[63] to ensure the full spatial separation of the photons. In this experiment, the sub-shot-noise nature of the correlations was simultaneously detected. Cameras allow not only the characterization of very high-dimensional quantum correlation features[62,63] through the great number of pixels they possess (typically ~300,000–1,000,000 pixels) but also the opportunity to perform highly parallel detections of such quantum correlations. Using a similar scheme, the EPR paradox was shown with only a single pair of frames in each of the two configurations (position or momentum detection)[64]. This signifies that no temporal averaging had to be performed to detect these features. Instead, by using only single frames, the number of synchronously recorded samples of the state in one frame was sufficient to perform the statistical averaging. The total acquisition time for such an acquisition requires only two exposures of 0.03 seconds each.

Other demonstrations led to fast characterization of correlations in the space domain using single-pixel cameras[65,66]. This was done with a combination of a digital micromirror device and a single-pixel single-photon avalanche diode (SPAD)[67,68]. Using compressive sensing techniques relying on sparsity in spatial correlations between entangled photons, they were able to demonstrate 1,000-fold improvement in the acquisition times over conventional raster-scanning techniques (reduced from 310 days to 8 hours).

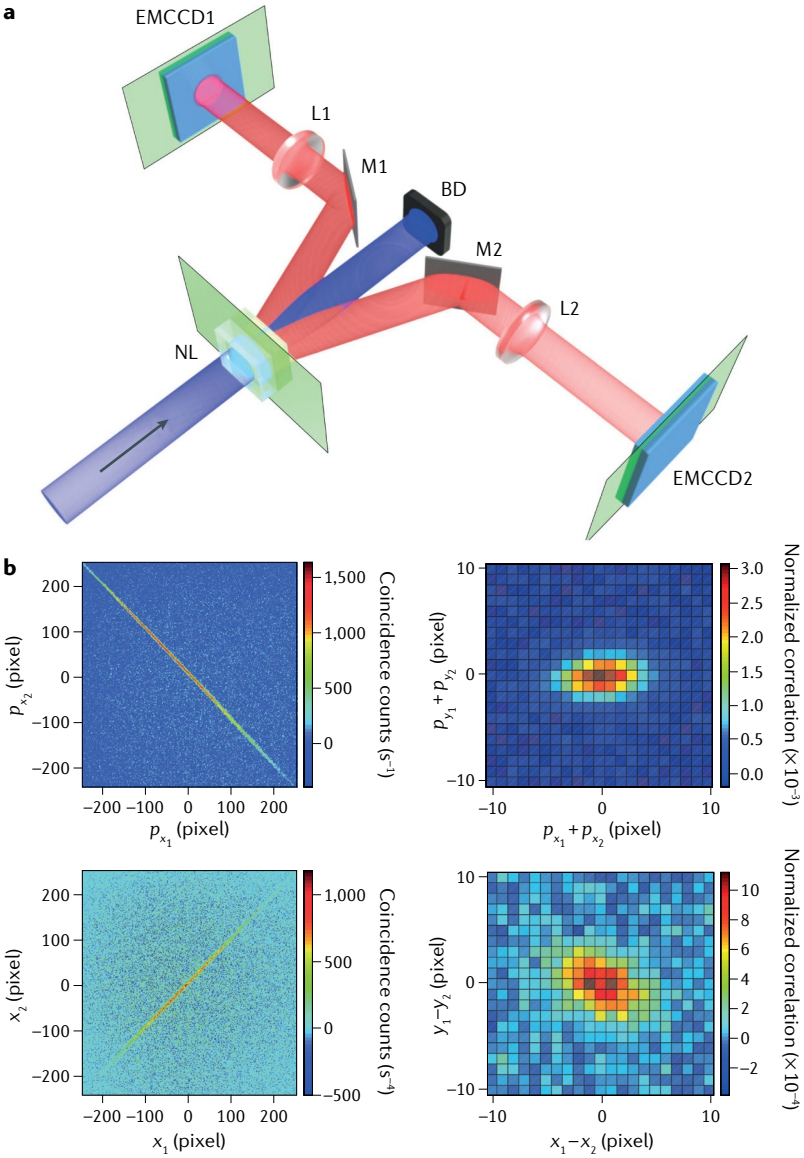


Fig. 2 | **Experimental test of Einstein–Podolsky–Rosen paradox in images.** **a** | Experimental setup used to demonstrate a 2D Einstein–Podolsky–Rosen (EPR) paradox with a pair of synchronized electron-multiplying charge-coupled device cameras (EMCCD1 and EMCCD2). A nonlinear crystal (NL) cut for type II down-conversion is pumped with a UV laser and the two spatially separated beams are then sent to two cameras, either by reimaging the crystal plane as shown here (the green planes indicate the crystal plane and the crystal image planes) or by imaging a Fourier plane of the crystal to detect the momenta of the photons. The pump is represented by a blue beam and the signal and idler are represented by red beams. x_i and y_i are the transverse positions of detection of photon $i = \{1, 2\}$ along the horizontal (x) and vertical (y) directions, respectively; p_{xi} and p_{yi} are the transverse momenta of photon $i = \{1, 2\}$ along the horizontal and vertical directions, respectively. **b** | Detected conditional probability distribution of bi-photons in the acquired images. The results exhibit quantum correlations in both momentum (top) and position (bottom). The right column corresponds to the cross-correlations of the images composed of single-photon events extracted from the two cameras. The correlation peaks are the signature of 2D quantum correlations that can be shown to demonstrate a high-dimensional EPR paradox. BD, beam dump; L1 and L2, lenses; M1 and M2, mirrors. Panel **b** is reproduced with permission from REF.[63], APS.

Table 1 | **Comparison of different camera technologies used in quantum imaging**

Type of camera	Overall detection efficiency	Lowest accessible light regime (photons per pixel per frame)	Typical noise at lowest accessible light regime (counts equivalent photons per pixel per frame)	Main utility in quantum imaging
Scientific	Up to ~95%	>1,000–10,000	1–5	Detecting intensity correlations
Electron-multiplying charge-coupled device	~60% after thresholding; quantum efficiency >80% (at −90 °C)	0.01–0.15	~0.002 after thresholding	Fast statistical characterization of correlations in photon counting[193]; relatively fast but relatively noisy single-photon pair identification[194]
Intensified	~10–20% after thresholding	10^{-3}–10^{-4}	~10^{-4} after thresholding, that is, few photons per frame	Low-noise single-photon pair identification

Intensified cameras. Another type of camera that is useful in the context of quantum imaging is the intensified camera. Intensified cameras are usually scientific CCD or complementary metal-oxide semiconductor (CMOS) cameras that have an image intensifier placed before the sensor. The image intensifiers[69] are composed of a photocathode that converts the photons into electrons, followed by a microchannel plate that multiplies the electrons through the influence of high voltage but very short — of the order of a few nanoseconds — electrical pulses, and finally a phosphor screen that reconverts electrons back into photons. The photons emitted by the phosphor screen are then detected by the camera. With such an amplification happening before the detection, a light beam arriving into the intensifier — which is composed of only a single photon — is converted into an amplified signal of many photons with very little additional noise, owing to the short time gates that limit the influence not only of the dark-current noise but also of incoming spurious light. One can then acquire images in which the huge spikes that appear correspond to single-photon detection events. By applying a detection threshold to such images, one may obtain images of true single-photon detection events.

As mentioned before, the earliest use of an ICCD camera to record correlations of quantum origin was performed in 1998 (REF.[30]). This demonstration inspired further measurements of the correlations[70,71], until the technology became mature enough to lead to substantial use of such cameras in quantum imaging. Several new realizations used ICCDs to perform quantum imaging experiments. EPR-based imaging was demonstrated[72] by triggering an ICCD camera with a SPAD whose detection of a photon heralds the arrival of its entangled twin. In the same year, real-time imaging of two-photon entanglement in two modes was demonstrated using a similar acquisition setup[73]. Another important quantum phenomenon was later evidenced through the use of an intensified camera when a shot-by-shot observation of a Hong–Ou–Mandel effect was performed[74]. The authors had previously shown that the intensified CMOS camera they used was able to perform spatially resolved multiphoton counting[75]. This work led to subsequent demonstrations using a similar setup, such as the acquisition of holograms in a single-photon regime[76], the demonstration of bi-photon mode engineering for quantum-enhanced interferometry[77] and the demonstration of a wave-vector multiplexed quantum memory for photons interacting with cold atoms[78].

Other camera technologies. We have seen in this section three main types of camera technologies that can be used to perform quantum imaging. In TABLE 1, we report some of the most important characteristics of such cameras in the context of quantum imaging. It is useful to note that new technologies such as SPAD arrays[79–82], matrices of superconducting nanowires single-photon detectors[83,84] or new back-side-illuminated CMOS technologies[85] are able to resolve the number of photons and are very promising alternatives to the cameras presented here. However, these technologies are not yet sufficiently mature to be implemented in quantum imaging applications involving correlated photons.

Improved imaging with quantum light

So far we have seen how quantum imaging and especially the use of commercially available single-photon-sensitive cameras can be used to efficiently detect correlations between photons in high spatial dimensions. These quantum properties can also be harnessed using similar techniques and tools with potentially improved performance compared with what can be accessible via purely classical schemes. Here, we review the various studies that have been conducted along these lines. For this Review, we distinguish two categories in image improvement targeted by researchers: the first is a reduction of the noise in the recorded phase or intensity of the images, and the second is the improved resolution of such images.

Improved optical metrology. With the emergence of the concept and method of generating quantum squeezing[86,87] and the definite number of photon states[39,88,89], new schemes were devised that were able to harness quantum properties of light to reach levels of sensitivity

Quantum squeezing
A state is said to be squeezed if the noise of one observable measured on that state is below the symmetric Heisenberg limit; this implies that the conjugate variable noise is itself above that limit, as imposed by the Heisenberg uncertainty principle.

beyond that achievable classically[43,90–92]. In the context of optics, a squeezed state can be defined as a state that presents a reduced uncertainty along one of the two field quadratures, compared with that of the quadratures for a coherent or vacuum state (state of an ideal laser). If the quadratures are bounded by the Heisenberg uncertainty principle, the uncertainty on each one is not fundamentally bounded.

Another class of states present a reduced uncertainty compared with a coherent state. These states that have a definite number of photons are also called Fock states. Compared with coherent states, the intensity of which is uncertain, the intensity of such states is perfectly defined. The Heisenberg trade-off being that the phase of a Fock state is perfectly uncertain. In the case of both squeezed and Fock states, the reduced uncertainty they present can be exploited to increase the measurement sensitivity.

Such techniques can be included in the general domain of quantum metrology[93,94], which aims to use quantum properties to perform improved measurements. The domain was largely initiated by the desire to improve the sensitivity of gravitational wave detectors, which led to the early theoretical developments of quantum non-demolition measurement[95] and the use of squeezed light in interferometric gravitational wave detectors[96,97].

In the context of imaging, one application of quantum metrology arises in the measurement of delicate samples[98,99]. By enabling the use of sub-Poissonian statistics of light and the possibility to surpass the classical noise limit, quantum metrology schemes allow imaging of an object by exposing it to fewer photons than for a classical, shot-noise-limited, measurement[100].

For spatially single-mode measurements, squeezing would appear as an opportunity to perform improved measurements over classical techniques in both phase[86,95] and absorption[101] estimation. The quantum advantage accessible through squeezing is indeed potentially important as it is possible to produce states exhibiting squeezing as high as 15 dB (REF.[102]). The use of spatial squeezing in imaging could potentially lead to interesting applications[93,103]. Thus far, spatially multimode squeezed states have been used only to improve beam localization[104,105] and in the detection of entanglement between a few spatial modes[106–108]. The restricted application to date is mainly due to the difficulty in generating these states and building spatially resolved homodyne detectors.

An alternative form of quadrature squeezing suitable for absorption measurements is to use bright amplitude squeezed light states that can exhibit spatial correlations, such as the light emitted by an optical parametric oscillator (OPO) when running above threshold[41]. An OPO allows the correlated nature of the signal and idler beams to be used to improve the sensitivity of absorption measurements[44,92]. There are two limitations of such realizations. First, as in the case of phase quadrature squeezing, the technique is highly sensitive to the technical noise that is present at low frequencies in the source, and, therefore, measurements need to be shifted to frequencies of a few megahertz. The second limitation is due to the thermal nature of the down-converted beams, as the stimulated re-emission of the pairs is non-negligible when operating the OPO above the threshold, that is, for pump power leading to a gain that is greater than the intracavity losses[41]. In such a context, the metrology schemes become extremely sensitive to losses because a noisy thermal contribution is added to the estimated experimental parameter by reintroducing into the statistics thermal light that is no longer correlated. As a consequence, such schemes are usually limited to low-absorption samples.

Another strategy to limit these drawbacks is to remain in a regime dominated by SPDC. Two techniques were proposed to use SPDC to perform sub-shot-noise evaluation of the transmission of a sample for a single-mode measurement[39]. One of the two methods was based on the feedforward method to generate Fock states to illuminate the sample. This method was recently implemented in single-mode transmission metrology[109]. However, even more interestingly in the context of imaging, it was shown that one can use the same intensity correlated nature of SPDC beams to produce quantum-improved estimation of a channel transmission with conventional — non-photon-counting — photodiodes[43].

Such a regime of bright SPDC is similar to the regime proposed in REF.[50] and exploited later[51] to detect and use quantum correlations with low-noise conventional CCD cameras. Interestingly, the same regime was used again in the demonstration of the first sub-shot-noise imaging experiment[52] referred to above. In this remarkable realization, type II SPDC beams pumped with long pulse duration were used to make the stimulated emission negligible. In this experiment, one of the two beams was sent through a low-absorption object (~5%) imaged on the camera, whereas the second beam was propagated freely before being detected on a different part of the same camera in an optically equivalent plane as the first beam (FIG. 3).

Owing to the presence of spatial correlations between the two beams, the shot-noise-caused intensity fluctuations will be the same within the two beams at a particular transverse position **r**. As a consequence, and because the object absorption was relatively low (therefore preserving therefore the correlations between the beams), one can remove some of the measurement noise (instantaneous fluctuation) present in the first beam simply by subtracting the detected image intensity of the second beam, following the scheme proposed in REF.[50]. By doing so, it is possible to obtain sub-shot-noise images of a low-absorption object[52]. The same approach was also implemented within a wide-field microscope[110]. However, this subtraction method is limited to the imaging of low-absorption objects because simply subtracting the intensity of the two beams to estimate the absorption of the object is a suboptimal estimator that leads to a rapid loss of the quantum advantage for objects with higher absorption. Another optimized estimator was reported[111] that is less sensitive to losses. See REF.[112] for a systematic comparison of this new estimator with estimators previously used. This new estimator was used to demonstrate an absolute (unconditional) quantum advantage in absorption

Field quadratures
Operators that correspond to the real and imaginary parts of the amplitude of the quantized electromagnetic field. They compose a basis for the phase space of the quantized field.

Quantum non-demolition measurement
A type of measurement of a quantum system that preserves the uncertainty of the measured observable. This implies, in particular, that the system is not destroyed by the measurement, for example, a measured photon would not be absorbed during the measurement process.

Homodyne detectors
A detector used to measure different components of the quantized electromagnetic phase space. It is based on detecting the interference occurring on the two outputs of a beam splitter that mixes a controlled bright local oscillator and the state of light that is to be measured.

Thermal light
Light whose statistic is similar to that of thermal radiation. As a result, such light is subject to super-Poissonian intensity fluctuations.

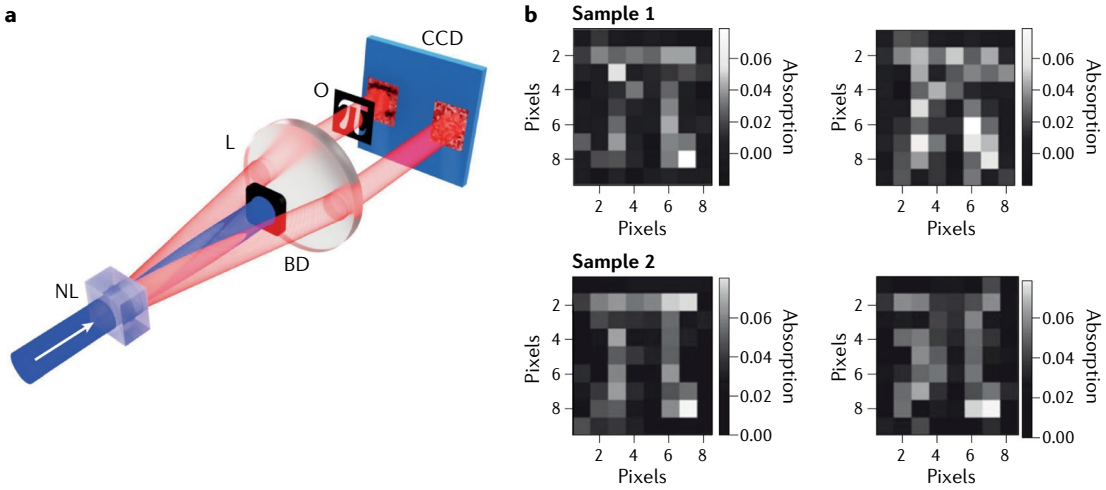


Fig. 3 | **Sub-shot-noise quantum imaging. a** | Quantum correlated beams are generated in a barium borate nonlinear crystal (NL) through type II spontaneous parametric down-conversion. One of the beams probes a low-absorptive object before being detected on a camera; the second beam is directly detected on a different part of the same camera. By subtracting the intensities detected within each of the beams, it is possible to remove some of the shot noise in the acquired image of the object. **b** | Two examples of images acquired: the images on the left are obtained after subtraction; the images on the right are the images recorded directly by the camera. One can see that the images on the left appear less noisy, which is owing to the sub-shot-noise nature of the correlations between the beams. It was shown that such images themselves exhibit sub-shot-noise qualities. BD, beam dump; L, lense; O, imaging object. Panel **b** is reproduced from REF.[52], Springer Nature Limited.

estimation for an object presenting absorption up to 50% in spatially single-mode measurements[111]. In addition, a heralded source of multimode mesoscopic sub-Poissonian light was shown through post-selection of the detected intensities[113] with the potential to bring previous transmission metrology demonstration to brighter regimes.

Using quantum states of light can also lead to improved estimation of the optical phase[93,114]. The interferometric behaviour of NOON states can be used to increase the phase measurement sensitivity within an interferometer with Heisenberg scaling, that is, an uncertainty on the phase estimation $\Delta\varphi$ scaling as $\Delta\varphi = 1/N$, where N is the number of photons in the NOON state. This can be explained by the fact that the photonic de Broglie wavelength of such a state is equivalent to that of a single particle with wavelength λ/N (REFS[115,116]). The use of NOON states was implemented in the form of an interferometric microscope setup in which a phase object was raster scanned to give an image with precision beating the standard quantum limit as dictated by the shot noise[117].

Another quantum interferometric technique that can reach Heisenberg-limited sensitivities is the so-called SU(1,1) nonlinear interferometric method[118–120]. In contrast to the NOON state interferometry, it has the advantage that the quantum correlations are generated inside the interferometer, as the scheme is implemented as a Mach–Zehnder interferometer in which the two beam splitters are replaced by nonlinear active elements pumped by the same source. This allows the preservation of good-quality entanglement inside the interferometer and makes the method resilient to detection losses[121,122]. Experimental demonstrations of enhanced sensitivity have been performed[123–125]. Such a scheme may also be implemented to perform Heisenberg-limited phase imaging.

In addition to improving the fundamental limits of precision, quantum correlations can be harnessed to give technical ameliorations in imaging. For example, an implementation of a technique called heralded imaging allows the use of quantum temporal correlations to trigger an intensified CCD camera for approximately 4 ns only when a signal photon that has probed an object is likely to strike the sensor[126]. This heralding has the advantage of removing some of the sensor and environmental parasitic noise, enabling the acquisition of images containing only a few photons[126]. The same technique is anticipated to be implemented in the context of LiDAR systems to generate quantum rangefinders[127]. In the context of a LiDAR system, the ability to overcome some of the technical noise can help such a system to work with fewer photons with the aim to see without being seen. Moreover, such schemes could be further improved by ad hoc implementations of the quantum illumination protocol proposed in the context of quantum information schemes[128].

Super-resolution in quantum imaging. The quantum improvements in imaging are not only limited to decreasing noise. Resolution advantages can also be obtained by using the quantum behaviour of light. Two main methods have been devised that harness quantum states to go beyond the diffraction limit.

The first method allows the standard quantum limit in resolution to be reached and goes beyond the diffraction limit by detecting quantum correlations between N photons; such a limit scales as $\frac{1}{\sqrt{N}}$ (REF.[129]). It was shown that in this context of raster-scan imaging techniques, it is possible to post-select a number of photons

NOON states
A state composed of N particles in a superposition of being all in one mode or all in a second mode.

LiDAR systems
A system that emits light pulses and measures the time-of-flight of their echoes to assess the distance to reflecting objects. It is based on the same principle as a RADAR system but uses light instead of radio waves.

within classical light focused on an object to access the same kind of advantage[80,130].

It is also possible to obtain a quantum enhancement in resolution with classical illumination when imaging fluorescent single-photon emitters[131]. The light emitted by such objects exhibits photon anti-bunching, which can be harnessed to obtain a standard quantum-limited resolution enhancement. Experimental realizations have been performed to demonstrate resolution improvement using colloidal quantum dots[132,133] and nitrogen-vacancy colour centres in diamond in the context of fluorescence confocal microscopy[134]. Interestingly, such techniques can be used in conjugation with classical techniques allowing super-resolution imaging to be achieved[135]. This was demonstrated experimentally on biological samples stained with fluorescent quantum dots by combining the anti-bunching resolution advantage of quantum dots with the classical advantage of structured illumination[136]. Finally, it was shown that using photon-counting strategies with classical illumination can lead to resolution enhancement even for the observation of non-fluorescent objects[137].

In the context of full-field imaging of non-fluorescing objects (that is, without scanning), states exhibiting quantum-correlated illumination can be used to gain a resolution improvement[129]. Recently, we have demonstrated a resolution enhancement in full-field imaging of non-fluorescing objects[138] using a centroid measurement detection method for bi-photons[139].

The second method allowing Rayleigh's limit of diffraction to be surpassed is called quantum lithography. It uses the interference exhibited by NOON states to reach an improvement that scales as $\frac{1}{N}$ (Heisenberg scaling) in the size of projected interference fringes[140]. To access such Heisenberg scaling, it is required that the ensemble of photons 'simulate' the behaviour of an indissociable photon that in an interferometer is in a superposition of being found in one arm or the other. The equivalent situation with N photons is therefore for them to all be in a superposition of being found together in one arm of the interferometer or together in the other arm. Such a state is exactly a NOON state. In this situation, the super-resolution phenomenon emerges in the N-photon interference pattern, so that the pattern requiring a multiphoton absorption process is detected or printed on a material (FIG. 4).

The difficulty in finding materials or detectors that are capable of performing multiphoton absorption has considerably limited the use of these two methods, and also the performance of the earliest realizations of quantum lithography[141,142]. However, it was suggested that to detect such interference patterns, one could simply proceed to optical centroid measurements of the N detected photons of the NOON state[139]. This method was later implemented[143] for two-photon NOON states and for up to four-photon NOON states[144,145]. Finally, it has been shown that multiphoton interference with independent single-photon light sources can also lead to a similar super-resolved interference pattern[146], without using path-entangled states. This is enabled by an effect equivalent to the extension of the Hanbury Brown–Twiss effect for intensity correlations with more than two photons[147].

Photon anti-bunching
A property of light in which photons are more evenly spaced in time than in an ideal laser beam (coherent state). Anti-bunched light will exhibit sub-shot-noise statistics over time.

Hanbury Brown–Twiss effect
A correlation effect observed between the intensities detected by two detectors when each receive light from two independent sources. It requires the interference of two photons to occur to be explained at a quantum level.

New imaging techniques

In addition to improving the images obtained through conventional imaging techniques, quantum effects have also allowed new methods of imaging to be developed. Here, we report some examples, including ghost imaging. This technique arguably initiated the field of quantum imaging in that it was the first use of light containing spatial quantum correlations to illuminate the object to be imaged.

Ghost imaging. Ghost imaging utilizes correlations between spatially separated light fields to record an image of an object using photons that have not interacted with the object[148]. This technique uses quantum-entangled photons produced via SPDC within a nonlinear medium and exploits quantum spatial correlations between the photon pairs that comprise the signal and idler output. The ghost imaging scheme was proposed originally in the late 1980s[149] and then first realized in 1995 (REFS[33,34]). A typical ghost imaging setup comprises the spatial separation of the signal and idler photons, in which the idler interacts with the object and is subsequently detected by a non-spatially resolving (bucket) detector; coincidence detection of idler photons at the bucket detector and signal photons at the imaging detector is then performed to select the correlated photon pairs to build an image of the object. Of the detected signal and idler light fields, neither beam alone contains the information required to reconstruct an image of the object. The bucket detector is spatially unresolved, simply detecting all of the idler photons passed by the object. Similarly, the spatially resolving detector measures the position of all of the signal photons incident on it without any information about the object. However, the correlation between these datasets can be exploited to extract an image. Through integrating over a number of acquired events, an image of the object may be recovered from the subset of the signal light field that is correlated with the idler light field detected by the bucket detector. Although initial realizations of ghost imaging entailed the use of a raster-scanning technique[33,34,150], more recent ghost imaging schemes utilize a spatially resolving detector — such as a time-gated ICCD camera triggered by a SPAD — to enable imaging across the full field of view without the inherent limitation in detector efficiency of $1/n$ for n pixels for implementations based on scanning[72,126,151].

After the earliest realizations of ghost imaging[33,34], it was unclear to the community whether entanglement was actually needed to perform ghost imaging. However, it was later demonstrated that it is possible to perform ghost imaging by using a classical source, that is, a laser beam, deflected by a variable amount and then passed through a beam splitter[152] or thermal light split in two beams on a beam splitter[153]. Regarding the potential advantages of quantum versus classical ghost imaging, it is now recognized that these methods produce images of a similar resolution[154,155]. The main advantage of quantum light is found at low light levels, at which it exhibits greater visibility and a greater signal-to-noise ratio[154,156]. Nevertheless, classical ghost imaging techniques have inspired a new type of imaging based on

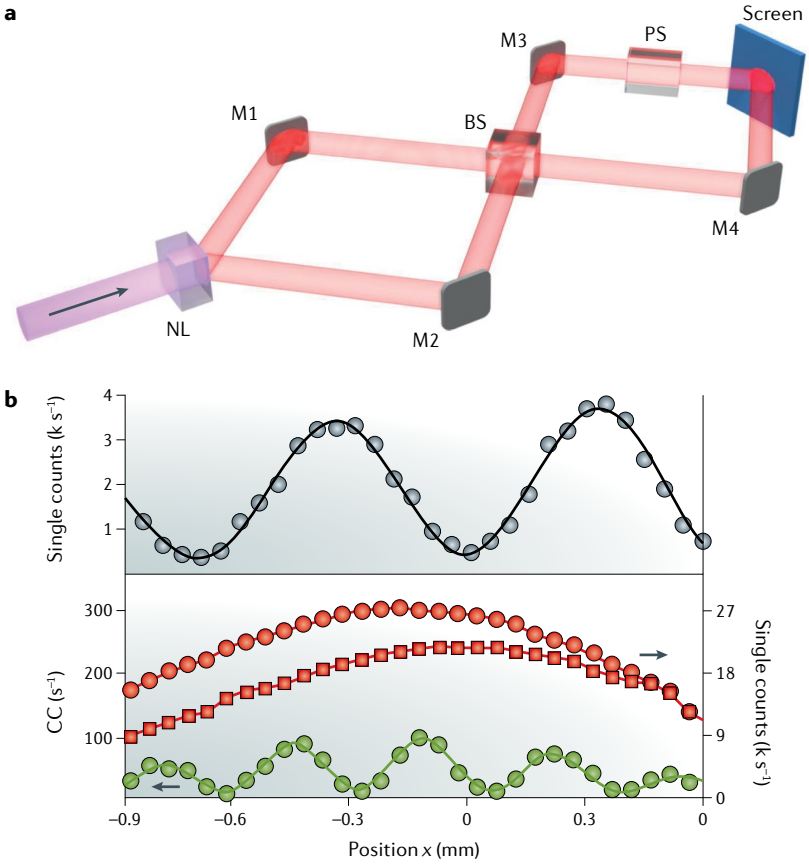


Fig. 4 | **Principle of quantum lithography. a** | Simplified version of a quantum lithography experimental scheme. A NOON state with $N = 2$ is generated at the output of a beam splitter (BS) through a Hong–Ou–Mandel effect by recombining two photons generated by spontaneous parametric down-conversion (SPDC). The two photons are then in a superposition state of being both in the upper arm or both in the lower arm of the interferometer situated between the BS and the screen. A phase shifter (PS) can be added in one of the paths. One can also displace two adjacent detectors in the plane of the screen to detect two photon coincidences and compute the centroid of such detected bi-photons. **b** | Experimental results evidencing the principle of quantum lithography. The black circles correspond to the single-count interference pattern obtained with a classical coherent state. In the bottom panel, the two red curves correspond to single counts detected at the two detectors (right arrow). The green curve corresponds to the coincidence count (CC) centroid measurements (left arrow). One can observe that the period of the interference fringes on this later figure is approximately half that of the classical interference pattern. k/s, kilo counts per second; M1–M4, mirrors; NL, nonlinear crystal. Panel **b** is reproduced with permission from REF.[143], APS.

the use of classical correlations[157–159]. For an overview of the comparison between classical and quantum ghost imaging, see REFS[154,160,161].

A degenerate quantum ghost imaging system in which the signal and idler photons are of the same wavelength has applications for the imaging of samples under low-light conditions[126], for example, in compressed sensing and object tracking[162]. However, it is possible to design a non-degenerate ghost imaging system in which the signal and idler photons are of a different wavelength. The use of such a non-degenerate down-conversion source enables the imaging of objects in wavebands in which spatially resolved detectors are impractical, expensive or ineffective in terms of resolution and, therefore, cannot be used in imaging applications. To perform ghost imaging in such wavebands, only a bucket detector is required while the imaging detector operates in a waveband in which spatially resolved detectors are relatively efficient and inexpensive.

Non-degenerate ghost imaging was carried out in 2015 (REF.[163]) using an experimental setup as modelled in FIG. 5a. In this setup, the signal and idler photons at 460 nm and 1,550 nm, respectively, are separated at the dichroic mirror D; an object with features observable in the infrared is probed by the idler photons in the ghost imaging arm and detected by the non-spatially resolving SPAD, whereas the signal photons are detected using the spatially resolving ICCD camera. Non-degenerate ghost imaging allows an object to be visualized in the infrared domain, using photons of a visible wavelength to reconstruct the image (FIG. 5b).

In the aforementioned study[163], the objects were gold patterned onto silicon wafer using electron beam lithography, of which the silicon is transmissive for the infrared photons whereas the gold is not (FIG. 5b). Non-degenerate ghost imaging using idler wavelengths outside the current spectral range of spatially resolving detectors potentially would allow the imaging of objects and their internal structure using far-infrared and terahertz wavelengths. These wavelengths have applications in biological, industrial and security imaging applications in which raster-scanning techniques using the aforementioned non-spatially resolving detectors are too slow in the construction of an image[164]. As for the resolution of non-degenerate ghost imaging, theoretical studies indicate that the resolution does not lead to improvement over the classical methods[165,166]; furthermore, the resolution will still be limited by the point spread function of the imaging system and may be degraded by reducing the strength of correlation between the photon pairs[155].

Finally, quantum correlated sources have been used to perform ghost acquisitions in other domains. For example, temporal ghost imaging has been performed using optical correlations[167]. However, it has also found usage outside of conventional optics, with recent demonstrations performed in the X-ray domain[168] and using beams of correlated atoms[169].

Imaging with undetected photons. Further to the aforementioned method of ghost imaging — in which the detection of the idler photon is used to herald the arrival of its twin on an imaging detector and to select a subset of the signal photons to produce an image — it has been shown[170,171] that it is not necessary to detect the idler photon at all to form an image using the signal photons. The physical basis of this technique was first introduced and demonstrated in the context of mono-mode quantum interference[172,173]. In these studies, it was shown that a nonlinear quantum interferometer can be built by using two nonlinear crystals, and that by feeding the idler wave emerging from the first nonlinear crystal into the second crystal, one can induce coherence between the two signal beams emitted by the crystal without inducing emission (that is, with amplification of the idler wave).

In these experiments, a laser beam is split into two beams that pump coherently a pair of nonlinear crystals that are phase matched for non-degenerate down-conversion. The signal and idler waves emitted through

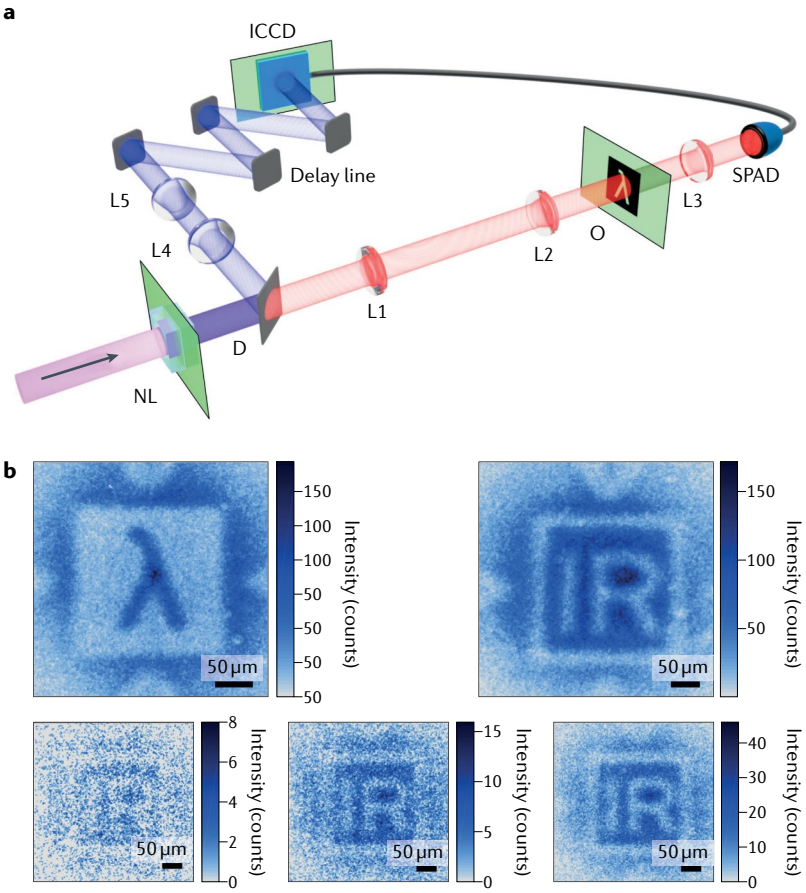


Fig. 5 | **Non-degenerate quantum ghost imaging. a** | Model of the experimental setup for non-degenerate quantum ghost imaging. The non-degenerate signal and idler beams generated in a barium borate crystal cut for type I phase matching are separated at the dichroic mirror (D). The infrared idler photon interacts with the object and is detected by a non-spatially resolving single-photon avalanche diode (SPAD). The corresponding signal photons are detected by an intensified charge-coupled device (ICCD) camera. The ICCD camera is triggered by the arrival of a photon at the SPAD detector. **b** | Images of objects created by gold patterned onto a silicon wafer by electron beam lithography. Contrary to silicon, gold is non-transmissive at the idler wavelength of 1,550 nm. Both materials are non-transmissive at the signal wavelength of 460 nm. Ghost images of the object in the infrared are acquired. The three images in the bottom row are acquired with increasing number of photons. The colour bar represents the number of counts. L1–L5, lenses; NL, nonlinear crystal; O, imaging object. Panel **b** is reproduced with permission from REF.[163], OSA.

SPDC within the first crystal (NL1) are separated and the idler wave interacts with an object (FIG. 6).

After interaction with the object, the idler is then directed into the second crystal (NL2), and co-axially aligned with the spontaneous idler emanating from it. The signal wave at the output of NL2 is then separated from the idler waves that originate from either NL1 or NL2, and the signal waves from the pair of SPDC events, neither of which have interacted with the object, are combined at a beam splitter. In such conditions, the signal waves, even though they have not directly interacted with the object, will undergo interference dependant on the phase and transmission of the object as probed by the idler originating from NL1.

To understand this phenomenon, one can first remark that the superposition of the two idler waves generated in the two crystals makes it impossible to distinguish in which crystal an idler photon was created. This has the potential to induce coherence between the bi-photon states emitted by the two crystals. It can happen even without induced emission in the second crystal, which could be the consequence of an idler field at its input[173,174]. When the two signal waves are combined on a beam splitter, there is no way to distinguish from which crystal either of the signal or idler photons come from and interference patterns that appear are detectable directly on the intensities measured on the signal side. When an absorptive object is added between the two crystals on the idler beam path, some distinguishability is introduced and the interference visibility of the signal is reduced as the coherence is partially lost.

Using this method in the context of imaging, it was shown[170] that both intensity and phase objects can be imaged without having to detect the idler waves that have interacted with the object (note, however, that the object is still illuminated). They were able to show imaging of a phase object that is opaque to the wavelength of the detected signal photons (820 nm) when the object is probed by an idler wave at which it is transparent (1,515 nm) (FIG. 6). This capacity to image with undetected photons has an advantage over non-degenerate ghost imaging techniques owing to there being no requirement for a detector of any sort at the probe wavelength thereby overcoming constraints with regards to detector availability and detection efficiency within certain wavebands. A similar method has been applied to spectroscopy in which the spectrum of a sample in the infrared is obtained by detecting visible photons only[175]. The method may also find application in quantifying correlations between two beams without having to detect each of the two beams[176]. However, the fact that such a technique involves interferometry makes it more complex to implement and more susceptible to mechanical and thermal noise.

Interaction-free measurement. Previous methods have detailed the cases in which photons interacted with the object of interest, using either the time or position of the photon detection and of its entangled partner to obtain information about the object that has been imaged. However, it is also possible to acquire information regarding an object without a photon having interacted with it by performing interaction-free measurements.

The concept of interaction-free measurement was introduced in 1993 (REFS[177,178]). In this experiment, a Mach–Zehnder interferometer is set up with the two detectors D1 and D2 that are positioned for constructive and destructive interference, respectively. Any single photons injected into the system should therefore be detected at D1 and none at detector D2. A perfect absorbing object placed into one of the arms would be transmitting a single photon through the system. Should a single photon be detected at detector D2, then there must have been an object in one arm of the interferometer. However, as a single photon was detected it may not have interacted with the object and passed through the unobstructed arm. Note that despite its name, interaction-free measurement is not truly interaction free as there will be a coupling in any

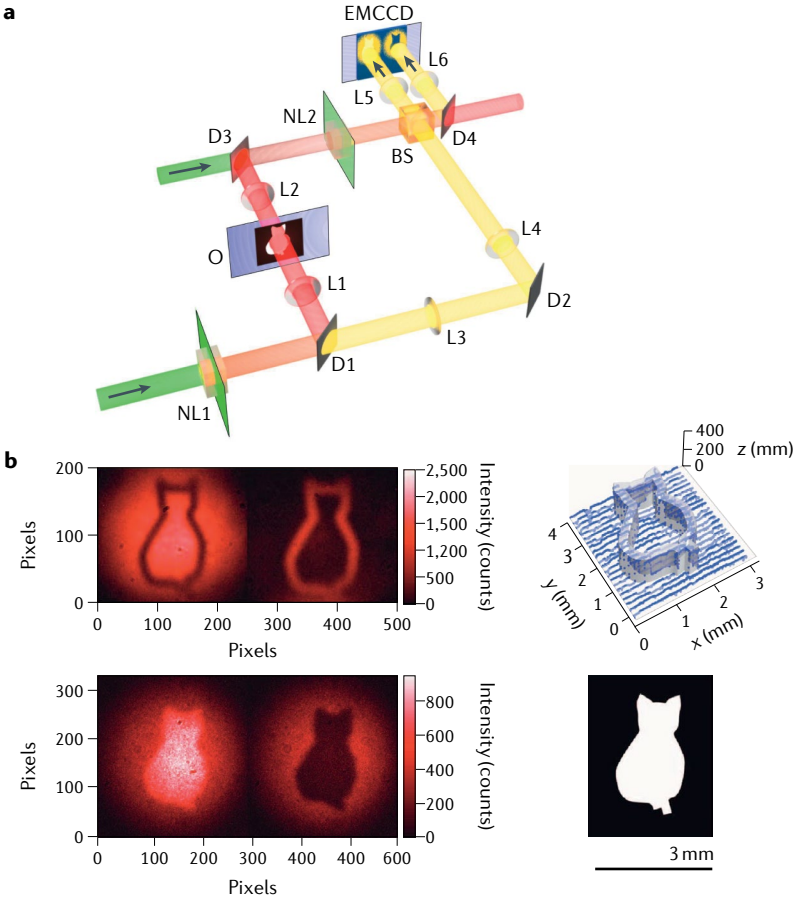


Fig. 6 | **Quantum imaging with undetected photons. a** | Model of the experimental setup used to perform imaging without detecting the photons that interact with the object. A nonlinear interferometer is built by seeding the idler produced in the first nonlinear crystal (NL1) into a second nonlinear crystal NL2 and recombining the signal waves emitted by the two crystals on a beam splitter (BS). Owing to quantum interference between the two photons' wavefunctions emitted by the crystals, an interference figure appears within the signal intensities outputting the BS. If one adds an object between NL1 and NL2 in the idler beam, one affects the whole wavefunction and as a consequence the interference of the signal waves after the BS. One can in such conditions acquire an image of the object without having to detect the photons that have interacted with it. **b** | Images of an object obtained by detection of the interference of signal photons that have not interacted with it. The idler photons that have interacted with the object remain undetected. The top row represents the imaging of a phase object, the blue dots on the right plot correspond to a scan of the object etch depth and the bottom row represents the imaging of a transmissive object. The colour bar represents the number of counts. EMCCD, electron-multiplying charge-coupled device camera; D1–D4, dichroic mirrors; L1–L6, lenses; O, imaging object. Panel **b** is reproduced from REF.[170], Springer Nature Limited.

quantum-mechanical or wave-like description of the system[179–181].

In their striking thought experiment, often referred to as the Elitzur–Vaidman bomb tester, Elitzur and Vaidman used a bomb that would explode should it detect a photon as the object in one of the arms[177,178]. Should the Mach–Zehnder interferometer be balanced, then the success rate of finding the bomb without exploding it would be $\eta = 1/3$. This rate is also referred to as the interaction-free efficiency. However, for an asymptotically fully unbalanced interferometer, this efficiency can tend towards $\eta = 1/2$. Although for a standard interferometer this is the efficiency limit, it is possible to use a different type of interferometer to implement an optical analogue of the quantum Zeno effect[182] that allows a lossless system to be created with respect to the bombs, with an efficiency tending to $\eta = 1$. This was proposed in 1995 (REF.[183]) and it is based on the principle of performing successive weak measurements of the presence of the object.

The Elitzur–Vaidman interaction-free detection scheme was experimentally demonstrated by using a SPDC source of photon pairs, one of which enters an unbalanced Michelson interferometer whereas the other is detected to herald the presence of the down-converted photon pairs, leading to efficiencies close to $\eta = 1/2$ (REF.[183]). The quantum Zeno effect version was realized within a Fabry–Perot interferometer with a detection efficiency of 85%[184] and through a looped polarization-sensitive interferometer[179,185] with an efficiency of 73%.

Interaction-free scanned imaging has been performed[186] by scanning an object at a focus point of the beam within a polarization-sensitive Mach–Zehnder interferometer for the purposes of determining the dimensions of objects placed in one of the arms. In this experiment, a number of objects were scanned across the beam and the dimensions of said objects, of the order 10–100 µm, were accurately assessed. Recently, the interaction-free imaging of a structured object has been demonstrated using a quantum ghost imaging setup[187].

Outlook

As we have seen, quantum imaging has allowed quantum-mechanic phenomena to be tested and also enabled the development of new imaging protocols. Quantum imaging has also contributed to the emergence of new 'quantum-inspired' imaging protocols such as classical ghost imaging[154] or single-pixel camera implementations[159]. The emergence of new, more efficient photon-counting cameras — such as superconducting nanowires, single-photon detector arrays, very low-noise back-side-illuminated CMOS technologies, and new sources such as quantum dots and exotic nonlinear sources, which are currently under development — gives confidence regarding the future of quantum imaging schemes that should soon reach the performance levels required to deliver practical implementations. An example would be the development of sources of pairs of photons with extremely different wavelengths, thereby overcoming the lack of high-fidelity detectors at exotic wavelengths. Such sources could be used advantageously for either imaging without a detection scheme or a non-degenerate ghost imaging scheme in which an interferometric scheme would be difficult to implement. The developments that are currently ongoing have the potential to bring efficient imaging techniques and sensors to new domains of optics. Further to the potential applications of quantum imaging schemes, it has been demonstrated that imaging schemes at conventional wavelengths can be improved by using quantum sources, either by enhancing the resolution or decreasing the noise of images[52,138]. Future developments in quantum imaging could come through new approaches

Weak measurements
Measurements for which the measuring device is weakly coupled with the measured system. Weak measurements disturb the measured system less than conventional projective measurements.

such as quantum image processing[188] or through exploiting quantum correlations via different methods such as correlation plenoptic imaging[189]. Moreover, early demonstrations of the principle of quantum imaging techniques are now increasingly transforming into real-world practical implementations from which new imaging technologies may emerge. Finally, the high dimensionality accessible in the space domain through imaging together with the increase in the efficiency of quantum imaging protocols should in the future enable quantum information protocols based on imaging that will allow the design of 'inherently efficient' information protocols in high dimensions. At a stage at which worldwide research funding bodies are pushing for the development of real-world quantum technologies through the so-called second quantum revolution[190–192], we believe that quantum imaging will have an important role to play in this movement.

Published online 28 May 2019

1. Franken, P. A., Hill, A. E., Peters, C. W. & Weinreich, G. Generation of optical harmonics. *Phys. Rev. Lett.* **7**, 118–119 (1961).
2. Wang, C. C. & Racette, G. W. Measurement of parametric gain accompanying optical difference frequency generation. *Appl. Phys. Lett.* **6**, 169–171 (1965).
3. Giordmaine, J. & Miller, R. C. Tunable coherent parametric oscillation in $LiNbO_3$ at optical frequencies. *Phys. Rev. Lett.* **14**, 973–976 (1965).
4. Kocher, C. A. & Commins, E. D. Polarization correlation of photons emitted in an atomic cascade. *Phys. Rev. Lett.* **18**, 575–577 (1967).
5. Freedman, S. J. & Clauser, J. F. Experimental test of local hidden-variable theories. *Phys. Rev. Lett.* **28**, 938–941 (1972).
6. Aspect, A., Dalibard, J. & Roger, G. Experimental test of Bell's inequalities using time-varying analyzers. *Phys. Rev. Lett.* **49**, 1804–1807 (1982).
7. Louisell, W., Yariv, A. & Siegman, A. Quantum fluctuations and noise in parametric processes. I. *Phys. Rev.* **124**, 1646–1654 (1961).
8. Haus, H. A. & Mullen, J. Quantum noise in linear amplifiers. *Phys. Rev.* **128**, 2407–2413 (1962).
9. Klyshko, D. Scattering of light in a medium with nonlinear polarizability. *Sov. Phys. JETP* **28**, 522–526 (1969).
10. Harris, S., Oshman, M. & Byer, R. Observation of tunable optical parametric fluorescence. *Phys. Rev. Lett.* **18**, 732–734 (1967).
11. Akhmanov, S., Fadeev, V., Khokhlov, R. & Chunaev, O. Quantum noise in parametric light amplifiers. *ZhETF Pisma Redaktsiiu* **6**, 575–578 (1967).
12. Burnham, D. C. & Weinberg, D. L. Observation of simultaneity in parametric production of optical photon pairs. *Phys. Rev. Lett.* **25**, 84–87 (1970).
13. Ghosh, R. & Mandel, L. Observation of nonclassical effects in the interference of two photons. *Phys. Rev. Lett.* **59**, 1903–1905 (1987).
14. Ou, Z. & Mandel, L. Violation of Bell's inequality and classical probability in a two-photon correlation experiment. *Phys. Rev. Lett.* **61**, 50–53 (1988).
15. Kwiat, P. G. et al. New high-intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett.* **75**, 4337–4341 (1995).
16. Shih, Y. Entangled biphoton source-property and preparation. *Rep. Prog. Phys.* **66**, 1009–1044 (2003).
17. Genovese, M. Research on hidden variable theories: a review of recent progresses. *Phys. Rep.* **413**, 319–396 (2005).
18. Hong, C.-K., Ou, Z.-Y. & Mandel, L. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.* **59**, 2044–2046 (1987).
19. Kim, Y.-H., Yu, R., Kulik, S. P., Shih, Y. & Scully, M. O. Delayed "choice" quantum eraser. *Phys. Rev. Lett.* **84**, 1–5 (2000).
20. Ma, X.-S., Kofler, J. & Zeilinger, A. Delayed-choice gedanken experiments and their realizations. *Rev. Mod. Phys.* **88**, 015005 (2016).
21. Ren, J.-G. et al. Ground-to-satellite quantum teleportation. *Nature* **549**, 70–73 (2017).
22. O'Brien, J. L., Pryde, G. J., White, A. G., Ralph, T. C. & Branning, D. Demonstration of an all-optical quantum controlled-not gate. *Nature* **426**, 264–267 (2003).
23. Qiang, X. et al. Large-scale silicon quantum photonics implementing arbitrary two-qubit processing. *Nat. Photon.* **12**, 534–539 (2018).
24. Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photon.* **8**, 595–604 (2014).
25. Shalm, L. K. et al. Strong loophole-free test of local realism. *Phys. Rev. Lett.* **115**, 250402 (2015).
26. Giustina, M. et al. Significant-loophole-free test of Bell's theorem with entangled photons. *Phys. Rev. Lett.* **115**, 250401 (2015).
27. Howell, J. C., Bennink, R. S., Bentley, S. J. & Boyd, R. Realization of the Einstein–Podolsky–Rosen paradox using momentum-and position-entangled photons from spontaneous parametric down conversion. *Phys. Rev. Lett.* **92**, 210403 (2004).
28. Einstein, A., Podolsky, B. & Rosen, N. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **47**, 777–780 (1935).
29. Klyshko, D. *Photons and Nonlinear Optics* (CRC Press, 1988).
30. Jost, B. M., Sergienko, A. V., Abouraddy, A. F., Saleh, B. E. & Teich, M. C. Spatial correlations of spontaneously down-converted photon pairs detected with a single-photon-sensitive CCD camera. *Opt. Express* **3**, 81–88 (1998).
31. Basden, A. G., Haniff, C. & Mackay, C. Photon counting strategies with low-light-level CCDs. *Mon. Not. R. Astron. Soc.* **345**, 985–991 (2003).
32. Rarity, J. & Tapster, P. Experimental violation of Bell's inequality based on phase and momentum. *Phys. Rev. Lett.* **64**, 2495–2498 (1990).
33. Pittman, T., Shih, Y., Strekalov, D. & Sergienko, A. Optical imaging by means of two-photon quantum entanglement. *Phys. Rev. A* **52**, R3429–R3432 (1995).
34. Strekalov, D. V., Sergienko, A. V., Klyshko, D. N. & Shih, Y. H. Observation of two-photon ghost interference and diffraction. *Phys. Rev. Lett.* **74**, 3600–3603 (1995).
35. Devaux, F. & Lantz, E. Spatial and temporal properties of parametric fluorescence around degeneracy in a type I LBO crystal. *Eur. Phys. J. D* **8**, 117–124 (2000).
36. Couteau, C. Spontaneous parametric down-conversion. *Contemp. Phys.* **59**, 291–304 (2018).
37. Boyd, R. W. *Nonlinear Optics* (Elsevier, 2003).
38. Jakeman, E. & Walker, J. Analysis of a method for the generation of light with sub-poissonian photon statistics. *Opt. Commun.* **55**, 219–222 (1985).
39. Jakeman, E. & Rarity, J. The use of pair production processes to reduce quantum noise in transmission measurements. *Opt. Commun.* **59**, 219–223 (1986).
40. Rarity, J., Tapster, P. & Jakeman, E. Observation of sub-Poissonian light in parametric downconversion. *Opt. Commun.* **62**, 201–206 (1987).
41. Heidmann, A. et al. Observation of quantum noise reduction on twin laser beams. *Phys. Rev. Lett.* **59**, 2555–2557 (1987).
42. Nabors, C. & Shelby, R. Two-color squeezing and sub-shot-noise signal recovery in doubly resonant optical parametric oscillators. *Phys. Rev. A* **42**, 556–559 (1990).
43. Tapster, P., Seward, S. & Rarity, J. Sub-shot-noise measurement of modulated absorption using parametric down-conversion. *Phys. Rev. A* **44**, 3266–3269 (1991).
44. Ribeiro, P. S. & C. Schwob, A. Sub-shot-noise high-sensitivity spectroscopy with optical parametric oscillator twin beams. *Opt. Lett.* **22**, 1893–1895 (1997).
45. Bondani, M., Allevi, A., Zambra, G., Paris, M. G. & Andreoni, A. Sub-shot-noise photon-number correlation in a mesoscopic twin beam of light. *Phys. Rev. A* **76**, 013833 (2007).
46. Iskhakov, T., Chekhova, M. V. & Leuchs, G. Generation and direct detection of broadband mesoscopic polarization-squeezed vacuum. *Phys. Rev. Lett.* **102**, 183602 (2009).
47. Jedrkiewicz, O. et al. Detection of sub-shot-noise spatial correlation in high-gain parametric down conversion. *Phys. Rev. Lett.* **93**, 243601 (2004).
48. Jedrkiewicz, O. et al. Quantum spatial correlations in high-gain parametric down-conversion measured by means of a CCD camera. *J. Mod. Opt.* **53**, 575–595 (2006).
49. Blanchet, J.-L., Devaux, F., Furfaro, L. & Lantz, E. Measurement of sub-shot-noise correlations of spatial fluctuations in the photon-counting regime. *Phys. Rev. Lett.* **101**, 233604 (2008).
50. Brambilla, E., Caspani, L., Jedrkiewicz, O., Lugiato, L. & Gatti, A. High-sensitivity imaging with multi-mode twin beams. *Phys. Rev. A* **77**, 053807 (2008).
51. Brida, G. et al. Measurement of sub-shot-noise spatial correlations without background subtraction. *Phys. Rev. Lett.* **102**, 213602 (2009).
52. Brida, G., Genovese, M. & Berchera, I. R. Experimental realization of sub-shot-noise quantum imaging. *Nat. Photon.* **4**, 227–230 (2010).
53. Jerram, P. et al. in *Proceedings of SPIE* Vol. 4306 (eds Sampat, N. et al.) 178–187 (International Society for Optics and Photonics, 2001).
54. Lantz, E., Blanchet, J.-L., Furfaro, L. & Devaux, F. Multi-imaging and Bayesian estimation for photon counting with EMCCDs. *Mon. Not. R. Astron. Soc.* **386**, 2262–2270 (2008).
55. Zhang, L., Neves, L., Lundeen, J. S. & Walmsley, I. A. A characterization of the single-photon sensitivity of an electron multiplying charge-coupled device. *J. Phys. B* **42**, 114011 (2009).
56. Blanchet, J.-L., Devaux, F., Furfaro, L. & Lantz, E. Purely spatial coincidences of twin photons in parametric spontaneous down-conversion. *Phys. Rev. A* **81**, 043825 (2010).
57. Toninelli, E. et al. Sub-shot-noise shadow sensing with quantum correlations. *Opt. Express* **25**, 21826–21840 (2017).
58. Reichert, M., Defienne, H., Sun, X. & Fleischer, J. W. Biphoton transmission through non-unitary objects. *J. Opt.* **19**, 044004 (2017).
59. Reichert, M., Defienne, H. & Fleischer, J. W. Massively parallel coincidence counting of high-dimensional entangled states. *Sci. Rep.* **8**, 7925 (2018).
60. Devaux, F., Mougin-Sisini, J., Moreau, P.-A. & Lantz, E. Towards the evidence of a purely spatial Einstein–Podolsky–Rosen paradox in images: measurement scheme and first experimental results. *Eur. Phys. J. D* **66**, 192 (2012).
61. Moreau, P.-A., Mougin-Sisini, J., Devaux, F. & Lantz, E. Realization of the purely spatial Einstein–Podolsky–Rosen paradox in full-field images of spontaneous parametric down-conversion. *Phys. Rev. A* **86**, 010101 (2012).
62. Edgar, M. P. et al. Imaging high-dimensional spatial entanglement with a camera. *Nat. Commun.* **3**, 984 (2012).
63. Moreau, P.-A., Devaux, F. & Lantz, E. Einstein–Podolsky–Rosen paradox in twin images. *Phys. Rev. Lett.* **113**, 160401 (2014).
64. Lantz, E., Denis, S., Moreau, P.-A. & Devaux, F. Einstein–Podolsky–Rosen paradox in single pairs of images. *Opt. Express* **23**, 26472–26478 (2015).
65. Takhar, D. et al. in *Proceedings of SPIE* Vol. 6065 (eds Bouman, C. A., Miller, E. L. & Pollak, I.) 606509 (International Society for Optics and Photonics, 2006).
66. Duarte, M. F. et al. Single-pixel imaging via compressive sampling. *IEEE Signal Process. Mag.* **25**, 83–91 (2008).
67. Howland, G. A. & Howell, J. C. Efficient high-dimensional entanglement imaging with a compressive-sensing double-pixel camera. *Phys. Rev. X* **3**, 011013 (2013).
68. Schneeloch, J., Dixon, P. B., Howland, G. A., Broadbent, C. J. & Howell, J. C. Violation of continuous-variable Einstein–Podolsky–Rosen steering with discrete measurements. *Phys. Rev. Lett.* **110**, 130407 (2013).

69. Lampton, M. The microchannel image intensifier. *Sci. Am.* **245**, 62–71 (1981).
70. Abouraddy, A. F., Nasr, M., Saleh, B. E., Sergienko, A. V. & Teich, M. C. Demonstration of the complementarity of one-and two-photon interference. *Phys. Rev. A* **63**, 063803 (2001).
71. Pires, H. D. L., Monken, C. H. & van Exter, M. P. Direct measurement of transverse-mode entanglement in two-photon states. *Phys. Rev. A* **80**, 022307 (2009).
72. Aspden, R. S., Tasca, D. S., Boyd, R. W. & Padgett, M. J. EPR-based ghost imaging using a single-photon-sensitive camera. *New J. Phys.* **15**, 073032 (2013).
73. Fickler, R., Krenn, M., Lapkiewicz, R., Ramelow, S. & Zeilinger, A. Real-time imaging of quantum entanglement. *Sci. Rep.* **3**, 1914 (2013).
74. Jachura, M. & Chrapkiewicz, R. Shot-by-shot imaging of Hong–Ou–Mandel interference with an intensified sCMOS camera. *Opt. Lett.* **40**, 1540–1543 (2015).
75. Chrapkiewicz, R., Wasilewski, W. & Banaszek, K. High-fidelity spatially resolved multiphoton counting for quantum imaging applications. *Opt. Lett.* **39**, 5090–5093 (2014).
76. Chrapkiewicz, R., Jachura, M., Banaszek, K. & Wasilewski, W. Hologram of a single photon. *Nat. Photon.* **10**, 576–579 (2016).
77. Jachura, M., Chrapkiewicz, R., Demkowicz-Dobrzański, R., Wasilewski, W. & Banaszek, K. Mode engineering for realistic quantum-enhanced interferometry. *Nat. Commun.* **7**, 11411 (2016).
78. Parniak, M. et al. Wavevector multiplexed atomic quantum memory via spatially-resolved single-photon detection. *Nat. Commun.* **8**, 2140 (2017).
79. Guerrieri, F., Tisa, S., Tosi, A. & Zappa, F. Two-dimensional spad imaging camera for photon counting. *IEEE Photon. J.* **2**, 759–774 (2010).
80. Guerrieri, F. et al. Sub-Rayleigh imaging via *N*-photon detection. *Phys. Rev. Lett.* **105**, 163602 (2010).
81. Veerappan, C. et al. A 160×128 single-photon image sensor with on-pixel 55ps 10b time-to-digital converter. In *Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2011 IEEE International* 312–314 (IEEE, 2011).
82. Gariepy, G. et al. Single-photon sensitive light-in-fight imaging. *Nat. Commun.* **6**, 6021 (2015).
83. Miki, S., Yamashita, T., Wang, Z. & Terai, H. A 64-pixel nbtin superconducting nanowire single-photon detector array for spatially resolved photon detection. *Opt. Express* **22**, 7811–7820 (2014).
84. Allman, M. S. et al. A near-infrared 64-pixel superconducting nanowire single photon detector array with integrated multiplexed readout. *Appl. Phys. Lett.* **106**, 192601 (2015).
85. Ma, J., Masoodian, S., Starkey, D. A. & Fossum, E. R. Photon-number-resolving megapixel image sensor at room temperature without avalanche gain. *Optica* **4**, 1474–1481 (2017).
86. Andersen, U. L., Gehring, T., Marquardt, C. & Leuchs, G. 30 years of squeezed light generation. *Phys. Scr.* **91**, 053001 (2016).
87. Schnabel, R. Squeezed states of light and their applications in laser interferometers. *Phys. Rep.* **684**, 1–51 (2017).
88. Mandel, L. Physical significance of operators in quantum optics. *Phys. Rev.* **136**, B1221 (1964).
89. Stoler, D. Photon antibunching and possible ways to observe it. *Phys. Rev. Lett.* **33**, 1397–1400 (1974).
90. Hollenhorst, J. N. Quantum limits on resonant-mass gravitational-radiation detectors. *Phys. Rev. D* **19**, 1669–1679 (1979).
91. Caves, C. M. Quantum-mechanical noise in an interferometer. *Phys. Rev. D* **23**, 1693–1708 (1981).
92. Snyder, J. J., Giacobino, E., Fabre, C., Heidmann, A. & Ducloy, M. Sub-shot-noise measurements using the beat note between quantum-correlated photon beams. *J. Opt. Soc. Am. B* **7**, 2132–2136 (1990).
93. Giovannetti, V., Lloyd, S. & Maccone, L. Quantum-enhanced measurements: beating the standard quantum limit. *Science* **306**, 1330–1336 (2004).
94. Degen, C. L., Reinhard, F. & Cappellaro, P. Quantum sensing. *Rev. Mod. Phys.* **89**, 035002 (2017).
95. Caves, C. M., Thorne, K. S., Drever, R. W., Sandberg, V. D. & Zimmermann, M. On the measurement of a weak classical force coupled to a quantum-mechanical oscillator. I. Issues of principle. *Rev. Mod. Phys.* **52**, 341–392 (1980).
96. Abadie, J. et al. A gravitational wave observatory operating beyond the quantum shot-noise limit. *Nat. Phys.* **7**, 962–965 (2011).
97. Aasi, J. et al. Enhanced sensitivity of the ligo gravitational wave detector by using squeezed states of light. *Nat. Photon.* **7**, 613–619 (2013).
98. Taylor, M. A. & Bowen, W. P. Quantum metrology and its application in biology. *Phys. Rep.* **615**, 1–59 (2016).
99. Wolfgramm, F., Vitelli, C., Beduini, F. A., Godbout, N. & Mitchell, M. W. Entanglement-enhanced probing of a delicate material system. *Nat. Photon.* **7**, 28–32 (2013).
100. Davidovich, L. Sub-poissonian processes in quantum optics. *Rev. Mod. Phys.* **68**, 127–173 (1996).
101. Xiao, M., Wu, L.-A. & Kimble, H. Detection of amplitude modulation with squeezed light for sensitivity beyond the shot-noise limit. *Opt. Lett.* **13**, 476–478 (1988).
102. Vahlbruch, H., Mehmet, M., Danzmann, K. & Schnabel, R. Detection of 15 dB squeezed states of light and their application for the absolute calibration of photoelectric quantum efficiency. *Phys. Rev. Lett.* **117**, 110801 (2016).
103. Kolobov, M. I. & Fabre, C. Quantum limits on optical resolution. *Phys. Rev. Lett.* **85**, 3789 (2000).
104. Treps, N. et al. Surpassing the standard quantum limit for optical imaging using nonclassical multimode light. *Phys. Rev. Lett.* **88**, 203601 (2002).
105. Treps, N. et al. A quantum laser pointer. *Science* **301**, 940–943 (2003).
106. Boyer, V., Marino, A. M., Pooser, R. C. & Lett, P. D. Entangled images from four-wave mixing. *Science* **321**, 544–547 (2008).
107. Lassen, M., Leuchs, G. & Andersen, U. L. Continuous variable entanglement and squeezing of orbital angular momentum states. *Phys. Rev. Lett.* **102**, 163602 (2009).
108. Wagner, K. et al. Entangling the spatial properties of laser beams. *Science* **321**, 541–543 (2008).
109. Sabines-Chesterking, J. et al. Sub-shot-noise transmission measurement enabled by active feed-forward of heralded single photons. *Phys. Rev. Appl.* **8**, 014016 (2017).
110. Samantaray, N., Ruo-Berchera, I., Meda, A. & Genovese, M. Realization of the first sub-shot-noise wide field microscope. *Light Sci. Appl.* **6**, e17005 (2017).
111. Moreau, P.-A. et al. Demonstrating an absolute quantum advantage in direct absorption measurement. *Sci. Rep.* **7**, 6256 (2017).
112. Losero, E., Ruo-Berchera, I., Meda, A., Avella, A. & Genovese, M. Unbiased estimation of an optical loss at the ultimate quantum limit with twin-beams. *Sci. Rep.* **8**, 7431 (2018).
113. Iskhakov, T. S. et al. Heralded source of bright multi-mode mesoscopic sub-Poissonian light. *Opt. Lett.* **41**, 2149–2152 (2016).
114. Nagata, T. et al. Beating the standard quantum limit with four-entangled photons. *Science* **316**, 726–729 (2007).
115. Jacobson, J., Björk, G., Chuang, I. & Yamamoto, Y. Photonic de Broglie waves. *Phys. Rev. Lett.* **74**, 4835–4838 (1995).
116. Fonseca, E., Monken, C. & Pádua, S. Measurement of the de Broglie wavelength of a multiphoton wave packet. *Phys. Rev. Lett.* **82**, 2868–2871 (1999).
117. Ono, T., Okamoto, R. & Takeuchi, S. An entanglement-enhanced microscope. *Nat. Commun.* **4**, 3426 (2013).
118. Yurke, B., McCall, S. L. & Klauder, J. R. SU(2) and SU(1,1) interferometers. *Phys. Rev. A* **33**, 4033–4054 (1986).
119. Leonhardt, U. Quantum statistics of a two-mode SU(1,1) interferometer. *Phys. Rev. A* **49**, 1231–1242 (1994).
120. Plick, W. N., Dowling, J. P. & Agarwal, G. S. Coherent-light-boosted, sub-shot noise, quantum interferometry. *New J. Phys.* **12**, 083014 (2010).
121. Marino, A. M., Trejo, N. C. & Lett, P. D. Effect of losses on the performance of an SU(1,1) interferometer. *Phys. Rev. A* **86**, 023844 (2012).
122. Ou, Z. Enhancement of the phase-measurement sensitivity beyond the standard quantum limit by a nonlinear interferometer. *Phys. Rev. A* **85**, 023815 (2012).
123. Jing, J., Liu, C., Zhou, Z., Ou, Z. & Zhang, W. Realization of a nonlinear interferometer with parametric amplifiers. *Appl. Phys. Lett.* **99**, 011110 (2011).
124. Hudelist, F. et al. Quantum metrology with parametric amplifier-based photon correlation interferometers. *Nat. Commun.* **5**, 3049 (2014).
125. Manceau, M., Leuchs, G., Khalili, F. & Chekhova, M. Detection loss tolerant supersensitive phase measurement with an SU(1,1) interferometer. *Phys. Rev. Lett.* **119**, 223604 (2017).
126. Morris, P. A., Aspden, R. S., Bell, J. E., Boyd, R. W. & Padgett, M. J. Imaging with a small number of photons. *Nat. Commun.* **6**, 5913 (2015).
127. Lanzagorta, M. Quantum radar. *Synth. Lect. Quantum Comput.* **3**, 1–139 (2011).
128. Lloyd, S. Enhanced sensitivity of photodetection via quantum illumination. *Science* **321**, 1463–1465 (2008).
129. Giovannetti, V., Lloyd, S., Maccone, L. & Shapiro, J. H. Sub-Rayleigh-diffraction-bound quantum imaging. *Phys. Rev. A* **79**, 013827 (2009).
130. Mouradian, S., Wong, F. N. & Shapiro, J. H. Achieving sub-Rayleigh resolution via thresholding. *Opt. Express* **19**, 5480–5488 (2011).
131. Schwartz, O. & Oron, D. Improved resolution in fluorescence microscopy using quantum correlations. *Phys. Rev. A* **85**, 033812 (2012).
132. Schwartz, O. et al. Superresolution microscopy with quantum emitters. *Nano Lett.* **13**, 5832–5836 (2013).
133. Israel, Y., Tenne, R., Oron, D. & Silberberg, Y. Quantum correlation enhanced super-resolution localization microscopy enabled by a fibre bundle camera. *Nat. Commun.* **8**, 14786 (2017).
134. Monticone, D. G. et al. Beating the Abbe diffraction limit in confocal microscopy via nonclassical photon statistics. *Phys. Rev. Lett.* **113**, 143602 (2014).
135. Classen, A., von Zanthier, J., Scully, M. O. & Agarwal, G. S. Superresolution via structured illumination quantum correlation microscopy. *Optica* **4**, 580–587 (2017).
136. Tenne, R. et al. Super-resolution enhancement by quantum image scanning microscopy. *Nat. Photon.* **13**, 116–122 (2019).
137. Tsang, M., Nair, R. & Lu, X.-M. Quantum theory of superresolution for two incoherent optical point sources. *Phys. Rev. X* **6**, 031033 (2016).
138. Toninelli, E. et al. Resolution-enhanced quantum imaging by centroid estimation of biphotons. *Optica* **6**, 347–353 (2019).
139. Tsang, M. Quantum imaging beyond the diffraction limit by optical centroid measurements. *Phys. Rev. Lett.* **102**, 253601 (2009).
140. Boto, A. N. et al. Quantum interferometric optical lithography: exploiting entanglement to beat the diffraction limit. *Phys. Rev. Lett.* **85**, 2733–2736 (2000).
141. D'Angelo, M., Chekhova, M. V. & Shih, Y. Two-photon diffraction and quantum lithography. *Phys. Rev. Lett.* **87**, 013602 (2001).
142. Chang, H. J., Shin, H., O'Sullivan-Hale, M. N. & Boyd, R. W. Implementation of sub-Rayleigh-resolution lithography using an *N*-photon absorber. *J. Mod. Opt.* **53**, 2271–2277 (2006).
143. Shin, H., Chan, K. W. C., Chang, H. J. & Boyd, R. W. Quantum spatial superresolution by optical centroid measurements. *Phys. Rev. Lett.* **107**, 083603 (2011).
144. Rozema, L. A. et al. Scalable spatial superresolution using entangled photons. *Phys. Rev. Lett.* **112**, 223602 (2014).
145. Matthews, J. C. Scalable imaging of superresolution. *Physics* **7**, 59 (2014).
146. Thiel, C. et al. Quantum imaging with incoherent photons. *Phys. Rev. Lett.* **99**, 133603 (2007).
147. Oppel, S., Büttner, T., Kok, P. & von Zanthier, J. Superresolving multiphoton interferences with independent light sources. *Phys. Rev. Lett.* **109**, 233603 (2012).
148. Moreau, P.-A., Toninelli, E., Gregory, T. & Padgett, M. J. Ghost imaging using optical correlations. *Laser Photon. Rev.* **12**, 1700143 (2018).
149. Klyshko, D. N. A simple method of preparing pure states of an optical field, of implementing the Einstein–Podolsky–Rosen experiment, and of demonstrating the complementarity principle. *Sov. Phys. Uspekhi* **31**, 74–85 (1988).
150. Pittman, T. B. et al. Two-photon geometric optics. *Phys. Rev. A* **53**, 2804–2815 (1996).
151. Aspden, R. S. et al. Photon-sparse microscopy: visible light imaging using infrared illumination. *Optica* **2**, 1049–1052 (2015).
152. Bennink, R. S., Bentley, S. J. & Boyd, R. W. Two-photon coincidence imaging with a classical source. *Phys. Rev. Lett.* **89**, 113601 (2002).
153. Gatti, A., Brambilla, E., Bache, M. & Lugiato, L. A. Ghost imaging with thermal light: comparing entanglement and classicalcorrelation. *Phys. Rev. Lett.* **93**, 093602 (2004).
154. Gatti, A., Brambilla, E. & Lugiato, L. Quantum imaging. *Prog. Opt.* **51**, 251–348 (2008).
155. Moreau, P.-A. et al. Resolution limits of quantum ghost imaging. *Opt. Express* **26**, 7528–7536 (2018).
156. Brida, G. et al. Systematic analysis of signal-to-noise ratio in bipartite ghost imaging with classical and quantum light. *Phys. Rev. A* **83**, 063807 (2011).

157. Baleine, E., Dogariu, A. & Agarwal, G. S. Correlated imaging with shaped spatially partially coherent light. *Opt. Lett.* **31**, 2124–2126 (2006).
158. Pepe, F. V. et al. Diffraction-limited plenoptic imaging with correlated light. *Phys. Rev. Lett.* **119**, 243602 (2017).
159. Altmann, Y. et al. Quantum-inspired computational imaging. *Science* **361**, eaat2298 (2018).
160. Shapiro, J. H. & Boyd, R. W. The physics of ghost imaging. *Quantum Inf. Process.* **11**, 949–993 (2012).
161. Genovese, M. Real applications of quantum imaging. *J. Opt.* **18**, 073002 (2016).
162. Magana-Loaiza, O. S., Howland, G. A., Malik, M., Howell, J. C. & Boyd, R. W. Compressive object tracking using entangled photons. *Appl. Phys. Lett.* **102**, 231104 (2013).
163. Aspden, R. S. et al. Photon-sparse microscopy: visible light imaging using infrared illumination. *Optica* **2**, 1049–1052 (2015).
164. Jansen, C. et al. Terahertz imaging: applications and perspectives. *Appl. Opt.* **49**, E48–E57 (2010).
165. Rubin, M. H. & Shih, Y. Resolution of ghost imaging for nondegenerate spontaneous parametric down-conversion. *Phys. Rev. A* **78**, 033836 (2008).
166. Chan, K. W. C., O'Sullivan, M. N. & Boyd, R. W. Two-color ghost imaging. *Phys. Rev. A* **79**, 033808 (2009).
167. Denis, S., Moreau, P.-A., Devaux, F. & Lantz, E. Temporal ghost imaging with twin photons. *J. Opt.* **19**, 034002 (2017).
168. Schori, A., Borodin, D., Tamasaku, K. & Shwartz, S. Ghost imaging with paired X-ray photons. *Phys. Rev. A* **97**, 063804 (2018).
169. Khakimov, R. I. et al. Ghost imaging with atoms. *Nature* **540**, 100–103 (2016).
170. Lemos, G. B. et al. Quantum imaging with undetected photons. *Nature* **512**, 409–412 (2014).
171. Lahiri, M., Lapkiewicz, R., Lemos, G. B. & Zeilinger, A. Theory of quantum imaging with undetected photons. *Phys. Rev. A* **92**, 013832 (2015).
172. Zou, X. Y., Wang, L. J. & Mandel, L. Induced coherence and indistinguishability in optical interference. *Phys. Rev. Lett.* **67**, 318–321 (1991).
173. Wang, L. J., Zou, X. Y. & Mandel, L. Induced coherence without induced emission. *Phys. Rev. A* **44**, 4614–4622 (1991).
174. Ou, Z. Y., Wang, L. J., Zou, X.-B. & Mandel, L. Coherence in two-photon down-conversion induced by a laser. *Phys. Rev. A* **41**, 1597–1601 (1990).
175. Kalashnikov, D. A., Paterova, A. V., Kulik, S. P. & Krivitsky, L. A. Infrared spectroscopy with visible light. *Nat. Photon.* **10**, 98–101 (2016).
176. Hochrainer, A., Lahiri, M., Lapkiewicz, R., Lemos, G. B. & Zeilinger, A. Quantifying the momentum correlation between two light beams by detecting one. *Proc. Natl Acad. Sci. USA* **114**, 1508–1511 (2017).
177. Elitzur, A. C. & Vaidman, L. Quantum mechanical interaction-free measurements. *Found. Phys.* **23**, 987–997 (1993).
178. Vaidman, L. On the realization of interaction-free measurements. *Quantum Opt. J. Eur. Opt. Soc. B* **6**, 119–126 (1994).
179. Kwiat, P. G. Experimental and theoretical progress in interaction-free measurements. *Phys. Scr.* **1998**, 115–121 (1998).
180. Vaidman, L. Are interaction-free measurements interaction free? *Opt. Spectrosc.* **91**, 352–357 (2001).
181. Geszti, T. Interaction-free measurement and forward scattering. *Phys. Rev. A* **58**, 4206–4209 (1998).
182. Misra, B. & Sudarshan, E. C. G. The Zeno's paradox in quantum theory. *J. Math. Phys.* **18**, 756–763 (1977).
183. Kwiat, P., Weinfurter, H., Herzog, T., Zeilinger, A. & Kasevich, M. A. Interaction-free measurement. *Phys. Rev. Lett.* **74**, 4763–4766 (1995).
184. Tsegaye, T. et al. Efficient interaction-free measurements in a high-finesse interferometer. *Phys. Rev. A* **57**, 3987–3990 (1998).
185. Kwiat, P. G. et al. High-efficiency quantum interrogation measurements via the quantum Zeno effect. *Phys. Rev. Lett.* **83**, 4725–4728 (1999).
186. White, A. G., Mitchell, J. R., Nairz, O. & Kwiat, P. G. Interaction-free imaging. *Phys. Rev. A* **58**, 605–613 (1998).
187. Zhang, Y. et al. Interaction-free ghost-imaging of structured objects. *Opt. Express* **27**, 2212–2224 (2019).
188. Yan, F., Iliyasu, A. M. & Le, P. Q. Quantum image processing: a review of advances in its security technologies. *Int. J Quantum Inf.* **15**, 1730001 (2017).
189. Di Lena, F., Pepe, F., Garuccio, A. & D'Angelo, M. Correlation plenoptic imaging: an overview. *Appl. Sci.* **8**, 1958 (2018).
190. Schleich, W. P. et al. Quantum technology: from research to application. *Appl. Phys. B* **122**, 130 (2016).
191. Barnett, S. M. Journeys from quantum optics to quantum technology. *Prog. Quantum Electron.* **54**, 19–45 (2017).
192. Mohseni, M. Commercialize quantum technologies in five years. *Nature* **543**, 171–175 (2017).
193. Lantz, E., Moreau, P.-A. & Devaux, F. Optimizing the signal-to-noise ratio in the measurement of photon pairs with detector arrays. *Phys. Rev. A* **90**, 063811 (2014).
194. Tasca, D. S., Edgar, M. P., Izdebski, F., Buller, G. S. & Padgett, M. J. Optimizing the use of detector arrays for measuring intensity correlations of photon pairs. *Phys. Rev. A* **88**, 013816 (2013).

Acknowledgements
This work was funded by the UK Engineering and Physical Sciences Research Council (EPSRC; QuantIC EP/M01326X/1) and the European Research Council (TWISTS, 340507, grant no. 192382). P.-A.M. acknowledges the support from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie fellowship grant agreement no. 706410, of the Leverhulme Trust through the Research Project Grant ECF-2018-634 and of the Lord Kelvin/Adam Smith Leadership Fellowship scheme. E.T. acknowledges the financial support from the EPSRC Centre for Doctoral Training Intelligent Sensing and Measurement (EP/L016753/1). T.G. acknowledges the financial support from the EPSRC (EP/N509668/1) and the Professor Jim Gatheral quantum technology studentship.

Author contributions
P.-A.M. and M.J.P. made substantial contributions to discussions of the content. P.-A.M., T.G. and M.J.P. researched data for the article. P.-A.M., E.T., T.G. and M.J.P. wrote the article and reviewed and/or edited the manuscript before submission.

Competing interests
The authors declare no competing interests.

nature COMMUNICATIONS

ARTICLE

Received 11 Apr 2013 | Accepted 9 Aug 2013 | Published 12 Sep 2013

DOI: 10.1038/ncomms3426

An entanglement-enhanced microscope

Takafumi Ono[1,2], Ryo Okamoto[1,2] & Shigeki Takeuchi[1,2]

Among the applications of optical phase measurement, the differential interference contrast microscope is widely used for the evaluation of opaque materials or biological tissues. However, the signal-to-noise ratio for a given light intensity is limited by the standard quantum limit, which is critical for measurements where the probe light intensity is limited to avoid damaging the sample. The standard quantum limit can only be beaten by using N quantum correlated particles, with an improvement factor of $\sqrt{N}$. Here we report the demonstration of an entanglement-enhanced microscope, which is a confocal-type differential interference contrast microscope where an entangled photon pair ($N=2$) source is used for illumination. An image of a Q shape carved in relief on the glass surface is obtained with better visibility than with a classical light source. The signal-to-noise ratio is 1.35 ± 0.12 times better than that limited by the standard quantum limit.

[1] Research Institute for Electronic Science, Hokkaido University, N20W10, Kita-Ward Sapporo 001 0020, Japan. [2] The Institute of Scientific and Industrial Research, Osaka University, Mihogaoka 8-1, Ibaraki, Osaka 567 0047, Japan. Correspondence and requests for materials should be addressed to S.T. (email: takeuchi@es.hokudai.ac.jp).

Quantum metrology involves using quantum mechanics to realize more precise measurements than those that can be achieved classically[1]. The canonical example uses entanglement of N particles to measure a phase with a precision $\Delta\phi = 1/N$, known as the Heisenberg limit. Such a measurement outperforms the $\Delta\phi = 1/\sqrt{N}$ precision limit possible with N unentangled particles—the standard quantum limit (SQL). Progress has been made with trapped ions[2–4] and atoms[5], whereas high-precision optical phase measurements have many important applications, including microscopy, gravity wave detection, measurements of material properties, and medical and biological sensing. Recently, the SQL has been beaten with two photons[6–10] and four photons[11–13].

Perhaps the next natural step is to demonstrate entanglement-enhanced metrology[14–16]. Among the applications of optical phase measurement, microscopy is essential in broad areas of science from physics to biology. The differential interference contrast microscope (DIM)[17] is widely used for the evaluation of opaque materials or the label-free sensing of biological tissues[18]. For instance, the growth of ice crystals has recently been observed with a single molecular step resolution using a laser confocal microscope (LCM) combined with a DIM[19]. The depth resolution of such measurements is determined by the signal-to-noise ratio (SNR) of the measurement, and the SNR is in principle limited by the SQL. In the advanced measurements using DIM, the intensity of the probe light, focused onto a tiny area of $\sim 10^{-13}\,\mathrm{m}^2$, is tightly limited for a non-invasive measurement, and the limit of the SNR is becoming a critical issue.

In this work, we demonstrate an entanglement-enhanced microscope, consisting of a confocal-type differential interference contrast microscope equipped with an entangled photon source as a probe light source, with an SNR of 1.35 times better than that of the SQL. We use an entangled two-photon source with a high fidelity of 98%, resulting in a high two-photon interference visibility in the confocal microscope setup of 95.2%. An image of a glass plate sample, where a Q shape is carved in relief on the surface with a ultra-thin step of ~ 17 nm, is obtained with better visibility than with a classical light source. The improvement of the SNR is 1.35 ± 0.12, which is consistent with the theoretical prediction of 1.35. We also confirm that the bias phase dependence of the SNR completely agrees with the theory without any fitting parameter. We believe this experimental demonstration is an important step towards entanglement-enhanced microscopy with ultimate sensitivity.

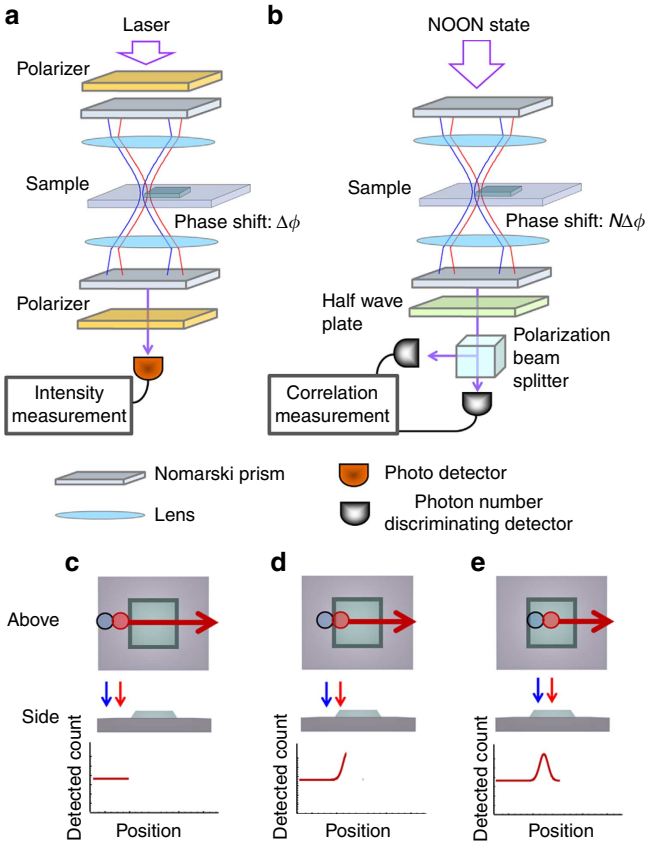


Figure 1 | LCM-DIM and the entanglement-enhanced microscope. (**a**) Illustration of LCM-DIM (**b**) Illustration of the entanglement-enhanced microscope. The red and blue lines indicate horizontally and vertically polarized light. (**c**–**e**) The change in the signal while the sample is scanned.

Results

The limit of differential interference contrast microscope. Our entanglement-enhanced microscope is based on a laser confocal microscope combined with a differential interference contrast microscope (LCM–DIM)[19,20]. An LCM–DIM can detect a very tiny difference between optical path lengths in a sample. The LCM–DIM works on the principle of a polarization interferometer (Fig. 1a). In this example, the horizontal (H) and vertical (V) polarization components are directed to different optical paths by a Nomarski prism. At the sample, the two beams experience different phase shifts ($\Delta\phi_\mathrm{H}$ and $\Delta\phi_\mathrm{V}$) depending on the local refractive index and the structure of the sample. After passing through the sample, the two beams are combined into one beam by another Nomarski prism. The difference in the phase shifts can be detected as a polarization rotation at the output, $\Delta\phi = \Delta\phi_\mathrm{V} - \Delta\phi_\mathrm{H}$.

We obtain differential interference contrast images for a sample by scanning the relative position of the focused beams on the sample (Fig. 1c–e). When two beams probe a homogeneous region, the output intensity is constant (Fig. 1c). At the boundary of the two regions, the signal intensity increases or decreases, as the difference in the phase shift $\Delta\phi$ becomes non-zero (Fig. 1d). The signal intensity returns to the original level after the boundary (Fig. 1e). The smallest detectable change in the phase shift is limited by the SNR, which is the ratio of the change in the signal intensity, $C(\phi)$, and the fluctuation of the uniform background level, ΔC, at a bias level of Φ_0. As is discussed in detail later, it is known that the SNR is limited by so-called 'shot noise' or the SQL, when classical light sources such as lasers or lamps are used. That is, for a limited number of input photons (N), the SNR is limited by $\sqrt{N}$. This SNR limits the height resolution of the LCM–DIM when used to observe elementary steps at the surface of ice crystals[19] or the difference in refractive indexes inside a sample. Thus, improving the SNR beyond the SQL is a revolutionary advance in microscopy.

Entanglement-enhanced microscope. We propose to use multi-photon quantum interference to beat this standard quantum limit (Fig. 1b). Instead of a classical light, we use an entangled photon state $((|N;0\rangle_\mathrm{HV} + |0;N\rangle_\mathrm{HV})/\sqrt{2})$, so-called 'NOON' state, which is a quantum superposition of the states 'N photons in the H polarization mode' and 'N photons in the V polarization mode'. The phase difference between these two states is $N\Delta\phi$ after passing through the sample, which is N times larger than the classical case ($N = 1$). At the output, the result of the multi-photon interference (the parity of the photon number in the output) is measured by a pair of photon number discriminating detectors[21,22].

As is well known from two-path interferometry with N-photon states, entanglement can increase the sensitivity of a phase measurement by a factor of $\sqrt{N}$. In the entanglement-enhanced microscope, we apply this effect to achieve an SNR that is $\sqrt{N}$ times higher than that of the LCM–DIM. If the average number of N-photon states that pass through the microscope during a given time interval is k, then the average number of detection events in the output is given by $C(\phi) = kP(\phi)$, where $P(\phi) = (1 - V_N \cos(N\phi + N\Phi_0))/2$ is the probability of detecting an odd (or even) number of photons in a specific output polarization (see Methods section). For a small positive phase shift of $\Delta\phi \ll 1/N$, the phase dependence of the signal is given by the slope of $C(\phi)$ at the bias phase Φ_0, $\lim_{\Delta\phi\to 0}|C(\Delta\phi) - C(0)| = |\partial C(\phi)/\partial\phi||_{\phi=0} \times \Delta\phi$, and the SNR is given by the ratio of the slope and the statistical noise of the detection. If the emission of the N-photon states is statistically independent, the statistical noise is given by $\Delta C|_{\phi=0} = \sqrt{kP(0)}$. The SNR is then given by

$$\mathrm{SNR} = (1-\xi)\sqrt{\frac{k}{2}}NV_N\frac{|\sin(N\Phi_0)|}{\sqrt{1 - V_N\cos(N\Phi_0)}}\times\Delta\phi \qquad (1)$$

where ξ is the normalized overlap region between the two beams at the sample plane (see Methods section). By maximizing the function of $\cos(N\Phi_0)$, we can find the maximum sensitivity ($\mathrm{SNR}_{\max}$) as follows:

$$\mathrm{SNR}_{\max} = (1-\xi)\sqrt{kN}\sqrt{1-\sqrt{1-V_N^2}}\times\Delta\phi \qquad (2)$$

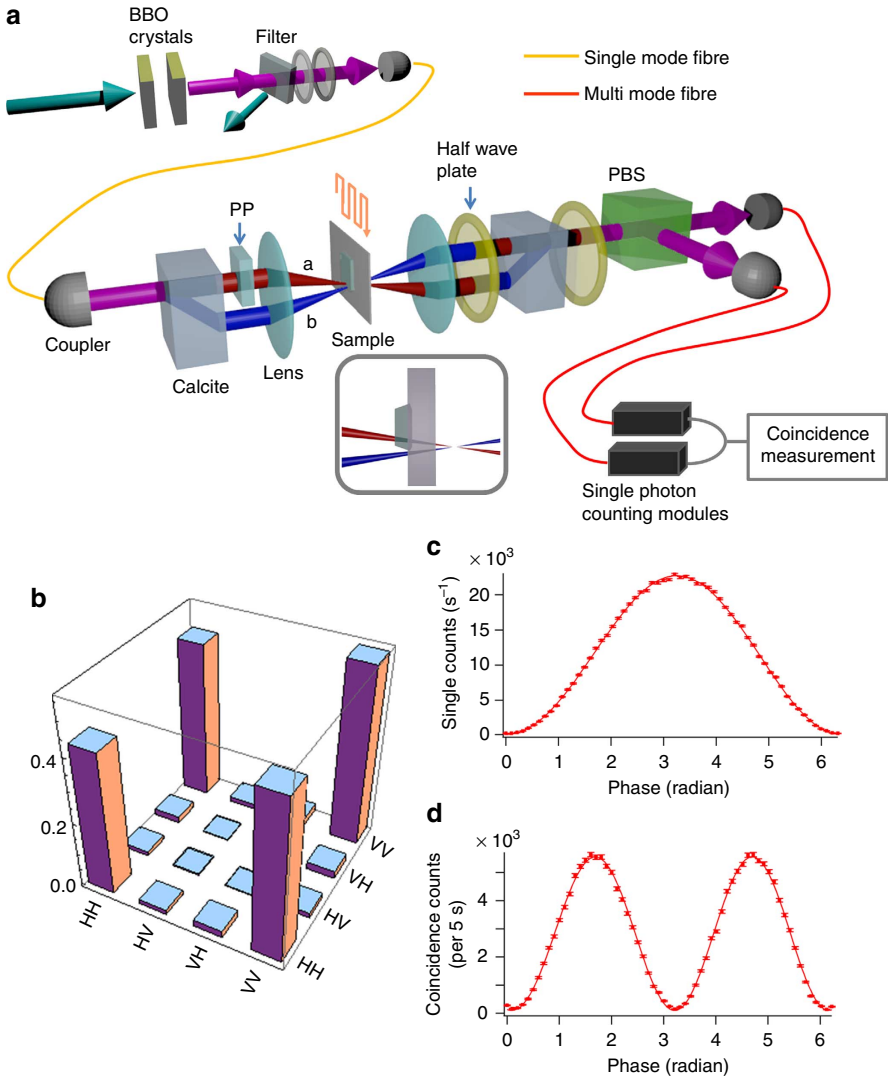


Figure 2 | Experimental setup for a two-photon entanglement-enhanced microscope. (**a**) BBO: beta barium borate; PP: phase plate; PBS: polarizing beam splitter. A 405-nm diode laser (line width <0.02 nm) was used for the pump beam. A sharp-cut filter with a cut-off wavelength below 715 nm and a band pass filter with 4 nm bandwidth were used. The beam displacement at the calcite crystal was 4 mm. PBS reflects vertical polarization component and transmits horizontal polarization. The blue and red lines indicate the optical paths for the horizontally and vertically polarized beams. The inset shows an illustration of the sample with the trajectory of the two beams. (**b**) The absolute value of the reconstructed density matrix of the generated state measured before the microscope setup (after the output coupler) using quantum state tomography[45]. HV denotes for the state where one photon is horizontally polarized and the other photon is vertically polarized. (**c**) Single-photon interference fringes of a classical microscope (counts per second) after the dark counts of the detectors (100 cps) subtracted. (**d**) Two-photon interference fringes of an entanglement-enhanced microscope (5 cps). While varying the phase by rotating the phase plate (PP), we counted the detected events in the output. The classical fringe was measured by inserting a polarizer transmitting the diagonally polarized photons and counting single-photon detection events. Solid lines in **c** and **d** are by theoretical fitting curve. Error bars are given by Poissonian statistics.

at a bias phase of

$$\cos(N\Phi_0) = \left(1 - \sqrt{1 - V_N^2}\right)/V_N. \quad (3)$$

For the ideal case of $V_N = 1$, the maximum sensitivity $\mathrm{SNR}_{\max} = \sqrt{k}N \times \Delta\phi$. As the SNR for a classical microscope using kN photons $\mathrm{SNR}_{\max} = \sqrt{kN} \times \Delta\phi$, an entanglement-enhanced microscope can improve the SNR by a factor of $\sqrt{N}$ compared with a classical microscope for the same photon number.

Experimental setup. We demonstrate an entanglement-enhanced microscope (Fig. 2a) using a two-photon NOON state ($N = 2$). First, a polarization-entangled state of photons $(|2;0\rangle_{\mathrm{HV}} + |0;2\rangle_{\mathrm{HV}})/\sqrt{2}$ is generated from two beta barium borate crystals[23,24] and is then delivered to the microscope setup via a single-mode fibre. The polarization-entangled state is then converted to a two-photon NOON state $(|2\rangle_a|0\rangle_b + |0\rangle_a|2\rangle_b)/\sqrt{2}$ using a calcite crystal[25] and focused by an objective lens. From the result of quantum state tomography (Fig. 2b), the fidelity of the state is 98% and the entanglement concurrence is 0.979, which ensures that the produced state is almost maximally entangled. The entangled photons pass through two neighbouring spots at the sample plane (Fig. 2a inset). Then, after passing through the collimating lens, the two paths are merged by a polarization beam splitter and the result of the two-photon interference is detected by a pair of single-

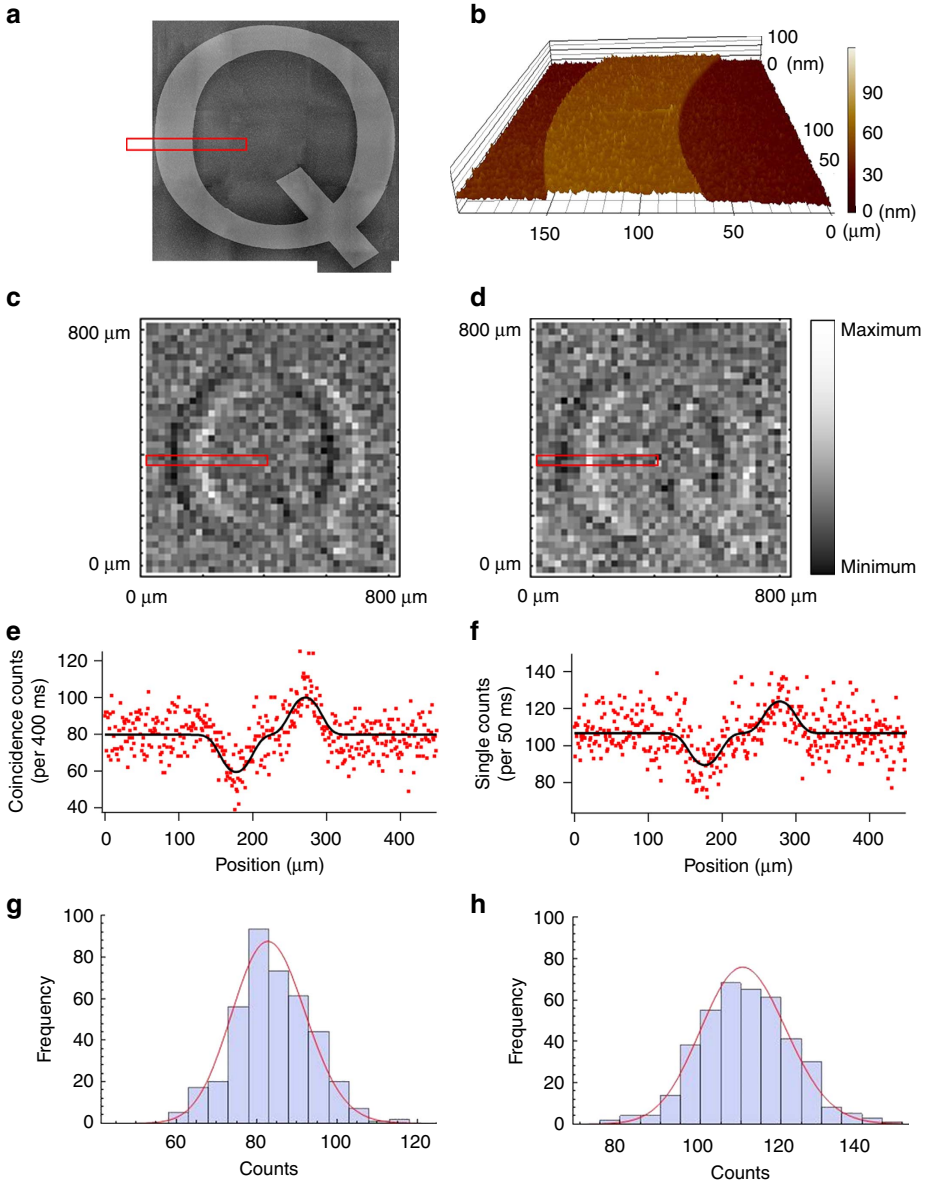


Figure 3 | Experimental results. (**a**) Atomic force microscope (AFM) image of a glass plate sample (BK7) on whose surface a Q shape is carved in relief with an ultra-thin step using optical lithography. (**b**) The section of the AFM image of the sample, which is the area outlined in red in **a**. The height of the step is estimated to be 17.3 nm from this data. (**c**) The image of the sample using an entanglement-enhanced microscope where two-photon entangled state is used to illuminate the sample. (**d**) The image of the sample using single photons (a classical light source). (**e**,**f**) One-dimensional fine scan data for the area outlined in red in **c** and **d** for the same photon number of 920. The measurement was made at a bias phase of 0.41 (**e**) and 0.66 (**f**), where optimal bias phases are 0.38 and 0.67, respectively. Solid lines are theoretical fitting curves (see text). (**g**,**h**) The histogram of the counts at 400 experimental points of the background level for **e** and **f**. Red curves are the Poisson distribution with the average of the counts at 400 points (83.3 and 110.9, respectively).

photon counters and a coincidence counter. The sample is scanned by a motorized stage to obtain an image. The beam diameters at the sample plane and the distance between the centre of the beams are all 45 μm ($\xi = 0.046$).

Figure 2c,d shows the single-photon and two-photon interference fringes using a classical light source and the NOON source, respectively. The fringe period of Fig. 2d is half that of Fig. 2c, which is a typical feature of NOON state interference. The visibilities of these fringes, $V_c = 97.1 \pm 0.4\%$ (Fig. 2c) and $V_q = 95.2 \pm 0.6\%$ (Fig. 2d), suggests the high quality of the classical and quantum interferences.

Obtained image beating the standard quantum limit. Figure 3 shows the main result of this experiment. We used a glass plate sample (BK7) on whose surface a Q shape is carved in relief with an ultra-thin step of ~17 nm using optical lithography (Fig. 3a,b). Figure 3c,d shows the two-dimensional (2D) scan images of the sample using entangled photons and single photons, respectively. The step of the Q-shaped relief is clearly seen in Fig. 3c, whereas it is obscure in Fig. 3d. Note that for both images we set the bias phases to almost their optimum values given in equation 3 and the average total number of photons ($N \times k$) contributed to these data are set to 920 per position assuming the unity detection efficiency.

For more detailed analysis, the cross-section of the images (coincidence count rate per single count rate at each position) are shown in Fig. 3e,f. The solid lines are theoretical fits to the data where the height and position of the step and the background level are used as free parameters. For Fig. 3e, the signal (the height of the peak of the fitting curve from the background level) is 20.21 ± 1.13, and the noise (the standard deviation of each experimental counts from the background level of the fitting curve) is 9.48 (Fig. 3g). Thus, the SNR is 2.13 ± 0.12. Similarly, the signal, the noise and the SNR are 17.7 ± 1.22, 11.25 (Fig. 3h) and 1.58 ± 0.11 for Fig. 3f, where classical light source (single photons) is used. The improvement in SNR is thus 1.35 ± 0.12, which is consistent with the theoretical prediction of 1.35 (equation 2). The estimated height of the step was 17.0 ± 0.9 nm (quantum) and 16.6 ± 1.1 nm (classical), and is consistent with the estimated value of 17.3 nm from the atomic force microscope image in Fig. 3b.

As shown in equation 1, the SNR depends on the bias phase. Finally, we test the theoretical prediction of the bias phase dependence given by equation 1 in actual experiments. Figure 4 shows the bias phase dependence of the SNR for the two-photon NOON source (Fig. 4a) and classical light source (Fig. 4b). The solid curve is the theoretical prediction calculated by equation (1), where we used the observed visibilities of the fringes in Fig 2c,d for V_N. The theoretical curves are in good agreement with the experimental results.

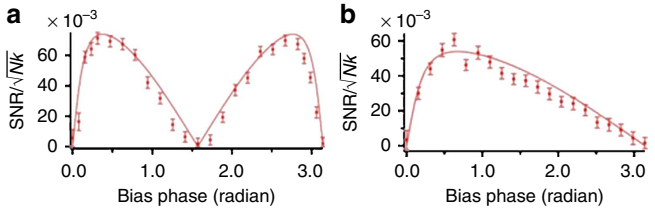


Figure 4 | Dependence of the SNR on the bias phase. (**a**) Dependence of the SNR on the bias phase using an entanglement-enhanced microscope ($N = 2$). (**b**) Dependence of the SNR on the bias phase using a classical microscope. The SNR and its error shown by error bars were calculated from the experimental data similar to Fig. 3e,f taken for different bias phases. The total photon number $Nk = 1{,}150$ for **a** and 1,299 for **b**. The solid line shows the theoretical curve using equation (1).

Discussion

Note that the entanglement-enhanced microscope we reported here is different from the 'entangled photon microscope' theoretically proposed by Teich and Saleh[26], which is the combination of two photon fluorescence microscopy and the entangled photon source. In the proposal, the increase in two-photon absorption rate and the flexibility in the selection of target regions in the specimen were predicted. The application of entangled photon sources for imaging also includes quantum lithography[27], where the lateral resolution of the generated pattern is improved[25,28], and ghost imaging[29], where the spatial correlation of entangled photons is utilized. In this context, this work is the first application of entanglement-enhanced optical phase measurement beyond the SQL for imaging including microscopy. Note also that the entanglement is indispensable to improve the SNR of the phase measurement beyond the SQL[11,30]. This situation is different from the improvement in the contrast of the ghost imaging using strong thermal light[31–37].

In conclusion, we proposed and demonstrated an entanglement-enhanced microscope, which is a confocal-type differential interference contrast microscope equipped with an entangled photon source as a probe light source, with an SNR 1.35 ± 0.12 times better than the SQL. Imaging of a glass plate sample with an ultra-thin step of ~17 nm under a low photon number condition shows the viability of the entanglement-enhanced microscope for light-sensitive samples. To test the performance of the entanglement-enhanced microscope, we used modest-efficiency detectors, however, recently developed high-efficiency number-resolving photon detectors would markedly improve detection efficiency[38,39]. We believe this experimental demonstration is an important step towards entanglement-enhanced microscopy with ultimate sensitivity, using a higher NOON state, a squeezed state[40,41] and other hybrid approaches[42] or adaptive estimation schemes[43,44].

Methods

SNR of an entanglement-enhanced microscope. To perform the parity measurement used by Gerry[21] and Seshadreesan *et al.*[22], it is required to count both of the events where 'even' and 'odd' number of photons are detected in the output. However, experimental implementations become much easier if it is sufficient for us to just count 'odd' (or 'even') number photon-detection events. In addition, the distance between the two beams and the beam size may have effect on the SNR. Here we consider these technical effects on SNR and derive equation (1).

To derive equation (1), we consider that the two beams at the sample are separated at a distance of α along the x axis, and each set of N photons has Gaussian distribution with a variance of σ in the x–y plane (Fig. 5). After passing through the sample, the two beams experience a phase shift (ϕ) in the grey region ($x > 0$). The state, $|\Psi(x, y, \phi)\rangle$, after the sample is written as

$$|\Psi(x,y,\phi)\rangle = \frac{1}{\sqrt{2}}\left(|\psi_{\mathrm{H}}(x,y,\phi)\rangle + \mathrm{e}^{iN\Phi_0}|\psi_{\mathrm{V}}(x,y,\phi)\rangle\right) \tag{4}$$

where $|\psi_{\mathrm{H}}(x,y,\phi)\rangle$ and $|\psi_{\mathrm{V}}(x,y,\phi)\rangle$ represents the states of N photons in the horizontal and vertical polarization modes, respectively, and Φ_0 is a bias phase. We assume that the phase shift is described by a step function and the N photons are in the same spatial modes. These states are written as

$$\begin{aligned}
|\psi_{\mathrm{H}}(x,y,\phi)\rangle &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \mathrm{e}^{-i\chi(x)N\phi}\sqrt{f(x-\alpha/2,y)}\,\frac{1}{\sqrt{N!}}\left(\hat{a}_{\mathrm{H}}^{\dagger}(x,y)\right)^N|0\rangle\,\mathrm{d}x\mathrm{d}y \\
&= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \mathrm{e}^{-i\chi(x)N\phi}\sqrt{f(x-\alpha/2,y)}|N;0,x,y\rangle_{\mathrm{HV}}\,dxdy, \\
|\psi_{\mathrm{V}}(x,y,\phi)\rangle &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \mathrm{e}^{-i\chi(x)N\phi}\sqrt{f(x+\alpha/2,y)}\,\frac{1}{\sqrt{N!}}\left(\hat{a}_{\mathrm{V}}^{\dagger}(x,y)\right)^N|0\rangle\,\mathrm{d}x\mathrm{d}y \\
&= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \mathrm{e}^{-i\chi(x)N\phi}\sqrt{f(x+\alpha/2,y)}|0;N,x,y\rangle_{\mathrm{HV}}\,\mathrm{d}x\mathrm{d}y,
\end{aligned} \tag{5}$$

where $|0\rangle$ is a vacuum state, $\hat{a}_{\mathrm{H}}^{\dagger}(x,y)$ and $\hat{a}_{\mathrm{V}}^{\dagger}(x,y)$ are the creation operators in H

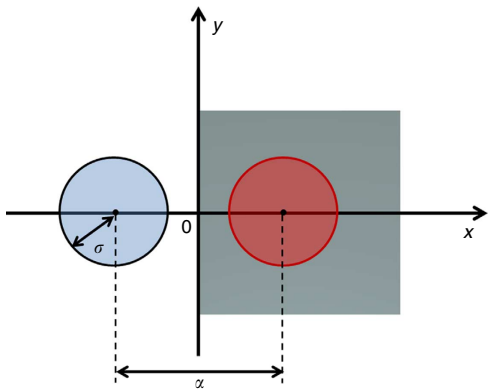


Figure 5 | The schematic of the two probe beams. The beams are in V polarization (blue) and H polarization (red) on the sample, corresponding to Fig. 1c–e. The grey shaded region has the phase change of ϕ.

and V polarization modes at the position of (x,y), respectively, and $\chi(x)$ is a step function that $\chi(x)=0$ for $x\leq 0$ and $\chi(x)=1$ for $x>0$. $f(x-\alpha/2, y)$ and $f(x+\alpha/2, y)$ represent the N-photon probability densities in the horizontal and vertical polarization modes written as

$$f(x,y)=\frac{1}{2\pi\sigma^2}e^{-\frac{(x^2+y^2)}{2\sigma^2}};\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}f(x,y)\mathrm{d}x\mathrm{d}y=1. \quad (6)$$

After passing through the second calcite crystal, the two beams are displaced at a distance of $-\alpha/2$ for H polarization and $\alpha/2$ for V polarization along the x axis, resulting in two beams in the same spatial mode. The state can then be written as

$$|\Psi'(x,y,\phi)\rangle=\frac{1}{\sqrt{2}}\left(|\psi_{\mathrm{H}}(x+\alpha/2,y,\phi)\rangle+e^{iN\Phi_0}|\psi_{\mathrm{V}}(x-\alpha/2,y,\phi)\rangle\right). \quad (7)$$

Here, we assume that the state is projected onto the state where odd number of photons are in the minus diagonal polarization mode at the output. The measurement operator in the basis of plus (P) and minus (M) diagonal polarization is therefore written as

$$\hat{\Pi}=\begin{cases}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\sum_{n=0}^{\infty}\sum_{m=1}^{N/2}|n;2m-1,x,y\rangle_{\mathrm{PM\,PM}}\langle n;2m-1,x,y|\,\mathrm{d}x\mathrm{d}y & \text{if } N \text{ is even}\\ \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\sum_{n=0}^{\infty}\sum_{m=1}^{(N+1)/2}|n;2m-1,x,y\rangle_{\mathrm{PM\,PM}}\langle n;2m-1,x,y|\,\mathrm{d}x\mathrm{d}y & \text{if } N \text{ is odd}\end{cases} \quad (8)$$

where

$$|n;m,x,y\rangle_{\mathrm{PM}}=\frac{1}{\sqrt{n!\,m!}}\left(\hat{a}_{\mathrm{P}}^{\dagger}(x,y)\right)^n\left(\hat{a}_{\mathrm{M}}^{\dagger}(x,y)\right)^m|0\rangle=\frac{1}{\sqrt{n!\,m!}}$$
$$\times\left(\frac{1}{\sqrt{2}}\left(\hat{a}_{\mathrm{H}}^{\dagger}(x,y)+\hat{a}_{\mathrm{V}}^{\dagger}(x,y)\right)\right)^n\left(\frac{1}{\sqrt{2}}\left(\hat{a}_{\mathrm{H}}^{\dagger}(x,y)-\hat{a}_{\mathrm{V}}^{\dagger}(x,y)\right)\right)^m|0\rangle. \quad (9)$$

The probability of odd number photon detection can then be written as

$$\begin{aligned}P(\phi)&=\langle\Psi'(x,y,\phi)|\hat{\Pi}|\Psi'(x,y,\phi)\rangle\\&=\tfrac{1}{2}(1-\cos(N\phi+N\Phi_0))(1-\xi(\alpha))+\tfrac{1}{2}(1-\cos(N\Phi_0))\xi(\alpha)\end{aligned} \quad (10)$$

where we denote the phase-independent term of $\int_{\infty}^{\infty}\int_{-\infty}^{-\alpha/2}f(x,y)\mathrm{d}x\mathrm{d}y+\int_{\infty}^{\infty}\int_{\alpha/2}^{\infty}f(x,y)\mathrm{d}x\mathrm{d}y$ as $\xi(\alpha)$ which is the overlap integral between H and V polarized beams at the sample plane.

We now calculate the SNR of our microscope using the NOON state including the effect of the overlap between the two beams at the sample plane. If the emission of the N-photon states is statistically independent, the statistical noise at the bias phase $\Delta C(\phi)\,|_{\phi=0}=\sqrt{kP(0)}$ is given by

$$\Delta C(0)=\sqrt{k}\sqrt{\frac{1}{2}(1-\cos(N\Phi_0))}. \quad (11)$$

For a small positive phase shift of $\Delta\phi\ll 1/N$, the signal is

$$|\partial(C(\phi))/\partial\phi||_{\phi=0}\times\Delta\phi=(1-\xi(\alpha))\frac{k}{2}N|\sin(N\Phi_0)|\times\Delta\phi. \quad (12)$$

Considering the visibility of the interference fringe V_N, the SNR is given by

$$\mathrm{SNR}=(1-\xi)\sqrt{\frac{k}{2}}NV_N\frac{|\sin(N\Phi_0)|}{\sqrt{1-V_N\cos(N\Phi_0)}}\times\Delta\phi. \quad (13)$$

Thus one can confirm that counting odd (or even) number photon-detection events can also achieve the phase super sensitivity. Note also that the dependence of SNR on the size and the distance between the two beams is simply given by $(1-\xi)$. This means that it is reasonable to compare the SNR between an entanglement-enhanced microscope and a classical microscope ($N=1$) for the same ξ.

References

1. Giovannetti, V., Lloyd, S. & Maccone, L. Quantum-enhanced measurements: beating the standard quantum limit. *Science* **306,** 1330–1336 (2004).
2. Meyer, V. *et al.* Experimental demonstration of entanglement-enhanced rotation angle estimation using trapped ions. *Phys. Rev. Lett.* **86,** 5870–5873 (2001).
3. Leibfried, D. *et al.* Creation of a six-atom 'Schrodinger cat' state. *Nature* **438,** 639–642 (2005).
4. Roos, C. F., Chwalla, M., Kim, K., Riebe, M. & Blatt, R. Designer atoms' for quantum metrology. *Nature* **443,** 316–319 (2006).
5. Widera, A. *et al.* Entanglement interferometry for precision measurement of atomic scattering properties. *Phys. Rev. Lett.* **92,** 160406 (2004).
6. Rarity, J. G. *et al.* Two-photon interference in a Mach-Zehnder interferometer. *Phys. Rev. Lett.* **65,** 1348–1351 (1990).
7. Kuzmich, A. & Mandel, L. Sub-shot-noise interferometric measurements with two-photon states. *Quant. Semiclass. Opt.* **10,** 493–500 (1998).
8. Fonseca, E., Monken, C. & Padua, S. Measurement of the de Broglie wavelength of a multiphoton wave packet. *Phys. Rev. Lett.* **82,** 2868–2871 (1999).
9. Edamatsu, K., Shimizu, R. & Itoh, T. Measurement of the photonic de Broglie wavelength of entangled photon pairs generated by spontaneous parametric down-conversion. *Phys. Rev. Lett.* **89,** 213601 (2002).
10. Eisenberg, H., Hodelin, J., Khoury, G. & Bouwmeester, D. Multiphoton path entanglement by nonlocal bunching. *Phys. Rev. Lett.* **94,** 090502 (2005).
11. Nagata, T., Okamoto, R., O'brien, J. L., Sasaki, K. & Takeuchi, S. Beating the standard quantum limit with four-entangled photons. *Science* **316,** 726–729 (2007).
12. Okamoto, R. *et al.* Beating the standard quantum limit: phase super-sensitivity of N-photon interferometers. *New J. Phys.* **10,** 073033 (2008).
13. Xiang, G. Y., Higgins, B. L., Berry, D. W., Wiseman, H. M. & Pryde, G. J. Entanglement-enhanced measurement of a completely unknown optical phase. *Nat. Photon.* **5,** 43–47 (2010).
14. Crespi, A. *et al.* Measuring protein concentration with entangled photons. *Appl. Phys. Lett.* **100,** 233704 (2012).
15. Wolfgramm, F., Vitelli, C., Beduini, F. A., Godbout, N. & Mitchell, M. W. Entanglement-enhanced probing of a delicate material system. *Nat. Photon.* **7,** 28–32 (2013).
16. Taylor, M. A. *et al.* Biological measurement beyond the quantum limit. *Nat. Photon.* **7,** 229–233 (2013).
17. Nomarski, M. G. Microinterféromètre différentiel à ondes polarisées. *J. Phys. Radium* **16,** 9S (1955).
18. Jesorka, A. *et al.* Generation of phospholipid vesicle-nanotube networks and transport of molecules therein. *Nat. Protoc.* **6,** 791–805 (2011).
19. Sazaki, G., Zepeda, S., Nakatsubo, S., Yokoyama, E. & Furukawa, Y. Elementary steps at the surface of ice crystals visualized by advanced optical microscopy. *Proc. Natl Acad. Sci. USA* **107,** 19702–19707 (2010).
20. Sazaki, G., Zepeda, S., Nakatsubo, S., Yokoyama, E. & Furukawa, Y. Quasi-liquid layers on ice crystal surfaces are made up of two different phases. *Proc. Natl Acad. Sci. USA* **109,** 1052–1055 (2012).
21. Gerry, C. Heisenberg-limit interferometry with four-wave mixers operating in a nonlinear regime. *Phys. Rev. A* **61,** 043811 (2000).
22. Seshadreesan, K. P., Kim, S., Dowling, J. P. & Lee, H. Phase estimation at the quantum Cramer-Rao bound via parity detection. *Phys. Rev. A* **87,** 043833 (2013).
23. Kwiat, P. G., Waks, E., White, A. G., Appelbaum, I. & Eberhard, P. H. Ultrabright source of polarization-entangled photons. *Phys. Rev. A* **60,** R773–R776 (1999).
24. White, A. G., James, D. F. V., Eberhard, P. H. & Kwiat, P. G. Nonmaximally entangled states: production, characterization, and utilization. *Phys. Rev. Lett.* **83,** 3103–3107 (1999).
25. Kawabe, Y., Fujiwara, H., Okamoto, R., Sasaki, K. & Takeuchi, S. Quantum interference fringes beating the diffraction limit. *Opt. Express* **15,** 14244–14250 (2007).
26. Teich, M. C. & Saleh, B. E. A. Entangled-photon microscopy. *Ceskoslovensky Casopis Pro Fyziku* **47,** 3–8 (1997); English translation is available at http://people.bu.edu/teich/pdfs/Cesk-English-47-3-1997.pdf (1997).
27. Boto, A. N. *et al.* Quantum interferometric optical lithography: exploiting entanglement to beat the diffraction limit. *Phys. Rev. Lett.* **85,** 2733–2736 (2001).
28. D'Angelo, M., Chekhova, M. & Shih, Y. Two-photon diffraction and quantum lithography. *Phys. Rev. Lett.* **87,** 013602 (2001).
29. Pittman, T. B., Shih, Y. H., Strekalov, D. V. & Sergienko, A. V. Quantum interferometric optical lithography: exploiting entanglement to beat the diffraction limit. *Phys. Rev. A* **52,** R3429–R3432 (1995).

30. Giovannetti, V., Lloyd, S. & Maccone, L. Quantum metrology. *Phys. Rev. Lett.* **96,** 010401 (2006).
31. Ou, L. H. & Kuang, L. M. Ghost imaging with third-order correlated thermal light. *J. Phys. B: At. Mol. Opt. Phys.* **40,** 1833–1844 (2007).
32. Cao, D. Z. *et al.* Enhancing visibility and resolution in Nth-order intensity correlation of thermal light. *Appl. Phys. Lett.* **92,** 201102 (2008).
33. Liu, Q., Chen, X. H., Luo, K. H., Wu, W. & Wu, L. A. Role of multiphoton bunching in high-order ghost imaging with thermal light sources. *Phys. Rev. A* **79,** 053844 (2009).
34. Chan, K. W. C., O'Sullivan, M. N. & Boyd, R. W. High-order thermal ghost imaging. *Opt. Lett.* **34,** 3343–3345 (2009).
35. Chan, K. W. C., Sullivan, M. N. O. & Boyd, R. W. Optimization of thermal ghost imaging: high-order correlations vs. background subtraction. *Opt. Express* **18,** 5562–5573 (2010).
36. Chen, X. H. *et al.* High-visibility, high-order lensless ghost imaging with thermal light. *Opt. Lett.* **35,** 1166–1168 (2010).
37. Cao, B. & Zhang, C. Third-order lensless ghost diffraction with classical fully incoherent light. *Opt. Lett.* **35,** 2091–2093 (2010).
38. Takeuchi, S., Kim, J., Yamamoto, Y. & Hogue, H. H. Development of a high-quantum-efficiency single-photon counting system. *Appl. Phys. Lett.* **74,** 1063–1065 (1999).
39. Fukuda, D. *et al.* Titanium-based transition-edge photon number resolving detector with 98% detection efficiency with index-matched small-gap fiber coupling. *Opt. Express* **19,** 870–875 (2011).
40. Goda, K. *et al.* A quantum-enhanced prototype gravitational-wave detector. *Nat. Phys.* **4,** 472–476 (2008).
41. Anisimov, P. M. *et al.* Quantum metrology with two-mode squeezed vacuum: parity detection beats the Heisenberg limit. *Phys. Rev. Lett.* **104,** 103602 (2010).
42. Ono, T. & Hofmann, H. F. Effects of photon losses on phase estimation near the Heisenberg limit using coherent light and squeezed vacuum. *Phys. Rev. A* **81,** 033819 (2010).
43. Okamoto, R. *et al.* Experimental demonstration of adaptive quantum state estimation. *Phys. Rev. Lett.* **109,** 130404 (2012).
44. Hannemann, T. h. *et al.* Self-learning estimation of quantum states. *Phys. Rev. A* **65,** 050303 (2002).
45. James, D. F. V., Kwiat, P. G., Munro, W. J. & White, A. G. Measurement of qubits. *Phys. Rev. A* **64,** 080504 (2001).

Acknowledgements

We thank Dr. Shouichi Sakakihara for sample fabrication, Professor Hidekazu Tanaka and Dr. Koichi Okada for atomic force microscope measurements. We also thank Professor Mitsuo Takeda, Professor Yoko Miyamoto, Professor Gen Sazaki, Professor Holger F. Hofmann and Professor Masamichi Yamanishi for helpful discussion. This work was supported in part by FIRST of JSPS, Quantum Cybernetics of JSPS, a Grant-in-Aid from JSPS, JST-CREST, Special Coordination Funds for Promoting Science and Technology, Research Foundation for Opto-Science and Technology and the GCOE programme.

Author contributions

Experiments, measurements and data analysis were performed by T.O. with assistance of R.O. and S.T. The project was planned by S.T. and supervised by R.O. and S.T. The manuscript was written by all the authors.

Additional information

Competing financial interests: The authors declare no competing financial interests.

Reprints and permission information is available online at http://npg.nature.com/reprintsandpermissions/

How to cite this article: Ono, T. *et al.* An entanglement-enhanced microscope. *Nat. Commun.* 4:2426 doi: 10.1038/ncomms3426 (2013).

REVIEW ARTICLE
https://doi.org/10.1038/s41566-018-0301-6

nature photonics

Advances in photonic quantum sensing

S. Pirandola[1,2*], B. R. Bardhan[3], T. Gehring[4], C. Weedbrook[5] and S. Lloyd[2,6]

Quantum sensing has become a broad field. It is generally related with the idea of using quantum resources to boost the performance of a number of practical tasks, including the radar-like detection of faint objects, the readout of information from optical memories, and the optical resolution of extremely close point-like sources. Here, we first focus on the basic tools behind quantum sensing, discussing the most recent and general formulations for the problems of quantum parameter estimation and hypothesis testing. With this basic background in hand, we then review emerging applications of quantum sensing in the photonic regime both from a theoretical and experimental point of view. Besides the state of the art, we also discuss open problems and potential next steps.

Quantum technologies are today developing at unprecedented pace. As a matter of fact, the technological applications of the field of quantum information[1–8] are many and promising. One of the most advanced areas is certainly quantum sensing. This is a broad term encompassing all those quantum protocols of estimation and discrimination able to outperform any classical strategy. One can leverage important quantum characteristics such as entanglement, single photons and squeezed states[5] to achieve orders-of-magnitude improvements in precision. In this scenario, the photonic regime is certainly the best setting thanks to the relative simplicity in the generation, manipulation and detection of such quantum features.

This Review aims to provide a survey of some recent advances in photonic quantum sensing. We refer the reader to ref. [9] for an overview of quantum sensing in non-photonic areas (spin qubits, trapped ions, for example). We also stress that we adopt a quantum information approach to quantum sensing, which clearly does not encompass all the possible methods known in the literature. We start with theoretical background in quantum parameter estimation[10–14] and hypothesis testing[15–18], presenting the most general adaptive formulation of these problems[19–28] and methods of channel simulation, based on programmability[29–31] and teleportation stretching[32–34]. This background will allow us to identify the goals, the structure, and the classical benchmarks for the following protocols of quantum sensing that we will discuss theoretically and experimentally.

Quantum hypothesis testing is at the very basis of quantum reading[35–53], where the information stored in an optical memory is efficiently retrieved by using just a few photons of quantum light. This light better senses the difference between the reflectivities of a memory cell, greatly improving the readout of information. Quantum hypothesis testing is also at the basis of quantum illumination[54–71], where the radar-like detection of remote and faint targets is boosted by the use of quantum correlations, even though entanglement may be destroyed in the process. Then, quantum parameter estimation is the core idea for the most recent advances in quantum imaging and optical resolution[72–88], where the 'Rayleigh's curse' may be dispelled by means of quantum metrological detection schemes[72–74].

Estimation and discrimination protocols

Consider a parameter θ encoded in a quantum channel $\mathcal{E}_\theta$, which is in turn stored in a black box, of which Alice may prepare the input and Bob may detect the output. In an estimation problem, θ is a continuous parameter, whereas in a discrimination problem, θ takes a discrete finite number of values with some prior probabilities. In particular, in a basic problem of binary symmetric discrimination, θ only takes two values, θ_0 (null hypothesis) or θ_1 (alternative hypothesis), with the same Bayesian cost and prior probability. In other words, there is a classical bit u encoded in the parameter θ_u.

Let us analyse the problem with an increasing level of complexity. In a 'block' protocol, Alice sends an input state ρ through the unknown channel $\mathcal{E}_\theta$ whose output $\mathcal{E}_\theta(\rho)$ is received by Bob. This process is identically performed n times, so that Alice sends n copies $\rho^{\otimes n}$ and Bob receives $\mathcal{E}_\theta(\rho)^{\otimes n}$. To retrieve θ, Bob applies a measurement on his n-copy output state. In channel estimation, the measurement is performed locally and identically on each single-copy output state. This measurement has a continuous outcome from which Bob constructs an unbiased estimator $\tilde{\theta}$ of θ, affected by some error variance $\delta\theta^2 := \langle(\tilde{\theta}-\theta)^2\rangle$. In channel discrimination, Bob uses a dichotomic measurement that provides the bit u with some mean error probability p_{err}. This measurement is optimal only if non-local, that is, jointly applied to all output copies.

In a sequential protocol, the approach is different. Instead of preparing a tensor product of n-copy input states (each one sent through an instance $\mathcal{E}_\theta$ of the unknown channel), Alice transmits an input state ρ through the sequence of channels $\mathcal{E}_\theta^n := \mathcal{E}_\theta \circ \cdots \circ \mathcal{E}_\theta$ whose output $\mathcal{E}_\theta^n(\rho)$ is then detected by Bob. The sequential protocol can also be seen as a scheme where the output state received by Bob in each transmission through the channel is teleported back as input. This happens n times, after which Bob performs his measurement.

More generally, the previously described protocols may be 'assisted'. This means that the parties may use additional reference systems, or idlers, that help the output measurement. In particular, there may be entanglement between these reference systems and the signal systems used to probe the box. For a block protocol, this means that Alice prepares n copies of a bipartite input state ρ_{sr} where the signal system s is transmitted through the channel $\mathcal{E}_\theta$, while the reference system r is subject to the identity map $\mathcal{I}$. Therefore, Bob receives $[\mathcal{E}_\theta \otimes \mathcal{I}(\rho_{sr})]^{\otimes n}$. For a sequential protocol, this means that the signal system is subject to the sequence $\mathcal{E}_\theta^n$ while the reference is subject to the identity. Therefore, Bob receives $\mathcal{E}_\theta^n \otimes \mathcal{I}(\rho_{sr})$.

[1]Computer Science and York Centre for Quantum Technologies, University of York, York, UK. [2]Research Laboratory of Electronics, MIT, Cambridge, MA, USA. [3]Department of Physics and Astronomy, State University of New York at Geneseo, Geneseo, NY, USA. [4]Department of Physics, Technical University of Denmark, Fysikvej, Kongens, Lyngby, Denmark. [5]Xanadu, Toronto, Ontario, Canada. [6]Department of Mechanical Engineering, MIT, Cambridge, MA, USA. *e-mail: stefano.pirandola@york.ac.uk

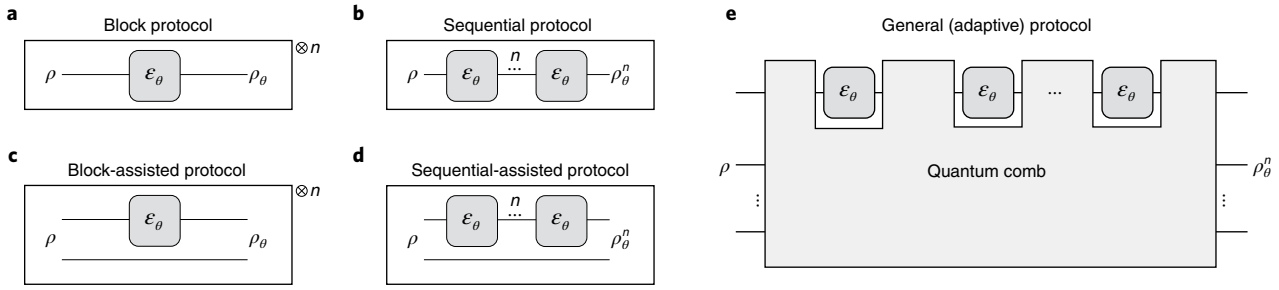


Fig. 1 | Protocols for quantum estimation and discrimination. a, Block protocol where channel $\mathcal{E}_\theta$ is probed n times in an identical and independent way. **b**, Sequential protocol where the input is transmitted through n consecutive instances of the channel. **c**, Block-assisted protocol where channel $\mathcal{E}_\theta$ is probed by a signal system coupled to a reference system. **d**, Sequential-assisted protocol where the input is bipartite and partially transmitted through n consecutive instances of $\mathcal{E}_\theta$. **e**, General (adaptive) protocol represented as a quantum comb. An input register with an arbitrary number of systems (wires) is prepared in a fundamental initial state ρ. Each probing of the unknown channel $\mathcal{E}_\theta$ is performed by inputting a system from the register and storing the output back in the register. Probings are interleaved by arbitrary QOs performed over the entire register. After n probings, the total output state ρ_θ^n is subject to a joint quantum measurement.

The most general protocol is based on unlimited entanglement and adaptive quantum operations (QOs), which are applied jointly by Alice and Bob[19–28]. As also discussed in ref. [34], this protocol can be represented as a quantum comb[89]. This is a quantum circuit board whose slots are filled with the unknown channel $\mathcal{E}_\theta$. The comb is based on a register with an arbitrary number of systems and prepared in a fundamental state ρ. The entire register undergoes arbitrary QOs before and after each probing of the channel, as depicted in Fig. 1. The QOs can always be assumed to be trace-preserving by adding extra systems and deferring measurements[1]. At the output of the comb, the state ρ_θ^n is detected by an optimal (non-local) quantum measurement whose outcome is classically processed. The quantum comb includes all the previous protocols as specific cases.

Performance of channel estimation

Assume that the quantum comb in Fig. 1 is used for quantum channel estimation. The ultimate performance is limited by the quantum Cramér–Rao bound (QCRB)

$$\delta\theta^2 \geq \frac{1}{\mathrm{QFI}(\rho_\theta^n)} \tag{1}$$

where QFI is the quantum Fisher information[10]

$$\mathrm{QFI}(\rho_\theta^n) = \frac{8[1-F(\rho_\theta^n, \rho_{\theta+\mathrm{d}\theta}^n)]}{\mathrm{d}\theta^2} \tag{2}$$

and $F(\rho,\sigma) := \mathrm{Tr}\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}$ is the Bures fidelity between ρ and σ. We are interested in the 'scaling' of the QCRB, that is, how $\delta\theta^2$ behaves for large n. There are two main behaviours[14]: the standard quantum limit (SQL), which is the typical scaling $\delta\theta^2 \gtrsim n^{-1}$ achievable in classical strategies, and the Heisenberg limit $\delta\theta^2 \gtrsim n^{-2}$, which is the ultimate scaling allowed by quantum mechanics. These have energetic analogues when we consider parameter estimation with bosonic channels. Assuming a single use of the comb ($n=1$) but allowing for N mean number of photons at the channel input, we have that $\delta\theta^2 \gtrsim N^{-1}$ corresponds to the SQL and $\delta\theta^2 \gtrsim N^{-2}$ to the Heisenberg limit.

As shown in refs [23,28], quantum teleportation[90] and port-based quantum teleportation[91,92] can be used as basic tools in quantum metrology. In particular, ref. [23] showed that teleportation covariance implies the SQL. Recall that a channel $\mathcal{E}$ is teleportation-covariant if, for any teleportation unitary U (Pauli or displacement operator), we can write[32]

$$\mathcal{E}(U\rho U^\dagger) = V\,\mathcal{E}(\rho)\,V^\dagger \tag{3}$$

with unitary V (here † means Hermitian conjugate). Then, a parametrized channel $\mathcal{E}_\theta$ is jointly teleportation-covariant[23,34] if equation (3) holds for any θ, that is, $\mathcal{E}_\theta(U\rho U^\dagger) = V\,\mathcal{E}_\theta(\rho)\,V^\dagger$ where V does not depend on θ. Because of this property, we may write the channel simulation[23,34]

$$\mathcal{E}_\theta(\rho) = \mathcal{T}(\rho \otimes \rho_{\mathcal{E}_\theta}) \tag{4}$$

where $\mathcal{T}$ is teleportation and $\rho_{\mathcal{E}} := \mathcal{E}\otimes\mathcal{I}(\Phi_{sr})$ is the Choi matrix of the channel (this is the state that is obtained by propagating part of a maximally entangled state Φ_{sr} through the quantum channel). Therefore, $\mathcal{E}_\theta$ is a specific type of programmable channel[29,30]. If $\mathcal{E}_\theta$ is bosonic, the simulation is asymptotic[34] with Choi matrix $\rho_{\mathcal{E}_\theta} := \lim_\mu \rho_{\mathcal{E}_\theta}^\mu$, where $\rho_{\mathcal{E}_\theta}^\mu := \mathcal{E}_\theta\otimes\mathcal{I}(\Phi_{sr}^\mu)$ is computed on a two-mode squeezed vacuum (TMSV) state[5] Φ_{sr}^μ with variance μ.

Replacing the simulation of equation (4) in each slot of the comb in Fig. 1 and stretching[32] the adaptive protocol, the output state becomes[23]

$$\rho_\theta^n = \Lambda(\rho_{\mathcal{E}_\theta}^{\otimes n}) \tag{5}$$

where Λ is a global quantum channel. Because the QFI is monotonic under channels and multiplicative over tensor products, equation (5) implies $\mathrm{QFI}(\rho_\theta^n) \leq n\mathrm{QFI}(\rho_{\mathcal{E}_\theta})$, so that the QCRB must satisfy the SQL[23]

$$\delta\theta^2 \geq [n\mathrm{QFI}(\rho_{\mathcal{E}_\theta})]^{-1} \tag{6}$$

where $\mathrm{QFI}(\rho_{\mathcal{E}_\theta}) := \lim_\mu \mathrm{QFI}(\rho_{\mathcal{E}_\theta}^\mu)$ for a bosonic channel. Thus, the general adaptive protocol is reduced to a block-assisted protocol, where n maximally entangled states $\Phi_{sr}^{\otimes n}$ probe $\mathcal{E}_\theta$.

Because the class of teleportation-covariant channels is wide, channel estimation is limited to the SQL in many situations. For instance, the estimation of the probability parameter p in depolarizing, dephasing or erasure channels is limited to[23] $\delta p^2 \geq p(1-p)n^{-1}$. The estimation of thermal noise $\bar{n}$ in a thermal-loss channel $\mathcal{E}_{\eta,\bar{n}}$ with fixed transmissivity η is limited to[23,24] $\delta\bar{n}^2 \geq \bar{n}(\bar{n}+1)n^{-1}$. By contrast, the ultimate estimation limit of the transmissivity η is not known, because $\mathcal{E}_{\eta,\bar{n}}$ is not jointly teleportation-covariant in η and equation (6) does not apply.

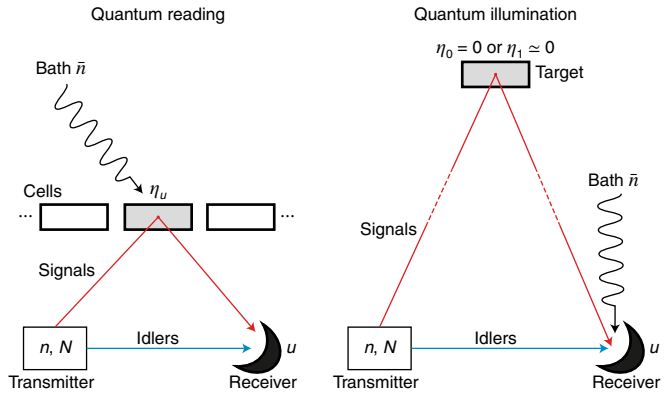


Fig. 2 | Technological applications of quantum channel discrimination. Quantum reading[35] (left) and Gaussian quantum illuminantion[55] (right). In the basic formulation, these are both based on an EPR transmitter, so that n two-mode squeezed vacuum (TMSV) states[5] irradiate N mean photons per mode over the cell (quantum reading) or target (quantum illumination) (where N is typically low). The reflected signals are combined with the retained idler (reference) modes in a joint detection, whose output u discriminates between two hypotheses. In quantum reading, the task is specifically the readout of data from an optical memory. In the simple single-cell model shown here, an information bit $u = 0,1$ is encoded in a cell with typically-high reflectivities, η_0 and η_1, and subject to (relatively low) thermal noise $\bar{n}$. Quantum features such as entanglement are typically preserved at the output receiver. In quantum illumination, the task is specifically target detection, where u is related with the absence ($\eta_0 = 0$) or the presence ($\eta_1 \simeq 0$) of a low-reflectivity object. Furthermore, the reflection is mixed with bright thermal noise $\bar{n} \gg 1$, so that entanglement is lost at the output receiver. These schemes are examples of block-assisted protocols for quantum channel discrimination. In the regimes considered, they largely outperform classical strategies, that is, corresponding schemes based on classical transmitters that are not entangled but composed of mixtures of coherent states.

The optimal adaptive estimation of bosonic loss is still an open problem. Solving it is of paramount importance because the transmissivity η of a quantum channel sets the ultimate limit of any point-to-point protocol of quantum or private communication. This limit is equal to $-\log_2(1-\eta)$ bits per use and known as the Pirandola–Laurenza–Ottaviani–Banchi bound[32]. The best performance in estimating η of a pure-loss channel $\mathcal{E}_\eta := \mathcal{E}_{\eta,0}$ is currently[93] $\delta\eta^2 \geq \eta(1-\eta)N^{-1}$ for N mean photons. This is a SQL in terms of the input mean number of photons N. However, note that the pre-factor $\eta(1-\eta)$ improves the performance that is achievable by using coherent states with the same input energy, that is, the scaling[94] $\delta\eta^2 \geq \eta N^{-1}$. The optimal performance of coherent states is also known as the shot-noise limit[14].

On the experimental side, the performance of absorption spectroscopy has been demonstrated to operate beyond the shot-noise limit in entanglement-assisted block protocols. In ref. [95], it was reported that photon pairs were generated with one of the photons being transmitted through an absorptive sample. At the output, coincidence counts were measured and post-processed. Quantum advantage over the shot-noise limit was also reported in refs [96,97], where the detection was based on intensity correlation measurements of signal and idler twin beams from a parametric downconversion source. Other multi-pixel experiments have also been performed where twin beams are used to enhance absorption microscopy[98,99].

Besides the estimation of bosonic loss, there is the complementary problem of phase estimation. Because phase shifts are unitary operations, they are not teleportation-covariant, so that their estimation is not necessarily limited to the SQL and, indeed, the Heisenberg scaling is achievable. The most famous phase estimation experiments are certainly the interferometer-based gravitational wave detectors. These kilometre-sized interferometers measure tiny phase shifts around a known phase and have recently been demonstrated to show an improved sensitivity beyond the SQL by injecting squeezed light[100,101].

Apart from squeezed light, the SQL has been surpassed in smaller-scale interferometric experiments using a variety of optical systems[102], in particular, with entangled states such as N00N states (a quantum superposition of N photons in one interferometer arm with no photons in the other and vice versa). While N00N states promise Heisenberg scaling, they are very fragile with respect to optical loss. For this reason, early experiments have surpassed the SQL only by conditioning on detected photons[103], while more recent experiments have been able to beat the SQL using photon sources and detectors with very high efficiency[104]. Other quantum states beyond N00N states have been engineered to be more loss-tolerant while still beating the SQL[105,106].

It is also important to remark that, in phase estimation, the SQL can be surpassed without using entanglement[14]. For instance, this is possible by applying the phase shift multiple times, that is, in a sequential protocol[107]. Using squeezed light, real-time phase tracking has been implemented using a feedback algorithm on the phase[108]. Ab initio phase estimation, that is, the estimation of the phase in a range without prior knowledge, has also been implemented to surpass the SQL, conditionally, with N00N states[109] and unconditionally, with squeezed states and using adaptive measurements[110].

Performance of channel discrimination

Assume that the comb in Fig. 1 is used for binary discrimination, so that parameter θ takes two values $\{\theta_0,\theta_1\}$ with the same probability. This is now a problem of channel discrimination between $\mathcal{E}_0 = \mathcal{E}_{\theta_0}$ and $\mathcal{E}_1 = \mathcal{E}_{\theta_1}$, where we aim to retrieve the classical bit $u = 0$, 1 encoded in $\mathcal{E}_u$. For a given comb with output state ρ_u^n, the minimum error probability affecting the channel discrimination is the Helstrom bound[15]

$$p_{\text{err}} = [1 - D(\rho_0^n, \rho_1^n)]/2 \tag{7}$$

where $D(\rho,\sigma) := ||\rho-\sigma||/2$ is the trace distance[1]. Equivalently, the maximum classical information J retrieved is

$$J = 1 - H_2(p_{\text{err}}) \tag{8}$$

where H_2 is the binary Shannon entropy.

The difficult part is the optimization of p_{err} over all possible adaptive protocols (combs). Remarkably, the problem can be solved if $\mathcal{E}_0$ and $\mathcal{E}_1$ are jointly teleportation-covariant, so that $\mathcal{E}_u(U\rho U^\dagger) = V\mathcal{E}_u(\rho)V^\dagger$ for any u. This allows us to use the teleportation simulation $\mathcal{E}_u(\rho) = \mathcal{T}(\rho \otimes \rho_{\mathcal{E}_u})$ over the Choi matrix $\rho_{\mathcal{E}_u}$. We may then stretch the comb and write its output as $\rho_u^n = \Lambda(\rho_{\mathcal{E}_u}^{\otimes n})$ for a global channel Λ. Because the trace distance is monotonic under Λ, we have $p_{\text{err}} \geq [1 - D(\rho_{\mathcal{E}_0}^{\otimes n}, \rho_{\mathcal{E}_1}^{\otimes n})]/2$ that holds for any comb. Then, we note that this bound is achievable by using maximally entangled states at the input, so that the minimum error probability in the adaptive discrimination of these types of channel is[23]

$$p_{\text{err}}(\mathcal{E}_0,\mathcal{E}_1) = [1 - D(\rho_{\mathcal{E}_0}^{\otimes n}, \rho_{\mathcal{E}_1}^{\otimes n})]/2 \tag{9}$$

where $D = \lim_\mu D(\rho_{\mathcal{E}_0}^{\mu\otimes n}, \rho_{\mathcal{E}_1}^{\mu\otimes n})$ in the bosonic case. In finite dimension, equation (9) establishes the diamond distance between jointly teleportation-covariant channels as $||\mathcal{E}_0 - \mathcal{E}_1||_\diamond = ||\rho_{\mathcal{E}_0} - \rho_{\mathcal{E}_1}||$. (Recall that the diamond distance between two arbitrary channels,

$\mathcal{E}_0$ and $\mathcal{E}_1$, is defined by the maximization of the trace distance $||\mathcal{I}_A \otimes \mathcal{E}_0(\rho_{AB}) - \mathcal{I}_A \otimes \mathcal{E}_1(\rho_{AB})||$ over all possible bipartite input states ρ_{AB}.)

Starting from equation (9), we write lower and upper bounds using the Fuchs–van de Graaf relations[111] and the quantum Chernoff bound (QCB)[17]. Recall that, in discriminating a pair of multicopy states $\rho_0^{\otimes n}$ and $\rho_1^{\otimes n}$, the minimum error probability $p_{\rm err} = [1 - D(\rho_0^{\otimes n}, \rho_1^{\otimes n})]/2$ satisfies the fidelity lower bound[111] and the QCB[17]

$$p_{\rm err} \geq \frac{1-\sqrt{1-F(\rho_0,\rho_1)^{2n}}}{2} := F_-^{(n)}(\rho_0,\rho_1) \tag{10}$$

$$p_{\rm err} \leq \frac{Q(\rho_0,\rho_1)^n}{2}, Q := \inf_{s\in[0,1]} {\rm Tr}(\rho_0^s \rho_1^{1-s}) \tag{11}$$

In particular, for arbitrary Gaussian states[5] ρ_0 and ρ_1, we know formulas for computing the fidelity[112] and the QCB[18]. These inequalities can be extended to the adaptive error probability of equation (9) valid for jointly teleportation-covariant channels, so that we may write[23]

$$F_-^{(n)}(\rho_{\mathcal{E}_0},\rho_{\mathcal{E}_1}) \leq p_{\rm err}(\mathcal{E}_0,\mathcal{E}_1) \leq \frac{Q(\rho_{\mathcal{E}_0},\rho_{\mathcal{E}_1})^n}{2} \tag{12}$$

with asymptotic functionals over bosonic Choi matrices.

The results from equations (9) and (12) apply to many cases, including the adaptive discrimination of Pauli channels, erasure channels, and noise parameters in bosonic Gaussian channels, such as the thermal number $\bar{n}$ of two thermal-loss channels $\mathcal{E}_{\eta,\bar{n}_0}$ and $\mathcal{E}_{\eta,\bar{n}_1}$. Unfortunately, they do not apply to the discrimination of transmissivity η, because $\mathcal{E}_{\eta_0,\bar{n}}$ and $\mathcal{E}_{\eta_1,\bar{n}}$ are not jointly teleportation-covariant. Thus, the optimal discrimination of bosonic loss is still unknown. What we currently know is that block-assisted strategies based on entangled states may greatly outperform block strategies without assistance, especially at the low-photon-number regime. This observation is at the basis of quantum reading and quantum illumination.

Quantum reading of classical data

In 2011, Pirandola[35] showed how the readout of classical data from an optical digital memory can be modelled as a problem of quantum channel discrimination. In the most basic description, an optical classical memory can be seen as an array of cells described as microscopic beamsplitters with different reflectivities. Each cell stores an information bit $u = 0,1$ in two equiprobable and typically-high reflectivities, the pit reflectivity $\eta_0 \in (0,1)$ and the land reflectivity $\eta_1 > \eta_0$ (Fig. 2). This single-cell model is equivalent to a black-box model read in reflection so that the reflectivity plays the role of the transmissivity parameter. The readout may also be affected by (relatively low) thermal noise, for example, due to stray photons generated by the source. Thus the readout corresponds to discriminating between two thermal-loss channels, $\mathcal{E}_0 := \mathcal{E}_{\eta_0,\bar{n}}$ and $\mathcal{E}_1 := \mathcal{E}_{\eta_1,\bar{n}}$, with different reflectivity, η_0 and η_1, but fixed thermal number $\bar{n}$. Other decoherence effects may be included[35], for example, optical diffraction, memory effects and inter-bit interference[36].

We may consider different 'transmitters' composed of signal modes probing the cell and reference modes assisting detection. The coherent-state transmitter only uses n signal modes in identical coherent states $|\alpha\rangle_s\langle\alpha|^{\otimes n}$. More powerfully, we may define a 'classical' transmitter in the quantum-optical sense. This is a block-assisted protocol employing mixtures of coherent states $\int {\rm d}^{2n}\boldsymbol{\alpha}\mathcal{P}(\boldsymbol{\alpha})|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|$, where $\mathcal{P}(\boldsymbol{\alpha})$ is a probability distribution of amplitudes $\boldsymbol{\alpha}$, and $|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|$ is a multimode coherent state with n signal modes and n reference modes. The optimal classical transmitter has to be compared with an Einstein–Podolsky–Rosen (EPR) transmitter. This is a block entanglement-assisted protocol where we send part of n TMSV states $\Phi_{sr}^{\mu\otimes n}$, so that each signal mode is entangled with a reference or 'idler' mode. For both classical and EPR transmitters, the input $2n$-mode state ρ_{sr} is transformed by the cell into an output state $\sigma_u := \mathcal{E}_u^{\otimes n} \otimes \mathcal{I}^{\otimes n}(\rho_{sr})$ for the n reflected signal modes and the n kept reference modes. This output is detected by an optimal quantum measurement[15] with some error probability. We then compare the information retrieved by the classical transmitter $J_{\rm class}$ and the EPR transmitter $J_{\rm EPR}$ in terms of gain $\Delta := J_{\rm EPR} - J_{\rm class}$. Positive values $\Delta > 0$ means quantum advantage.

A fair comparison between these transmitters involves fixing the mean number of signal photons probing the cell. One type of constraint is 'local', meaning that we fix the mean number of photons N in each probing, so that the total energy scales as nN. We may write the following bound for the error probability $p_{\rm class}$ achievable by any classical transmitter[35]

$$p_{\rm class} \geq \mathcal{C}(n,N) := \frac{1-\sqrt{1-F(N)^{2n}}}{2} \tag{13}$$

where $F(N)$ is the fidelity between $\mathcal{E}_0(|\sqrt{N}\rangle\langle\sqrt{N}|)$ and $\mathcal{E}_1(|\sqrt{N}\rangle\langle\sqrt{N}|)$ generated by an input coherent state with N mean photons. This leads to $J_{\rm class}(n,N) \leq 1 - H_2[\mathcal{C}(n,N)]$. For the EPR transmitter, the QCB provides $J_{\rm EPR} \geq 1 - H_2[Q(\rho_{\mathcal{E}_0}^{\mu},\rho_{\mathcal{E}_1}^{\mu})^n/2]$, where $\rho_{\mathcal{E}_u}^{\mu}$ is generated by a TMSV state Φ_{sr}^{μ} with $\mu = 2N+1$. These bounds provide a sufficient condition for proving $\Delta > 0$.

Positive values of Δ are typical at low signal photon numbers. When the land reflectivity is high $\eta_1 \to 1$ (ideal cell), one finds analytical expressions[37] and regimes where $\Delta \to 1$ bit per cell. This extremal value means that the EPR transmitter fully reads the cell, while classical transmitters do not retrieve information, an advantage that might be used to design cryptographic memories[38]. Another type of energy constraint is 'global', meaning that we fix the mean total number of photons $N_{\rm T}$, so that we employ an average of $N_{\rm T}/n$ photons per use. Let us call n the 'bandwidth' of the transmitter. One can show that, at sufficiently low photons $N_{\rm T} \lesssim 10$, a narrowband EPR transmitter (for example, monochromatic $n_{\rm EPR} = 1$) is able to beat arbitrary classical transmitters, even with extremely large bandwidths. Because a few entangled photons can retrieve more information than any classical source of light, one may work at very low energies, a regime that may potentially be mapped into faster optical readers and denser memories[35].

Quantum reading has been extensively studied[35–53] and the term is today unambiguously associated with the quantum-enhanced readout of classical information from optical memories (therefore it should not to be confused with other applications of channel discrimination, such as communication via control-unitaries between registers of a quantum computer[113]). Already in 2011, a follow-up work[39] extended the model to multi-cell error correction and introduced the notion of quantum reading capacity[36,39], later shown to be super-additive[40]. Another work[41] studied the error exponent for quantum reading and defined a similar notion of reading capacity[42], a quantity that has been recently reconsidered[43]. Note that a two-way notion of quantum reading capacity is immediately given by extending the original definition[39] to adaptive channel discrimination[23], with adaptive-to-block simplification[32] for jointly teleportation-covariant channels[23,34]. Then, ref. [44] showed that Fock states are optimal for (non-adaptive) reading of an ideal cell in noiseless conditions and that suitable entangled states (with the signal beam in a number-diagonal reduced state) may also provide a positive quantum advantage. This latter class of states was also found to be optimal for non-adaptive discrimination of single-mode and multi-mode pure-loss channels[45].

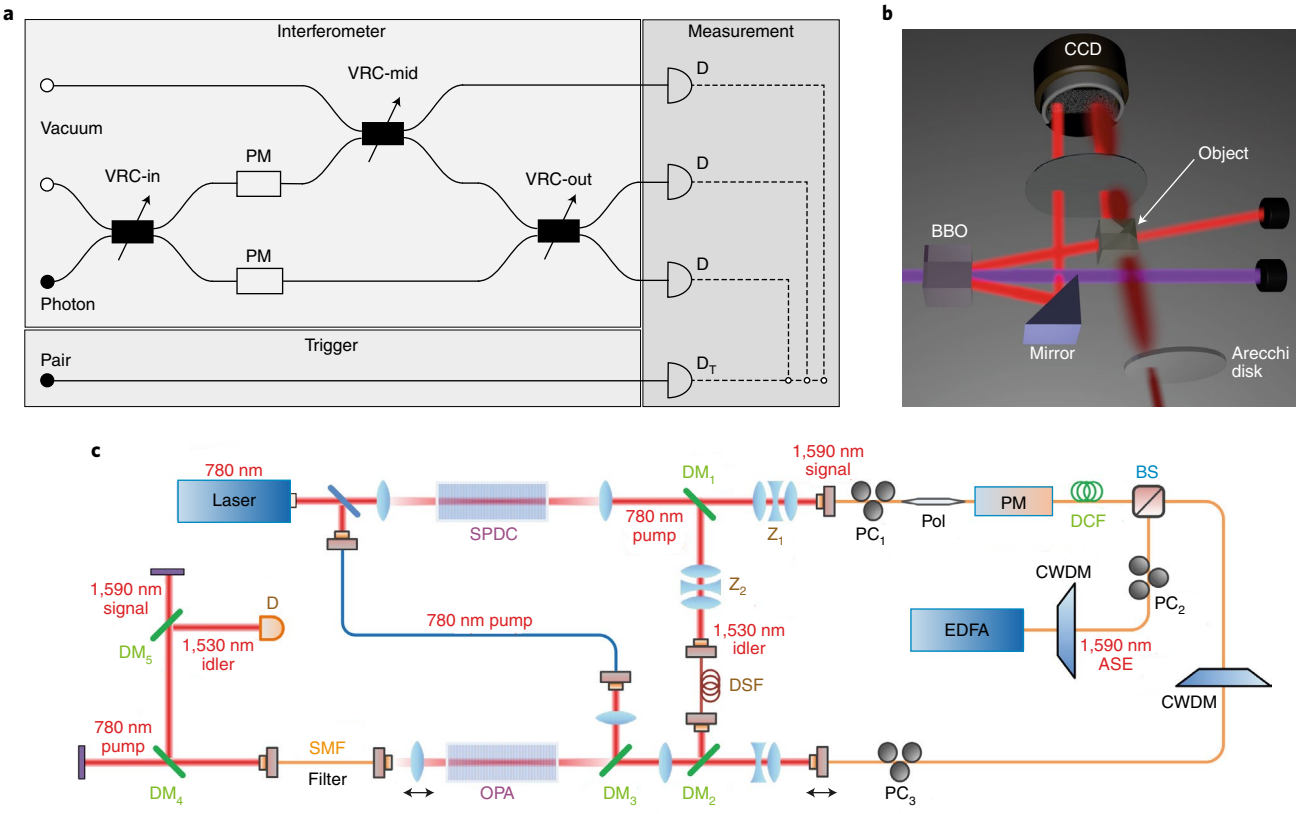


Fig. 3 | Experimental demonstrations of quantum reading and quantum illumination. a, Experimental set-up of perfect quantum reading[49]. A photon-pair source is used to generate a heralded single photon using a trigger detector (D_T). The heralded single photon is fed into a Mach–Zehnder interferometer with variable ratio couplers (VRCs) and phase modulators (PMs) to add additional phase shifts. Coincidence detection of the outputs are used to discriminate between two possible splitting ratios of VRC-mid. With the perfect beamsplitter under test ($\eta_1 = 1$), only one of the detectors (D) at the output of the interferometer would detect the photon (Hong–Ou–Mandel effect). For the non-perfect beamsplitter ($\eta_0 < 1$), any of the two other detectors would detect the photon (due to the additional phase shift). **b**, Quantum illumination experiment of Lopaeva et al.[67] (see also ref. [68]). Both beams of a photon-pair source are detected by a photon-counting CCD camera. In the experiment the target object is a 50:50 beamsplitter placed in one of the beams. The beamsplitter is simulated to be in a thermal environment by illuminating it with scattered light from an Arecchi disk. **c**, In the quantum illumination experiment of Zhang et al.[70], photon pairs are generated by spontaneous parametric downconversion (SPDC) at two different wavelengths and split using a dichroic mirror (DM). One of the photons is stored in a delay line using a dispersion-shifted LEAF fibre (DSF). The other photon is phase modulated (PM). A lossy and noisy environment is simulated by a beamsplitter (BS) and amplified spontaneous emission (ASE) from an erbium-doped fibre amplifier (EDFA). The joint detection is implemented using an optical parameteric amplifier (OPA) whose output is detected by a p–i–n photodetector (D). DCF, dispersion-compensating fibre; POL, polarizer; CWDM, coarse wavelength-division multiplexer; PC, polarization controller; Z, zoom lens. Thin lines are optical fibre, thick lines are unguided propagation. Figure adapted from: **a**, ref. [49], APS; **b**, ref. [67], APS; **c**, ref. [70], APS.

Reference [46] proposed an alternative model based on a binary phase encoding and showed how entangled coherent states may achieve error-free quantum reading. Non-Gaussian entangled states were also considered in other literature[47]. Reference [48] studied a noise-free unitary model of quantum reading where both the inputs of the unknown beamsplitter are accessible for probing and both its outputs for detection. Assuming a single probe per cell ($n = 1$), it was found that the optimal (non-adaptive) two-mode input is the superposition of a N00N state and the vacuum $|00\rangle$. This approach was extended[50] to unambiguous quantum reading, where the statistical error is replaced by an inconclusive result.

Similar to ref. [46], another work[49] also considered a version of perfect quantum reading with zero discrimination error. This is possible by designing an ideal cell that is either a beamsplitter with perfect reflectivity ($\eta_1 = 1$) or a beamsplitter with lower reflectivity $\eta_0 < 1$ and suitable $\pm\pi/2$ phase shifters at the input and output ports. This scheme was experimentally implemented[49]. The set-up consisted of a Mach–Zehnder interferometer with the variable beamsplitter situated in one arm. A single photon from a heralded single-photon source was injected into the interferometer and detected by one of the three detectors located at the two outputs of the interferometer and at the second output port of the beamsplitter under test. Coincidence counts with the heralding detector were measured. Due to the Hong–Ou–Mandel effect only coincidence counts with one of the detectors at the output were observed for the beamsplitter with perfect reflectivity. For the beamsplitters with lower reflectivity however, reduced coincidence counts were measured. See Fig. 3a for more details.

Quantum illumination of targets

Quantum sensing can be used not only to enhance the readout of information from classical systems, but also to boost the standoff detection of remote objects. This idea was first pushed forward by the efforts of Lloyd, Shapiro and collaborators[54–56]. In 2008, Lloyd[54] designed a qubit-based protocol of quantum illumination, showing how the detection of a low-reflectivity target object can be enhanced by quantum entanglement. The advantage of the entangled transmitter over non-entangled ones is achieved even if the entanglement

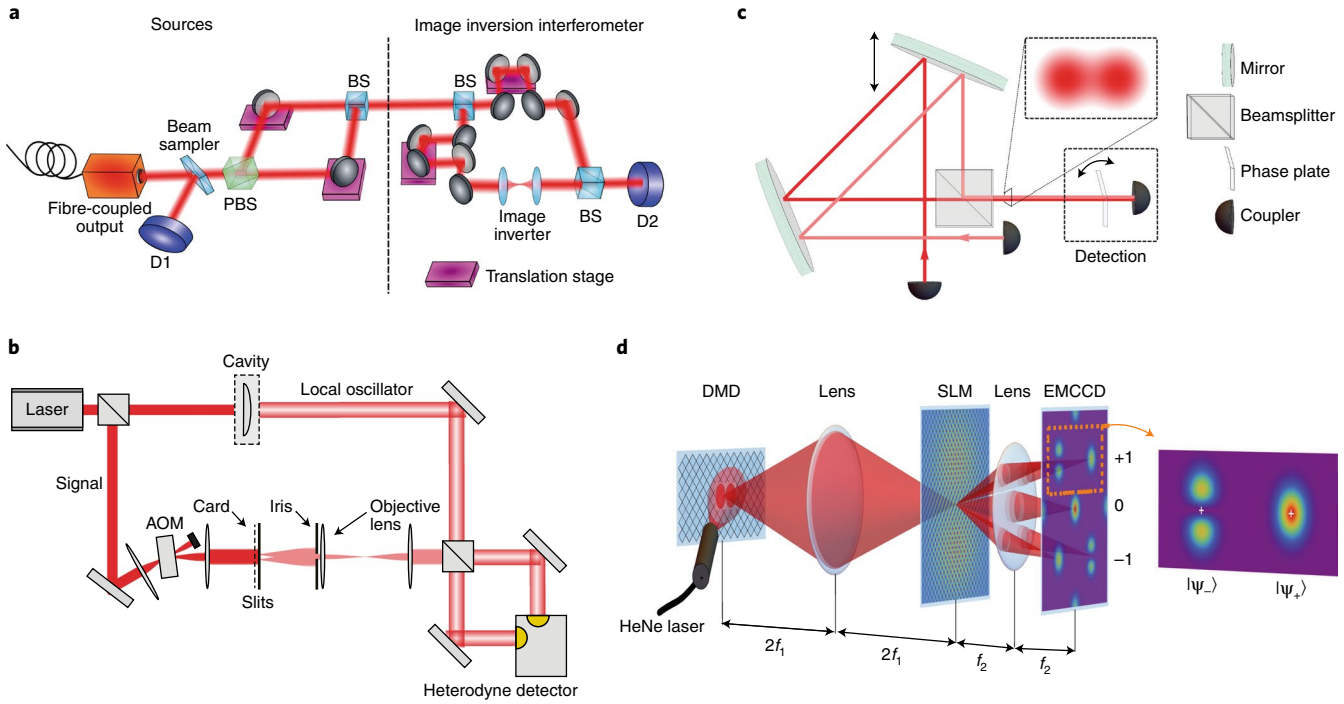


Fig. 4 | Proof-of-principle experiments demonstrating a quantum detection scheme able to measure a distance of two incoherent point-like sources better than the Rayleigh limit. a, In the experiment of Tang et al.[79], a HeNe laser with fibre-coupled output is split at a polarizing beamsplitter (PBS) into two beams of orthogonal polarization. They are recombined at a beamsplitter (BS) with a slight lateral displacement to simulate two incoherent light sources. The light sources are imaged using an image inversion interferometer, a Mach–Zehnder interferometer with an image inverter consisting of two lenses in one arm. One output of the interferometer is detected by a photodetector (D2). **b**, In the experiment of Yang et al.[81], the signal beam is frequency shifted by an acousto-optical modulator (AOM) and illuminates slits. A paper card is placed in front of the slits to make the illumination incoherent. The signal beam is measured by heterodyne detection using a local oscillator prepared in TEM_{01} mode by means of an optical cavity. **c**, In the experiment of Tham et al.[82], two partially overlapping beams (as shown in the upper inset) are generated by coupling laser light out of a fibre and combining them on a beamsplitter. The distance between the beams can be controlled by the position of the upper mirror. The separation of the two beams is detected by projecting the beams onto a mode orthogonal to TEM_{00}, in this case a spatially antisymmetric field mode. This is performed by passing the two beams through a phase plate that is built in such a way that it introduces different phase shifts between opposite halves of the beam and aligned such that coupling into a well-aligned fibre coupler is minimized. The coupling into a single-mode fibre corresponds to a projection onto the TEM_{00} mode, thus together with the phase plate the beams are projected onto a mode orthogonal to TEM_{00}. **d**, In the experiment of Paúr et al.[83], two closely spaced incoherent beams are generated by using a high-frequency switched digital micromirror chip (DMD) illuminated by a HeNe laser. The beam is projected onto different modes by an amplitude spatial light modulator (SLM) generating a digital hologram. The first-order diffraction spectrum is detected by an electron-multiplying CCD (EMCCD) camera. *f*, focal length; $|\psi_+\rangle$, symmetric state; $|\psi_-\rangle$, antisymmetric state. Figure adapted from: **a**, ref. [79], OSA; **b**, ref. [81], OSA; **c**, ref. [82], APS; **d**, ref. [83], OSA.

itself is completely lost after reflection from the target. In fact, the initial signal–idler entanglement is mapped into residual but yet quantum correlations between the reflected signal and the kept idler that a suitably designed quantum detector may 'amplify' with respect to the thermal background.

In the same year, a team led by Shapiro[55] proposed a practical version of quantum illumination based on continuous-variable systems[5,6]. In ref. [55], a Gaussian protocol is described where bosonic modes are prepared in Gaussian states and sent to detect an object with low reflectivity $\eta \simeq 0$ in a region with bright thermal noise, that is, with $\bar{n} \gg 1$ mean thermal photons. The detection process can be modelled as the discrimination between a zero-reflectivity thermal-loss channel $\mathcal{E}_{\eta=0,\bar{n}}$ (target absent) and a low-reflectivity thermal-loss channel $\mathcal{E}_{\eta,\bar{n}'}$ with $\eta \simeq 0$ and $\bar{n}' = \bar{n}/(1-\eta)$ (target present). Here the factor $(1-\eta)^{-1}$ excludes a 'passive signature' that is the possibility of detecting the target by just measuring a lower received background level. As also depicted in Fig. 2, one can assume that the detector's noise does not depend on the presence of the target.

In this set-up, we assume a local energy constraint, so that N mean photons are irradiated by each of the n bosonic modes sent over the target. Under this assumption, we compute the error probability associated with the various transmitters. In particular, we exploit the bounds in equations (10) and (11) to compare the performance of the EPR transmitter (based on TMSV states) with that of the classical transmitter. In the regime of low-energy signals ($N \ll 1$) and many modes ($n \gg 1$), the EPR transmitter has the scaling[55] $p_{\mathrm{EPR}}^{\mathrm{err}} \simeq \exp(-n\eta N/\bar{n})/2$, which clearly outperforms the classical transmitter $p_{\mathrm{class}}^{\mathrm{err}} \geq \exp(-n\eta N/2\bar{n})/4$. In particular, $p_{\mathrm{EPR}}^{\mathrm{err}}$ realizes a 6 dB advantage in the error-probability exponent over the coherent-state transmitter $p_{\mathrm{CS}}^{\mathrm{err}} \simeq \exp(-n\eta N/4\bar{n})/2$. Zhuang et al.[57] proved that the theoretical limit $p_{\mathrm{EPR}}^{\mathrm{err}}$ can be achieved by an explicit quantum receiver based on feed-forward sum-frequency generation. This receiver has also been used to show the quantum illumination advantage in terms of detection probability versus false-alarm probability[58].

In 2015, Gaussian quantum illumination was extended to the microwave regime, thus providing a prototype of quantum radar[59]. In this scheme, an electro-optomechanical converter[114,115] transforms an optical mode into microwave. If this transducer has high quantum efficiency, then optical–optical entanglement is translated into microwave–optical entanglement. The microwave signal is sent to probe the target region, while the optical idler is retained.

The microwave radiation collected from the target region is then phase conjugated and upconverted into an optical field by a second use of the transducer. The optical output is finally combined with the retained idler in a joint detection based on a practical receiver design[60]. In this way, ref. [59] reports that the error probability of microwave quantum illumination is superior to that of any classical radar of equal transmitted energy. A follow-up analysis has been recently carried out[61].

More recently, another study[62] considered the protocol of quantum illumination using the tools of quantum metrology so as to measure the reflectivity of the target. They employed the QFI to bound the error probability showing a 3-dB enhancement of the signal-to-noise ratio with respect to the use of local measurements. They also considered non-Gaussian Schrödinger's cat states. Other studies have quantified the quantum illumination advantage in terms of 'consumption' of discord associated with the target[63], and in terms of mutual information[64]. Finally note that quantum illumination has been also studied as an asymmetric Gaussian discrimination problem[65,66,116,117]. In this asymmetric setting, TMSV states have been identified as optimal probes for asymptotic discrimination, also in the adaptive case[66,117]. However, in the standard symmetric setting, finding the ultimate adaptive performance achievable by Gaussian quantum illumination remains an open question, while this problem has been recently solved for the discrete-variable version[28].

Several experiments of quantum illumination have been reported[67–70]. As depicted in Fig. 3b, Lopaeva et al.[67] exploited a parametric downconversion source using a beta-barium borate (BBO) crystal to generate two intensity-correlated light beams in orthogonal polarizations at 710 nm. Both beams were detected by a photon-counting high-quantum-efficiency charge-coupled device (CCD) camera. The target object, a 50:50 beamsplitter in the experiment, was placed in one of the two entangled beams before detection. The beamsplitter object was illuminated by photons scattered on an Arecchi's rotating ground glass to simulate a thermal environment. A single captured image was used to measure the second-order correlations between the two beams. The implementation shows robustness against noise and losses; it also demonstrates a quantum enhancement in target detection in thermal environments even when non-classicality is lost. However, coincidence detection of spontaneous parametric downconversion is not the optimal detection method to extract the most information from the signal–idler entangled modes, and the implemented classical scheme using weakly thermal states is also non-optimal.

Adopting a different approach, in 2013 Zhang et al.[69] reported a secure communication experiment based on quantum illumination, in a set-up of two-way quantum key distribution[118]. More recently, Zhang et al.[70] demonstrated the advantage of quantum illumination over coherent states by using broadband entangled Gaussian states, as produced by continuous-wave spontaneous parametric downconversion. In the experiment shown in Fig. 3c, the signal modes were phase modulated before probing the weakly reflecting target, while the idler modes were stored in a delay line. The joint measurement was performed by combining the reflected signal modes and the idler modes with a pump in another optical parametric amplifier. The output on the order of nanowatts was then detected by a p–i–n photodetector with high gain and low noise. They showed a 20% improvement of the signal-to-noise ratio in comparison to the optimal classical scheme in an environment exhibiting 14 dB loss and a thermal background 75 dB above the returned probe light.

Optical resolution beyond the Rayleigh limit

The Rayleigh criterion is a well-known result in classical imaging. Two point-like sources cannot be optically resolved (in the far field) if they are closer than the Rayleigh length $\simeq \lambda/a$, where λ is the wavelength of the emitted light and a is the numerical aperture of the observing lens. For this reason, if we use a converging optical system to focus light on a screen and an array of detectors to measure the intensity, the Rayleigh's criterion together with the presence of photon shot noise, can lead to severe limitations in resolving point-like sources.

Various approaches have been implemented to beat the Rayleigh limit in both the near field[119–122] and the far field[123–126]. Achieving sub-diffraction resolution is clearly a well-desired result in microscopy, otherwise limited to features no closer than 0.2 μm. In the far field, the most notable breakthroughs have been achieved in fluorescence microscopy where diffraction has been overcome by stimulated emission depletion (STED)[123]. In STED, the idea is to use a light pulse to excite a volume of fluorescent molecules, followed by another pulse quenching fluorescence from all molecules but a middle nanometre-sized volume. While scanning the sample, only the light levels from the central volumes are registered, so that an image is reconstructed with nanometre resolution[124]. In general, far-field super-resolved microscopy[124,125] is based on switchable fluorophores and localization algorithms, with the positions of the fluorophores being inferred from the images[126]. Point sources may be imaged via direct photon-counting, with the Cramér–Rao bound setting the limit for any unbiased estimator[127–129].

The quantum-metrology-inspired measurements can achieve much higher Fisher information and a much lower error than the limits derived in the previous classical techniques. Furthermore, there is no need for switchable fluorophores so that the quantum approach is suitable for both microscopy and telescopy. By considering a fully quantum description of the light and the measurement apparatus, Tsang et al.[72] showed the existence of a quantum detection scheme able to measure the distance between two point-like sources with a constant accuracy, even when the sources have sub-wavelength separation. This ground-breaking result was achieved by addressing the resolution of two incoherent point-like sources with the tools of quantum estimation theory.

The theory behind these results was extended from incoherent sources emitting faint pulses to thermal sources of arbitrary brightness[73,74]. In general, ref. [73] established a connection between optical resolution and bosonic channel estimation, so that measuring the separation between two point-like sources is equivalent to estimating the loss parameters of two lossy channels. In this way, the authors of ref. [73] developed a theory of super-resolution for point-like sources emitting light in a generic state, that is, attenuated or bright, classical, coherent, incoherent, as well as entangled (for example, in a microscope set-up). The ultimate resolution was found as a function of the optical properties of the two sources and their separation[73] (see also the adaptive lower bound in ref. [28]). In particular, super-resolution can be enhanced when the sources emit entangled or quantum-correlated (discordant) light[73].

More recently, ref. [75] extended Tsang and colleagues' analysis from a Gaussian point spread function to a hard-aperture pupil, proving the information optimality of image-plane sinc-Bessel modes. They also generalized the result to an arbitrary point spread function. Another work[76] investigated the optimal measurements for beating the Rayleigh limit, while ref. [77] explored the use of homodyne or heterodyne detection. Finally, ref. [78] reported the quantum-optimal detection of one-versus-two incoherent optical sources.

Shortly after the idea of Tsang et al.[72] was presented, it was experimentally verified in several proof-of-principle experiments. The first experiment by Tang et al.[79] was based on super-localization by image inversion interferometry[80]. As shown in Fig. 4a, they used an image inversion interferometer to determine the separation of two incoherent point sources, generated by two laser beams in orthogonal polarizations stemming from the same HeNe laser. Using the light from the simulated sources as input, the interferometer was implemented as a Mach–Zehnder interferometer with image inversion generated by a lens system in one arm. The other arm was

delayed so that the detector at the output of the interferometer ideally showed no response for zero separation due to destructive interference. With growing separation of the two sources the destructive interference becomes more and more imperfect, yielding an optical resolution beyond the Abbe–Rayleigh limit.

Yang et al.[81] used heterodyne detection with a local oscillator in TEM_{01} mode to detect the separation of the two slits in a double-slit configuration beyond the classical resolution limit. As depicted in Fig. 4b, they used paper to achieve incoherence and diffuse transmission. Measuring at a frequency of some MHz to avoid noise at lower frequencies, the beat between the local oscillator and the beam illuminating the slits becomes zero if the separation is zero. Separating the two slits yields a measurement beyond the Abbe limit. While the scheme requires the two sources to be exactly aligned to the centre of the TEM_{01} mode, using higher-order TEM modes will provide general sub-Rayleigh imaging. Other experiments by Tham et al.[82] and Paúr et al.[83] are reported in Fig. 4c,d. Let us conclude that super-resolving quantum imaging is a hot topic and other experiments could be mentioned[84–86].

Discussion and outlook

Quantum sensing is a rapidly evolving field with many potential implications. Despite the great advances that have been achieved in recent years, a number of problems and experimental challenges remain open. From the point of view of the basic theoretical models of quantum metrology and hypothesis testing, we may often compute the ultimate performances allowed by quantum mechanics. However, we do not know in general how to implement the optimal measurements achieving these performances and/or what optimal states we need to prepare at the input of the unknown quantum channel. Then, do we need to consider feedback and perform adaptive protocols? For instance, this is an open question for both estimation and discrimination of bosonic loss, which is at the basis of quantum reading, Gaussian quantum illumination and quantum-enhanced optical super-resolution.

From a more practical and experimental point of view, there are non-trivial challenges as well. Despite a first proof-of-principle demonstration[49] based on the unitary discrimination of beamsplitters, we do not have yet a truly quantum reading experiment where a single output of the cells is effectively accessed for the readout. A full demonstration would involve an actual (one- or two-dimensional) array of optical cells, where information is stored with classical codes and the quantum readout is performed on blocks of cells. This idea may be further developed into an experiment of bosonic quantum pattern recognition where the use of entanglement across an array may boost the resolution of problems of data clustering.

Quantum illumination has had various experimental demonstrations[67–70]. Challenges become non-trivial when we consider the microwave regime[59]. Here the development of highly efficient microwave–optical converters could mitigate experimental issues related with the generation of microwave entanglement and the detection of microwave fields at the single-photon level. Furthermore these converters are highly desired for other applications, in particular as interfaces between superconducting quantum chips and optical fibres in a potential hybrid quantum Internet[92].

Other designs of quantum radar are possible. For instance, as already suggested in ref. [59], a fully microwave implementation of quantum illumination (without converters) may be achieved using a superconducting Josephson parametric amplifier to generate signal–idler microwave entanglement. Reflected signals could then be phase conjugated via another parametric amplifier, recombined with the idlers, and finally measured, for example, by using a transmon qubit as a single-photon detector. The idea of using Josephson mixers and photocounters was later studied [71] with the aim of using microwave quantum illumination to reveal phase shift induced by cloaking.

Other experimental challenges need to be addressed in order to build an actual quantum radar. An important aspect is the preservation of the idler modes while the signals are being propagated forward and back from the target. The idlers should be kept in a low-loss delay line or stored in quantum registers with sufficiently long coherence times, until the final joint detection. Then, unlike classical radars, whose performance improves as the signal power is increased at constant bandwidth, for the quantum counterpart the bandwidth needs to be increased at constant signal brightness. The challenge is therefore to generate microwave pulses with a time–bandwidth product of 10^6 modes or more. Furthemore, classical radars can interrogate many potential target bins with a single pulse, while present models of quantum radar may only query a single polarization, azimuth, elevation, range, Doppler bin at a time. This is an area that needs development with very promising steps forward[130].

On the basis of current and next-available quantum technology, it is foreseen that the main application of quantum radar will be at relatively short ranges, where it may achieve the same detection performance of classical radars but using orders-of-magnitude fewer numbers of photons. In general, low-power radars are interesting not only for stealthy short-range target detection but also for proximity sensing and environmental scanning in robotic applications. The principles of quantum radar may also be developed into a non-invasive form of quantum microwave spectroscopy, with direct applications to condensed-matter physics (solid or atomic spins) and rotational spectroscopy (molecular rotors, organic molecules).

Regarding the experimental challenges for super-resolution[79], most of the current schemes, from spatial-mode demultiplexing to super-localization by image inversion and heterodyne, rely on the assumption that we need to know the location of the centroid of the sources in order to get full quantum-optimal resolution. In general, this location is not exactly known[79,81–83], so that achieving maximum alignment before estimating the separation becomes an important step to optimize the performance in a realistic implementation. On the theoretical side, it would be interesting to quantify the performance of adaptive quantum schemes, for instance in microscope-like set-ups.

Received: 21 February 2018; Accepted: 18 October 2018;
Published online: 28 November 2018

References

1. Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
2. Hayashi, M. *Quantum Information Theory: Mathematical Foundation* (Springer-Verlag, Berlin, Heidelberg, 2017).
3. Watrous, J. *The Theory of Quantum Information* (Cambridge University Press, Cambridge, 2018).
4. Andersen, U. L., Neergaard-Nielsen, J. S., van Loock, P. & Furusawa, A. Hybrid discrete- and continuous-variable quantum information. *Nat. Phys.* **11**, 713–719 (2015).
5. Weedbrook, C. et al. Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621–669 (2012).
6. Braunstein, S. L. & Van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* **77**, 513–577 (2005).
7. Adesso, G., Ragy, S. & Lee, A. R. Continuous variable quantum information: Gaussian states and beyond. *Open Syst. Inf. Dyn.* **21**, 1440001 (2014).
8. Serafini, A. *Quantum Continuous Variables: A Primer of Theoretical Methods* (Taylor & Francis, Oxford, 2017).
9. Degen, C. L., Reinhard, F. & Cappellaro, P. Quantum sensing. *Rev. Mod. Phys.* **89**, 035002 (2017).
10. Braunstein, S. L. & Caves, C. M. Statistical distance and the geometry of quantum states. *Phys. Rev. Lett.* **72**, 3439–3443 (1994).
11. Braunstein, S. L., Caves, C. M. & Milburn, G. J. Generalized uncertainty relations: theory, examples, and Lorentz invariance. *Ann. Phys.* **247**, 135–173 (1996).
12. Giovannetti, V., Lloyd, S. & Maccone, L. Quantum-enhanced measurements: beating the standard quantum limit. *Science* **306**, 1330–1336 (2004).

13. Giovannetti, V., Lloyd, S. & Maccone, L. Advances in quantum metrology. *Nat. Photon.* **5**, 222–229 (2011).
14. Braun, D. et al. Quantum enhanced measurements without entanglement. *Rev. Mod. Phys.* **90**, 035006 (2018).
15. Helstrom, C. W. *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
16. Barnett, S. M. & Croke, S. Quantum state discrimination. *Adv. Opt. Photon.* **1**, 238–278 (2009).
17. Audenaert, K. M. R. et al. Discriminating states: the quantum Chernoff bound. *Phys. Rev. Lett.* **98**, 160501 (2007).
18. Pirandola, S. & Lloyd, S. Computable bounds for the discrimination of Gaussian states. *Phys. Rev. A* **78**, 012331 (2008).
19. Hayashi, M. Discrimination of two channels by adaptive methods and its application to quantum system. *IEEE Trans. Inf. Theory* **55**, 3807–3802 (2009).
20. Harrow, A. W., Hassidim, A., Leung, D. W. & Watrous, J. Adaptive versus nonadaptive strategies for quantum channel discrimination. *Phys. Rev. A* **81**, 032339 (2010).
21. Cooney, T., Mosonyi, M. & Wilde, M. M. Strong converse exponents for a quantum channel discrimination problem and quantum-feedback-assisted communication. *Commun. Math. Phys.* **344**, 797–829 (2016).
22. Giovannetti, V., Lloyd, S. & Maccone, L. Quantum metrology. *Phys. Rev. Lett.* **96**, 010401 (2006).
23. Pirandola, S. & Lupo, C. Ultimate precision of adaptive noise estimation. *Phys. Rev. Lett.* **118**, 100502 (2017).
24. Takeoka, M. & Wilde, M. M. Optimal estimation and discrimination of excess noise in thermal and amplifier channels. Preprint at https://arxiv.org/abs/arXiv:1611.09165 (2016).
25. Zhou, S., Zhang, M., Preskill, J. & Jiang, L. Achieving the Heisenberg limit in quantum metrology using quantum error correction. *Nat. Commun.* **9**, 78 (2018).
26. Demkowicz-Dobrzanski, R., Czajkowski, J. & Sekatski, P. Adaptive quantum metrology under general Markovian noise. *Phys. Rev. X* **7**, 041009 (2017).
27. Cope, T. P. W. & Pirandola, S. Adaptive estimation and discrimination of Holevo-Werner channels. *Quantum Meas. Quantum Metrol.* **4**, 44–52 (2017).
28. Pirandola, S., Laurenza, R. & Lupo, C. Fundamental limits to quantum channel discrimination. Preprint at https://arxiv.org/abs/arXiv:1803.02834 (2018).
29. Nielsen, M. A. & Chuang, I. L. Programmable quantum gate arrays. *Phys. Rev. Lett.* **79**, 321–324 (1997).
30. Ji, Z., Wang, G., Duan, R., Feng, Y. & Ying, M. Parameter estimation of quantum channels. *IEEE Trans. Inf. Theory* **54**, 5172–5185 (2008).
31. Demkowicz-Dobrzański, R. & Maccone, L. Using entanglement against noise in quantum metrology. *Phys. Rev. Lett.* **113**, 250801 (2014).
32. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017).
33. Pirandola, S. et al. Theory of channel simulation and bounds for private communication. *Quantum Sci. Technol.* **3**, 035009 (2018).
34. Laurenza, R., Lupo, C., Spedalieri, G., Braunstein, S. L. & Pirandola, S. Channel simulation in quantum metrology. *Quantum Meas. Quantum Metrol.* **5**, 1–12 (2018).
35. Pirandola, S. Quantum reading of a classical digital memory. *Phys. Rev. Lett.* **106**, 090504 (2011).
36. Lupo, C., Pirandola, S., Giovannetti, V. & Mancini, S. Quantum reading capacity under thermal and correlated noise. *Phys. Rev. A* **87**, 062310 (2013).
37. Spedalieri, G., Lupo, C., Mancini, S., Braunstein, S. L. & Pirandola, S. Quantum reading under a local energy constraint. *Phys. Rev. A* **86**, 012315 (2012).
38. Spedalieri, G. Cryptographic aspects of quantum reading. *Entropy* **17**, 2218–2227 (2015).
39. Pirandola, S., Lupo, C., Giovannetti, V., Mancini, S. & Braunstein, S. L. Quantum reading capacity. *New J. Phys.* **13**, 113012 (2011).
40. Lupo, C. & Pirandola, S. Super-additivity and entanglement assistance in quantum reading. *Quantum Inf. Comput.* **17**, 0611–0622 (2017).
41. Guha, S. & Shapiro, J. H. Reading boundless error-free bits using a single photon. *Phys. Rev. A* **87**, 062306 (2013).
42. Guha, S., Dutton, Z., Nair, R., Shapiro, J. H. & Yen, B. Information capacity of quantum reading. In *Conference on Laser Science XXVII* Paper LTuF2 (OSA, 2011).
43. Das, S. & Wilde, M. M. Quantum reading capacity: general definition and bounds. Preprint at https://arxiv.org/abs/arXiv:1703.03706 (2017).
44. Nair, R. Discriminating quantum-optical beam-splitter channels with number-diagonal signal states: applications to quantum reading and target detection. *Phys. Rev. A* **84**, 032312 (2011).
45. Nair, R. & Yen, B. J. Optimal quantum states for image sensing in loss. *Phys. Rev. Lett.* **107**, 193602 (2011).
46. Hirota, O. Error free quantum reading by quasi Bell state of entangled coherent states. *Quantum Meas. Quantum Metrol.* **4**, 70–73 (2017).
47. Prabhu Tej, J., Usha Devi, A. R. & Rajagopal, A. K. Quantum reading of digital memory with non-Gaussian entangled light. *Phys. Rev. A* **87**, 052308 (2013).
48. Bisio, A., Dall'Arno, M. & D'Ariano, G. M. Tradeoff between energy and error in the discrimination of quantum-optical devices. *Phys. Rev. A* **84**, 012310 (2011).
49. Dall'Arno, M. et al. Experimental implementation of unambiguous quantum reading. *Phys. Rev. A* **85**, 012308 (2012).
50. Invernizzi, C., Paris, M. G. A. & Pirandola, S. Optimal detection of losses by thermal probes. *Phys. Rev. A* **84**, 022334 (2011).
51. Dall'Arno, M., Bisio, A. & D'Ariano, G. M. Ideal quantum reading of optical memories. *Int. J. Quantum Inf.* **10**, 1241010 (2012).
52. Wilde, M. M., Guha, S., Tan, S.-H., & Lloyd, S. Explicit capacity-achieving receivers for optical communication and quantum reading. In *Proc. 2012 IEEE Int. Symposium on Information Theory* 551–555 (IEEE, 2012).
53. Roga, W. & Buono, D. & Illuminati, F. Device-independent quantum reading and noise-assisted quantum transmitters. *New J. Phys.* **17**, 013031 (2015).
54. Lloyd, S. Enhanced sensitivity of photodetection via quantum illumination. *Science* **321**, 1463–1465 (2008).
55. Tan, S.-H. et al. Quantum illumination with Gaussian states. *Phys. Rev. Lett.* **101**, 253601 (2008).
56. Shapiro, J. H. & Lloyd, S. Quantum illumination versus coherent-state target detection. *New J. Phys.* **11**, 063045 (2009).
57. Zhuang, Q., Zhang, Z. & Shapiro, J. H. Optimum mixed-state discrimination for noisy entanglement-enhanced sensing. *Phys. Rev. Lett.* **118**, 040801 (2017).
58. Zhuang, Z., Zhang, Z. & Shapiro, J. H. Entanglement-enhanced Neyman–Pearson target detection using quantum illumination. *J. Opt. Soc. Am. B* **34**, 1567–1572 (2017).
59. Barzanjeh, Sh. et al. Microwave quantum illumination. *Phys. Rev. Lett.* **114**, 080503 (2015).
60. Guha, S. & Erkmen, B. I. Gaussian-state quantum-illumination receivers for target detection. *Phys. Rev. A* **80**, 052310 (2009).
61. Xiong, B., Li, X., Wang, X.-Y. & Zhou, L. Improve microwave quantum illumination via optical parametric amplifier. *Ann. Phys.* **385**, 757–768 (2017).
62. Sanz, M., Las Heras, U., Garca-Ripoll, J. J., Solano, E. & Di Candia, R. Quantum estimation methods for quantum illumination. *Phys. Rev. Lett.* **118**, 070803 (2017).
63. Weedbrook, C., Pirandola, S., Thompson, J., Vedral, V. & Gu, M. How discord underlies the noise resilience of quantum illumination. *New J. Phys.* **18**, 043027 (2016).
64. Ragy, S. et al. Quantifying the source of enhancement in experimental continuous variable quantum illumination. *J. Opt. Soc. Am. B* **31**, 2045–2050 (2014).
65. Wilde, M. M., Tomamichel, M., Lloyd, S. & Berta, M. Gaussian hypothesis testing and quantum illumination. *Phys. Rev. Lett.* **119**, 120501 (2017).
66. De Palma, G. & Borregaard, J. The minimum error probability of quantum illumination. *Phys. Rev. A* **98**, 012101 (2018).
67. Lopaeva, E. D. et al. Experimental realization of quantum illumination. *Phys. Rev. Lett.* **110**, 153603 (2013).
68. Meda, A. et al. Photon-number correlation for quantum enhanced imaging and sensing. *J. Opt.* **19**, 094002 (2017).
69. Zhang, Z., Tengner, M., Zhong, T., Wong, F. N. C. & Shapiro, J. H. Entanglement's benefit survives an entanglement-breaking channel. *Phys. Rev. Lett.* **111**, 010501 (2013).
70. Zhang, Z., Mouradian, S., Wong, F. N. C. & Shapiro, J. H. Entanglement-enhanced sensing in a lossy and noisy environment. *Phys. Rev. Lett.* **114**, 110506 (2015).
71. Las Heras, U. et al. Quantum illumination reveals phase-shift inducing cloaking. *Sci. Rep.* **7**, 9333 (2017).
72. Tsang, M., Nair, R. & Lu, X.-M. Quantum theory of superresolution for two incoherent optical point sources. *Phys. Rev. X* **6**, 031033 (2016).
73. Lupo, C. & Pirandola, S. Ultimate precision bound of quantum and subwavelength imaging. *Phys. Rev. Lett.* **117**, 190802 (2016).
74. Nair, R. & Tsang, M. Far-field superresolution of thermal electromagnetic sources at the quantum limit. *Phys. Rev. Lett.* **117**, 190801 (2016).
75. Kerviche, R., Guha, S. & Ashok, A. Fundamental limit of resolving two point sources limited by an arbitrary point spread function. Preprint at https://arxiv.org/abs/1701.04913 (2017).
76. Rehacek, J., Paúr, M., Stoklasa, B., Hradil, Z. & Sánchez-Soto, L. L. Optimal measurements for resolution beyond the Rayleigh limit. *Opt. Lett.* **42**, 231–234 (2017).
77. Yang, F., Nair, R., Tsang, M., Simon, C. & Lvovsky, A. I. Fisher information for far-field linear optical superresolution via homodyne or heterodyne detection in a higher-order local oscillator mode. *Phys. Rev. A* **96**, 063829 (2017).

78. Lu, X.-M., Krovi, H., Nair, R., Guha, S. & Shapiro, J. H. Quantum-optimal detection of one-versus-two incoherent optical sources with arbitrary separation. Preprint at https://arxiv.org/abs/1802.02300 (2018).
79. Tang, Z. S., Durak, K. & Ling, A. Fault-tolerant and finite-error localization for point emitters within the diffraction limit. *Opt. Express* **24**, 22004–22012 (2016).
80. Nair, R. & Tsang, M. Interferometric superlocalization of two incoherent optical point sources. *Opt. Express* **24**, 3684–3701 (2016).
81. Yang, F., Taschilina, A., Moiseev, E. S., Simon, C. & Lvovsky, A. I. Far-field linear optical superresolution via heterodyne detection in a higher-order local oscillator mode. *Optica* **3**, 1148–1152 (2016).
82. Tham, W. K., Ferretti, H. & Steinberg, A. M. Beating Rayleigh's curse by imaging using phase information. *Phys. Rev. Lett.* **118**, 070801 (2017).
83. Paúr, M., Stoklasa, B., Hradil, Z., Sánchez-Soto, L. L. & Rehacek, J. Achieving the ultimate optical resolution. *Optica* **3**, 1144–1147 (2016).
84. Gatto Monticone, D. et al. Beating the Abbe diffraction limit in confocal microscopy via nonclassical photon statistics. *Phys. Rev. Lett.* **113**, 143602 (2014).
85. Treps, N. et al. Surpassing the standard quantum limit for optical imaging using nonclassical multimode light. *Phys. Rev. Lett.* **88**, 203601 (2014).
86. Classen, A. et al. Superresolving imaging of arbitrary one-dimensional arrays of thermal light sources using multiphoton interference. *Phys. Rev. Lett.* **117**, 253601 (2016).
87. Tsang, M. Quantum imaging beyond the diffraction limit by optical centroid measurements. *Phys. Rev. Lett.* **102**, 253601 (2009).
88. Rozema, L. A. et al. Scalable spatial superresolution using entangled photons. *Phys. Rev. Lett.* **112**, 223602 (2014).
89. Chiribella, G., D'Ariano, G. M. & Perinotti, P. Quantum circuit architecture. *Phys. Rev. Lett.* **101**, 060401 (2008).
90. Bennett, C. H. et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70**, 1895–1899 (1993).
91. Ishizaka, S. & Hiroshima, T. Asymptotic teleportation scheme as a universal programmable quantum processor. *Phys. Rev. Lett.* **101**, 240501 (2008).
92. Pirandola, S., Eisert, J., Weedbrook, C., Furusawa, A. & Braunstein, S. L. Advances in quantum teleportation. *Nat. Photon.* **9**, 641–652 (2015).
93. Adesso, G., Dell'Anno, F., Siena, S. D., Illuminati, F. & Souza, L. A. M. Optimal estimation of losses at the ultimate quantum limit with non-Gaussian states. *Phys. Rev. A* **79**, 040305(R) (2009).
94. Monras, A. & Paris, M. G. A. Optimal quantum estimation of loss in bosonic channels. *Phys. Rev. Lett.* **98**, 160401 (2007).
95. Whittaker, R. et al. Absorption spectroscopy at the ultimate quantum limit from single-photon states. *New J. Phys.* **19**, 023013 (2017).
96. Moreau, P.-A. et al. Demonstrating an absolute quantum advantage in direct absorption measurement. *Sci. Rep.* **7**, 6256 (2017).
97. Losero, E., Berchera, I. R., Meda, A., Avella, A. & Genovese, M. Unbiased estimation of an optical loss at the ultimate quantum limit with twin-beams. *Sci. Rep.* **8**, 7431 (2018).
98. Samantaray, N., Berchera, I. R., Meda, M. & Genovese, M. Realization of the first sub-shot-noise wide field microscope. *Light Sci. Appl.* **6**, e17005 (2017).
99. Brida, G., Genovese, M. & Berchera, I. R. Experimental realization of sub-shot-noise quantum imaging. *Nat. Photon.* **4**, 227–230 (2010).
100. Abadie, J. et al. A gravitational wave observatory operating beyond the quantum shot-noise limit. *Nat. Phys.* **7**, 962–965 (2011).
101. Schnabel, R., Mavalvala, N., McClelland, D. E. & Lam, P. K. Quantum metrology for gravitational wave astronomy. *Nat. Commun.* **1**, 121 (2010).
102. Banaszek, K., Demkowicz-Dobrzański, R. & Walmsley, I. A. Quantum states made to measure. *Nat. Photon.* **3**, 673–676 (2009).
103. Nagata, T., Okamoto, R., O'Brien, J. L., Sasaki, K. & Takeuchi, S. Beating the standard quantum limit with four-entangled photons. *Science* **316**, 726–729 (2007).
104. Slussarenko, S. et al. Unconditional violation of the shot-noise limit in photonic quantum metrology. *Nat. Photon.* **11**, 700–703 (2017).
105. Dorner, U. et al. Optimal quantum phase estimation. *Phys. Rev. Lett.* **102**, 040403 (2009).
106. Kacprowicz, M., Demkowicz-Dobrzański, R., Wasilewski, W., Banaszek, K. & Walmsley, I. A. Experimental quantum-enhanced estimation of a lossy phase shift. *Nat. Photon* **4**, 357–360 (2010).
107. Higgins, B. L., Berry, D. W., Bartlett, S. D., Wiseman, H. M. & Pryde, G. J. Entanglement-free Heisenberg-limited phase estimation. *Nature* **450**, 393–396 (2007).
108. Yonezawa, H. et al. Quantum-enhanced optical phase tracking. *Science* **337**, 1514–1517 (2012).
109. Xiang, G. Y., Higgins, B. L., Berry, D. W., Wiseman, H. M. & Pryde, G. J. Entanglement-enhanced measurement of a completely unknown optical phase. *Nat. Photon.* **5**, 43–47 (2011).
110. Berni, A. A. et al. Ab initio quantum-enhanced optical phase estimation using real-time feedback control. *Nat. Photon.* **9**, 577–581 (2015).
111. Fuchs, C. A. & van de Graaf, J. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Trans. Inf. Theory* **45**, 1216–1227 (1999).
112. Banchi, L., Braunstein, S. L. & Pirandola, S. Quantum fidelity for arbitrary Gaussian states. *Phys. Rev. Lett.* **115**, 260501 (2015).
113. Bose, S., Rallan, L. & Vedral, V. Communication capacity of quantum computation. *Phys. Rev. Lett.* **85**, 5448–5451 (2000).
114. Barzanjeh, Sh., Abdi, M., Milburn, G. J., Tombesi, P. & Vitali, D. Reversible optical-to-microwave quantum interface. *Phys. Rev. Lett.* **109**, 130503 (2012).
115. Barzanjeh, Sh., Vitali, D., Tombesi, P. & Milburn, G. J. Entangling optical and microwave cavity modes by means of a nanomechanical resonator. *Phys. Rev. A* **84**, 042342 (2011).
116. Spedalieri, G. & Braunstein, S. L. Asymmetric quantum hypothesis testing with Gaussian states. *Phys. Rev. A* **90**, 052307 (2014).
117. Berta, M., Hirche, C., Kaur, E. & Wilde, M. M. Amortized channel divergence for asymptotic quantum channel discrimination. Preprint at https://arxiv.org/abs/arXiv:1808.01498 (2018).
118. Pirandola, S., Mancini, S., Lloyd, S. & Braunstein, S. L. Continuous-variable quantum cryptography using two-way quantum communication. *Nat. Phys.* **4**, 726–730 (2008).
119. Novotny, L. & Hecht, B. *Principles of Nano-Optics* (Cambridge University Press, Cambridge, 2006).
120. Pendry, J. B. Negative refraction makes a perfect lens. *Phys. Rev. Lett.* **85**, 3966–3969 (2000).
121. Liu, Z., Lee, H., Yi, X., Sun, C. & Zhang, X. Far-field optical hyperlens magnifying sub-diffraction-limited objects. *Science* **315**, 1686 (2007).
122. Smolyaninov, I. I., Hung, Y.-J. & Davis, C. C. Magnifying superlens in the visible frequency range. *Science* **315**, 1699–1701 (2007).
123. Hell, S. W. & Wichmann, J. Breaking the diffraction resolution limit by stimulated emission: stimulated-emission-depletion fluorescence microscopy. *Opt. Lett.* **19**, 780–782 (1994).
124. Hell, S. W. Far-field optical nanoscopy. *Science* **316**, 1153–1158 (2007).
125. Betzig, E. et al. Imaging intracellular fluorescent proteins at nanometer resolution. *Science* **313**, 1642–1645 (2006).
126. Small, A. & Stahlheber, S. Fluorophore localization algorithms for super-resolution microscopy. *Nat. Methods* **11**, 267–279 (2014).
127. Tsai, M. J. & Dunn, K. P. *Performance Limitations on Parameter Estimation of Closely Spaced Optical Targets Using Shot-Noise Detector Model* Technical Report ADA073462 (Lincoln Laboratory, MIT, 1979).
128. Bettens, E. et al. Model-based two-object resolution from observations having counting statistics. *Ultramicroscopy* **77**, 37–48 (1999).
129. Ram, S., Ward, E. S. & Ober, R. J. Beyond Rayleigh's criterion: a resolution measure with application to single-molecule microscopy. *Proc. Natl Acad. Sci. USA* **103**, 4457–4462 (2006).
130. Zhuang, Q., Zhang, Z. & Shapiro, J. H. Entanglement-enhanced lidars for simultaneous range and velocity measurements. *Phys. Rev. A* **96**, 040304(R) (2017).

Acknowledgements

The authors would like to thank U. L. Andersen, L. Banchi, Sh. Barzanjeh, J. Borregaard, S. L. Braunstein, V. Giovannetti, S. Guha, C. Lupo, A. Lvovsky, M. Miková, M. Tsang and Z. Zhang for feedback. S.P. would like to specifically thank J. H. Shapiro and A. Farina for discussions on the experimental challenges related with a quantum radar, and R. Nair for the feedback on the experimental challenges in optical super-resolution. S.P. thanks support from the EPSRC via the 'UK Quantum Communications Hub' (EP/M013472/1). T.G. would like to acknowledge support from the Danish Research Council for Independent Research (Sapere Aude 4184-00338B) as well as the Innovation Fund Denmark (Qubiz) and the Danish National Research Foundation (Center for Macroscopic Quantum States, bigQ DNRF142).

Competing interests

The authors declare no competing interests.

Additional information

Reprints and permissions information is available at www.nature.com/reprints.

Correspondence should be addressed to S.P.