Lecture 5

Quantum Cryptography and Quantum Money

Quantum Cryptography

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 pf 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.

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.

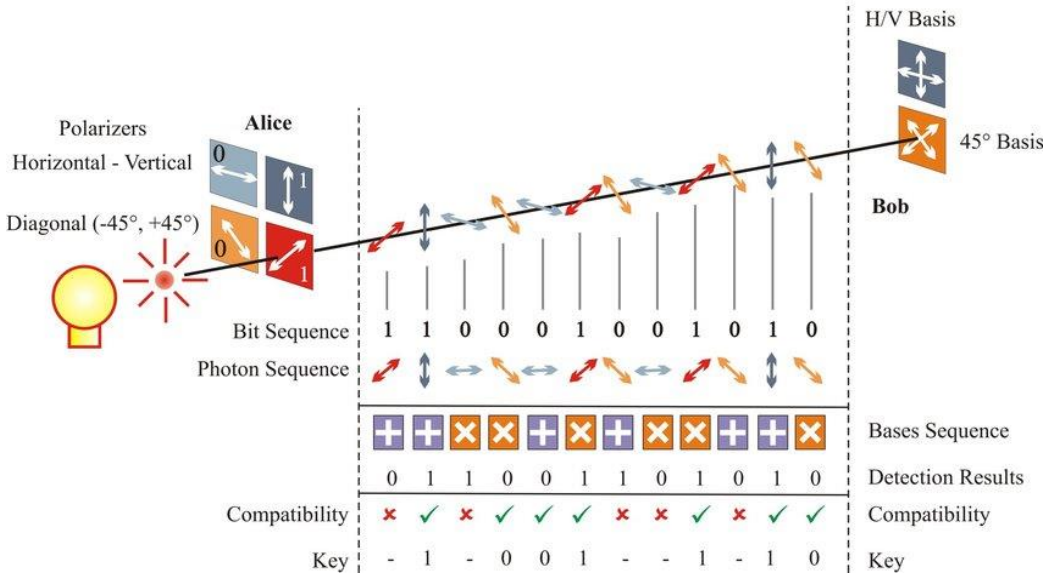
To make hacking impossible, each encryption key must be used only once (one time pad). This means there are two channels: a quantum channel to share quantum bits and a classical channel to distil the key and to share the encrypted message.

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). Alice keeps her basis choices for herself.

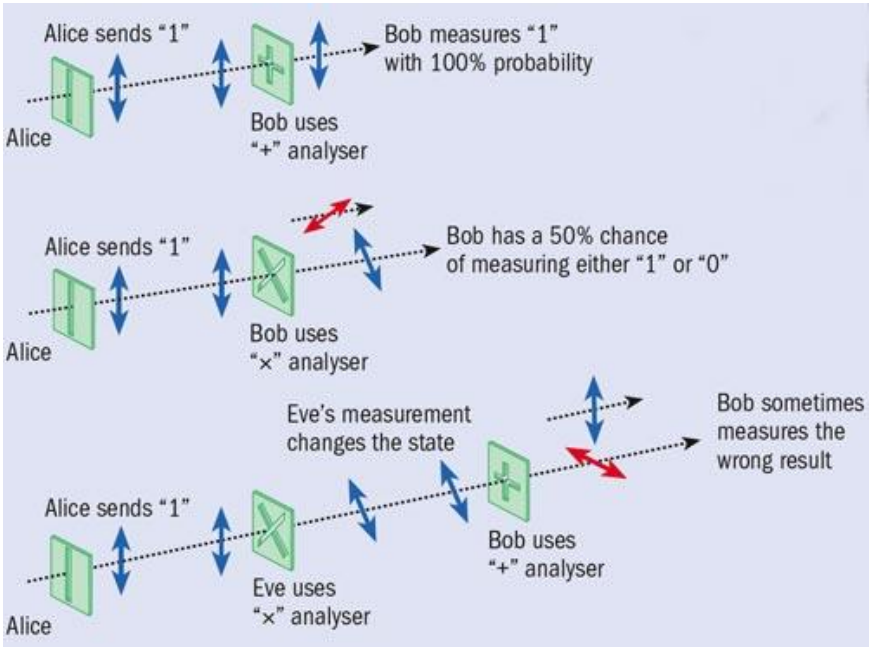
Bob measures the photons sent by Alice in random polarization basis (HV or DA) and keeps track of the detection events as well as the basis he used for each measurement.

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, 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. 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 aloow 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.

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.

The entangled photon pair source can be located anywhere between Alice and Bob, the polarization randomness is given by quantum mechanics: (I HV > + I VH >)

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).

Not 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. 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 a common technology. 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).

<u>Quantum Money</u>

Proposed by Stephen Wiener in 1983. Possibly the first ever quantum technology concept.

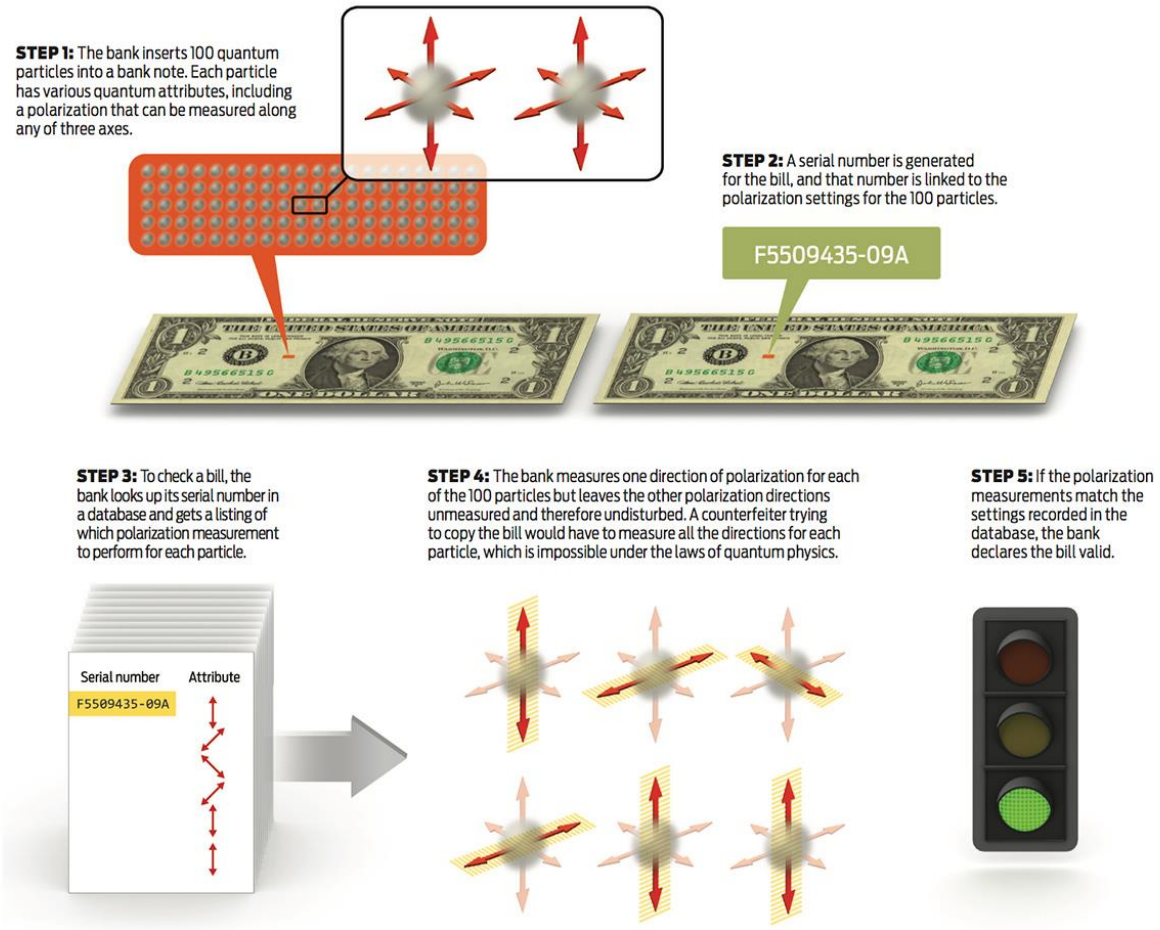
Each issued banknote is given a classical serial number and a set of isolated quantum systems (electron spins, photon polarization…)

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.

When a transaction takes place, the bank checks 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 ¾ to duplicate correctly (1/2 in the right basis, when in the wrong basis ½ chance to guess right).

For N qubits, probability to pass the bank test is $(3/4)^N$

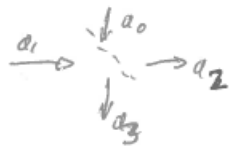
For 20 qubits $(3/4)^{20}$ = 0.003 this shows that a limited number of qubits are needed (compared to a quantum computer) but that their lifetime must be very long. Here again, the n0-cloning theorem is used to certify the origin of a message.



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

The beam splitter and Hong-Ou Mandel interference

A beam splitter has two input ports and two output ports.



There is always a phase shift between the transmitted and reflected beam.

We consider a 50:50 beam splitter where the reflected beam undergoes a p/2 phaseshift.

- If there is no input:

  $|0\rangle_0 |0\rangle_1 \rightarrow |0\rangle_2 |0\rangle_3$ this is rather obvious, nothing goes in and nothing goes out.

- One photon at one input port:

  $$|0\rangle_0 |1\rangle_1 \rightarrow \frac{1}{\sqrt{2}} \left(i a_2^+ + a_3^+\right) |0\rangle_2 |0\rangle_3$$
  $$= \frac{1}{\sqrt{2}} \left(i |1\rangle_2 |0\rangle_3 + |0\rangle_2 |1\rangle_3\right)$$

  The photon comes out randomly in one of the output ports.

- The Hong Ou Mandel interference: two photons are impinging on the beam splitter at each input.

  $$|1\rangle_0 |1\rangle_1 = a_0^+ a_1^+ |0\rangle_0 |0\rangle_1$$
  $$|1\rangle_0 |1\rangle_1 \rightarrow \frac{1}{2} \left(a_2^+ + i a_3^+\right)\left(i a_2^+ + a_3^+\right) |0\rangle_2 |0\rangle_3$$
  $$= \frac{i}{2} \left(a_2^+ a_2^+ + a_3^+ a_3^+\right) |0\rangle_2 |0\rangle_3$$
  $$= \frac{i}{2} \left(|2\rangle_2 |0\rangle_3 + |0\rangle_2 |2\rangle_3\right)$$

  The two photons always emerge together, the case where they come out one in each output interfere.

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).