

# On the quantum threat to cryptography, its mitigation, and our quantum cryptanalysis research

Martin Ekerå<sup>1</sup>

<sup>1</sup> Swedish NCSA, Swedish Armed Forces, SE-107 85 Stockholm, Sweden  
CDIS Spring Conference 2025, Stockholm, Sweden, May 22, 2025



SWEDISH ARMED FORCES

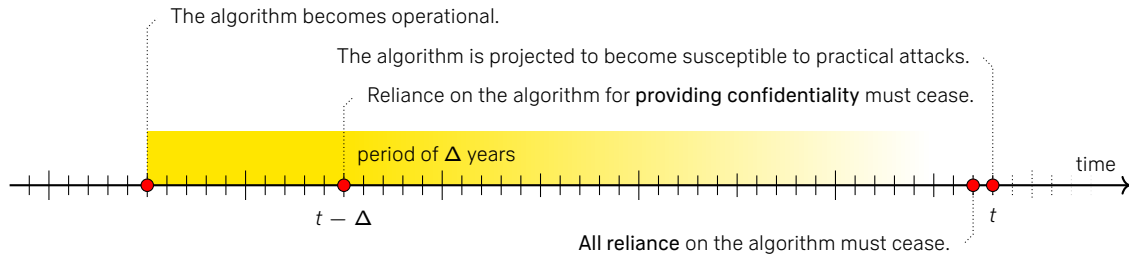


# Introduction

## Introduction

- ▶ Virtually all historically widely deployed commercial *asymmetric* cryptography will be broken if sufficiently capable quantum computers are built in the future.
- ▶ It is conceivable that such computers may be built sometime after the year 2030.
- ▶ Needless to say, it is very hard to make predictions about the future, but we need to make a prediction to set the time plan for mitigation efforts.

# When are mitigating actions required at the latest?



## Intermediary periods and confidentiality

- ▶ For plaintexts that we encrypt today to remain confidential for a period of  $\Delta$  years, the algorithm we rely upon must remain secure for a period of  $\Delta$  years.
- ▶ Prioritize taking mitigating actions for algorithms that provide confidentiality.

# Contents

## 1. Introduction

## 2. Mitigating the threat

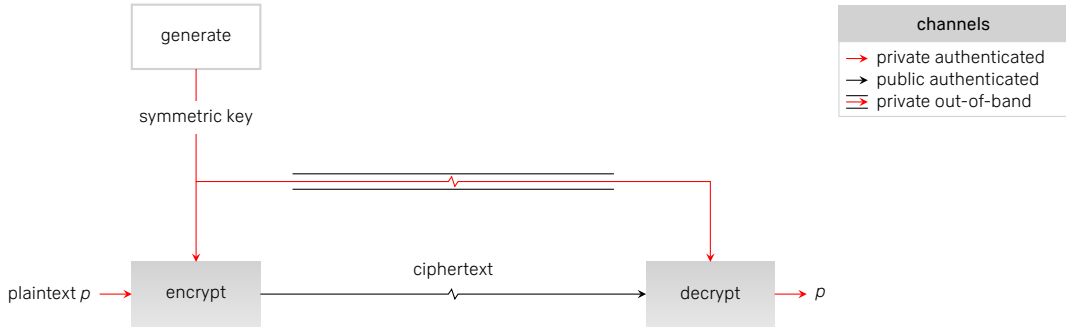
- Symmetric keying
- Asymmetric keying
- Hybrid keying

## 3. Quantum cryptanalysis

- Our research contributions
- Timeline projections
- Industry roadmaps
- Recent algorithmic developments

## 4. Summary and conclusion

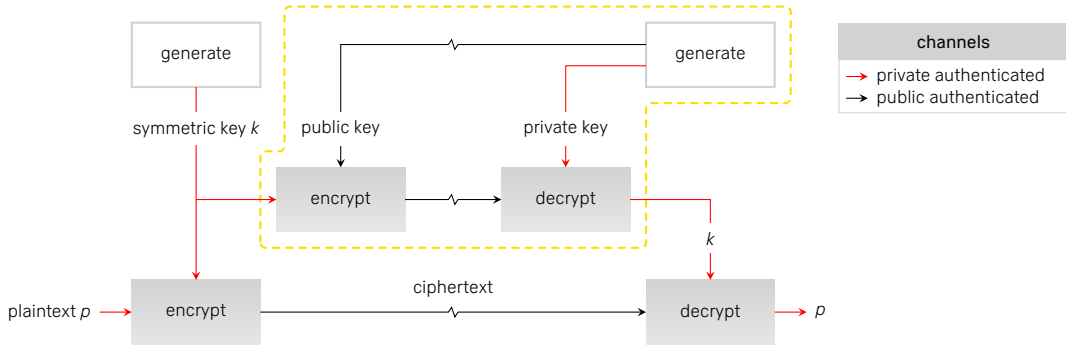
# Symmetric keying



1. Use symmetric keying, whenever feasible, with secure out-of-band key distribution.

- ▶ Limit the use contexts and validity periods of keys. Provides robust security, but no forward secrecy (FS). Suitable baseline for closed high-security networks.

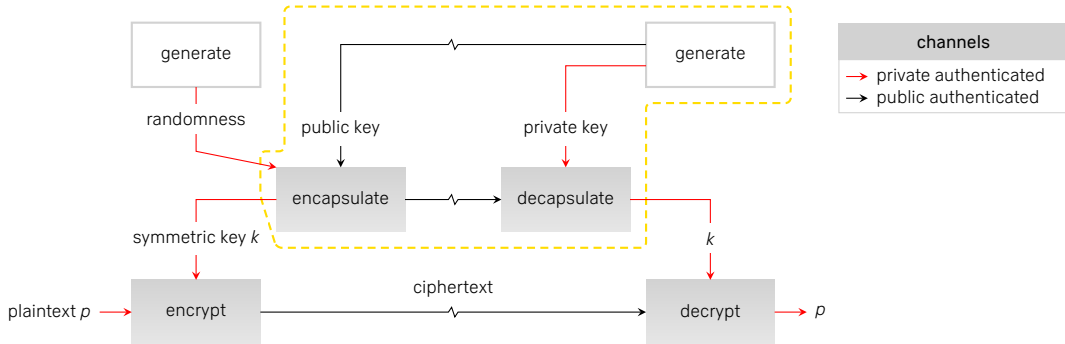
# Asymmetric keying via public-key encryption



2. Use post-quantum secure asymmetric keying, e.g. via public-key encryption.

- ▶ Less robust than symmetric keying but can provide forward secrecy (FS). Suitable baseline for open networks when symmetric keying is not feasible.

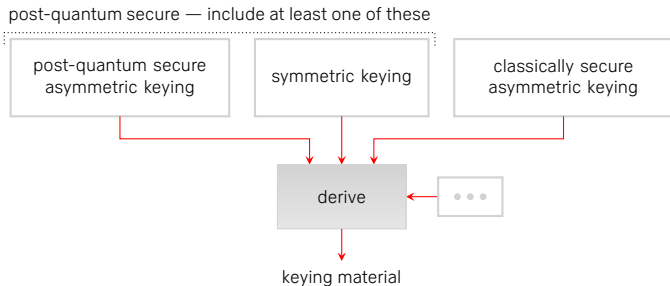
# Asymmetric keying via public-key encapsulation



2. Use post-quantum secure asymmetric keying, e.g. via public-key encapsulation.

- ▶ Less robust than symmetric keying but can provide forward secrecy (FS). Suitable baseline for open networks when symmetric keying is not feasible.

# Hybrid keying

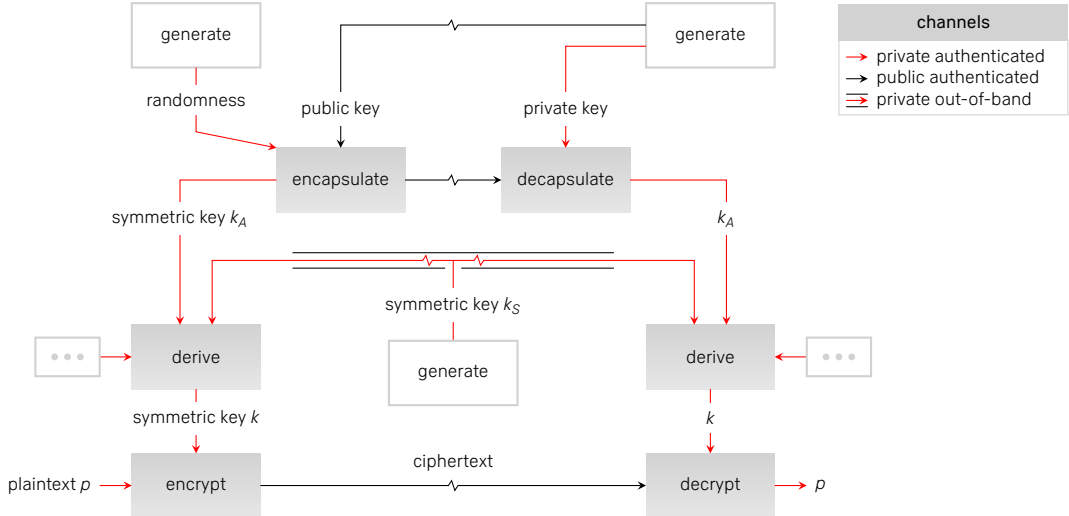


3. Hybridize keying methods, e.g. via key derivation or layered encryption, with the aim of all methods having to be broken for the resulting hybrid method to be broken.

- ▶ At least one method must be post-quantum secure. Use symmetric keying as a baseline whenever feasible. Hybridize with asymmetric keying for FS.
- ▶ Keep current classically secure methods to ensure security cannot be degraded.



# Hybrid symmetric and asymmetric keying



# Further reading

- ▶ Be conservative. Prioritize. Use symmetric keying if feasible.
- ▶ Key encapsulation options:
  - ▶ FrodoKEM
  - ▶ ML-KEM
  - ▶ Classic McEliece
  - ▶ HQC
  - ▶ ...
- ▶ Signature options:
  - ▶ SLH-DSA
  - ▶ XMSS/LMS
  - ▶ ML-DSA
  - ▶ ...
- ▶ Hybridize all non-hash-based schemes. Avoid Level I–II for non-hash-based schemes.



# Contents

## 1. Introduction

## 2. Mitigating the threat

- Symmetric keying
- Asymmetric keying
- Hybrid keying

## 3. Quantum cryptanalysis

- Our research contributions
- Timeline projections
- Industry roadmaps
- Recent algorithmic developments

## 4. Summary and conclusion

# Primary quantum algorithms for cryptanalysis

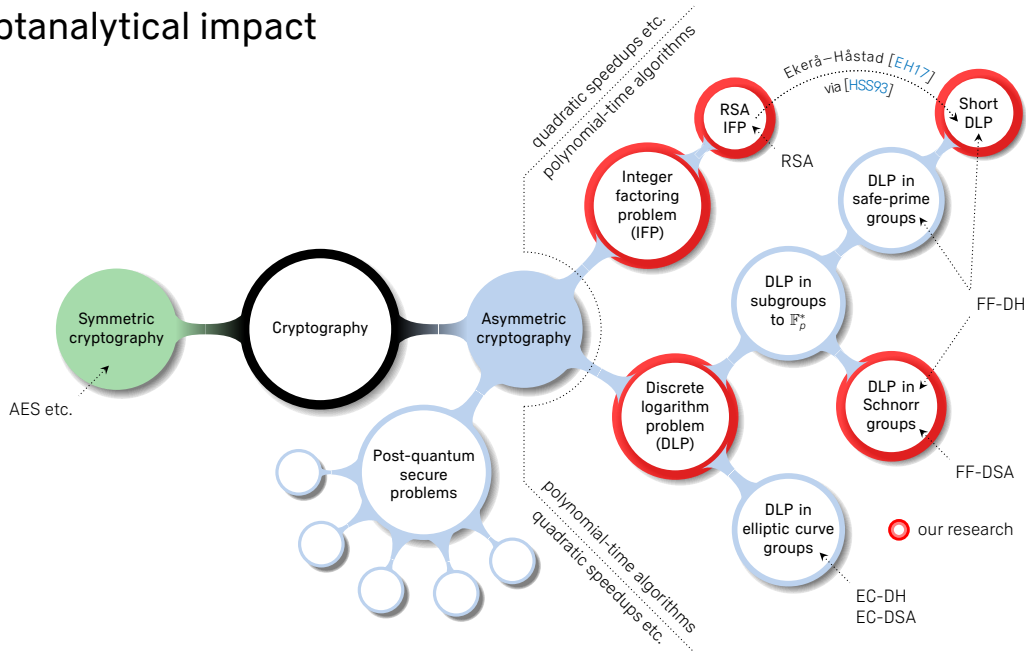
## Shor's algorithms

- ▶ [[Shor94](#)] solve both the integer factoring problem (IFP), and the discrete logarithm problem (DLP) in finite cyclic groups, in polynomial time and space.
- ▶ Asymmetric cryptography based on either of these problems is vulnerable.

## Grover's algorithm

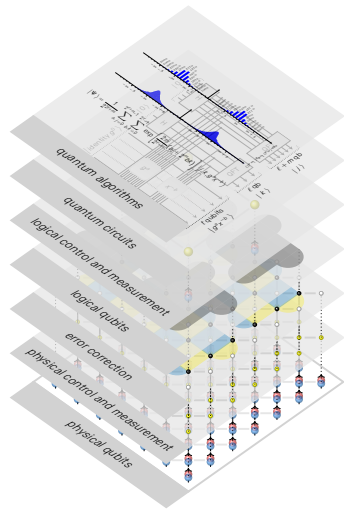
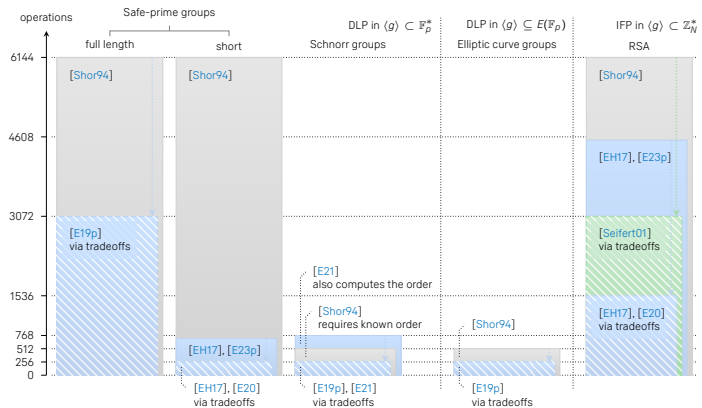
- ▶ [[Grover96](#)] provides a quadratic speedup for exhaustive search — in theory.
- ▶ In practice, due to overheads, the slow speed of quantum computers, and poor parallelization, it is not clear if [[Grover96](#)] provides a speedup. Easily mitigated.

# Cryptanalytical impact



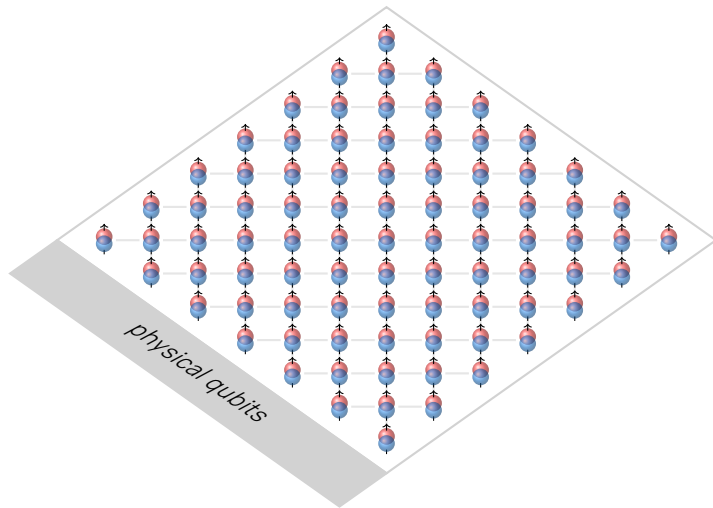
# Our quantum cryptanalysis research

Fig.: Group operations per run for a 128-bit classical strength level

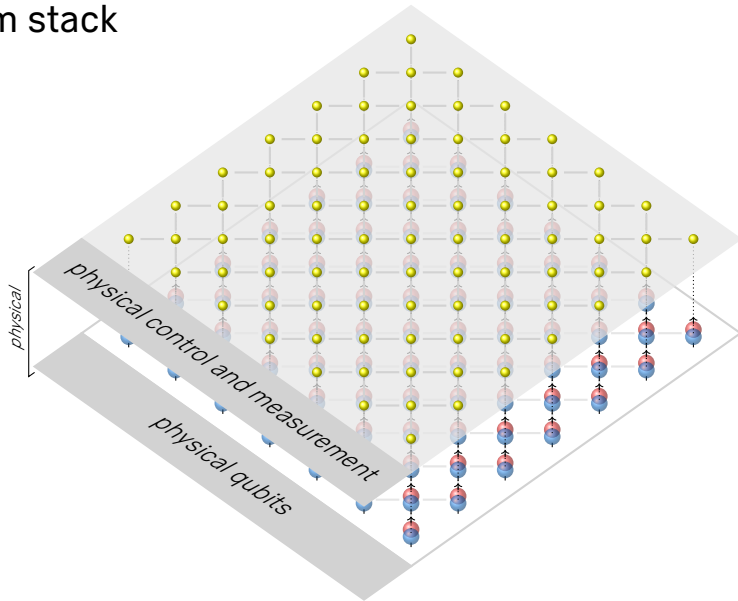


- I have developed state-of-the-art quantum algorithms for breaking widely deployed asymmetric cryptography and costed these to inform mitigation timelines.

# The quantum stack

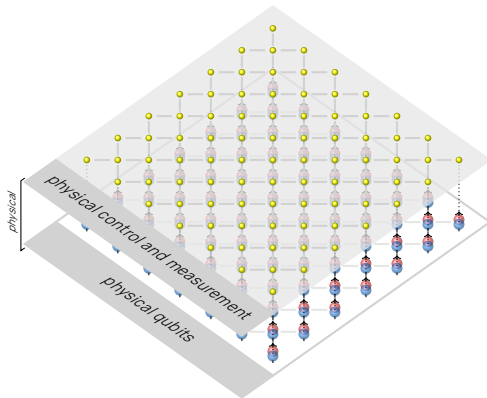


# The quantum stack

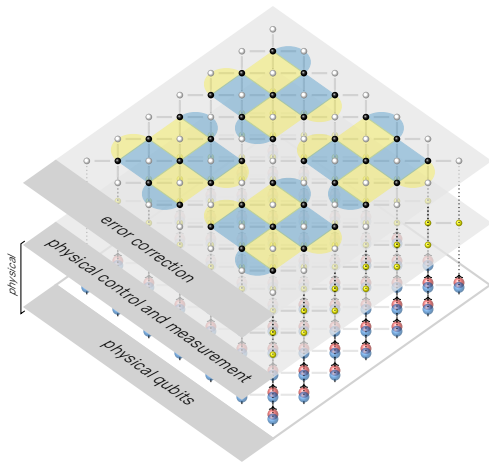




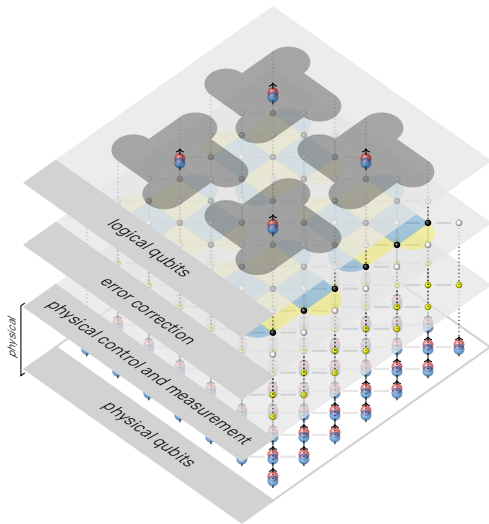
# The quantum stack



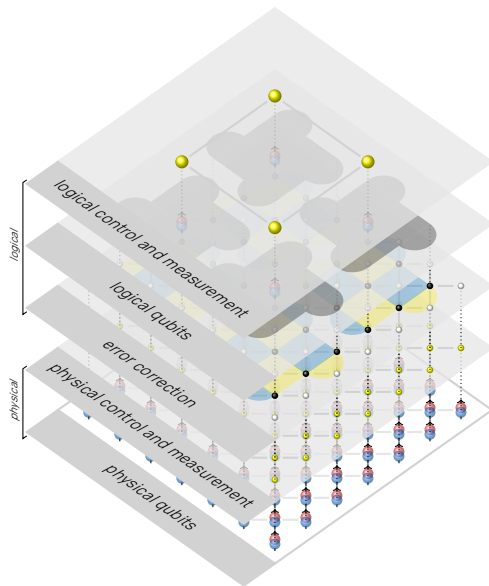
# The quantum stack



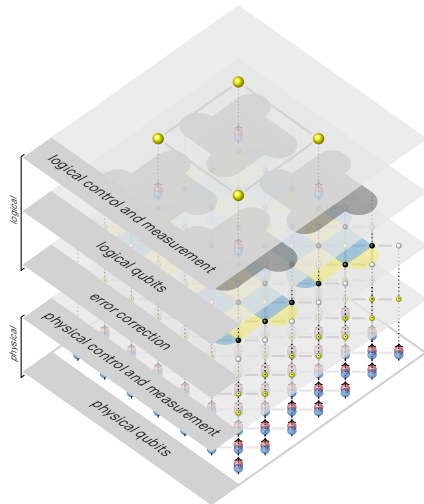
# The quantum stack



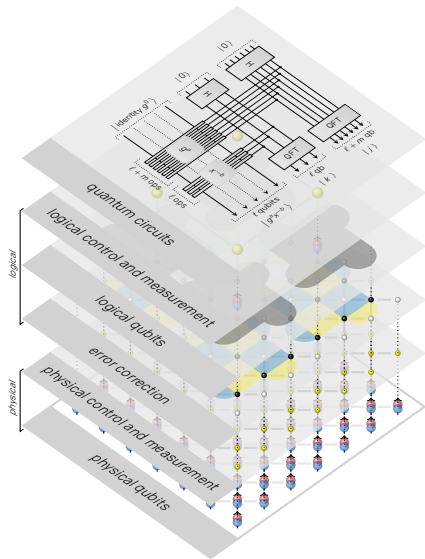
# The quantum stack



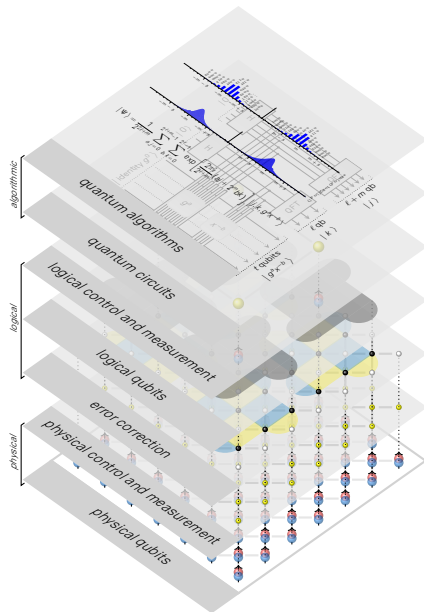
# The quantum stack



# The quantum stack



# The quantum stack

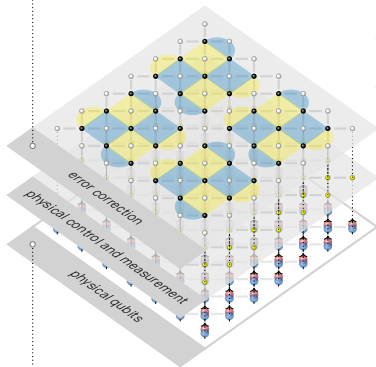


# Full-stack cost estimates [GE21]

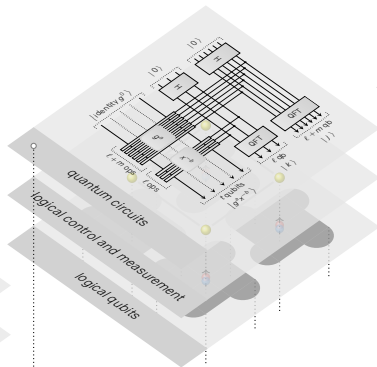
## Efficient error correction



Austin Fowler  
Craig Gidney



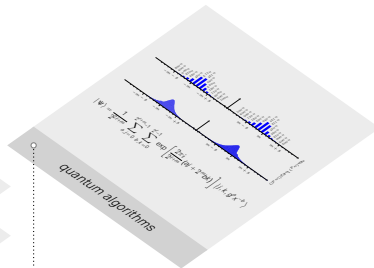
Plausible physical assumptions



Efficient approximate modular  
integer arithmetic



Craig Gidney



Efficient quantum algorithms



Martin Ekerå  
Johan Håstad

Efficient classical post-processing  
and tight probability estimates



Martin Ekerå

This part is a joint work with people at



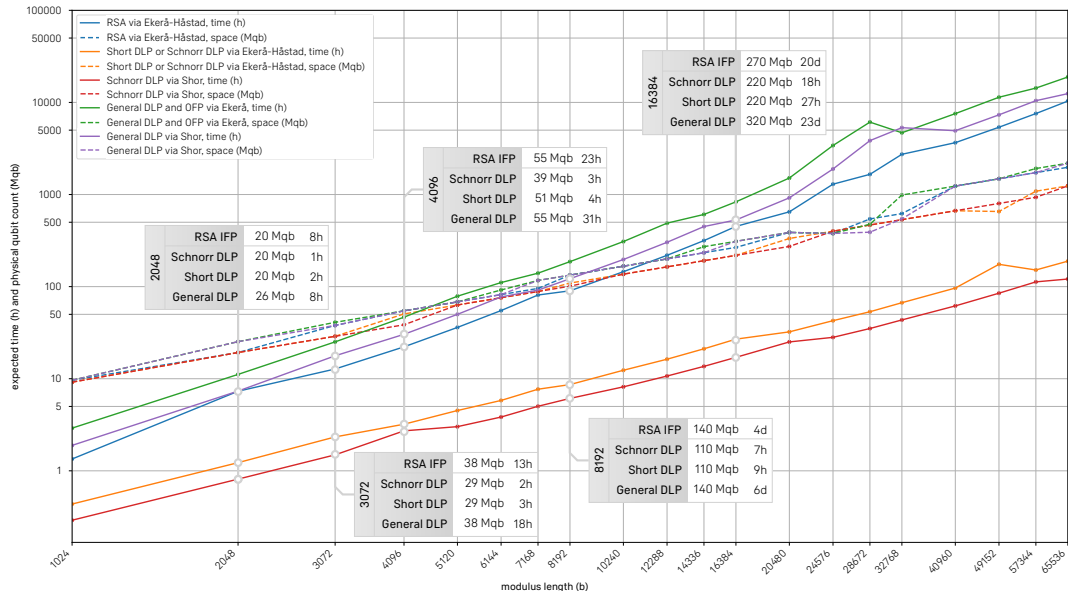
and



Google AI  
Quantum

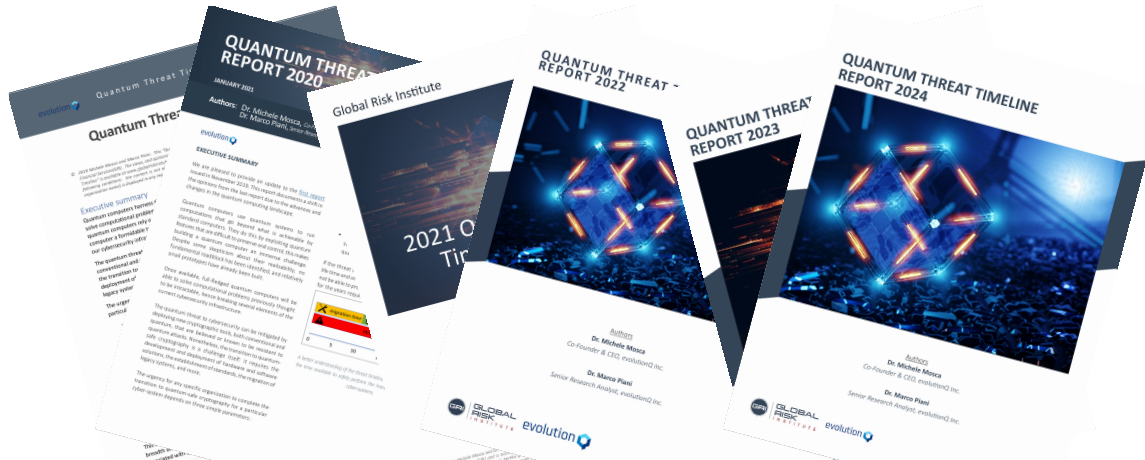


# Full-stack cost estimates [GE21]



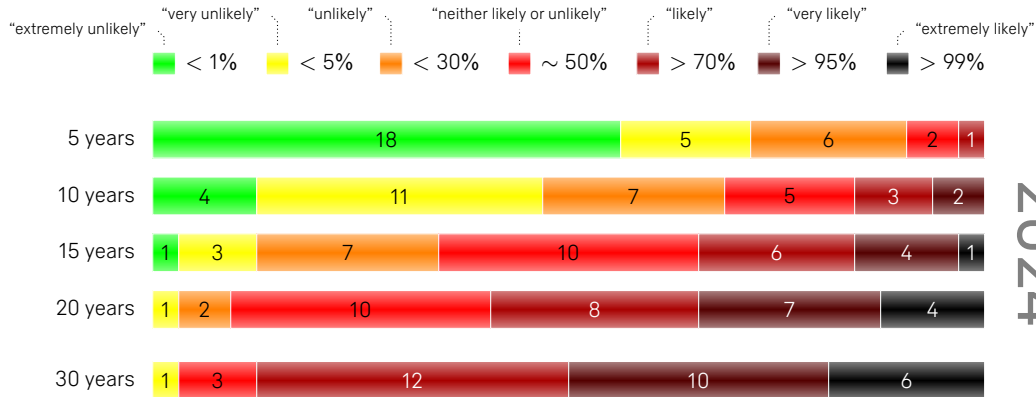
These estimates are from [GE21], see the paper and abstract for details on assumptions. Specifically, they are for factoring RSA integers, for solving the DLP in Schnorr groups, and for solving the general and short DLP in safe-prime groups, without making tradeoffs with respect to the number of runs required. The costs reported were obtained by optimizing the skewed volume, again see the paper for details. The classical strength level  $z$  is estimated using the model in FIPS 140-2 IG. For Schnorr groups, the order  $r$  is of length  $2z$  bits. For safe-prime groups, the short exponent  $d$  is of length  $2z$  bits.

# What does this mean for the timeline?



Respondents 2019–2024: Dorit Aharonov • Alexandre Blais • Ignacio Cirac • Bill Coish • David DiVincenzo • Martin Ekerå • Artur Ekert • Daniel Gottesman • Andrea Morello • Tracy Northup • Stephanie Simmons • Peter Shor • Frank Wilhelm-Mauch • Shengyu Zhang — Additional respondents 2024: Sergio Boixo • Earl Campbell • Andrew Childs • Joe Fitzsimons • Jay Gambetta • Yvonne Gao • Aram Harrow • Winfried Hensinger • Elham Kashefi • Yi-Kai Liu • Klaus Mølmer • William John Munro • Nicolas Menicucci • Kae Nemoto • Francesco Petruccione • Simone Severini • Gregor Weihs • David J. Wineland

# What is the likelihood of quantumly breaking RSA-2048 in 24 hours?



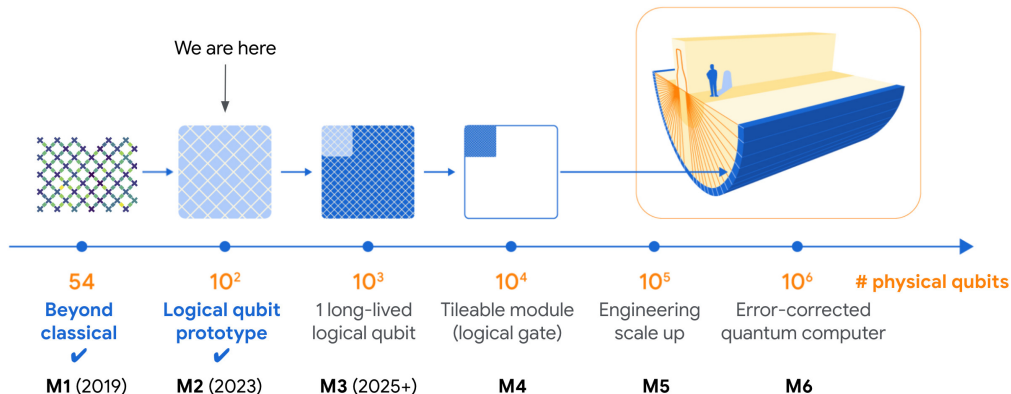
A key question in this survey [M. Mosca and M. Piani, Quantum Threat Timeline Report] was: “Please indicate how likely you estimate it is that a quantum computer able to factorize a 2048-bit number in less than 24 hours will be built within the indicated number of years. (For reference, you might want to take into account recent estimates for resources that might be required for such a task, like the ones provided in [C. Gidney and M. Ekerå, Quantum 5, 433 (2021)].)”

# Roadmap from IBM Quantum (2024)



Cropped roadmap adapted from the roadmap in the "IBM Quantum 2024 State of the Union" by J. Gambetta et al.

# Roadmap from Google Quantum AI (2022)



Roadmap presented by H. Neven in his talk "Google Quantum AI update" at Quantum Summer Symposium 2022. The high-resolution image was retrieved from the "Our quantum error correction milestone" article on the Google Quantum AI website. In a later revision, the 2025+ target for M3 was removed, and logical qubit error rates specified:  $10^{-2}$  for M2,  $10^{-6}$  for M3–M5, and  $10^{-13}$  for M6. The original roadmap specified a 2029 target for M6.

## Selected recent algorithmic developments

## An Efficient Quantum Factoring Algorithm

Oded Regev\*

### Abstract

**Abstract**  
We show that  $n$ -bit integers can be factored by independently running a quantum circuit with  $O(n^{3/2})$  gates for  $\sqrt{n} + 4$  times, and then using polynomial-time classical post-processing. The correctness of the algorithm relies on a number-theoretic heuristic assumption reminiscent of those used in subexponential classical factorization algorithms. It is currently not clear if the  $n^{3/2}$  gate complexity is the best possible for this approach.

# Extending Regev's Factoring Algorithm to Compute Discrete Logarithms

Martin Elser<sup>1,2</sup> (0000-0001-7061-2174) and Joel Gärtner<sup>1,2</sup> (0000-0002-3726-2064)

<sup>2</sup> NTFR 80-1-1-1.

\* Swedish NCSA, Stockholm.

**Abstract.** *Reges* recently introduced a quantum factoring algorithm (which may be perceived as a d-dimensional variation of Shor's factoring algorithm). In this work, we extend Reges's factoring algorithm to arbitrary bases, we discuss natural extensions of Reges's algorithm to arbitrary order finding, and to factoring completely via order finding. For all of these algorithms, we discuss various practical implementation considerations, including in particular the robustness of the post-processing.

**Keywords:** Quantum computing, Factoring, Order finding, Post-processing

**Keywords:** Quantum cryptanalysis · Discrete logarithms · Factoring

Space-Efficient and Noise-Robust  
Quantum Factoring

Sreyon Raveen  
MIT  
sraveen@mit.edu

Vinod Vaidyanathan  
MIT  
vino@mit.edu

June 27, 2024

## Abstract

We provide two improvements to Reger's quantum factoring algorithm [arXiv:1808.06671], enhancing its space efficiency and its asymptotic space efficiency of Reger's algorithm while

One first contribution to improve the quantum space efficiency of Shor's algorithm is due to Shor and Pippenger [19]. They observe that the quantum circuit for Shor's algorithm can be decomposed into two parts: a quantum circuit for computing the discrete logarithm and a quantum circuit for computing the discrete Fourier transform. The discrete logarithm circuit can be implemented using  $O(\sqrt{n})$  qubits and  $O(n^{3/2})$  gates. The discrete Fourier transform circuit can be implemented using  $O(\sqrt{n})$  qubits and  $O(n^{3/2})$  gates. The total quantum space complexity is  $O(\sqrt{n})$  qubits and  $O(n^{3/2})$  gates. This is a significant improvement over the original Shor's algorithm, which required  $O(n)$  qubits and  $O(n^3)$  gates.

[illegible]

Our second contribution is to show that Nave's classical postprocessing procedure can be modified to tolerate a constant fraction of the quantum circuit runs being corrupted by errors. In contrast, Nave's analysis of his classical postprocessing procedure requires all  $\sqrt{n}$  runs to be successful. In a nutshell, we achieve this using lattice reduction techniques to detect and filter out corrupt samples.

## Regev Factoring Beyond Fibonacci: Optimizing Prefactors

Sreyon Ragavan  
MIT  
sragavan@mit.edu

July 1, 2024

## Abstract

In this note, we propose the space-efficient variant of Rigter’s quantum factoring algorithm [Rig20] as introduced by Ragunani and Vaidyanathan [RV24] by constant factors in space and/or time. This allows us to bridge the significant gap in concrete efficiency between the circuits by [RG23] and [RV24]. [RG23] uses the lower circuit, while [RV24] uses the lower qubit.

The main observation is that the space-efficient quantum number representations technique in [RV24] can be modified to work with more general sequences of integers (than the Fibonacci numbers). We parametrize this in terms of a linear recurrence relation, and through this framework construct three different circuits for quantum factoring.

- A circuit that uses  $\approx 20.4n$  qubits and  $\approx 61.2n^{1/2}$  multiplications of  $n$ -bit integers.
- A circuit that uses  $(3 + \epsilon)n$  qubits and  $O(n^{1/2})$  multiplications of  $n$ -bit integers, for any  $\epsilon > 0$ .
- A circuit that uses  $(24 + \epsilon)n^{1/3}$  multiplications of  $n$ -bit integers, and  $O(n)$  qubits, for any  $\epsilon > 0$ .

In comparison, the original circuit by [Rog23] uses at least  $3n/2\sqrt{n}$  qubits and  $6n^{3/2}$  and  $n^{3/2}$  multiplications of  $n$ -bit integers, while the space-efficient variant by [RV24] uses  $n$   $16$ -bits qubits and  $\approx 129$   $n^{3/2}$  multiplications of  $n$ -bit integers (although a very simple modification of their  $\Phi$ -based circuit uses  $n$   $31$ -bits qubits and only  $\approx 86$   $n^{3/2}$  multiplications of  $n$ -bit integers). The improvements proposed in this note take effect for sufficiently large values of  $n$ ; it remains to be seen whether they can also provide benefits for practical problem sizes.

UNCONDITIONAL CORRECTNESS OF RECENT QUANTUM ALGORITHMS  
FOR FACTORING AND COMPUTING DISCRETE LOGARITHMS

CHÉRONC PILATTE

**ABSTRACT.** In 1984, Shor introduced his famous quantum algorithm to factor integers and compute discrete logarithms in polynomial time. In 2005, Shor proposed a multi-dimensional version of Shor's algorithm that requires far fewer quantum gates. His algorithm relies on a number-theoretic lemma that Shor's algorithm that requires far fewer quantum gates. His algorithm relies on a number-theoretic lemma that Shor's algorithm that requires far fewer quantum gates. His algorithm relies on a number-theoretic lemma that Shor's algorithm that requires far fewer quantum gates.

## A COMPREHENSIVE ANALYSIS OF REGEV'S QUANTUM ALGORITHM

BARNAB BARDULESCU, MUGUREL BARCAU, AND VICENTIU PAȘOL

**ABSTRACT.** Public-key cryptography can be based on integer factorization and the discrete logarithm problem (DLP), applicable to multiplicative groups and the elliptic curves. Ragué's recent quantum algorithm was initially designed for the elliptic curves. Ragué's recent quantum algorithm was initially designed for the elliptic curves. Ragué's recent quantum algorithm was initially designed for the elliptic curves. In this article, we further extend the algorithm to address the DLP for elliptic factorizations and now later extended to the DLP in the multiplicative group. In this article, we further extend the algorithm to address the DLP for elliptic factorizations and now later extended to the DLP in the multiplicative group. In this article, we further extend the algorithm to address the DLP for elliptic factorizations and now later extended to the DLP in the multiplicative group.

power. Notably, because the degree of the Sierpinski triangle can be applied, our algorithm is acceptably faster than those algorithms that can be applied. We analyze the complexity of most cases where Sierpinski's triangle can be applied and offer a geometric interpretation of the framework of the algorithm. In this analysis, we use the complexity of the algorithm to find a particular instance where running it is the fastest of the algorithms. This analysis also demonstrates that there are some cases where the algorithm is not the fastest.

In the case of edge orientation, we demonstrate that the algorithm is not the fastest. In the case of edge orientation, we demonstrate that the algorithm is not the fastest. In the case of edge orientation, we demonstrate that the algorithm is not the fastest.

# A high-level comparison of state-of-the-art quantum algorithms for breaking asymmetric cryptography

Martin Ekerå<sup>1,2</sup> and Joel Gärtner<sup>1,2</sup>

<sup>2</sup> Swedish NCSA, Swedish Aligned Forum, Stockholm, Sweden

**Abstract.** We provide a high-level cost comparison between Regge's quantum algorithm with Rivest-Girault's extension on the one hand, and existing state-of-the-art quantum algorithms for factoring and computing discrete logarithms on the other. This when comparing factoring cryptographically relevant problem instances, accounting for the complexity of reducing modular multiplication to modular addition, to Regge's algorithm, assuming optimizations of Rivest-Girault's algorithm, and when relating algorithms. Our conclusion is that Regge's algorithm, when applied to the factoring problem, may achieve a proven advantage, but not a cost advantage, the quantum discrete logarithm problem is cheap. Regge's algorithm with the optimizations does not achieve an advantage, but, since it thus meets computational complexity bounds, it may be useful in some applications, such as in the construction of a quantum stateful pseudorandom number generator.

**Keywords:** Rivest's algorithm · Cost estimates · Factoring · Discrete logarithms

## Reducing the Number of Qubits in Quantum Factoring

Chimère Chevignard, Pierre-Klaus Foppe, and André Schottenlocher  
Eric Rouven, Italia, CNRS, IERSA  
firstname.lastname@ier.fr

**Abstract.** This paper focuses on the optimization of the number of logical qubits in quantum algorithms for factoring and computing discrete logarithms in  $\mathbb{Z}_N^*$ . These algorithms contain an exponentiation circuit modulo  $N$ , which is responsible for most of the complexity of the factoring and operations.

In this paper, we show that using only  $\mathcal{O}(\log N)$  work qubits, one can obtain the least significant bits of the modular exponentiation output. We combine this result with May and Meule's recent observation (May2022) and the Elven-Rotated variant of Shor's factorization algorithm (ToSC2022) to solve the discrete logarithm problem in  $\mathbb{Z}_N^*$  using only  $\mathcal{O}(\log N)$  qubits, where  $N$  is the bit-size of the modulus. Consequently, we can factorize integers  $n$  using  $\mathcal{O}(\sqrt{n}) + \mathcal{O}(n)$  qubits, while current envisioned algorithms need  $\Omega(n)$  qubits.

measurable probability. For RSA factorization, we can use a gate count  $O(n^3)$  for a depth  $O(n^2 \log n)$ , which gives us a gate count  $O(n^5)$  (the number of measurements required by Eqs. (1)–(4)). In an RSA-2048 instance, we estimate that 1720 logical qubits and 40000 gates will suffice for a single run, and the algorithm needs an average 40 runs. To make a classical-quantum instance of 224 bits (212 classical and 12 quantum qubits), we estimate that 2240 logical qubits would suffice, and 20 runs with  $2^{22}$  Tdahlqvist gates each.

**Keywords:** Quantum cryptanalysis, Shor's algorithm, Integer factoring, Discrete Logarithm, Residue number system.

The papers by Regev, by Ragavan and Vaikuntanathan, by Ragavan, and by Chevignard, Fouque and Schrottenloher, are all CC-BY v4.0. The paper by Barbulescu, Barcau and Paşol is CC0 v1.0, i.e. public domain. The paper by Pilatte is included with the author's permission.

# Contents

## 1. Introduction

## 2. Mitigating the threat

- Symmetric keying
- Asymmetric keying
- Hybrid keying

## 3. Quantum cryptanalysis

- Our research contributions
- Timeline projections
- Industry roadmaps
- Recent algorithmic developments

## 4. Summary and conclusion

# Summary and conclusion

## Summary and conclusion

- ▶ Virtually all historically widely deployed commercial *asymmetric* cryptography will be broken if sufficiently capable quantum computers are built in the future.
- ▶ It is conceivable that such computers may be built sometime after the year 2030.

## Mitigation advice for vulnerable asymmetric cryptography

- ▶ Prioritize taking mitigating actions with respect to providing confidentiality.
- ▶ If feasible, use symmetric keying as a baseline, in combination with asymmetric keying. Otherwise, use post-quantum secure asymmetric keying as a baseline.
- ▶ Be mindful of the timeframes. Early mitigation is an affordable insurance.



