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

Martin Ekerå [1]

[1] Swedish NCSA, Swedish Armed Forces, SE-107 85 Stockholm, Sweden

CDIS Spring Conference 2025, Stockholm, Sweden, May 22, 2025

SWEDISH ARMED FORCES

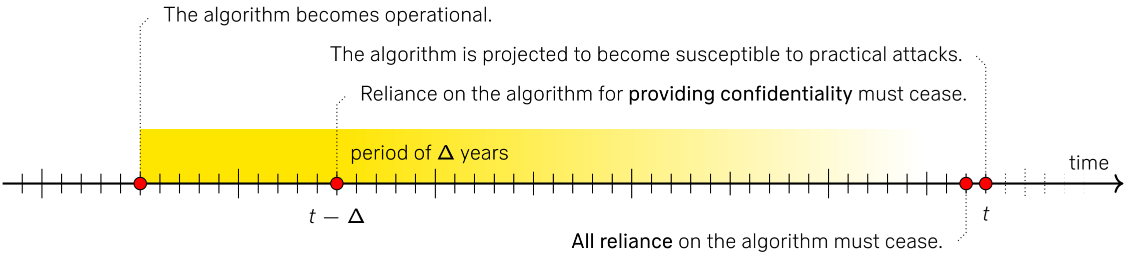
KTH VETENSKAP OCH KONST

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?

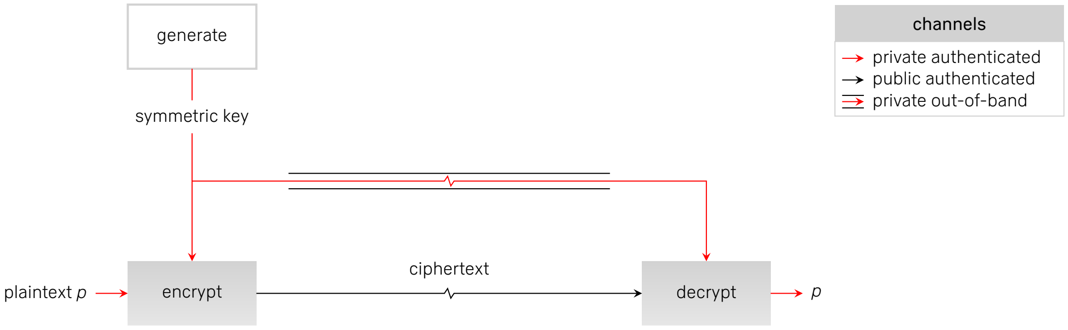


Intermediary periods and confidentiality

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

Contents

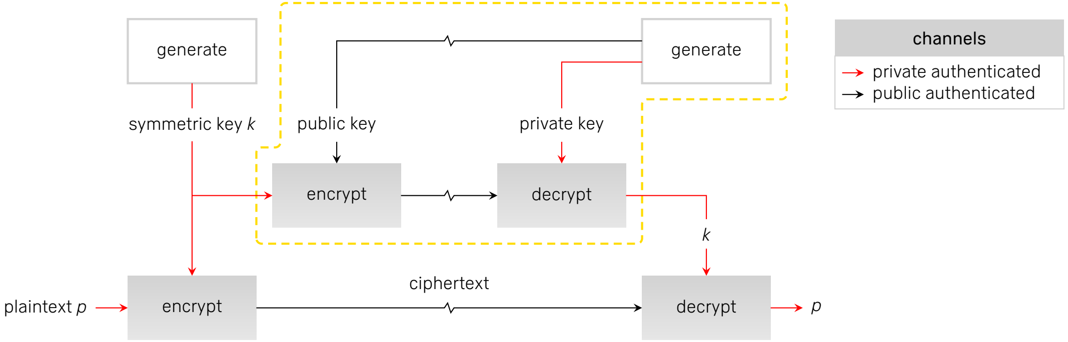
Symmetric keying



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.

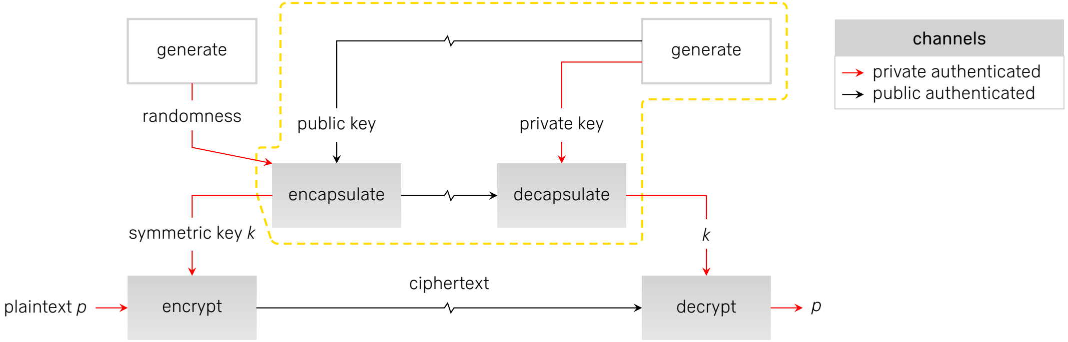
Asymmetric keying via public-key encryption



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.

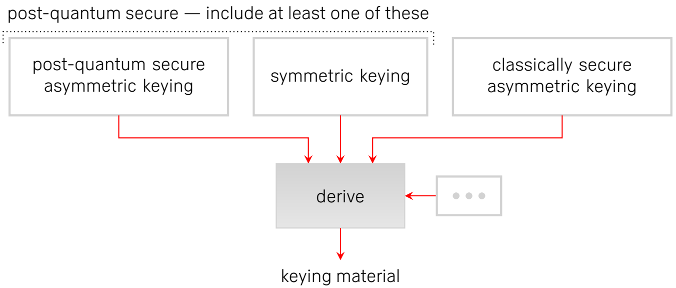
Asymmetric keying via public-key encapsulation



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.

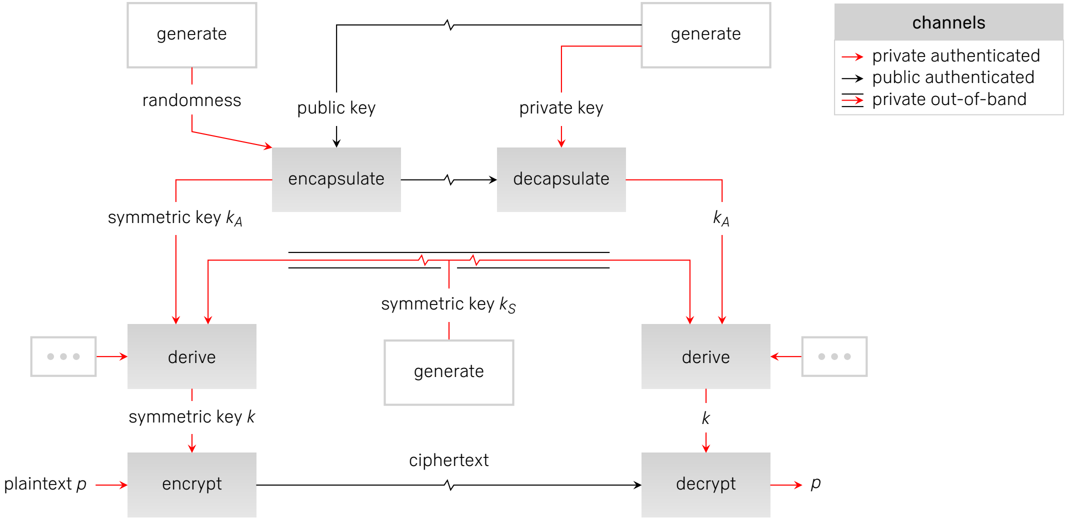
Hybrid keying



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

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.

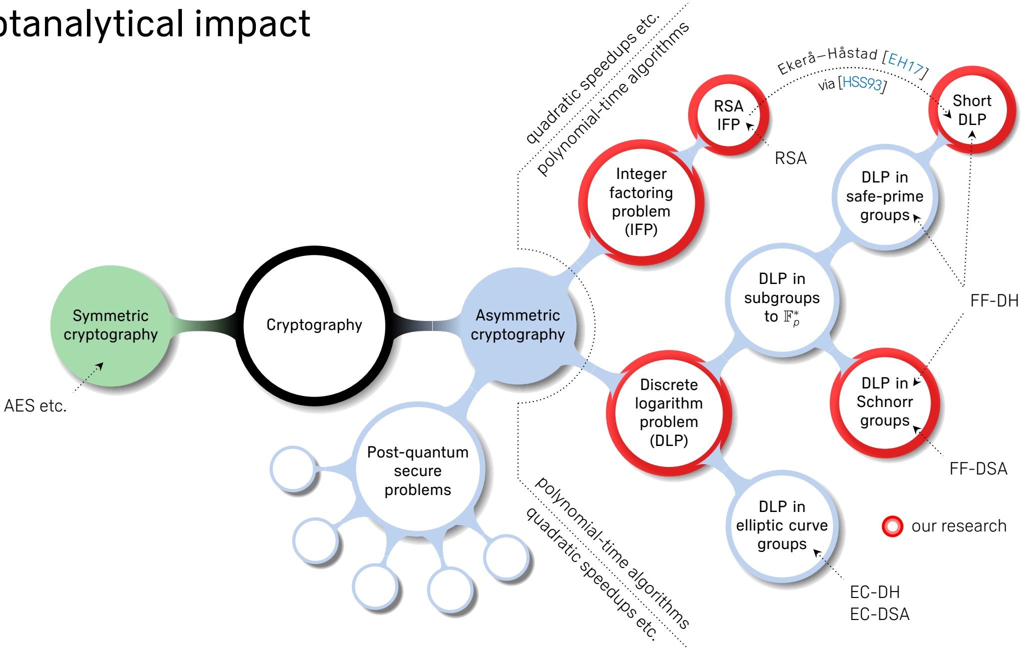
- Asymmetric cryptography based on either of these problems is vulnerable.

Grover's algorithm

- [Grover96] provides a quadratic speedup for exhaustive search — in theory.

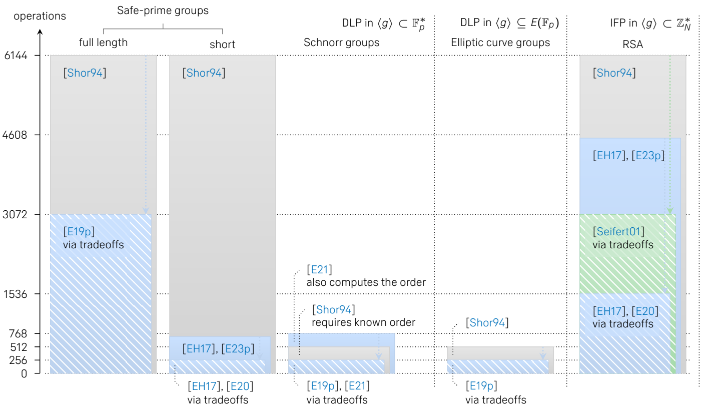
- In practice, due to overheads, the slow speed of quantum computers, and poor parallelization, it is not clear if [Grover96] provides a speedup. Easily mitigated.

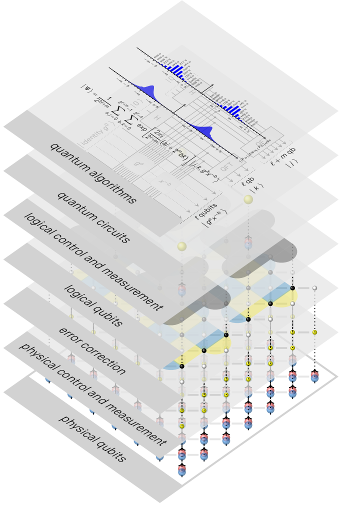
Cryptanalytical impact



Our quantum cryptanalysis research

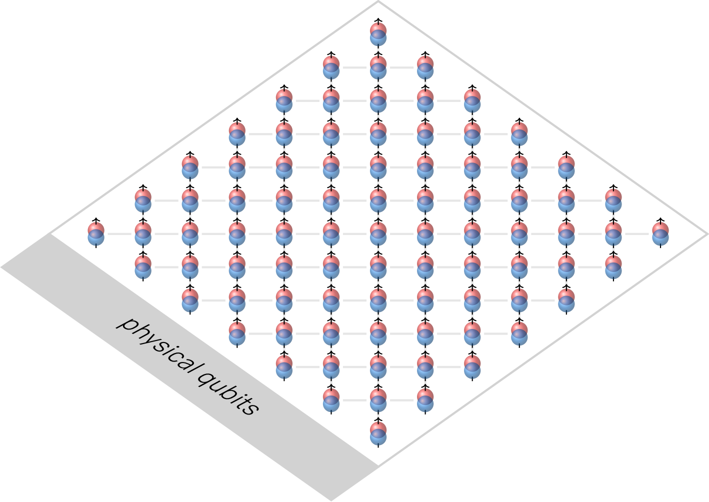
Fig.: Group operations per run for a 128-bit classical strength level



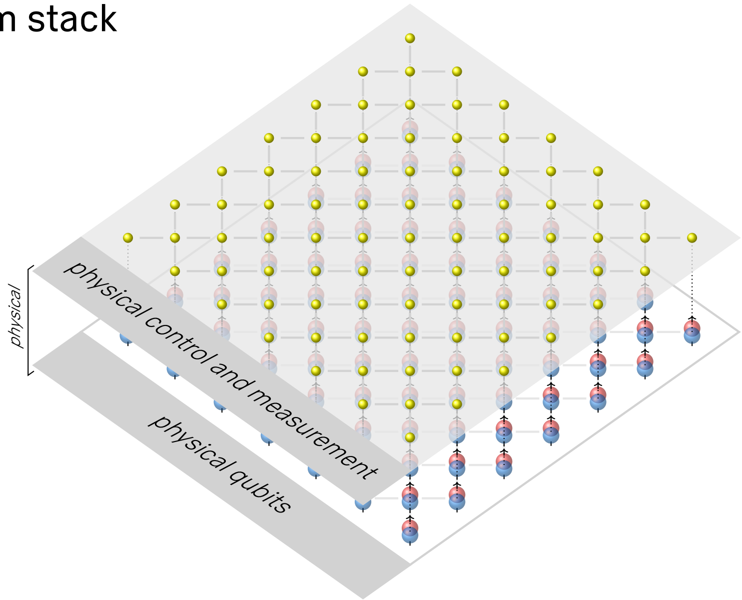


► I have developed state-of-the-art quantum algorithms for breaking widely deployed asymmetric cryptography and costed these to inform mitigation timelines.

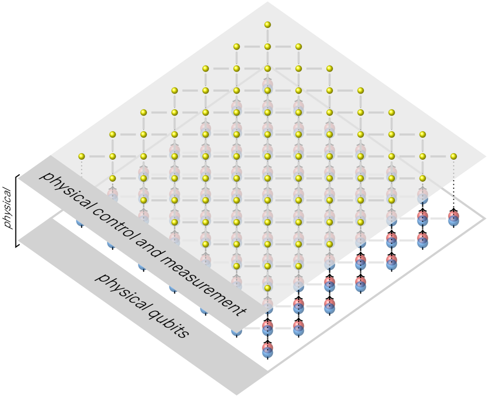
The quantum stack



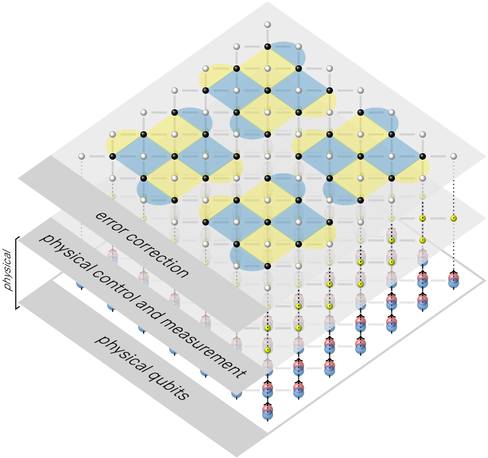
The quantum stack



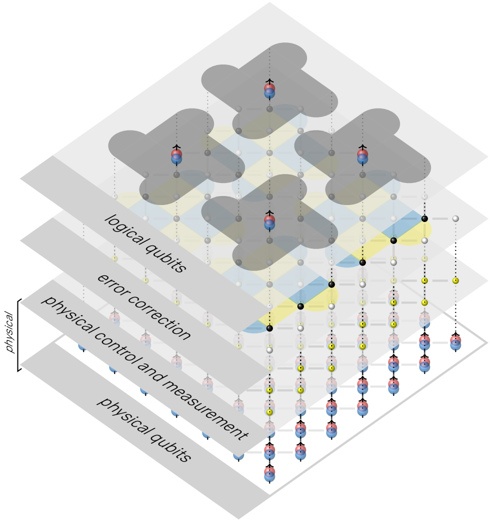
The quantum stack



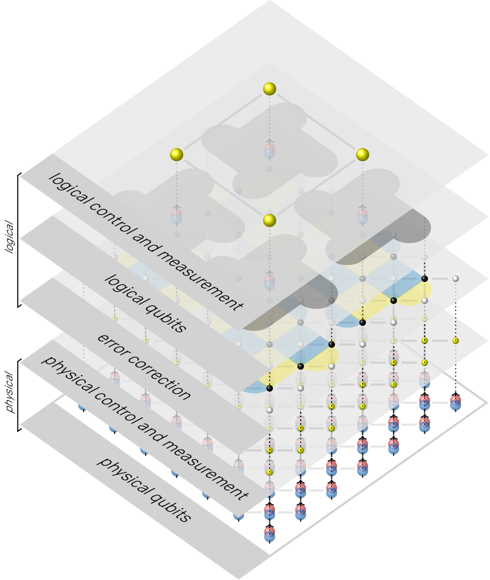
The quantum stack



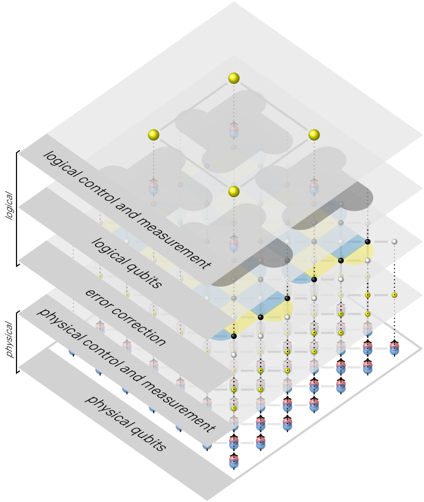
The quantum stack



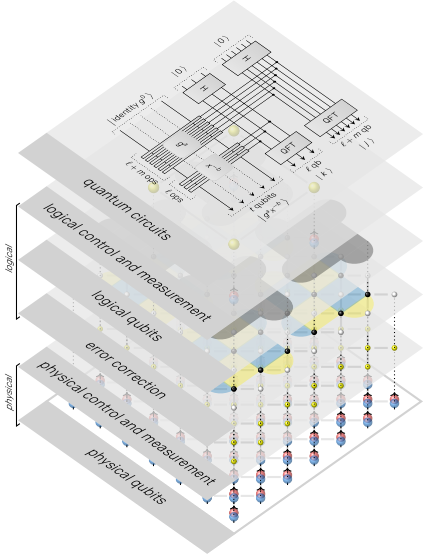
The quantum stack



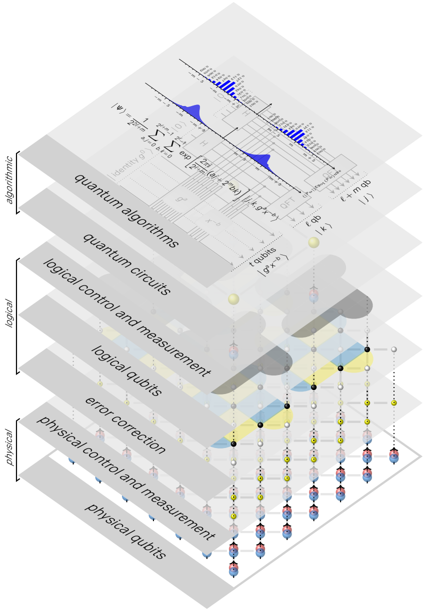
The quantum stack



The quantum stack



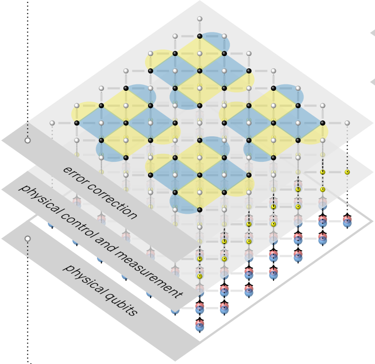
The quantum stack



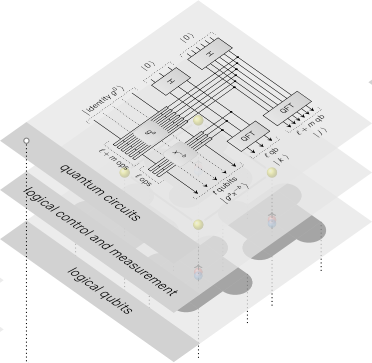
Full-stack cost estimates [GE21]

Efficient error correction

Austin Fowler
Craig Gidney

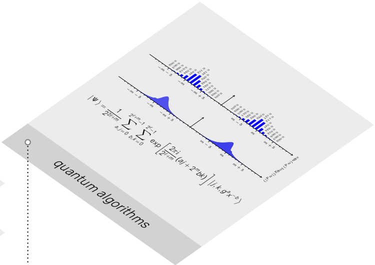


Plausible physical assumptions



Efficient approximate modular integer arithmetic

Craig Gidney



Efficient quantum algorithms

Martin Ekerå
Johan Håstad

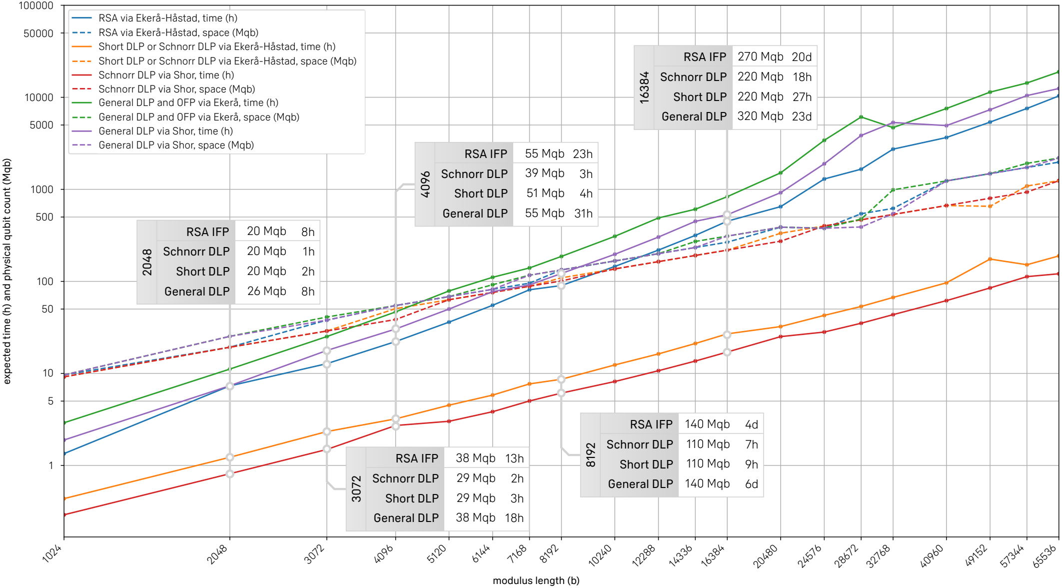
Efficient classical post-processing and tight probability estimates

Martin Ekerå

This part is a joint work with people at KTH and Google AI Quantum

(Photo of Johan Håstad by Håkan Lindgren.)

Full-stack cost estimates [GE21]

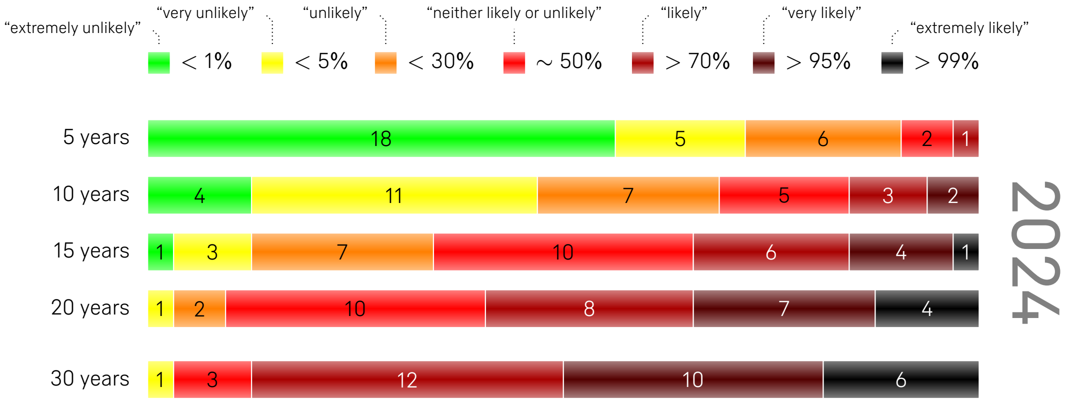


These estimates are from [GE21], see the paper and abstract for details on assumptions. Specifically, they are for factoring RSA integers, for solving the DLP in Schnorr groups, and for solving the general and short DLP in safe-prime groups, without making tradeoffs with respect to the number of runs 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?

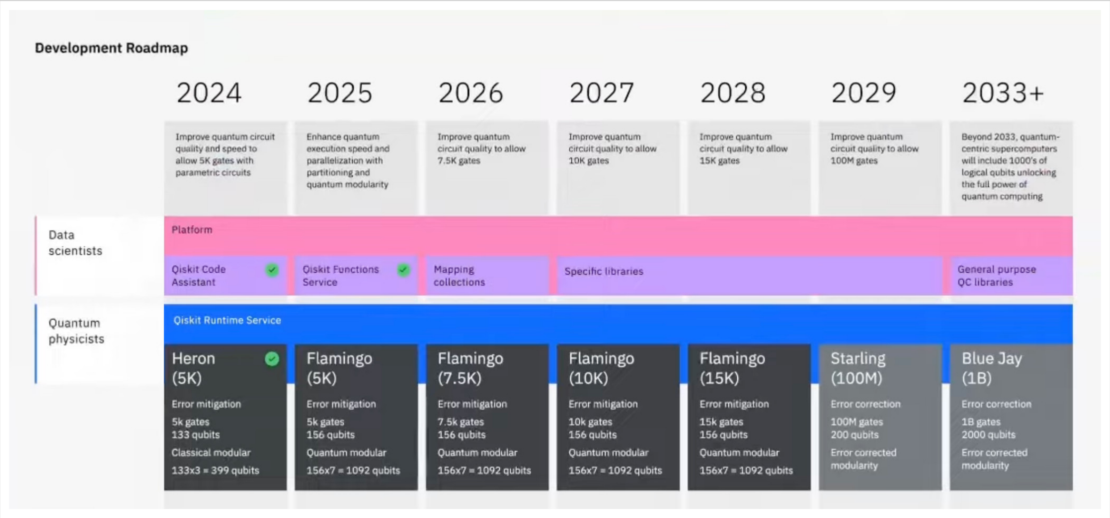
Respondents 2019–2024: Dorit Aharonov • Alexandre Blais • Ignacio Cirac • Bill Coish • David DiVincenzo • Martin Ekerå • Artur Ekert • Daniel Gottesman • Andrea Morello Tracy Northup • Stephanie Simmons • Peter Shor • Frank Wilhelm-Mauch • Shengyu Zhang — **Additional respondents 2024:** Sergio Boixo • 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?



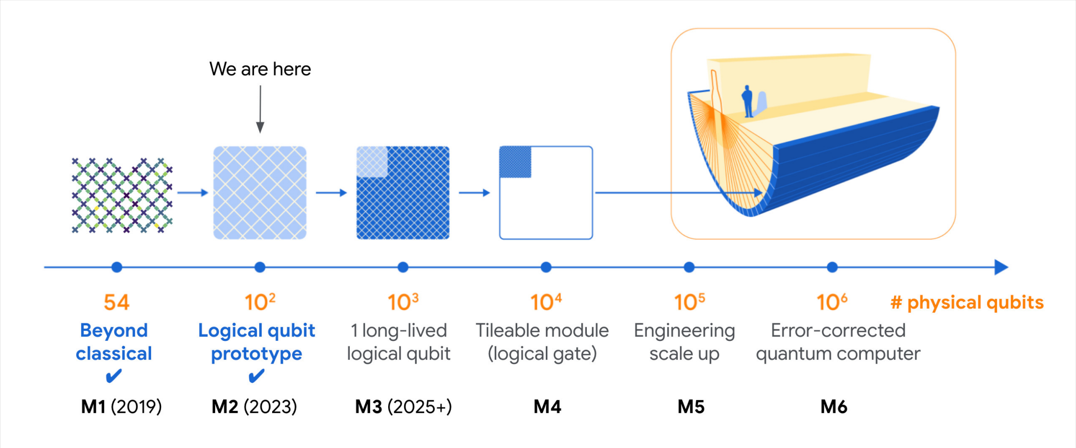
A key question in this survey [M. Mosca and M. Piani, Quantum Threat Timeline Report] was: "Please indicate how likely you estimate it is that a quantum computer able to factorize a 2048-bit number **in less than 24 hours** will be built within the indicated number of years. *(For reference, you might 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

Contents

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.

KTH
VETENSKAP
OCH KONST