Security in Times of Quantum

Tanja Lange

Department of Mathematics and Computer Science & QT/e
Eindhoven University of Technology
the Netherlands

Cryptography

Post-quantum cryptography:

Post-quantum cryptography:

Cryptography designed under the assumption
that the **attacker** (not the user!)
has a large quantum computer.

Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

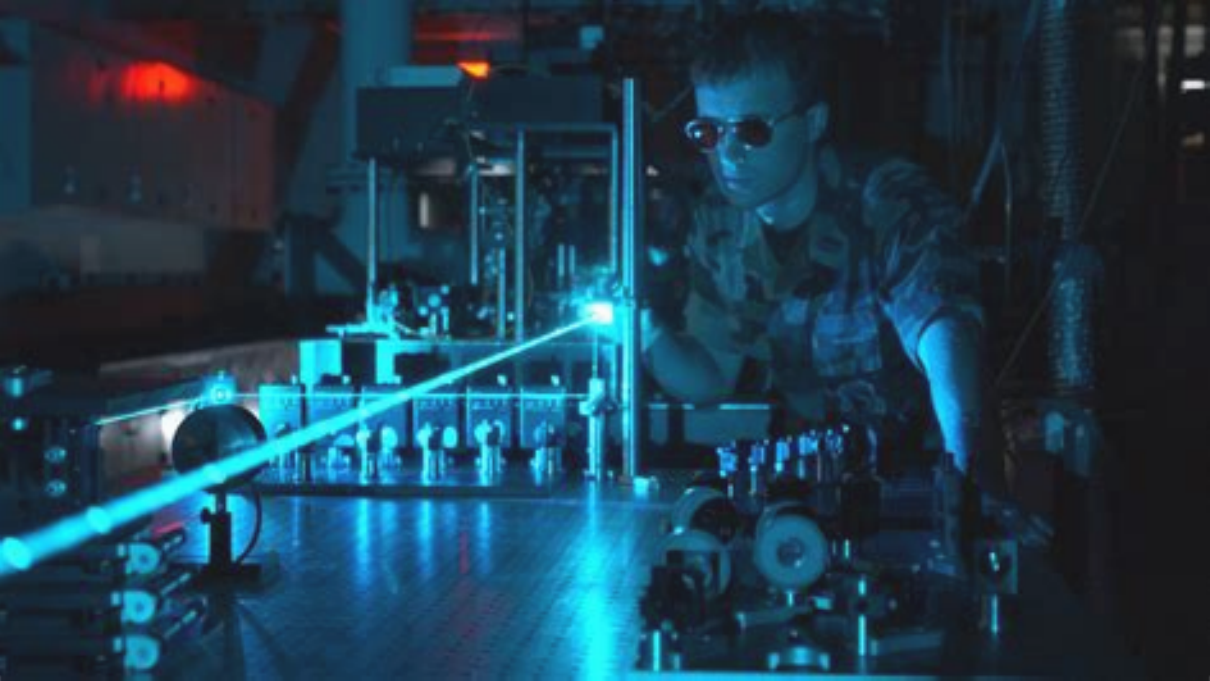
Abstract

A computer is generally considered to be a universal computational device; i.e., it is believed able to simulate any physical computational device with a cost in computation time of at most a polynomial factor. It is not clear whether this is still true when quantum mechanics is taken into consideration. Several researchers, starting with David Deutsch, have developed models for quantum

[1, 2]. Although he did not ask whether quantum mechanics conferred extra power to computation, he did show that a Turing machine could be simulated by the reversible unitary evolution of a quantum process, which is a necessary prerequisite for quantum computation. Deutsch [9, 10] was the first to give an explicit model of quantum computation. He defined both quantum Turing machines and quantum circuits and investigated some of their properties.

The next part of this paper discusses how quantum com-

Back to the stone age?



Post-quantum cryptography:

Post-quantum cryptography:

Algorithmic cryptography with attack model quantum cryptanalysis

Urgency of moving to post-quantum cryptography

White House briefing urges move to PQC.
Deadline: 2035.

2024 EU PQC transition roadmap (link)

COMMISSION RECOMMENDATION

of 11.4.2024

on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography

(5) Member States should consider migrating their current digital infrastructures and services for public administrations and other critical infrastructures to Post-Quantum Cryptography as soon as possible, inducing a fundamental shift in cryptographic algorithms, protocols and systems. As highlighted in the Commission's recent White Paper “How to master Europe’s digital infrastructure needs”, this requires a coordinated effort involving government agencies, standardization bodies, industry stakeholders, researchers and cybersecurity professionals.

(9) Member States and the Union should continue to cooperate actively with their international strategic partners in the development of international standards in Post-Quantum Cryptography with a view to ensuring interoperability of communications going forward.

27 Nov 2024: Joint statement by 17 EU countries (Link)

Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography

To this end, a Work Stream on PQC, co-chaired by France, Germany and the Netherlands, has been created as part of the NIS Cooperation Group following a recommendation [9] of the European Commission. **We encourage active engagement from all EU member states in this work stream** throughout the process of preparing a roadmap for the transition to Post-Quantum Cryptography to ensure the quantum resilience of the European Union's digital infrastructures.

[..]

27 Nov 2024: Joint statement by 17 EU countries (Link)

Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography

> To this end, a Work Stream on PQC, co-chaired by France, Germany and the Netherlands, has been created as part of the NIS Cooperation Group following a recommendation [9] of the European Commission. **We encourage active engagement from all EU member states in this work stream** throughout the process of preparing a roadmap for the transition to Post-Quantum Cryptography to ensure the quantum resilience of the European Union's digital infrastructures.

[..]
we recommend that these should be protected against 'store now, decrypt later' attacks as soon as possible, latest by the end of 2030. Moreover, we also recommend to develop detailed transition plans for public-key infrastructure systems in the same timeframe.

Australian Government

Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre

Information Security Manual

Last updated: December 2024

Guidelines for Cryptography

Disallows pre-quantum by 2030

Store now, decrypt later

Math problems hard for quantum computers

- Code-based encryption and signatures.
- Hash-based signatures.
- Isogeny-based encryption and signatures.
- Lattice-based encryption and signatures.
- Multivariate-quadratic encryption and signatures.

These are broad categories.
We have good instantiations for the essential building blocks: key agreement and signatures.
Research needed on advanced building blocks, efficient & secure implementation (side channels), (quantum) cryptanalysis

Standardization of PQC

- Stateful hash-based signatures:
  RFC 8391 XMSS and RFC 8554 LMS in CFRG, NIST SP 800-208 (also XMSS and LMS), ISO SC27 JTC1 WG2 14888-4.
- FIPS standards for
  - FIPS 203 ML-KEM (Kyber), based on lattices
  - FIPS 204 ML-DSA (Dilithium), based on lattices
  - FIPS 205 SLH-DSA (SPHINCS+), based on hash functions
- 3 more candidates in Round-4 of NIST, more signatures in on ramp.
- Internet Engineering Task Force (IETF) is working on drafts for various schemes, methods for combining them with elliptic-curve crypto, and networking protocols.
- ISO 18033-2 Asymmetric ciphers, Amendment 2 in DAmd 2 stage, reportedly covering Classic McEliece, FrodoKEM, and Kyber/ML-KEM.

Where to go from here?

- Some deployment needs interoperability and agreements/standards.
  But much data and traffic could be protected now already.

Where to go from here?

- Some deployment needs interoperability and agreements/standards.
  But much data and traffic could be protected now already.
- Migration needs testing phase and safety nets.
  Dangerous to remove pre-quantum crypto now & no harm keeping.
- Several recommendations available already, to highlight two from the European Union Agency for Cybersecurity (ENISA)
  - Current state and quantum mitigation
  - Post-Quantum Cryptography – Integration study

  (Disclaimer: I contributed to these documents.)
- Several positive signs of awareness and progress in migration, but much more work needed.

- PQConnect `https://www.pqconnect.net/` ready-to-use software for adding extra PQC layer.

Where to go from here?

- Some deployment needs interoperability and agreements/standards.
  But much data and traffic could be protected now already.
- Migration needs testing phase and safety nets.
  Dangerous to remove pre-quantum crypto now & no harm keeping.
- Several recommendations available already, to highlight two from the European Union Agency for Cybersecurity (ENISA)
  - Current state and quantum mitigation
  - Post-Quantum Cryptography – Integration study

  (Disclaimer: I contributed to these documents.)
- Several positive signs of awareness and progress in migration, but much more work needed.
- New EU project PQCSA on migration and standardization (just started).
- PQConnect `https://www.pqconnect.net/` ready-to-use software for adding extra PQC layer.

Further information

- NIST PQC competition.
- Quantum Threat Timeline 2019; updates from 2021, 2022, 2023, and 2024.
- Status of quantum computer development (by German BSI).
- ENISA studies: Post-quantum cryptography: Integration study, Post-quantum cryptography: current state and quantum mitigation
- YouTube channel Tanja Lange: Post-quantum cryptography.
- `https://2017.pqcrypto.org/school`: PQCRYPTO summer school with 21 lectures on video; slides; exercises.
- Less math, more perspective: `https://2017.pqcrypto.org/exec` and `https://pqcschool.org`.
- `https://pqcrypto.org` our overview page.
- PQCrypto 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024 slides + videos.
- PQCRYPTO project (ran till 2018, but still lots of useful resources).
- PQCSA coming to `https://pqcsa.eu.org` soon.
- PQConnect `https://www.pqconnect.net/` ready-to-use adding extra PQC layer.