Migration roadmaps and timelines
A European perspective

(and that of a scientist in the field)

Tanja Lange

Eindhoven University of Technology, the Netherlands

CODE × ACE 2025

Who am I?

- Professor in Eindhoven (NL), Department Math & CS.
- Trained mathematician & cryptographer
  (minor and teaching qualification in physics).
- Co-organizer PQCrypto 2006: International Workshop on Post-Quantum Cryptography (held at KU Leuven, Belgium, part of EU project ECRYPT).
  Now chair of PQCrypto Steering Committee.
- Coordinated PQCRYPTO EU project (2015 – 2018)

- Expert for NEN (NL standardization body), co-editor in ISO SC27/JTC1 WG2, expert for ISO TC68/SC2 WG1 and CCSDS.
- Submitter of Classic McEliece, NTRU Prime, and SPHINCS+ to NIST PQC competition.
- Co-authored two ENISA studies on PQC 2021 and 2022.

Store now, decrypt later

National Academy report on quantum computing

Quantum Computing: Progress and Prospects (2018)

DETAILS

202 pages | 6 x 9 | PAPERBACK
ISBN 978-0-309-47969-1 | DOI 10.17226/25196

http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=25196

National Academy report on quantum computing

Don't panic. "Key Finding 1: Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm-based public key cryptosystems will be built within the next decade."

National Academy report on quantum computing

Don't panic. "Key Finding 1: Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm-based public key cryptosystems will be built within the next decade."

Panic. "Key Finding 10: Even if a quantum computer that can decrypt current cryptographic ciphers is more than a decade off, the hazard of such a machine is high enough—and the time frame for transitioning to a new security protocol is sufficiently long and uncertain—that prioritization of the development, standardization, and deployment of post-quantum cryptography is critical for minimizing the chance of a potential security and privacy disaster."

Full report at https://nap.edu/25196 (scroll down for free pdf).

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

23 Jun 2025. 1st NIS2 PQC workstream roadmap (link)

A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography

The EU Member States, supported by the Commission, issued a roadmap and timeline to start using a more complex form of cybersecurity, the so-called post-quantum cryptography (PQC).

Quantum computing has been identified as a threat to many cryptographic algorithms used to protect the confidentiality and authenticity of data. This threat can be countered by a timely, comprehensive and coordinated transition to Post-Quantum Cryptography (PCQ).

AdobeStock © ipopba

Timeline for the transition to PQC

1. By **31.12.2026**:
   - At least the *First Steps* have been implemented by all Member States.
   - Initial national PQC transition roadmaps have been established by all Member States.
   - PQC transition planning and pilots for high- and medium-risk use cases have been initiated.
2. By **31.12.2030**:
   - The *Next Steps* have been implemented by all Member States.
   - The PQC transition for high-risk use cases has been completed.
   - PQC transition planning and pilots for medium-risk use cases have been completed.
   - Quantum-safe software and firmware upgrades are enabled by default.
3. By **31.12.2035**:
   - The PQC transition for medium-risk use cases has been completed.
   - The PQC transition for low-risk use cases has been completed as much as feasible.

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
- HQC selected 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 past DIS stage, covering Classic McEliece, FrodoKEM, and Kyber/ML-KEM.
- 14888-6 Stateless hash-based mechanisms (in WD stage).
- 14888-5 Lattice-based mechanisms (upcoming).

Where to go from here?

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

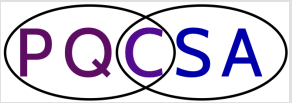
Where to go from here?

- Some deployment needs interoperability and agreements/standards.
  But much data and traffic could be protected now already.
- PQConnect `https://www.pqconnect.net/` ready-to-use software for adding extra PQC layer.
- 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
- TNO, AIVD, CWI (all NL) The PQC Migration Handbook
- Several positive signs of awareness and progress in migration, but much more work needed.

Where to go from here?

- Some deployment needs interoperability and agreements/standards.
  But much data and traffic could be protected now already.
- PQConnect `https://www.pqconnect.net/` ready-to-use software for adding extra PQC layer.
- 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
- TNO, AIVD, CWI (all NL) The PQC Migration Handbook
- Several positive signs of awareness and progress in migration, but much more work needed.
- New EU project PQCSA on migration and standardization (started January 2025). `https://www.pqcsa.eu/`

WP3: Migration roadmap



This work package drafts the roadmap for migration to post-quantum cryptography. The objectives of this work package are as follows:

- 3.1 Prepare the supply chain for the demand in PQC solutions.
- 3.2 Provide stakeholders with a roadmap of how to migrate to PQC.
- 3.3 Establish that the PQCSA migration to PQC roadmap is fit for purpose.
- 3.4 Demonstrate that the versatility of the PQCSA migration to PQC roadmap on at least one sector.

Expect our first draft roadmap before April 2026
(with actual technical recommendations).

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 2025.
- PQCRYPTO project (ended in 2018, but still lots of useful resources).
- PQCSA `https://pqcsa.eu.org`.
- PQConnect `https://www.pqconnect.net/` ready-to-use adding extra PQC layer.