Post-Quantum Cryptography: International Trend Analysis

Tanja Lange

Academia Sinica &
Eindhoven University of Technology

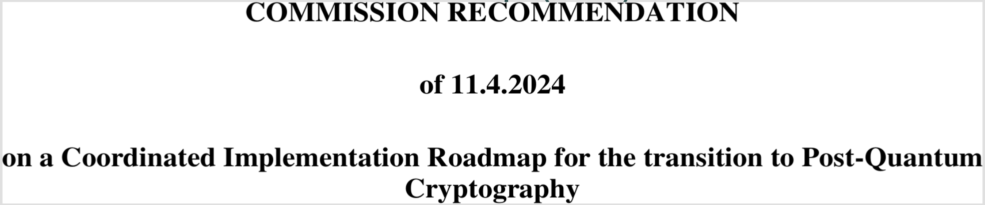
PQC Cybersecurity Industry Alliance
Inauguration and International Symposium
16 May 2024

EU impact on post-quantum cryptography

- PQCrypto 2006: International Workshop on Post-Quantum Cryptography. Held at KU Leuven, Belgium, organized by EU project ECRYPT.
- PQCrypto 2008 (US), PQCrypto 2010 (DE), PQCrypto 2011 (TW) . . . PQCrypto now annual international conference.
- 2014 EU publishes H2020 call including post-quantum crypto as topic. PQCRYPTO and SAFEcrypto projects are funded.
- September 2015: Initial recommendations by PQCRYPTO.
- 2018 Two more PQC EU projects (PROMETHEUS and FutureTPM) funded.
- 2022 Two more PQC EU projects (PQ-REACT and QUBIP) funded. Call limited to partners from EU member states, no associate partners.
- 2024 Standardisation and awareness of the European transition to post-quantum cryptography even excludes entities not under EU control.

PQCRYPTO
ICT-645622

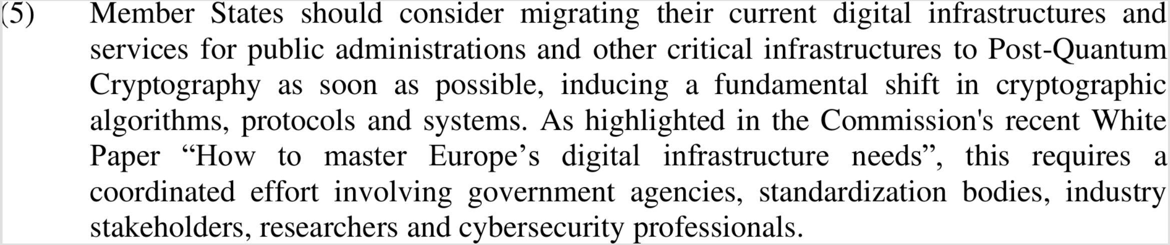
2024 EU PQC transition roadmap (link)



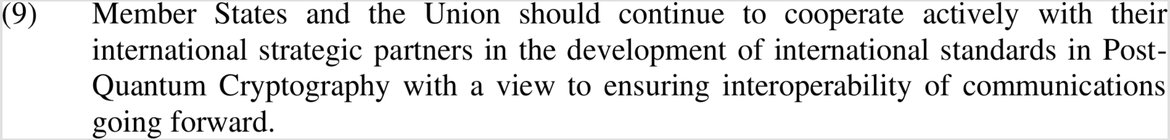
COMMISSION RECOMMENDATION

of 11.4.2024

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

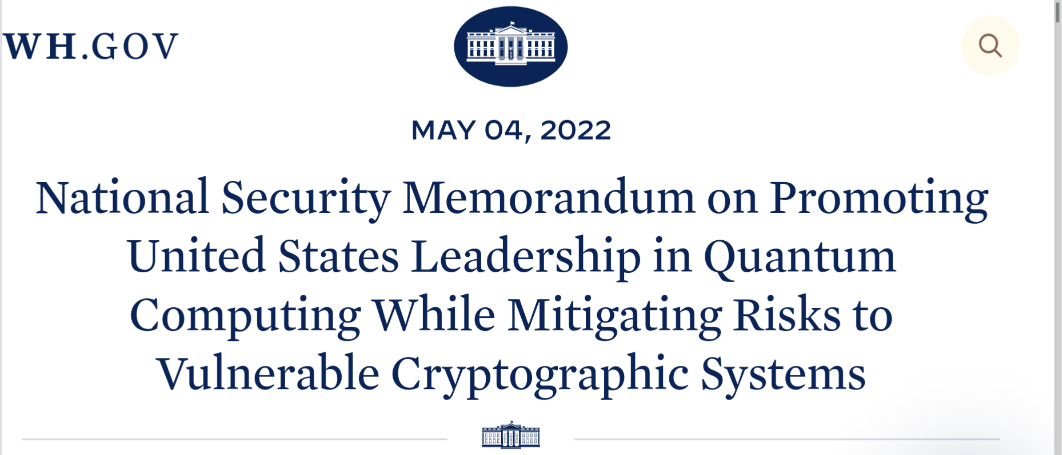


(5) Member States should consider migrating their current digital infrastructures and services for public administrations and other critical infrastructures to Post-Quantum Cryptography as soon as possible, inducing a fundamental shift in cryptographic algorithms, protocols and systems. As highlighted 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.

Efforts do not exist in a vacuum



WH.GOV

MAY 04, 2022

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

White House briefing urges move to PQC, but no public funding for PQC.
National Strategic Overview for Quantum Information Science says "DHS, NIST, NSA" are engaged in post-quantum crypto.

US advising against using PQC – for now

2021.07 Matthew Scholl, Chief of the Computer Security Division in NIST's Information Technology Laboratory: "Don't let folks start to buy and implement unstandard, unknown, potentially unsecured implementations before we as a general community have agreed upon standardization."

2021.08 NSA: "The intention is to update CNSA to remove quantum-vulnerable algorithms and replace them with a subset of the quantum-resistant algorithms selected by NIST ... NSA is waiting for the NIST process to be completed and for standards to be published. ... NSS customers are reminded that NSA does not recommend and policy does not allow implementing or using unapproved, non-standard or experimental cryptographic algorithms. The field of quantum-resistant cryptography is no exception."

2021.09 DHS: Do not use "post-quantum cryptographic industry products until standardization, implementation, and testing of replacement products with approved algorithms are completed by NIST."

Some comments on timing

- Everybody agrees on urgency due to intense funding into building quantum computers and “store now decrypt later” problem.
- Some delay may be justified as NIST process is close to finishing

Some comments on timing

- Everybody agrees on urgency due to intense funding into building quantum computers and “store now decrypt later” problem.
- Some delay may be justified as NIST process is close to finishing since 2.5 years.
  - NIST was due to announce late 2021, announced July 2022.
  - Drafts of 3 of the 4 “winners” available for comments August 2023.
  - New versions expected this summer.
  - 4th round with alternative encryption options still running, no date set.

Some comments on timing

- Everybody agrees on urgency due to intense funding into building quantum computers and “store now decrypt later” problem.
- Some delay may be justified as NIST process is close to finishing since 2.5 years.
  - NIST was due to announce late 2021, announced July 2022.
  - Drafts of 3 of the 4 “winners” available for comments August 2023.
  - New versions expected this summer.
  - 4th round with alternative encryption options still running, no date set.
- Some deployment needs interoperability and agreements/standards; but much could be protected now already.

Some comments on timing and hybrids

- Everybody agrees on urgency due to intense funding into building quantum computers and “store now decrypt later” problem.
- Some delay may be justified as NIST process is close to finishing since 2.5 years.
  - NIST was due to announce late 2021, announced July 2022.
  - Drafts of 3 of the 4 “winners” available for comments August 2023.
  - New versions expected this summer.
  - 4th round with alternative encryption options still running, no date set.
- Some deployment needs interoperability and agreements/standards; but much could be protected now already.
- Migration needs testing phase and safety nets.
  Dangerous to remove pre-quantum crypto now & no harm keeping.
  NSA announcement about remove and replace is worrisome.
  EU roadmap document foresees hybrid deployment.

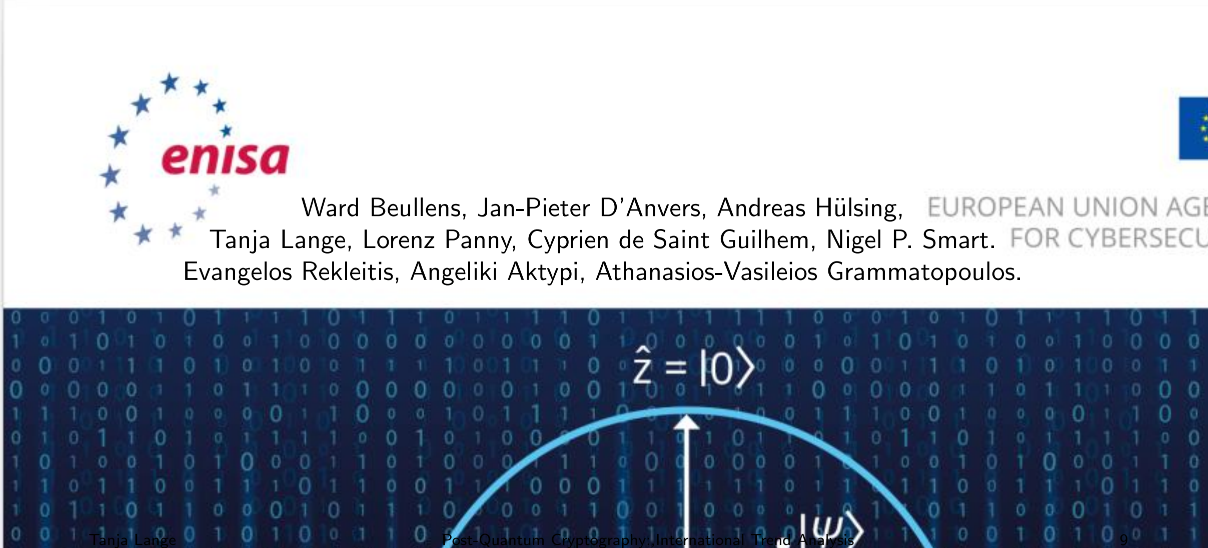
US ANSI X9 on PQC hybrids

2021: “As we transition from classical cryptography to post-quantum cryptography (PQC), there is a need to understand the proper ways to use both methods simultaneously. PQC methods will not be able to be used as a direct replacement in all cases. And the confidence and broad acceptance of PQC methods will not be as great as classical cryptography. **Simultaneous use of both classical cryptography and PQC methods for both security and acceptance** is required during a transition and may be required long term as well. There are improper and insecure ways of implementing a hybrid of classical and PQC methods. Specifying the proper methods of using both are required.” (emphasis added)

ANSSI (French agency) on PQC hybrids

2022: “Although this new post-quantum toolbox may seem handy for developers, the maturity level of the post-quantum algorithms presented to the NIST process should not be overestimated. Many aspects lack cryptanalytical hindsight or are still research topics, e.g. analysis of the difficulty of the underlying problem in the classical and quantum computation models, dimensioning, integration of schemes in protocols and more importantly the design of secure implementations. This situation will probably last some time after the publication of NIST standards. **Acknowledging the immaturity of PQC is important: ANSSI will not endorse any direct drop-in replacement of currently used algorithms in the short/medium term.** However, this immaturity should not serve as an argument for postponing the first deployments.” (emphasis added)

Post-Quantum Cryptography:
Current state and quantum mitigation



enisa

EUROPEAN UNION AGE
FOR CYBERSECU

Ward Beullens, Jan-Pieter D'Anvers, Andreas Hülsing,
Tanja Lange, Lorenz Panny, Cyprien de Saint Guilhem, Nigel P. Smart.
Evangelos Rekleitis, Angeliki Aktypi, Athanasios-Vasileios Grammatopoulos.

ENISA studies: Current state and quantum mitigation (2021)
Post-Quantum Cryptography - Integration study (2022)

Table of contents:

1. Introduction
2. Families of Post-Quantum Algorithms
3. Security Notions and Generic Transforms
4. NIST Round 3 Finalists
5. Alternate Candidates
6. Quantum Mitigation
   - 6.1 Hybrid schemes
   - 6.2 Protective measures for pre-quantum cryptography

1. Introduction
2. Integrating post-quantum systems into existing protocols
3. New protocols designed around post-quantum systems
4. Double encryption and double signatures
5. Security proofs in the presence of quantum attackers
6. Standardization efforts for protocols

Reports available here and here from ENISA's website.

Efforts in other countries and standardization (incomplete)

- China ran its own competition (2018 - 2020), in China, by China, and for China . . .

Efforts in other countries and standardization (incomplete)

- China ran its own competition (2018 - 2020), in China, by China, and for China . . . without much international attention.
  (Winner LAC discarded by NIST in Round 2.)
- Korea runs KpqC competition. Aims to improve national PQC competence. Submission teams require Koreans. KpqC seeks international attention.
- Internet Engineering Task Force (IETF) has already standardized XMSS & LMS (two stateful hash-based signatures).
  Working on drafts for various schemes (Kyber, Classic McEliece, NTRU, NTRU Prime) and methods for combining them with elliptic-curve crypto.
- ISO has 14888-4 Stateful hash-based mechanisms under publication.
  18033-2 Asymmetric ciphers, Amendment 2 in working-draft stage, reportedly covering Classic McEliece, FrodoKEM, and Kyber/ML-KEM.

Further information

- NIST PQC competition.
- Quantum Threat Timeline, 2019; 2021 update.
- 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 (upcoming) slides + videos.
- PQCRYPTO recommendations.
- Post-quantum cryptography transition next EU call, deadline Nov 2024.