Roadmap for the Transition to Post-Quantum Cryptography

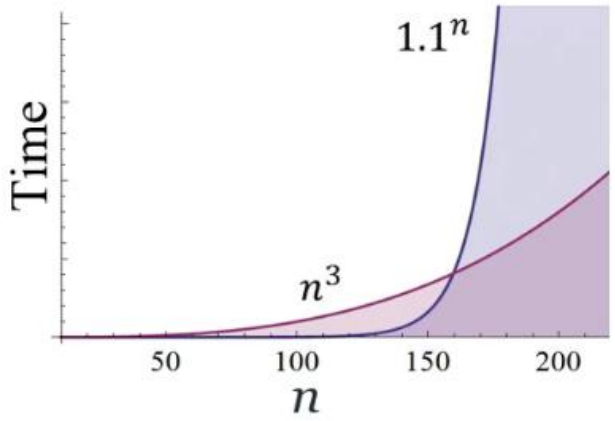
Fabiana Da Pieve

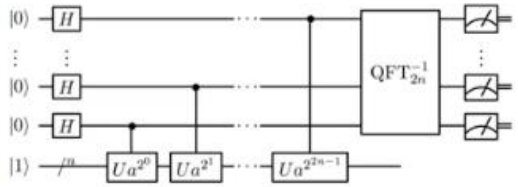
Program Manager
Unit C.4 “Emerging and Disruptive Technologies”
Directorate General for Communications Networks, Content, and Technology (DG CONNECT)

Shor's and Grover's algorithms

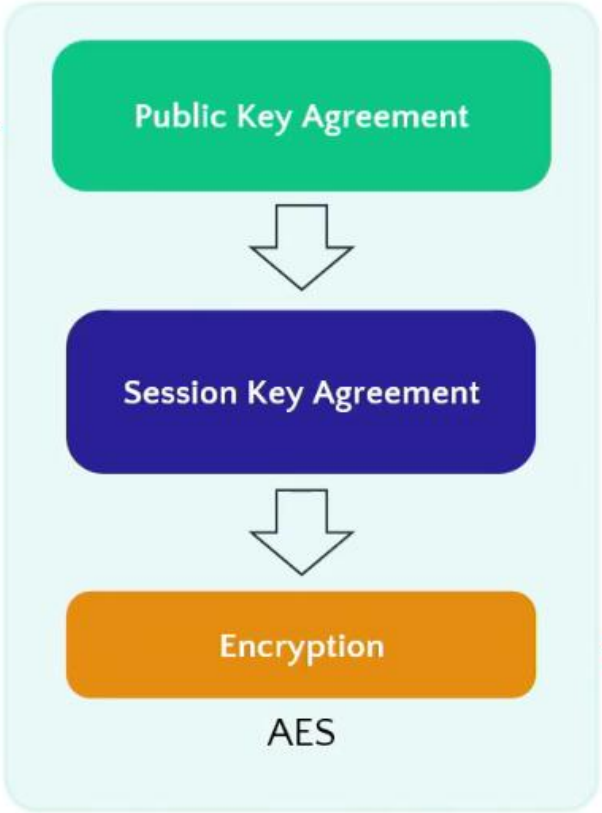
Exponential speed-up in factoring!

breaks



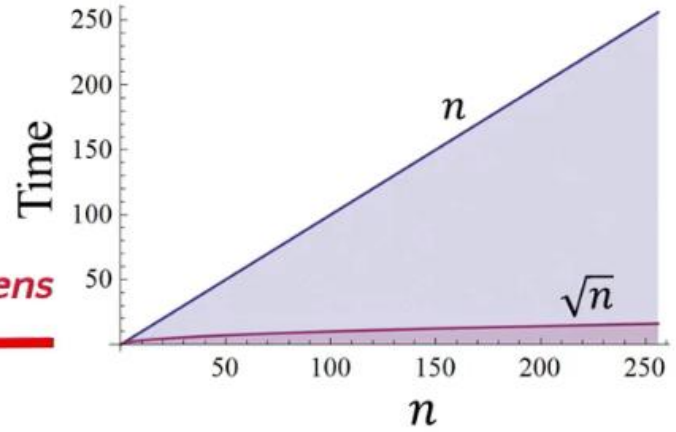


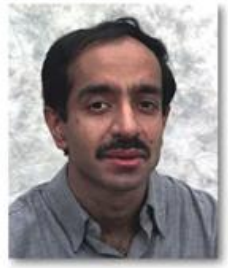
P. W. Shor, **Algorithms for quantum computation: Discrete logarithms and factoring,** *Proc. 35nd Annual Symposium on Foundations of Computer Science* (Shafi Goldwasser, ed.), IEEE Computer Society Press (1994), 124-134.

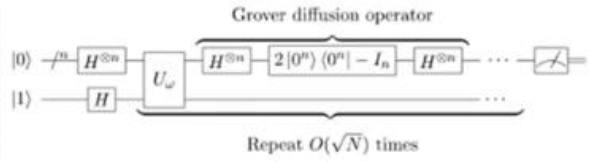


weakens

Quadratic speed-up in searching!







Quantum Mechanics Helps in Searching for a Needle in a Haystack

Lov K. Grover
Phys. Rev. Lett. **79**, 325 – Published 14 July 1997

If a large quantum computer can be built … what happens ?

Devastating effects on society at all levels, economy, political stability …

At risk: everything ! Data in transit, data at rest, data-in-use

Harvest now-decrypt later attacks already occurring, forging signatures will come later

All modern public-key cryptography has to be replaced [Shor'94]

- RSA
- Diffie-Hellman (including elliptic curves)

For symmetric crypto; huge devices would be needed to break it; serial algorithm does not scale impressively

You may double things … but not at the price of public-key cryptography:

Symmetric key sizes: x2 [Grover'96]

Hash function outputs x2 [Grover'96]

See Sam Jacques CHES'24: https://www.youtube.com/watch?v=eB4po9Br1YY

There are, in fact, several transitions

Confidentiality (& could authenticate):
KEY ENCAPSULATION MECHANISMs (KEMs)
Urgent !

- ML-KEM (FIPS 203) – despite some occasional difficulty with its larger key sizes, in several cases it allows for a drop-in upgrade – at least for Post-Quantum Internet
- Sectors with constrained devices: problems

Authentication, integrity and non-repudiation:
SIGNATURES & CERTIFICATES
less urgent but more complex !

- attacks in real time
- use of digital signatures more complex than key agreement
- none of the current PQC signatures scheme is ideal

Other transitions: advanced cryptographic schemes

(anonymous credentials, FHE, …attribute-based encryption, …)

EUROPEAN COMMISSION

Brussels, 11.4.2024
C(2024) 2393 final

COMMISSION RECOMMENDATION

of 11.4.2024

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

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 292 thereof,

Having regard to Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148[1] (NIS 2 Directive).

HAS ADOPTED THIS RECOMMENDATION

1. SCOPE AND OBJECTIVES

The purpose of this Recommendation is to foster the transition to Post-Quantum Cryptography for the protection of digital infrastructures and services for public administrations and other critical infrastructures in the Union by enabling Member States to:

(1) define a 'Post-Quantum Cryptography Coordinated Implementation Roadmap' aimed at synchronising the efforts of Member States to design and implement national transition plans while ensuring cross-border interoperability;

(2) support the evaluation and selection of relevant Post-Quantum Cryptography EU algorithms with the help of cybersecurity experts, and further adoption of such algorithms as Union standards that should be implemented across the Union as part of the Post-Quantum Cryptography Coordinated Implementation Roadmap.

(3) take appropriate and proportionate measures to prepare for this transition.

2. COORDINATED IMPLEMENTATION ROADMAP ADDRESSING THE TRANSITION TO POST-QUANTUM CRYPTOGRAPHY

(4) This Recommendation encourages Member States to coordinate their actions at Union level through a dedicated Member States forum. For this purpose, the Commission recommends that Member States take advantage of existing structures at Union level in the area of cybersecurity and establish a sub-group of the NIS Cooperation Group. Such sub-group could include representatives of national security agencies and cybersecurity experts, notably from national cybersecurity authorities and ENISA. The sub-group may invite representatives of relevant stakeholders to participate in its work such as those of advisory bodies of public organisations, industry, service providers, and operators, with a view to gather input and exchange information on the transition of digital infrastructures and services for public administrations and other critical infrastructures to Post-Quantum Cryptography in different sectors, coordinate their efforts at national level, and develop the Post-Quantum Cryptography Coordinated Implementation Roadmap, in accordance with the Union competition rules and Union data protection law.

(5) This sub-group on Post-Quantum Cryptography should consider appropriate, effective and proportionate measures for defining and coordinating the development of the Post-Quantum Cryptography Coordinated Implementation Roadmap. The sub-group on Post-Quantum Cryptography is encouraged to engage in discussions with other relevant bodies, such as Europol, NATO, or others, to avoid duplication of efforts and ensure a cohesive approach to addressing emerging challenges.

(6) To this effect, soon after the publication of this Recommendation, Member States are invited to establish such a sub-group on Post-Quantum Cryptography pursuant to Commission implementing decision (EU)2017/179 and to appoint expert representatives who should work in close cooperation with the Commission and who should be tasked to define and develop the Post-Quantum Cryptography Coordinated Implementation Roadmap.

(7) The Post-Quantum Cryptography Coordinated Implementation Roadmap should be available after a period of two years following the publication of this Recommendation, which will be followed by the development and further adaptation of Post-Quantum Cryptography transition plans of individual Member States, in accordance with the principles set out in the Post-Quantum Cryptography Coordinated Implementation Roadmap.

ACTIONS AT UNION LEVEL

(8) The overall work will be monitored and assessed periodically by the Commission in cooperation with the expert representatives of the Member States.

(10) On the basis of those and all other available information the Commission will assess the designed measures and the operation of the network of Member States' representatives and determine whether additional actions, including proposing binding acts of Union law, are required.

experts

targets

by when

what

active role

monitoring

who will do the work

additional measures

Roadmap for a Coordinated Transition across EU

New PQC workstream in the NIS Cooperation Group created

First version of the Roadmap released (June 2025):

Timeline:

- By 31/12/2026. PQC roadmaps defined in each MS. Planning for high- and medium-risk use cases will be underway.
- By 21/12/2030: high-risk use case migrated: critical infrastructure (eg water, energy, health care, finance and transportation) and high-risk domains. Quantum-safe software and firmware upgrades are enabled by default. Transition planning for medium-risk ones.
- By 31/12/2035. All of the migrations should be completed for every risk level.

https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

Strong hook to the Cyber Resilience Act in the Roadmap

Necessity for consideration of EU Cybersecurity Policies in National Actions

Roadmap – more in detail – first and next steps

End of 2026 **End of 2030** **End of 2035**

Milestone 1: 31.12.2026

- First Steps:
  - Identify and involve stakeholders.
  - Support mature cryptographic asset management.
  - Create dependency maps.
  - Perform quantum risk analysis.
  - Include the supply chain.
  - Create a national awareness and communication program.
  - Share knowledge and get involved with the NIS CG work stream on PQC.
  - Develop a timeline and an implementation plan.
- **Main achievements**:
  - PQC transition planning and pilots for high- and medium-risk use cases have been initiated.
  - Initial national PQC transition roadmaps have been established by all Member States.

Milestone 2: 31.12.2030

- Next Steps:
  - Support cryptographic agility and a quantum-safe upgrade path.
  - Allocate resources for the transition.
  - Adapt certification schemes.
  - Evolve the rules.
  - Look for opportunities within the ecosystem.
  - Considering transversal activities throughout the creation and implementation of the roadmap.
  - Implement pilot use cases and contribute to testing centres.
- **Main achievements**:
  - The PQC transition for high-risk use cases has been completed.
  - PQC transition planning and pilots for medium-risk use cases has been completed.
  - Quantum-safe software and firmware upgrades are enabled by default.

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.

Strong hook to the Cyber Resilience Act in the Roadmap

Necessity for consideration of EU Cybersecurity Policies in National Actions

Roadmap builds on lessons learnt from the past

Take action as soon as possible !
We don't know when quantum computers will break today's crypto, but:

- attackers store now, decrypt later;
- devices deployed today remain in the field for decades;
- migration takes time and may not be smooth.

Use hybrid deployments

- Combine PQC with traditional schemes – traditional schemes must NOT be weakened
- Security as long as one of the two schemes is secure
- Weakened encryption impedes the migration to PQC

Supply chain security (HW and SW) – and contribute to transparent standardization activities

- Enabling Quantum-safe software and firmware upgrades by default, by 2030

Symmetric methods instead of public-key cryptography are also worthwhile to consider, depending on the application

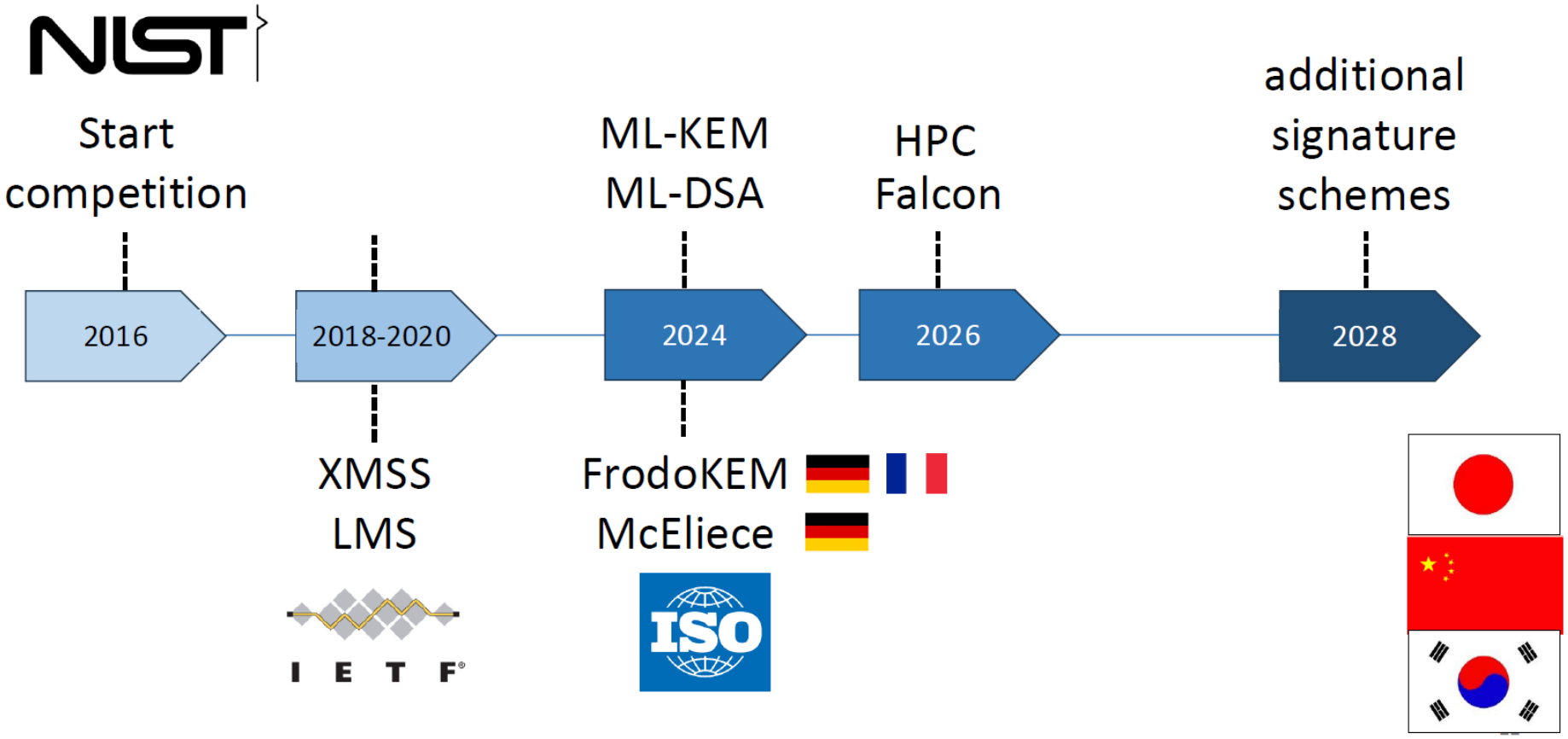
Crypto-Agility as fundamental aspect

It is important that all implementations of cryptography be “crypto-agile”: cryptographic routines and ciphers can be easily upgraded or replaced without having to completely replace the underlying application or device.

Need for: Interoperability, diverse technical requirements, rapid update cycles

Type of Agility	Definition
Implementation	The Capability to swiftly configure interfaces and implement updates across various systems or applications
Compliance	The capacity to adapt cryptographic configurations in accordance with compliance requirements.
Security Strength	The capability to dynamically adjust the level of security strength based on configuration, allowing for scalable security measures.
Migration	The capability to transition and convert between cryptographic algorithms seamlessly.
Retirement	Ability to retire obsolete or insecure cryptographic algorithms
Composability	The capability to securely integrate multiple cryptographic primitives for composability.
Platform	Ability to use assured cryptographic algorithms across different platform types
Context	Ability to use a derived cryptographic algorithm policy with the flexibility from system attributes

Timeline standardization



Impact of the PQC transition on (some of the) relevant areas related to data protection

EUDI wallet

Data and personal data processing (Cloud, AI-training, ...)

Age verification protocols

Impact of the PQC transition on EUDI Wallet is **pervasive**

https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng

"Technologies used to achieve those objectives should be developed aiming towards ***the highest level of security, privacy, user convenience, accessibility, wide usability and seamless interoperability.*** *"*

"Trust in European Digital Identity Wallets would be enhanced if issuing and managing parties are required to implement appropriate technical and organisational measures to ensure ***the highest level of security that is commensurate to the risks raised for the rights and freedoms of the natural persons****, in accordance with Regulation (EU) 2016/679."*

"European Digital Identity Wallets should ensure ***the highest level of data protection and security for the purposes of electronic identification and authentication to facilitate access to public and private services, irrespective of whether such data is stored locally or on cloud-based solutions****, taking due account of the different levels of risk."*

"European Digital Identity Wallets should be secure-by-design and should implement advanced security features to protect against identity and other data theft, denial of service and any other cyber threat. Such security should include ***state-of-the-art encryption and storage methods that are accessible only to, and decryptable only by, the user and that rely on end-to-end encrypted communication with other European Digital Identity Wallets and relying parties****."*

→ at this moment PQC for such advanced applications is under strong investigation efforts, and must be ready by 2030

Impact of the PQC transition on EUDI Wallet is **pervasive**
(continuation)

https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng

"To ensure that the European Digital Identity Framework is open to innovation, technological development and future-proof,"
→ seems mostly about testing ....
however, it ends with *"thus preventing the development of solutions that do not comply with Union law on data protection or that are open to security vulnerabilities."*
→ So development NOT allowed for unsecure solutions ! a quantum computer would bring an acute security vulnerability
→ And CRA anyway requires long-term security

"Trust service providers should use cryptographic methods reflecting ***current best practices and trustworthy implementations*** *of those algorithms in order to ensure security and reliability of their trust services."*

"Member States should integrate different privacy-preserving technologies, such as zero knowledge proof, into the European Digital Identity Wallet. Those cryptographic methods should allow a relying party to validate whether a given statement based on the person's identification data and attestation of attributes is true, without revealing any data on which that statement is based, thereby preserving the privacy of the user."

Impact of the PQC Roadmap on the EUDIW

Anonymous credential systems

Current plans seem to be suboptimal in terms of Security AND Privacy

- commodity random-oracle signature scheme (**ECDSA**) and hacky ad-hoc techniques to achieve (some of) the privacy properties
- users will get batches of many signatures at a time so that they only need to present each signature once

This does NOT:

- prevent linkeability with respect to the issuing party, required from the law
- offer quantum-resistance …

So … which PQC digital signatures ? Instantiated by which Zero-Knowledge Proofs ?

- Possibly, development general lattice-based zero-knowledge proof systems that are easy to use for proving standard schemes with their symmetric-key primitives
- Improvement of their performance and proof sizes to levels that are orders of magnitude better than now

Impact of the PQC transition on data and personal data processing (Cloud, AI-training, …)

Numerous cloud-based applications, where data is not only externally stored, but externally computed upon

Data confidentiality can hence be lost to the cloud provider, any entity who hacks the cloud provider, and any entity that has legal authority on the cloud provider

Protection needed for numerous cloud-based applications:

- database management
- delegation of machine learning inference and training
- delegated statistics, etc notably for financial data, medical data, government data and individuals' private data

Specific examples:

Protecting huge databases (biometrics, searches in text, searches in DNA, searches in movies) - compute on data protected via quantum-safe Fully Homomorphic Encryption (FHE) → avoid personal data leakage

Protecting machine learning queries and model training. AI requires a lot of data to be effective, but this impacts privacy. FHE allows to remove this tension between functionality and privacy.

Need for: theory, computational acceleration, standardization and certification

Conclusions

We do not know with 100% certainty if or when a quantum computer will break RSA & ECC

But we can’t take the risk

Need to move:

- risk-based approach
- crypto-agility
- hybrid deployments (PQC & current public-key cryptography)
- **we need a huge efforts in pilot projects with testing PQC-solutions**
- refinement EU-level strategy

Thank you for your attention