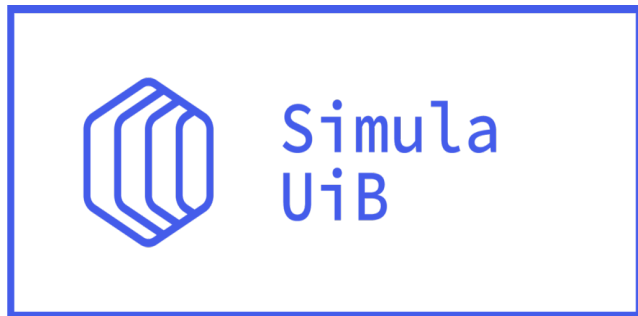


Welcome to the NorPQC workshop



Outline of the Day

0900 - 0930 Introduction, background and context

0930 - 1045 Understanding the risks of PQC and urgency of migration

Break

1100 - 1200 Discovering cryptography in use

Lunch

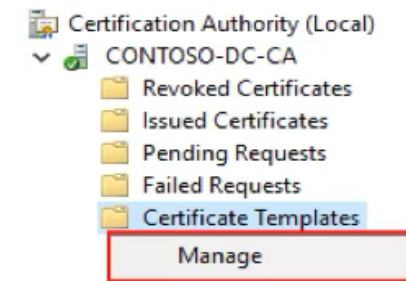
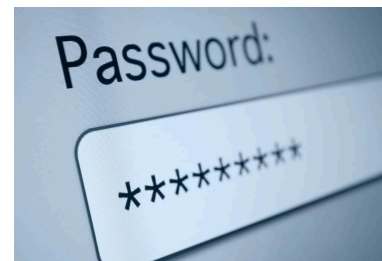
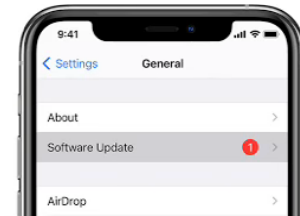
1245 - 1400 Planning and executing migration

Break

1415 - 1530 Technical PQC deep dive

Use cases of cryptography

- **Internet traffic**, secured with TLS, IPsec, SSH all rely on both public key and symmetric cryptography
- **Messaging services** use end-to-end encryption
- **Software updates** are digitally signed
- Key management for long-term **secure storage** solutions
- **Secure identity** management
- Public key **certificates**




Security of public key cryptography

- Security relies on mathematical problems that are hard to solve

- Factoring large integers
- Solving discrete logarithm problem
- Finding the shortest vector in a lattice
- Decoding unstructured linear code
- Solving non-linear equation systems

Easy to solve with
quantum computer



Quantum computers

- Fundamentally different from classical computers
- Classical
 - bits can be either 0 or 1
 - Value of bits are independent of each other
- Quantum
 - qubits can be 0, 1, or a combination of 0 and 1
 - Qubits can be entangled => their values are linked
- Quantum computations can be massively parallel

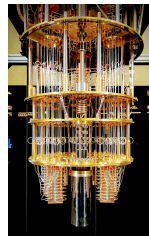
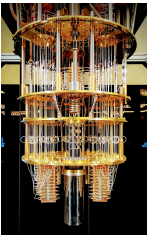
Threat from quantum computer

Digital signatures

Asymmetric encryption
Key exchange

Factorization

DLP

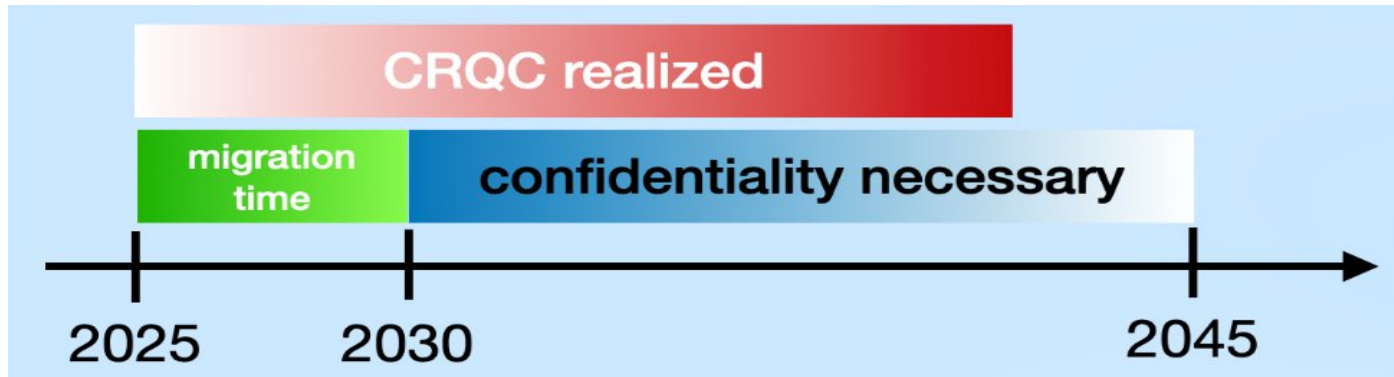


**Shor's algorithm (1994):
Known for 30 years that a
large quantum computer
can efficiently solve
factorization and discrete
logarithm problem**

Cryptographically
Relevant Quantum
Computer (CRQC)

Harvest now decrypt later

- For how long does your data need to be confidential?
- Encrypted communication can be (is?) stored now, to be decrypted when a CRQC is available (**harvest now – decrypt later**)

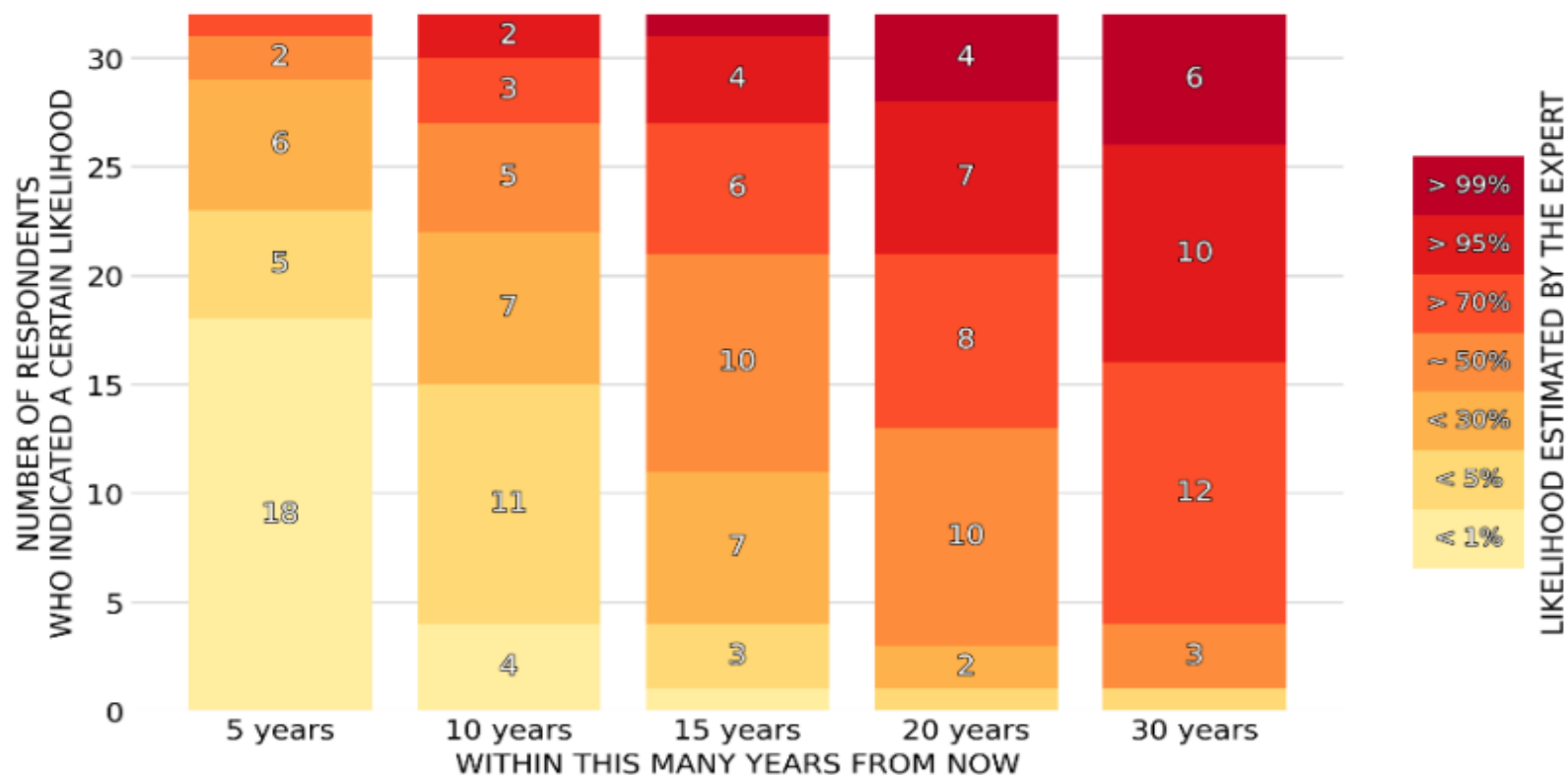


Quantum threat timeline

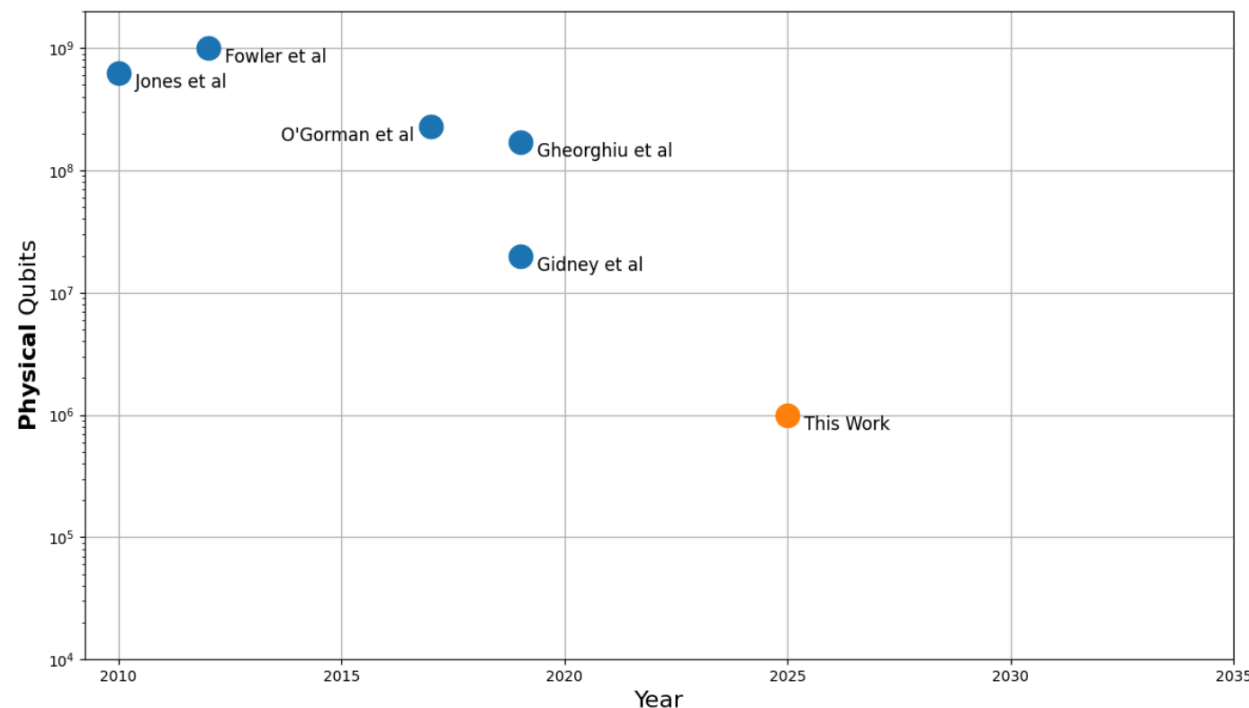
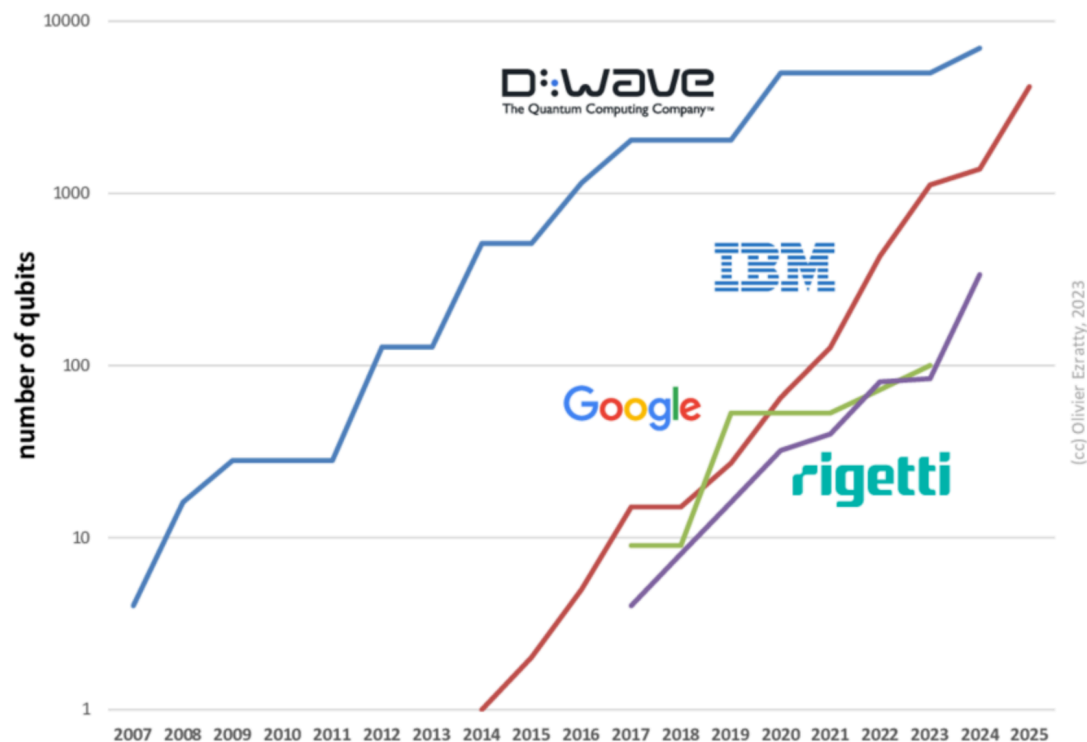


2024 EXPERTS' ESTIMATES OF LIKELIHOOD OF A QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS

The experts indicated their estimate for the likelihood of a quantum computer that is cryptographically relevant—in the specific sense of being able to break RSA-2048 quickly—for various time frames, from a short term of 5 years all the way to 30 years.



When to expect a CRQC?




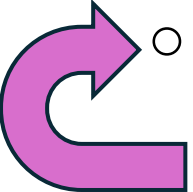
<https://arxiv.org/pdf/2505.15917>

For breaking RSA-2048

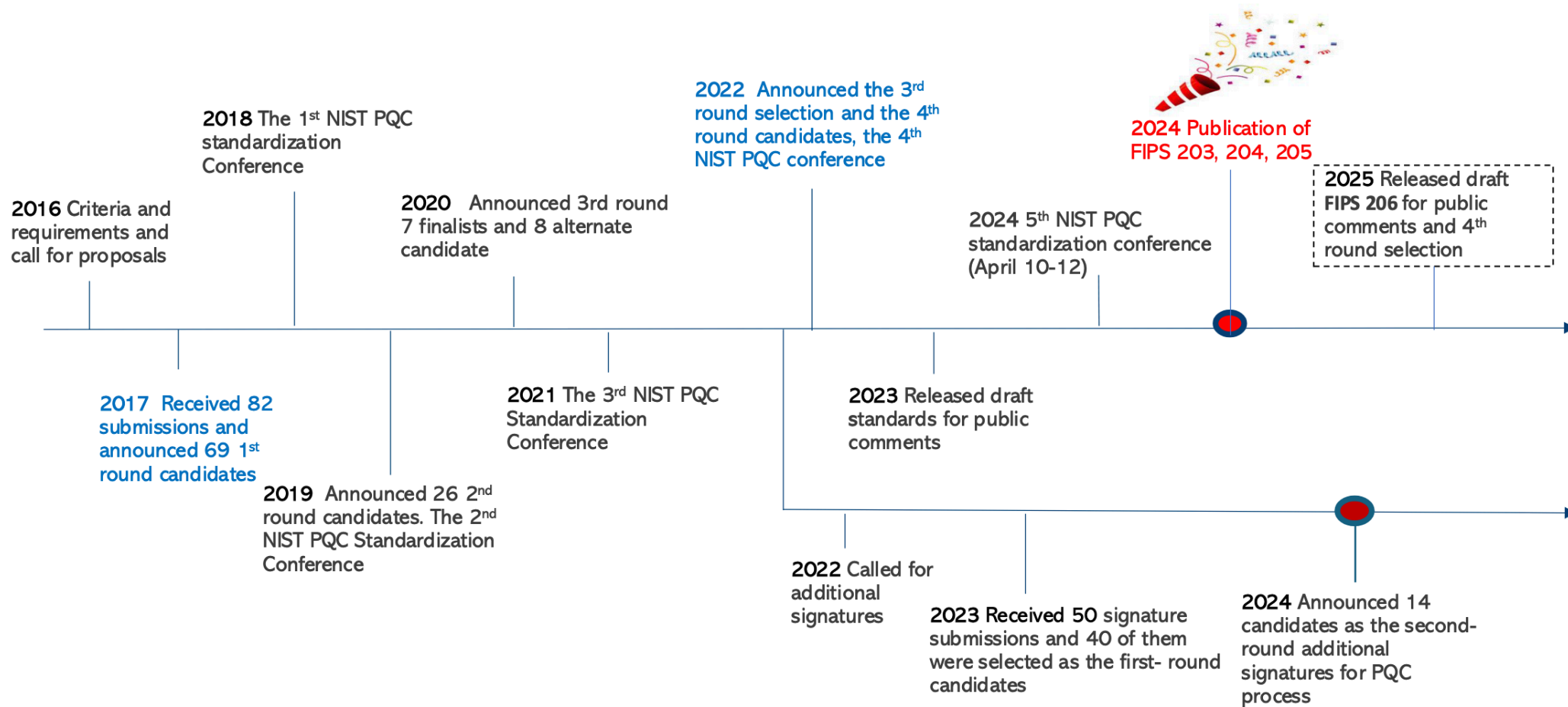
Is migration urgent?

- PQC compliancy will become a requirement
- Confidentiality: urgent
- Authenticity: less urgent
- Urgency varies across data and organizations, but...
- ...everyone needs to do risk assessment as soon as possible

Post-quantum cryptography (PQC)

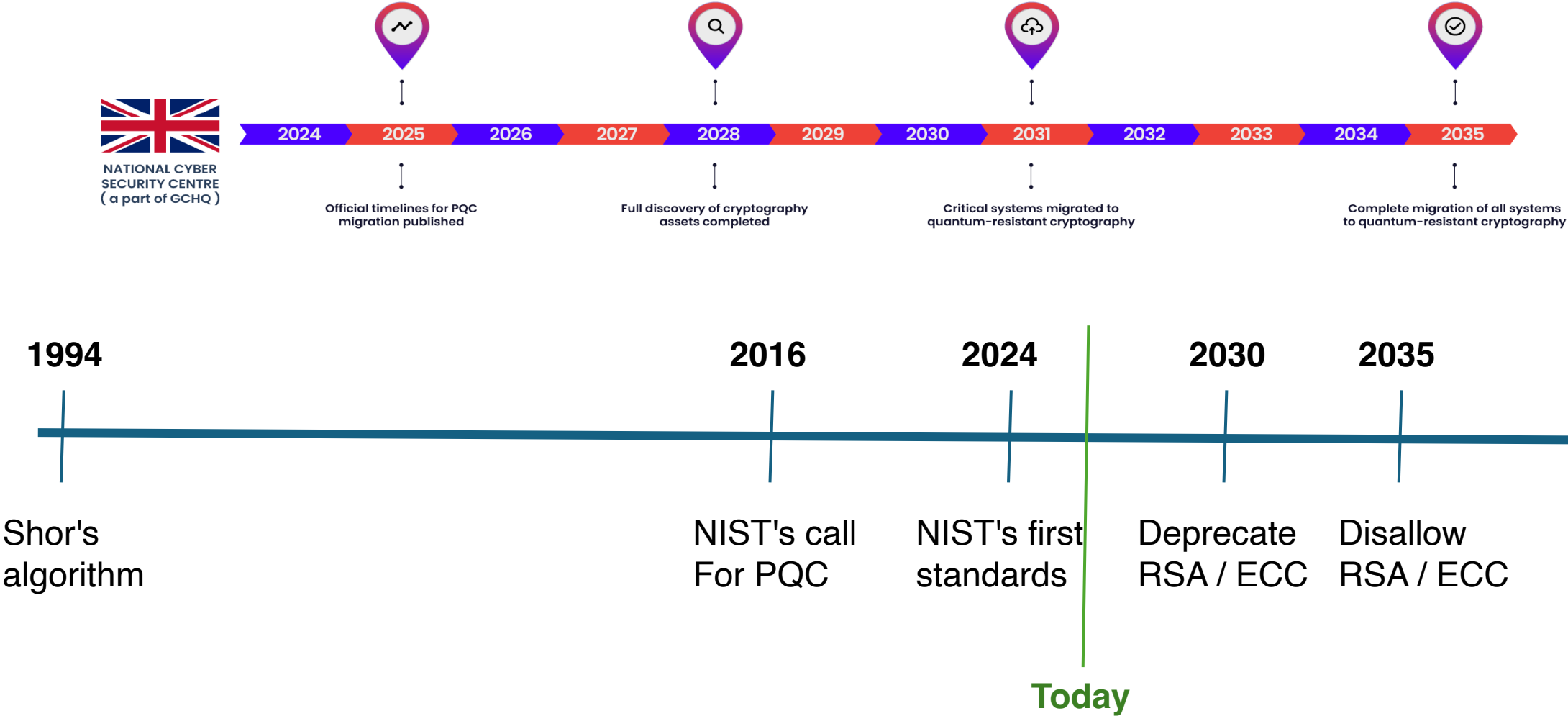
- PQC = cryptography that is secure against both classical and quantum computers
- Need to replace affected cryptography with PQC alternatives
 - Develop and standardize PQC algorithms  **Partly finished**
 -  ◦ Replace vulnerable cryptography with PQC alternatives everywhere it is found
Work to be started now: PQC migration

NIST's PQC standardisation process



<https://csrc.nist.gov/Presentations/2025/nist-pqc-the-road-ahead>

Road ahead



Priority (EU, November 2024)

*Securing Tomorrow,
Today: Transitioning
to Post-Quantum
Cryptography*

A joint statement from partners from 18 EU member states:

Secure Information Technology Center Austria, Centre for Cybersecurity Belgium, National Cyber and Information Security Agency Czech Republic, Centre for Cyber Security Denmark, Information System Authority Estonia, Finnish transport and Communication Agency, French National Agency for the Security of Information Systems, Federal Office for Information Security Germany, National Cyber Security Authority Hellenic Republic, National Cyber Security Centre Ireland, National Cybersecurity Agency Italy, Ministry of Defense Latvia, National Cyber Security Centre Ministry of Defense Lithuania, High Commission for National Protection Luxemburg, Netherlands National Communication Security Agency, Ministry of Interior and Kingdom Relations Netherlands, National Cyber Security Centre Ministry of Security and Justice Netherlands, Research and Academic Research Center Poland, Government Information Security Office Slovenia, National Cryptologic Center Spain

We urge public administration, critical infrastructure providers, IT providers, as well as all of industry, to **make the transition to post-quantum cryptography a top priority**. For the reasons outlined above, organizations and governments should **start the transition now** by working on the following steps (we refer to [5] and [6] for more details):

Priority (EU, June 2025)

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

Part 1, Version: 1.1, EU PQC Workstream

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.

Therefore, the PQC transition requires a well-prepared, systematic and persistent treatment. National governments will have to act now in order to complete the transition to PQC in time and shall be supported by the European Union in this process.

Priority (Norway, March 2025)



NSM
CENTRE FOR
APPLIED CRYPTOLOGY

Guidance document

NSM Cryptographic Recommendations

There is a need to migrate to quantum-resistant cryptography. It is recommended to start the migration process as soon as possible, which first and foremost involves getting an overview of one's cryptographic inventory, see Section [1.3](#). Additionally, the principles of cryptographic agility in Section [1.4](#) are important to be well-prepared for a migration to quantum-resistant cryptography. For further information and guidance, see nsm.no/kvantemigrasjon.

Schedule

0930 - 1045 Determining critical assets

1100 - 1200 Discovering cryptography in use

1200 – 1245 Lunch

1245 - 1400 Planning for replacement

1415 - 1530 Technical PQC deep dive