

Understanding Post-Quantum Cryptography (PQC):

What Is PQC and Why Do We Need It?

Ruxandra F. Olimid

University of Bucharest

17 October 2026



/q-fence



@ q-fence

<https://qfence-project.eu>

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement N° 101225708, as well as the Swiss State Secretariat for Education, Research and Innovation (SERI).



**Funded by
the European Union**

Project funded by

 Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research SERI
State Secretariat for Education,
Research and Innovation SERI

What is PQC?

- What is **cryptography**?

*“**Cryptography** is a vital **part of cybersecurity**. Security properties such as confidentiality, integrity, authentication and non-repudiation rely on strong cryptographic mechanisms, especially in an always connected, seamless online world.”*

[Source: <https://www.enisa.europa.eu/topics/digital-identity-and-data-protection/cryptography>]

Why do we need PQC?

*“The **art and science of using mathematics** to secure information and create a high degree of trust in the electronic realm.”*

[Source: <https://csrc.nist.gov/glossary/term/cryptography>]

TRUE or FALSE?

Post-Quantum Cryptography (PQC) is cryptography running on quantum computers.

- FALSE!



What is PQC?

- What is cryptography?
- What is **PQC**?

Why do we need PQC?

***“Post-quantum cryptography**, usually abbreviated as **PQC**, studies cryptographic algorithms that can run on **ordinary computers** but are designed to resist attacks performed with **both classical and quantum computers**.”*

[Source: <https://www.qfence-project.eu/what-is-post-quantum-cryptography-and-why-it-matters/>]

***“Post-quantum cryptography** is an area of cryptography in which systems are studied under the security assumption that **the attacker has a quantum computer**.”*

[Source: <https://csrc.nist.gov/glossary/term/cryptography>]

***“An area of cryptography** that researches and advances the use of **quantum-resistant primitives**, with the goal of keeping existing public key infrastructure intact in a future era of quantum computing.”*

[Source: <https://csrc.nist.gov/topics/security-and-privacy/cryptography/post-quantum-cryptography>]

Honest users: classical computer

Adversary: quantum (and classical) computer

Security reasoning changes

- Move from **Random Oracle Model (ROM)** to **Quantum-accessible ROM (QROM)**: allows to make a query on a superposition of inputs to receive a superposition of outputs; limits the value of security proofs in ROM (schemes that can be proved secure in ROM are insecure in QROM)
- Implications on techniques such as **rewinding** to an earlier state is challenging in the quantum world (measurement operations are not reversible)

Security models:

- **Q1 model:** the attacker is allowed to only **execute classical queries**, but the adversary can perform offline quantum computation (in the ideal model, the adversary has quantum access to oracles that simulates ideal functionalities but only classical access to keyed oracles)
- **Q2 model:** the attacker is allowed to **execute quantum superposition queries** (in the ideal model, the adversary has quantum access to both keyed oracles and oracles that simulate ideal functionalities)

- **Post-Quantum Cryptography**
 - Solutions that can work **on classical computers**, believed to be **resistant to both classical and quantum attacks**
 - Runs on **existing computers**
 - Examples: **ML-KEM (Kyber)**, **ML-DSA**, **SLH-DSA**
- **Quantum Cryptography**
 - Solutions that **use quantum physics**
 - Requires **specialized hardware**
 - Example: **Quantum Key Distribution (QKD)**

What is PQC?

- What is cryptography?
- What is PQC?

“... the quantum threat **is not a generic fear that “future computers will be faster”**. It is a **precise weakness in the mathematical foundations** of many public-key systems that are used today...”

[Source: <https://www.qfence-project.eu/what-is-post-quantum-cryptography-and-why-it-matters/>]

Why do we need PQC?

- What is the quantum threat?

Shor (1994): shows that quantum computers can solve problems such as the **factorization problem** and the **discrete logarithm problem** much more efficiently than classical computers

Shor, P. W. (1994, November). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science* (pp. 124-134). IEEE.

TRUE or FALSE?

The quantum threat is mostly impacting public-key cryptography.

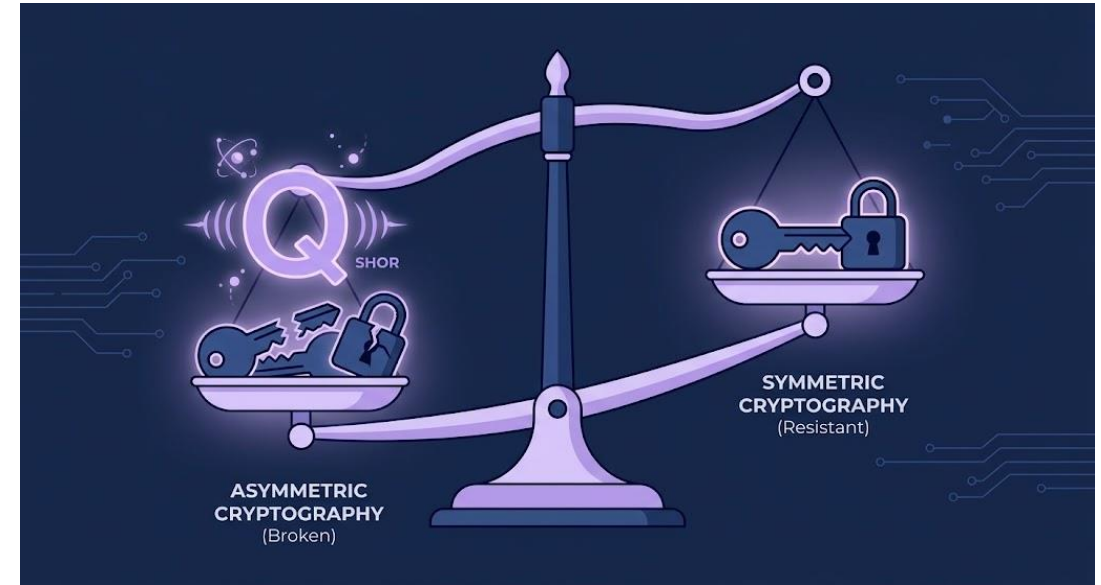
- TRUE!



Impact on Asymmetric vs. Symmetric Cryptography

- Asymmetric cryptography is fundamentally broken
- [The quantum threat] “... is a ***precise weakness in the mathematical foundations*** of many public-key systems that are used today”
- “**Symmetric encryption and hash functions** are affected in a different way and can usually be adapted by choosing stronger parameters.”

[Source: <https://www.qfence-project.eu/what-is-post-quantum-cryptography-and-why-it-matters/>]



[Source: Generated with AI (Gemini 3.6 Thinking)]

What is PQC?

- What is cryptography?
- What is PQC?

Why do we need PQC?

- What is the quantum threat?
- Are CRQC available today?

“Cryptographically Relevant Quantum Computers (CRQC) are not publicly available today”

[Source: <https://www.qfence-project.eu/what-is-post-quantum-cryptography-and-why-it-matters/>]

Limitations:

- Low no. of logic Q-bits/ fault tolerance
- Q-bits are fragile, quantum decoherence, noise
- Quantum error correction is complex, high error rates
-

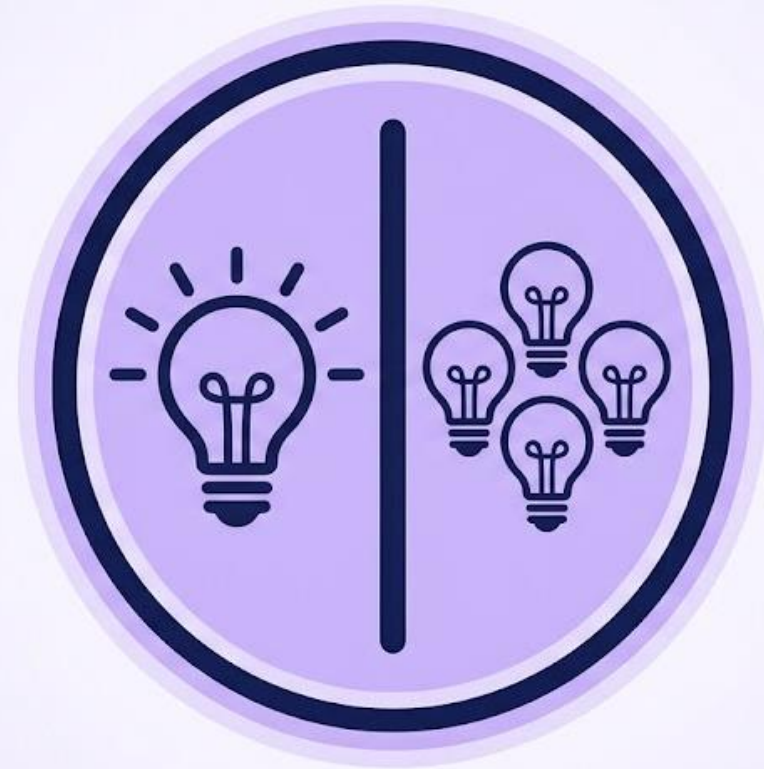
What is PQC?

- What is cryptography?
- What is PQC?

Why do we need PQC?

- What is the quantum threat?
- Are CRQC available today?
- Why act now?

- *Why to act now if Cryptographically Relevant Quantum Computers (CRQC) are not publicly available today?*
- Transition is slow
- “Harvest Now, Decrypt Later (HNDL)”



Transition is Slow

Talk

Talk

Talk

Talk

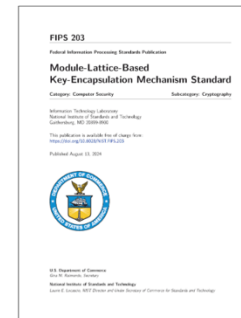
- “Algorithms must be **standardised**, **implemented** in libraries, **integrated** into protocols, **tested** in products, **certified** where necessary, and finally **deployed** ...”

[Source: <https://www.qfence-project.eu/what-is-post-quantum-cryptography-and-why-it-matters/>]

PQC Standards

In August 2024, NIST released its principal PQC standards (as Federal Information Processing Standards, or FIPS), specifying key establishment and digital signature schemes based on candidates evaluated and selected through this multi-year process.

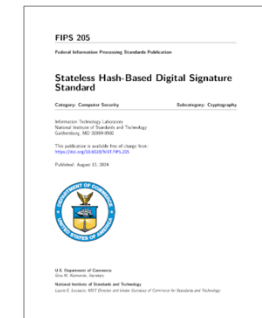
NIST PQC Standardization Timeline



FIPS 203
Module-Lattice-Based
Key-Encapsulation Mechanism Standard
(ML-KEM)



FIPS 204
Module-Lattice-Based
Digital Signature Standard
(ML-DSA)



FIPS 205
Stateless Hash-Based
Digital Signature Standard
(SLH-DSA)

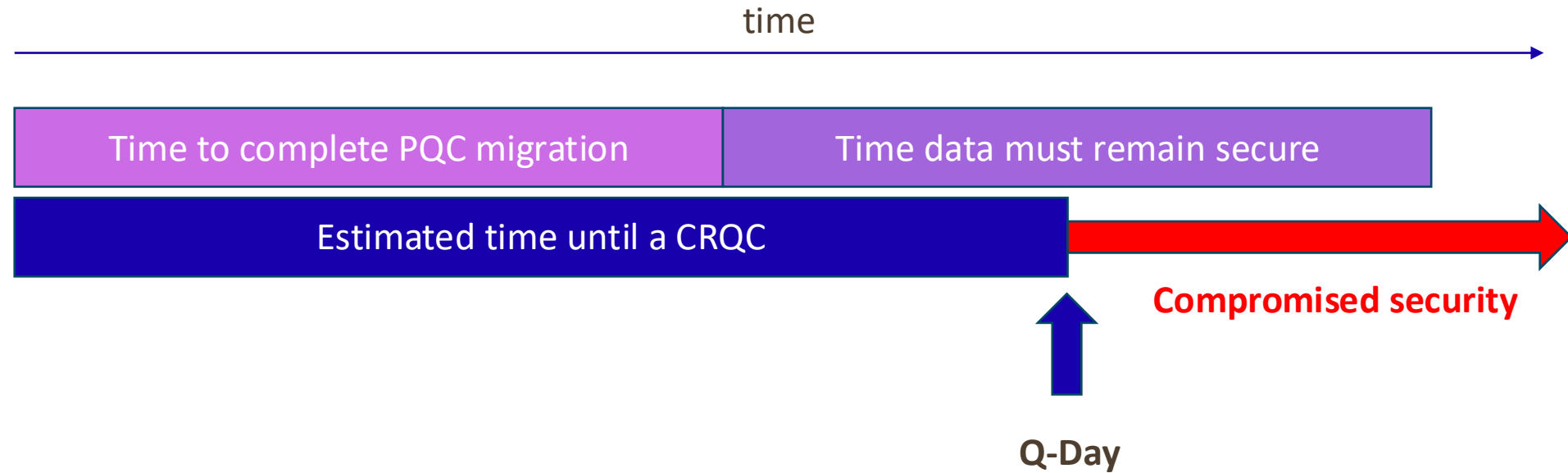
<https://csrc.nist.gov/projects/post-quantum-cryptography>

Harvest Now, Decrypt Later (HNDL)

DATA STEALERS: THE LONG GAME



<https://www.qfence-project.eu/the-quantum-time-bomb-understanding-the-harvest-now-decrypt-later-cyber-threat/>



Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready?. *IEEE Security & Privacy*, 16(5), 38-41.

What is PQC?

- What is cryptography?
- What is PQC?

Why do we need PQC?

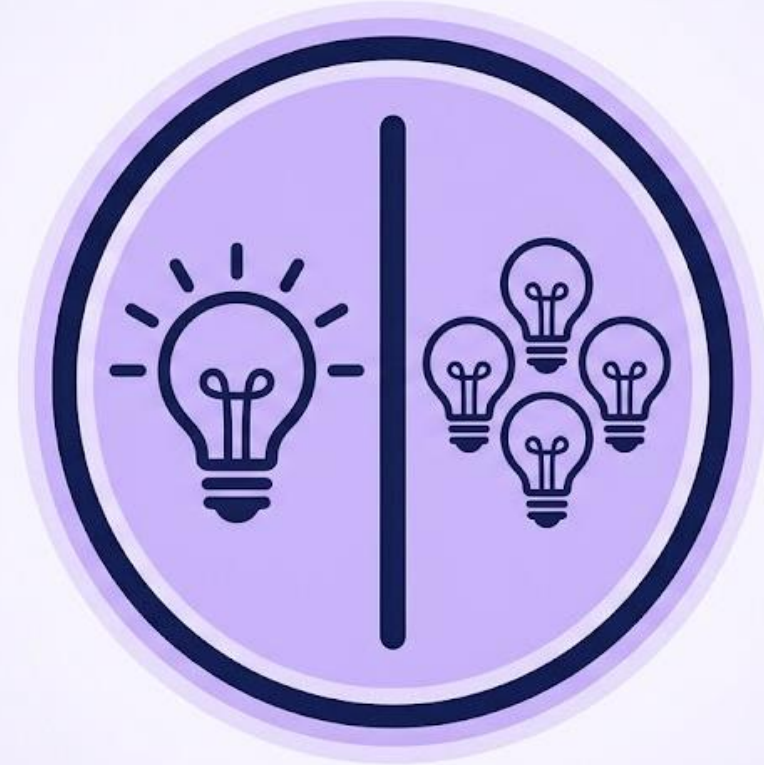
- What is the quantum threat?
- Are CRQC available today?
- Why act now?
- **Why do we need PQC?**

- “The mathematical threat of quantum computing requires a mathematical defense.”

[Source: <https://www.qfence-project.eu/the-quantum-time-bomb-understanding-the-harvest-now-decrypt-later-cyber-threat/>]

- It runs on classical systems, so PQC can be integrated into the existing systems
- **Crypto-agility:** cryptographically adapt fast, safe, cost-efficient ...
- PQC relies on mathematical problems that are considered to be resistant against quantum attacks too (lattice-based, code-based, hash-based, isogeny-based, multi-variate based)

- *Have you ever used/ worked/ experienced with PQC before? (including university projects/ assignments).*



- Test of time!
- Think of PQC as an **addition** rather than a **replacement** for previous cryptography
- System security should be as strong as **at least one of its components** (pre- and post-quantum)

Thank you!

ruxandra.olimid@fmi.unibuc.ro

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement N° 101225708, as well as the Swiss State Secretariat for Education, Research and Innovation (SERI).



Funded by
the European Union



/q-fence



@q-fence

<https://qfence-project.eu>