Post-Quantum

Cryptography Conference

# Investigating Post-Quantum Cryptography: building a PQC decision tree for developers

**Jelle Don**
Researcher at Centrum Wiskunde & Informatica (CWI)

**Alessandro Amadori**
Cryptographer at TNO

# Investigating Post-quantum Cryptography

Building a PQC Decision tree for developers

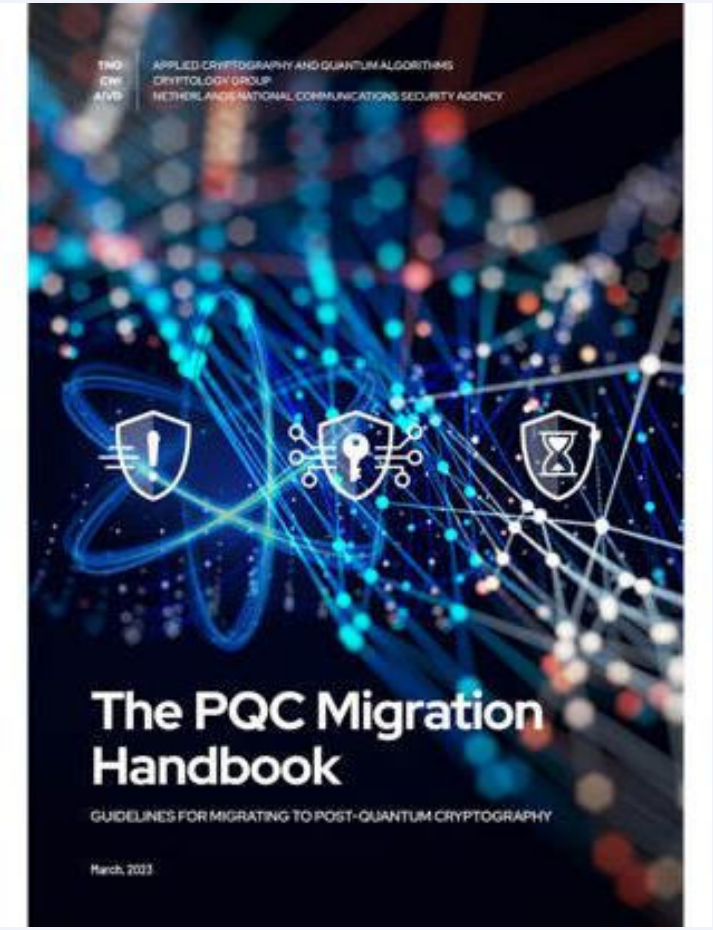
**Dr. A. Amadori, Jelle Don | PKI Consortium**

TNO innovation for life

# Previously on PQC

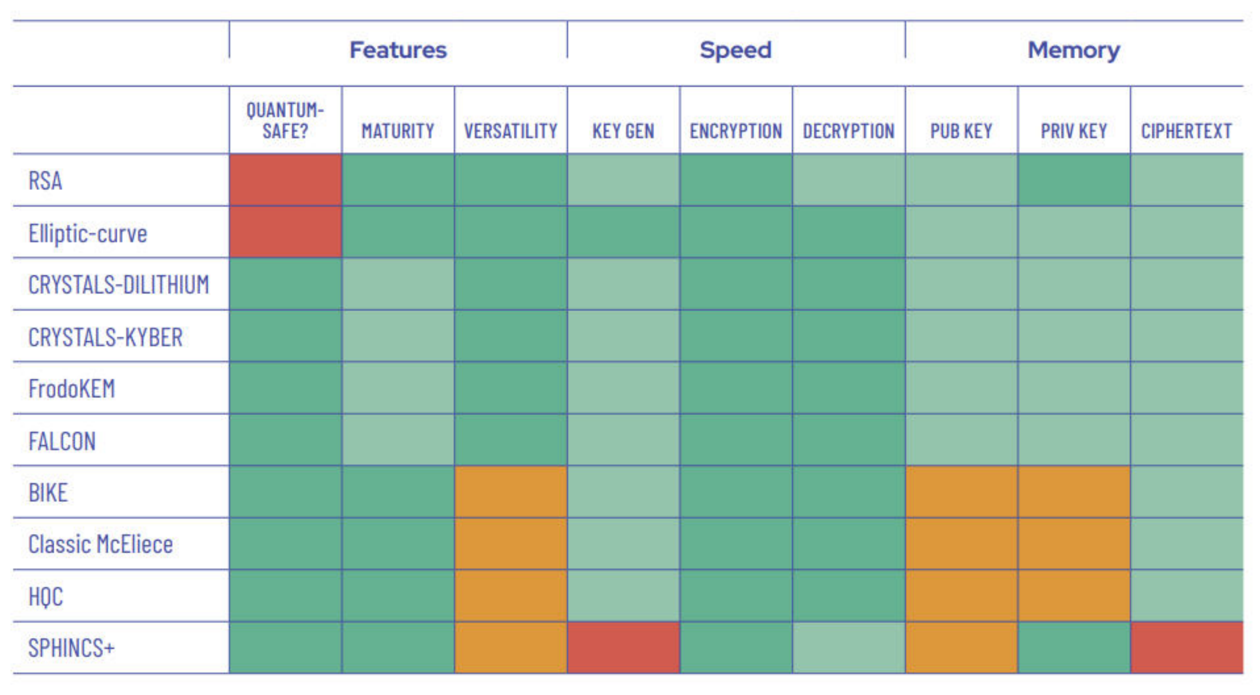
- Cryptography crucial for cyber security → omni-present
- Emergence of quantum computer
- Variety of PQC algorithms
- PQC migration handbook:
  1. Identifying vulnerable systems
  2. PQC Personas
  3. Migration planning
  4. Choosing a replacement
  5. Migration execution

In this project we aim to help companies make good, future-proof choices for replacing their traditional crypto systems with PQC



# Main Takeaways

- Guidelines for the migration: focus on personas
  - Very high-level overview on the post-quantum alternatives
  - A great start, but not very applicable



PKI Consortium

# The standards

FIPS 203 (Draft)

Federal Information Processing Standards Publication

Module-Lattice-based

Internet Research Task Force (IRTF)
Request for Comments: 8391
Category: Informational

## Post-Quantum Cryptography: Digital Signature Schemes

### Round 1 Additional Signatures

rds Publication

### PQC Fourth Round Candidate Key-Establishment Mechanisms (KEMs)

The following candidate KEM algorithms will advance to the fourth round:

| Public-Key Encryption/KEMs |
|---|
| BIKE |
| Classic McEliece |
| HQC |
| SIKE |

sed Digital
d

blication

ital Signature

FALCON WILL ALSO BE STANDARDIZED

## Specification

The current version of the FrodoKEM specification is the Preliminary Standardization Proposal submitted to ISO (2023/03/14):

# Different Recommendations

Common Criteria

Bundesamt
für Sicherheit in der
Informationstechnik

NIST

# The questions

Many alternatives, many standards, many recommendations:

- Key-Encapsulation Mechanisms
  - Kyber
  - FrodoKEM
  - Classic McEliece
  - …
- Digital Signatures
  - Dilithium
  - Falcon
  - SPHINCS+
  - XMSS
  - …

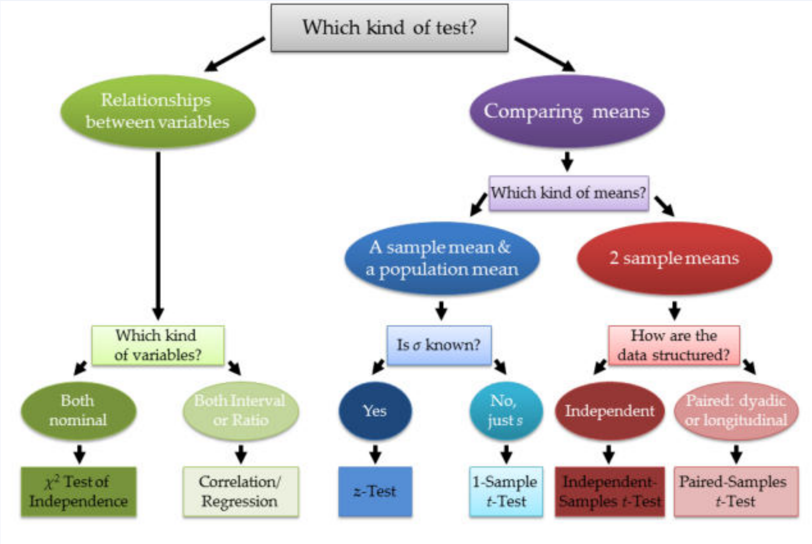
Which one to choose?

What are the differences?

# A PQC Decision Tree

THE GOAL

- To bring clarity in the realm of PQC
  - By creating characteristics matrices for KEMs and DSSs .
  - Inspecting security and implementation aspects.
- To assist in the choice of the most suitable PQC scheme for their application
  - By creating an interactive questionnaire. (Under Development)



# The TEAM

dcypher

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Ministerie van Economische Zaken en Klimaat

TNO innovation for life

CWI
Centrum Wiskunde & Informatica

NXP

Compumatica
SECURE NETWORKS

FOX IT

Technolution

# The scope

Many alternatives, many standards, many recommendations:

- Key-Encapsulation Mechanisms
    - Kyber
    - FrodoKEM
    - Classic McEliece
    - …
- Digital Signatures
    - Dilithium
    - Falcon
    - SPHINCS+
    - XMSS
    - …

Which one to choose?

# The scope

Many alternatives, many standards, many recommendations:

- Key-Encapsulation Mechanisms
  - Kyber – future NIST standard
  - FrodoKEM – future ISO standard
  - Classic McEliece – conservative and mature option

- Digital Signatures
  - Dilithium – future NIST standard
  - Falcon – future NIST standard
  - SPHINCS+ – future NIST standard
  - XMSS – already standardized, formally verified implementation exists

# The characteristics - implementation

Implementation characteristics:

- Computational complexity
- Memory usage
- Maturity
- Reference implementation

| Implementation | | | |
|---|---|---|---|
| Maturity | | Hardware Support | |
| Level of Standardisation | Reference Implementations | Integration in Existing Hardware | Hardware Accelerators |
| | | | |
| | | | |
| | | | |
| | | | |
| NIST FIPS 203 (Draft) | pqm4, Wolfssl, liboqs, PQClean, official website | ARM Cortex M53,ARM Cortex-A, ARM Cortex M4, ARM Cortex M4F, ARM Cortex M0+, FPGA , ASIC, SLE 78, AVR Microcontroller, RISC-V, | RISC-V: masked hardware accelerator (no implementation provided), Acceleration using a SLE 78 co-processor using standard RSA/ ECC accelerators, Artix 7, Xilinx UltraScale+, AVX2, ARM Cortex -A supporting an AES accelerator |
| NIST Round 4 | liboqs, Sage implementation, PQClean. pqcryptotw, official website | FPGA, ARM Cortex M4 | Xilinx Ultrascale+, AVX2 |

# The characteristics - security

Security characteristics:

- Security levels
- Validation of hardness assumption
- Reputation
  - Cryptanalysis effort
  - Security assumptions & properties
- Formal verification
- Resistance to SCA

| Reputation | | Formal Verification | SCA resistance |
|---|---|---|---|
| Security Assumptions | Security Properties | Formally Verified | Mitigations |
| | | *Under which assumptions, by which tool?* | *Are implementation SCA vulnerabilities mitigated?* |
| NTRU-SIS | XOF is SHAKE-256 only. GPV has natural proofs to sEUF-CMA security in the (q)ROM. However there is no formal proof that FALCON fits the collision resistant preimage sampleable functions definition of GPV. | Since there is no formal security argument given, a formal verification of such would require a security proof to be explicitated. | Constant time implementations exist, but FALCON's heavy use of floating points and the discrete Gaussian sampling subroutine make e.g. masking based countermeasures extremely challenging. |

# Some considerations...

On the matrix:

- Are we redoing NIST's job?
- Too technical?
- Qualitative vs. Quantitative

| KEM | Kyber | McEliece | FrodoKEM |
|---|---|---|---|
| Keygen | ++ | -- | 0 |
| Enc speed | + | 0 | - |
| Dec speed | + | 0 | - |
| PK size | ++ | - | 0 |
| SK size | ++ | + | + |
| Ciphertext size | 0 | + | - |
| Hardness assumptions | + | ++ | ++ |
| Hardware integration | ++ | 0 | + |
| Side channel attacks | - | ++ | + |

| DSS | Falcon | Dilithium | XMSS[1] | SPHINCS+ |
|---|---|---|---|---|
| Keygen | - | + | | -- |
| Signing speed | 0 | + | | -- |
| Verification speed | + | 0 | | - |
| PK size | 0 | - | ++ | ++ |
| SK size | - | 0 | | ++ |
| Signature size | + | 0 | | - |
| Hardness assumptions | 0 | 0 | 0 | + |
| Hardware integration | ++ | ++ | 0 | + |
| Side channel attacks | 0 | + | + | + |

# Some considerations...

On the decision tree:

- Which characteristics are relevant in which use-cases?
- What is the minimal set of questions to determine the user's context?
- Static tree or interactive tool?
- One recommendation or a ranking with motivation?

  - Are you required to use standardized algorithms?
    - Yes
    - No
    - I don't know

  → Kyber score + 5 (FIPS 203 Draft)
  → FrodoKem score + 2 (ISO proposal)
  → Classic McEliece + 1 (Considered for standardization in round 4)

- .... to be continued :)

# Participate with your Feedback!

Expected Release of the Decision Tree:

- February 2024
- Opensource
- Publish all artifacts

We want this resource to be usable by anyone working on future-proofing their company:

- We would love to assess its practicality and user friendliness.
- If your company is thinking of someday migrating to PQC:

## REACH OUT TO US!

Alessandro Amadori
alessandro.amadori@tno.nl

Post-Quantum

Cryptography Conference

PKI Consortium