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
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
The standards

Module-Lattice-based

Post-Quantum Cryptography: Digital Signature Schemes

Round 1 Additional Signatures

PQC Fourth Round Candidate Key-Establishment Mechanisms (KEMs)

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

<table>
<thead>
<tr>
<th>Public-Key Encryption/KEMs</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIKE</td>
</tr>
<tr>
<td>Classic McEliece</td>
</tr>
<tr>
<td>HQC</td>
</tr>
<tr>
<td>SIKF</td>
</tr>
</tbody>
</table>

Specification

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

FALCON WILL ALSO BE STANDARDIZED
Different Recommendations

Common Criteria
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 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

<table>
<thead>
<tr>
<th>Implementation</th>
<th>Maturity</th>
<th>Hardware Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level of Standardisation</td>
<td>Reference Implementations</td>
<td>Integration in Existing Hardware</td>
</tr>
<tr>
<td>NIST FIPS 203 (Draft)</td>
<td>pqm4, WolfSSL, liboqs, PQCLean, official website</td>
<td>ARM Cortex M3, 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</td>
</tr>
<tr>
<td>NIST Round 4</td>
<td>liboqs, Sage implementation, PQCLean, pqcryptobw, official website</td>
<td>FPGA, ARM Cortex M4</td>
</tr>
</tbody>
</table>
# The characteristics - security

Security characteristics:

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

<table>
<thead>
<tr>
<th>Security Assumptions</th>
<th>Security Properties</th>
<th>Formally Verified</th>
<th>Mitigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>Since there is no formal security argument given, a formal verification of such would require a security proof to be explicitated.</td>
<td>Under which assumptions, by which tool?</td>
<td>Are implementation SCA vulnerabilities mitigated?</td>
</tr>
<tr>
<td>NTRU-SIS</td>
<td>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.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Some considerations...

On the matrix:

- Are we redoing NIST's job?
- Too technical?
- Qualitative vs. Quantitative
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 → Kyber score + 5 (FIPS 203 Draft)
  - No → FrodoKem score + 2 (ISO proposal)
  - I don't know → Classic McEliece + 1 (Considered for standardization in round 4)

- .... to be continued :)

PKI Consortium
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