QUBIP

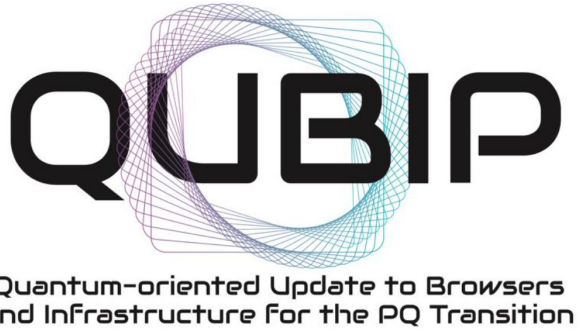
Quantum-oriented Update to Browsers and Infrastructure for the PQ Transition

POST QUANTUM NEWS

MOLTENI MARIA CHIARA | SECURITY PATTERN

QUBIP Horizon Europe

GA 101119746



- Started September 2023
- 3 years project

We are a multi-disciplinary team of experts united by a single goal, to design a reference and replicable transition process to Post-Quantum Cryptography of protocols, networks and systems

NIST PQ standards released

- August 13, 2024: first standard specifications for PQC algorithms from NIST

- **FIPS 203**: **ML-KEM** (Module-Lattice-Based)
  - Based on **CRYSTALS-Kyber**
  - https://csrc.nist.gov/pubs/fips/203/final
- **FIPS 204**: **ML-DSA** (Module-Lattice-Based)
  - Based on **CRYSTALS-Dilithium**
  - https://csrc.nist.gov/pubs/fips/204/final
- **FIPS 205**: **SLH-DSA** (Stateless Hash-based)
  - Based on **SPHINCS+**
  - https://csrc.nist.gov/pubs/fips/205/final
- **FIPS 206**, based on **FALCON**, is expected by the end of 2024

Comments addressed by the FIPS standards

- Are **test vectors** included in the standards?
  - No, but they will be available on NIST website.
- Past inconsistency with FIPS 203 and 204 interfaces with respect to the **usage of SHAKE**.
  - A new API is now used to invoke functions from the SHAKE family.
  - The SHA3 specification will be revised.
- Is **guidance for transitioning** to PQC algorithms included in the standards?
  - No, this are only technical standards. NIST will provide additional guidance separately.
- Is **guidance for side-channel** included in the standards?
  - No, it is out of scope.
- What about **hybrid algorithms**?
  - NIST will not mandate hybrid implementation of PQC algorithms.

https://www.federalregister.gov/documents/2024/08/14/2024-17956/announcing-issuance-of-federal-information-processing-standards-fips-fips-203-module-lattice-based

Comments addressed in FIPS 203

- The core algorithms within ML-KEM are difficult to test because they are non-deterministic
  - **NIST reconfigured the ML-KEM functions**
- Is guidance on the secure usage of ML-KEM or KEMs in general included?
  - No, but will be in the forthcoming SP 800-227
- Is it possible to store a **small seed string** in place of the larger keys for ML-KEM?
  - Yes. Specifications for this procedure have been added in the standard.

Comments addressed in FIPS 204

- Clarification was requested about how ML-DSA handles **messages that are pre-hashed**.
  - FIPS 204 specifies that signature should include an identifier that indicates whether the message is pre-hashed or not
- Is it possible to store a **small seed string** in place of the larger keys for ML-DSA?
  - Yes
- Can a reduced round version of SHAKE (e.g. TurboShake) be allowed for use?
  - Yes

Comments addressed in FIPS 205

- Can **additional parameter sets** be specified that have smaller signature sizes, but for which the number of signatures that can safely be generated is less than 2^64?
  - They will be published in a separate document
- Clarification was requested about how SLH-DSA handles messages that are **pre-hashed**
  - Also in this case, identifiers were added

And now?

- The National Security Memorandum (NSM-10) (2022) outlines the U.S. administration's policy to PQC
- Points about **quantum-vulnerable crypto deprecation deadlines:**
  - **Timelines for deprecation in standards** will be issued within **90** days of the release of the first set of NIST standards
  - **Timelines for deprecation in NSS** (National Security Systems) will be issued within **180** days of the release
  - The goal: no vulnerable crypto from 2035
- With NIST standards, US government agencies are allowed to commercially sell PQ cryptographic solutions

https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

Go uses hybrid KEM in TLS

- Go announced the use of quantum-safe encryption
- Go has implemented an hybrid Kyber/ECC algorithm, using the popular ciphersuite **X25519Kyber768Draft00**.
- PQC will be implemented by default in the forthcoming version Go 1.23rc2

https://sam-burns.com/posts/post-quantum-webserver/?utm_source=x

Swiss startup unveils PQC library for devs

- **Terra Quantum**: **TQ42**, an open-source C++ suite of PQ algorithms
  - Mobile, web, IoT, cloud and other applications
- Encryption, hashing, digital signatures, and secure key management
  - SHA3, AES-256, classic McEliece, Falcon, PBKDF2 and the 3 NIST winners
  - Comply with the latest NIST standards
  - Validation through the NIST Cryptographic Algorithm Validation Program (CAVP)

https://github.com/terra-quantum-public/tq42-pqc-oss

Whitehouse “Report on PQ Cryptography”

- The document describes the US national strategy to PQ transition:
  - cryptographic inventory
  - Migrating public-key crypto to PQC will require planning over multiple years
  - Interoperability
  - Systems that will not be able to support PQC must be identified as early as possible
- It estimates the government funding needed
  - **$7.1 billion**
- It summarizes the work done already, mostly by NIST

https://www.whitehouse.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf

PQC for non-cryptographers

- Blog post written by Sophie Schmieg (cryptography engineer at Google)
  - Blog post on post quantum topic, easily to be read also by non-technical people
- Many sections:
  - A part on **KEMs** and a part on **digital signatures**, with different algos (not only PQ)
    - Security levels
    - Performances
    - Hybrid solutions

https://keymaterial.net/2024/08/30/pqc-for-non-cryptographers/

QUBIP

Quantum-oriented Update to Browsers and Infrastructure for the PQ Transition

The QUBIP project (https://www.qubip.eu) is funded by the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].