QUBIP

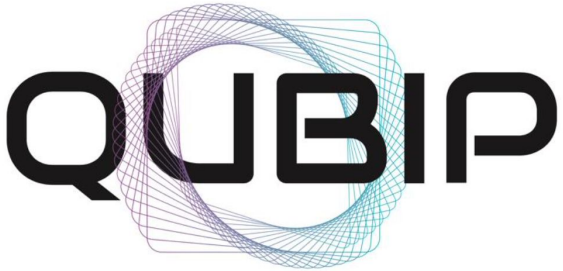
Quantum-oriented Update to Browsers and Infrastructure for the PQ Transition

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

Definition of cryptoagility

- **Cryptoagile product**
  - Updatable
    - Without physical substitution of the device
- **Cryptoagility**
  - Extra surface for updates
  - Ready to react to:
    - Recommendations
    - Standards updates

PQ Cryptography Conference

- Organized by PKI Consortium (second venue)
- November 2023 in Amsterdam

https://pkic.org/events/2023/pqc-conference-amsterdam-nl/

Takeaways (1)

PQC conference

- Stop calling it **post-quantum** cryptography
  - The **transition** from quantum-insecure to quantum-resistant cryptography is **urgent**
    - Potential risk of **store and decrypt attacks**
- Quantum Computing: start planning and preparing for now using **hybrid cryptography**

Takeaways (2)

PQC conference

- Cryptographic **inventory** and **risk analysis** for PQC readiness and agility
- **NIST's first PQC standards** are coming in early 2024
- Being **crypto-agile** is crucial and is everyone's responsibility
- **Collaboration** between global regions and industries
  - *We need to connect more, coordinate better, and share more information*

Status update from NIST

PQC conference

- **Criteria for the selection** of the algorithms:
  - Secure against attacks both in *classical* and *PQ environments*
  - *Performances* measured on various platforms
  - Others props
- First **PQ standards** (draft):
  - FIPS 203, ML-KEM (KYBER)
  - FIPS 204, ML-DSA (DILITHIUM)
  - FIPS 205, SLH-DSA (SPHINCS+)
  - FN-DSA (FALCON) - under development
- First standards probably will be ready in April 2024

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

PQ challenges in embedded applications

PQC conference

- **Key sizes, performances and memory usage**
  - Possibility of trade-off between performances and memory
- **Side-channel protection**
  - The **Fujisaki-Okamoto transform**
    - Increasing of the surface for side-channel and fault-injection attacks
    - Protection against these attacks causes a significant impact on performance and memory usage

https://www.youtube.com/watch?v=ffBickBkvAk

German BSI: PQ migration

PQC conference

- 15 years to migrate their public key infrastructure to quantum-safe algorithms
- Their **first production-ready PQC** root CA will enter in service in **2027**
- Choices of **algorithms**:
  - SLH-DSA, for security over simplicity
  - No complete faith in lattices-based algorithms

French ANSSI: PQ migration

- ANSSI has a role of **advisory** and **regulatory**
  - It **promotes** the use of state-of-the-art cryptographic algorithms
- ANSSI introduces a *provisional transition agenda* to prevent quantum threat
  - Provides **directions** to industrials developing security products
- No complete replacement of currently used algorithms in the short/medium term
  - **Smooth transition** with **hybrid mechanism**

https://cyber.gouv.fr/en/publications/anssi-views-post-quantum-cryptography-transition

QUBIP

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

Thank for the attention

https://qubip.eu/