QUBIP

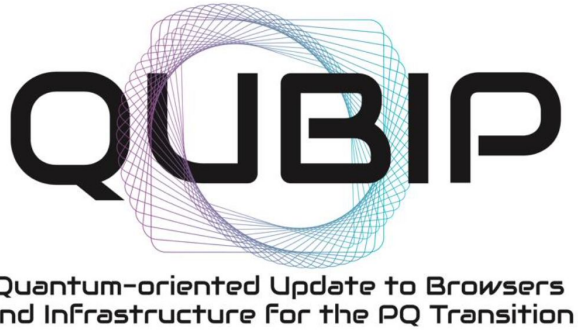
Quantum-oriented Update to Browsers and Infrastructure for the PQ Transition

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

10th ETSI-IQC QSC Conference

- Executive track
  - Focus on standardization efforts
  - Prepare for known quantum attacks but also for future advances
    1. **Cryptographic Inventory** (CBOM)
    1. **Quantum Risk Assessment** (QRA)
    2. **Crypto defense-In-Depth**
    3. **Cryptoagility**
- Technical track
  - Advances in PQC
  - Quantum Key Distribution (QKD) deployment issues
  - Quantum Cloud systems

https://www.etsi.org/events/2284-10th-etsi-iqc-quantum-safe-cryptography-event

NOSTRADAMUS project

- EU project
- Consortium responsible for building EU's quantum communications testing infrastructure
  - Partners: Thales and the AIT Austrian Institute of Technology
- Main goals:
  - Describe the **blueprint for a Testing & Validation Infrastructure**
  - Implement and operate a **prototypical testbed facility**

https://www.thalesgroup.com/en/worldwide/space/press_release/eu-launches-nostradamus-and-prepares-europe-quantum-world

Presented during the ETSI conference

EPOQUE project

- EPOQUE: Engineering post-quantum cryptography
- EU-funded project
  - From October 2018 to December 2023
- Focus on the engineering challenges of post-quantum cryptography
- Coordinated by STICHTING RADBOUD UNIVERSITEIT

https://cordis.europa.eu/project/id/805031

Takeaways from NIST's PQC Standardization Conference

- Fifth venue, on April in Rockville (Maryland)
- Main **objectives**:
  - Discuss various aspects and updates of the algorithms
  - Feedback/decisions on standardization
- Recent challenges for the algorithms in the **additional signature competition**:
  - BIKE: attack to this algo, non practical
  - Classic McEliece
  - FALCON: initial draft in the fall of 2024
    - They introduced ANTRAG
  - HQC: new security proofs
- There are some changes in **standards FIPS 203 and 204**

Takeaways from NIST's PQC Standardization Conference

- **Side-channels** topic came up several times
- Transition prep, key activities for the transition:
  - PKI objects
  - Data formats and technological constraints
  - Available open-source tools
- About SLH-DSA:
  - Research exploring parameter sets for specific use cases
  - Accelerate SLH-DSA by two orders of magnitude, but only for hardware
- **PQC will be here before we know it, and there's still a lot of preparation that needs to be done**

https://www.keyfactor.com/blog/top-takeaways-from-nists-fifth-pqc-standardization-conference/

PQC seminars by NIST

- Talks hosted by the NIST PQC team
  - Open to the public
  - Related to the NIST PQC standardization process
- For all the talks: slides and the video of the presentation

https://csrc.nist.gov/projects/post-quantum-cryptography/workshops-and-timeline/pqc-seminars

Zoom adopts PQ end-to-end encryption

- Zoom implements E2EE
- The PQ E2EE version uses Kyber 768 for encryption, available for version 6.0.10 or higher

https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0065408

QSNS2024 workshop

- In Paris, 26th June, co-located with the 29th IEEE Symposium on Computers and Communications
- Initiative of the **QUBIP** and **PQ-React** projects
- Topic: the transition to Post-Quantum Cryptography (PQC) of protocols, networks, and systems
  - **Cybersecurity challenges** of the quantum era
  - Aim of contributing to global efforts towards transition to PQC of the digital infrastructures

https://qubip.eu/qsns2024/

SPQR cluster

- **SPQR (Secure Post-Quantum eRa)** cluster
  - PQ-REACT and QUBIP Horizon EU projects
  - On April 2024
- Aim: help the transition to the PQC era
- Cluster roadmap and objectives:
  - Joint research activities
  - Joint publications
  - Feedback provision on pilot use cases
  - Co-organization of events
  - Joint communication campaigns

https://pqreact.eu/spqr-cluster-securing-eus-transition-towards-post-quantum-cryptography/

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].