QUBIP

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

# POST QUANTUM NEWS

Updates

MOLTENI MARIA CHIARA | SECURITY PATTERN

The QUBIP project is funded by the European Union
under the Horizon Europe framework programme
[Grant Agreement No. 101119746]

# QUBIP Horizon Europe

GA 101119746

QUBIP

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

- 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*

CSIC
Consejo Superior de Investigaciones Científicas

SECURITY PATTERN

Tampere University

Red Hat

Fondazione Links
Passion for Innovation

Telefónica
Telefónica Investigación y Desarrollo

Politecnico di Torino
1859

SMART FACTORY

CIBER VOLUNTARIOS.org

POLITÉCNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

# New standards

# NIST IR 8545

- **Status Report** on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process
  - Published in March 2025
- Four candidate algorithms for **key establishment**
  - BIKE, Classic McEliece, HQC, and SIKE
- The only key-establishment algorithm that will be standardized is **HQC**
- https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8545.pdf

# Agreed Cryptographic Mechanisms v 2.0

- **ECCG**, with the support of **ENISA**, has released version 2.0 of its **Agreed Cryptographic Mechanisms**
  - April 2025
- **Aim:** to ensure **consistency** and **security** across European cybersecurity certification schemes
- **Highlights**:
  - Approved PQC schemes in agreed mechanisms
  - *Hybridization is the key*
  - Symmetric and hash parameters upgraded
- **Deadlines**:
  - RSA with modulus < 3000 bits – Acceptable until 31 December 2025

# Side-channel attacks on PQC

# Side-Channel Attacks On Post-Quantum Cryptography

- **Main form of side-channel attack**: recovering information by observing side-channel information while a secret value is processed.
- **Belief propagation:** Side-channel information are accumulated
  - Useful in side-channel attacks on post-quantum cryptography
- The Fujisaki-Okamoto-style (FO) transforms used in ML-KEM and HQC are especially vulnerable to **chosen-ciphertext side-channel attacks** during the phase of re-encryption
- https://semiengineering.com/side-channel-attacks-on-post-quantum-cryptography/

# Side channel attack on Kyber

- Swedish researchers: **novel side channel attack** which can break a particular implementation of CRYSTALS-Kyber
  - **Deep learning** side channel attack
  - The presented approach is not specific for CRYSTALS-Kyber and can potentially be applied to other LWE/LWR PKE/KEM schemes
- https://eprint.iacr.org/2022/1713.pdf

# SHIFT SNARE: Uncovering Secret Keys in FALCON via Single-Trace Analysis

- Paper on arXiv from April
- They target the discrete Gaussian sampling operation within **FALCON's key generation scheme**
  - A single power trace is sufficient to mount a successful attack
  - There is a leak which enables full recovery of the secret key
- https://arxiv.org/pdf/2504.00320

# Post-Quantum Side-Channel Attack Resilience

- New European project
  - Start date: 1 May 2025
  - End date: 31 October 2026
- The project addresses the need for resilient **post-quantum** cryptographic solutions, focusing on developing and validating algorithms that are **resistant to side-channel attacks**
- Aim of the project: to create a **robust framework** for evaluating the resilience of cryptographic algorithms against quantum and side-channel attacks
- https://cordis.europa.eu/project/id/101189247

# Other News

# Majorana 1 from Microsoft

- Majorana 1 is a **hardware device** developed by **Microsoft**
  - Announced by Microsoft in February 2025
- Features:
  - It is a device that admits superconductivity at low temperatures
  - It can fit eight qubits
- Progress in Microsoft's long-running project to create a *quantum computer based on topological qubits*

# VTT and IQM 50-qubit quantum computer

- VTT and IQM launched the **first 50-qubit quantum computer** developed in Europe
  - The 50-qubit quantum computer is located at VTT’s premises in Micronova in Espoo, Finland
  - The 50-qubit quantum computer is available for companies and researchers through the VTT quantum computing service
- https://www.vttresearch.com/en/news-and-ideas/vtt-and-iqm-launch-first-50-qubit-quantum-computer-developed-europe

# Google adds quantum-safe digital signatures in Cloud KMS

- In February Google announced **quantum-safe digital signatures in Cloud KMS** for software-based keys
- Google's **approach** to quantum-safety includes:
  - Software and hardware support for standardized quantum-safe algorithms;
  - Supporting migration paths;
  - Analyzing the security and performance of PQC algorithms and implementations.
- **Roadmap**: NIST post-quantum cryptography standards in both software (Cloud KMS) and hardware (Cloud HSM)

QUBIP

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

# CONTACTS

**Molteni Maria Chiara**

**Security Pattern**

m.molteni@securitypattern.com

https://qubip.eu

The QUBIP project is funded by the European Union
under the Horizon Europe framework programme
[Grant Agreement No. 101119746]