



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

# POST QUANTUM NEWS

Updates

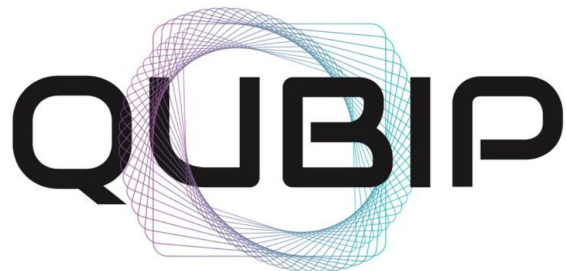
MOLTENI MARIA CHIARA | SECURITY PATTERN



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

# QUBIP Horizon Europe

GA 101119746



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

*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*

- Started September 2023
- 3 years project



# Quantum research



# Quantinuum launched Helios Quantum Computer

- **Quantinuum** is a world leader in quantum computing
- Helios: **accurate general-purpose commercial quantum computer**
  - Acceleration of quantum computing adoption by enterprises
- Improvements:
  - Helios enables developers to program a quantum computer in much the same way they program heterogeneous classical computer (modern Python-based programming language)
  - Helios unlocks the ability to **enhance GenAI** (Generative Quantum AI) **models** with quantum generated data
- <https://www.quantinuum.com/press-releases/quantinuum-announces-commercial-launch-of-new-helios-quantum-computer-that-offers-unprecedented-accuracy-to-enable-generative-quantum-ai-genqai#>

# Ocelot from Amazon

- Ocelot: new quantum computing chip from Amazon Web Services (AWS)
- Improvement: Ocelot can reduce the costs of implementing quantum error correction by up to 90%, compared to current approaches
  - Novel design building error correction in from the ground up and using the 'cat qubit'
- <https://www.aboutamazon.com/news/aws/quantum-computing-aws-ocelot-chip>

# Celtech record

- Caltech researchers announced that they were able to split a **laser beam** into 12 000 parts in order to trap 6 100 cesium atoms.
- These qubits stayed in superposition for 13 seconds, ten times longer than previous arrays.
- More **efficient error correction** and neutral atom approach to quantum computers.
- <https://www.caltech.edu/about/news/caltech-team-sets-record-with-6100-qubit-array>

# Quantum-Safe 360 Alliance

- IBM, Thales, Keyfactor, and Quantinuum
- Goal: help businesses to be prepared for quantum threats
- The alliance launched a new whitepaper that outlines:
  - The **key risks**
  - A set of **recommendations** to follow
- Focus: cryptographic agility, secure key management, and upgrading infrastructure in anticipation of post-quantum adoption
- [https://www.itpro.com/technology/what-quantum-safe-360-alliance-means-for-your-business-post-quantum-security?utm\\_source=chatgpt.com](https://www.itpro.com/technology/what-quantum-safe-360-alliance-means-for-your-business-post-quantum-security?utm_source=chatgpt.com)

# Applications





# Commercial applications of quantum computers

- September: **HSBC** improved their bond trading predictions by 34% compared to classical computing alone, using *IBM's Heron quantum computer*
  - <https://www.hsbc.com/news-and-views/news/media-releases/2025/hsbc-demonstrates-worlds-first-known-quantum-enabled-algorithmic-trading-with-ibm>
- March: **Ansys** used *IonQ's quantum computer* to speed up its analysis of fluid interactions in medical devices by 12% compared to classical computing alone
  - <https://ionq.com/news/ionq-and-ansys-achieve-major-quantum-computing-milestone-demonstrating>
- March: **Ford Otosan** used *D-Wave's quantum annealing technology* to reduce scheduling times from 30 minutes to less than five
  - <https://www.dwavequantum.com/company/newsroom/press-release/beyond-classical-d-wave-first-to-demonstrate-quantum-supremacy-on-useful-real-world-problem/>

# SSLBoard: Scanning PQ support server-side

- SSLBoard mission: bringing visibility, trust, and control to SSL/TLS certificates at scale
- Now the tool is able to **scan PQ support server-side of a domain and its subdomains**
- <https://sslboard.com/>

# ExpressVPN Adds Post-Quantum Encryption to WireGuard

- Paid VPN service which supports the WireGuard protocol to promote the industry's **post-quantum transition**
  - Integration of ML-KEM algorithm into its WireGuard support
- Example of post-quantum technology being rolled out in consumer tools
- [https://www.techradar.com/vpn/vpn-privacy-security/expressvpn-finally-supports-wireguard-but-adds-post-quantum-security?utm\\_source=chatgpt.com](https://www.techradar.com/vpn/vpn-privacy-security/expressvpn-finally-supports-wireguard-but-adds-post-quantum-security?utm_source=chatgpt.com)



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

# CONTACTS

**Molteni Maria Chiara**

**Security Pattern**

[m.molteni@securitypattern.com](mailto: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]