QUBIP Horizon Europe

GA 101119746
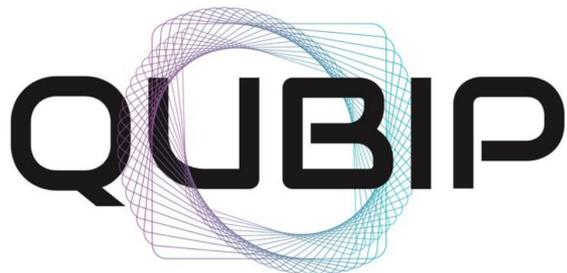
Quantum-oriented Update to Browsers
and Infrastructure for the PQ Transition

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

End of 2025

Quantinuum launched Helios Quantum Computer

- **Quantinuum:** a world leader in quantum computing

- Helios: the world's **most accurate general-purpose commercial quantum computer**,
    - Announced in November 2025
    - Designed to accelerate quantum computing adoption by enterprises

- Advantage: program a quantum computer similarly as a heterogeneous classical computer
    - Modern Python-based programming language

- Ability to **enhance GenAI** (Generative Quantum AI) **models** with quantum generated data
    - Data analysis, material design, and quantum chemistry

- 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#

QUBIP

Ocelot from Amazon

- **Ocelot** from Amazon Web Services (AWS)

- New quantum computing chip that can reduce the costs of implementing quantum error correction by up to 90%, compared to current approaches

    - Announced in February 2025

    - 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

Commercial applications of quantum computers

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

Caltech record

- **Caltech** (California Institute of Technology) researchers: they split a laser beam into 12 000 parts in order to trap 6 100 cesium atoms
  - September 2025
- These qubits stayed in superposition for 13 seconds and were even able to move the atoms round
- Results: more efficient error correction and key benefit of this neutral atom approach

- https://www.caltech.edu/about/news/caltech-team-sets-record-with-6100-qubit-array

Quantum-Safe 360 Alliance

- Alliance formed by IBM, Thales, Keyfactor, and Quantinuum

  - Summer 2025

- Goal: help businesses prepare for quantum threats

- New whitepaper that outlines the **key risks** and includes a set of **recommendations** to follow

- It focuses on 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

SSLBoard: Scanning PQ support server-side

- SSLBoard is an online tool

- 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/
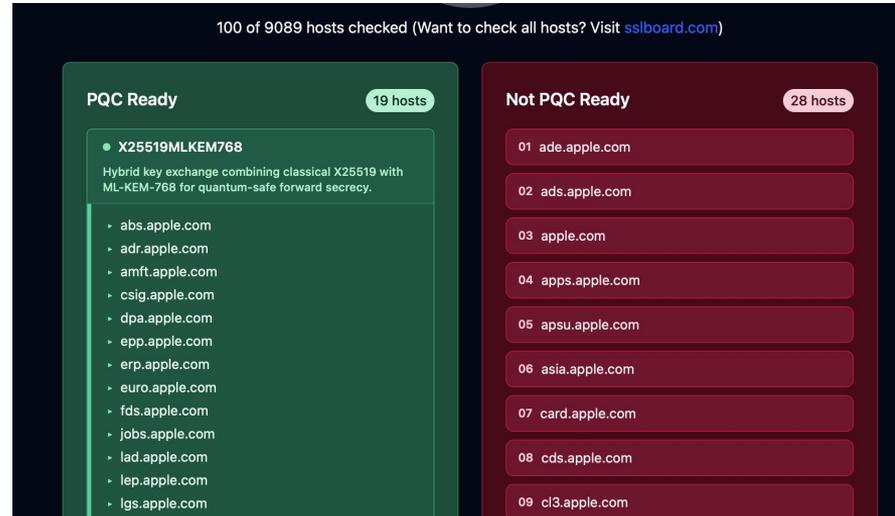
Beginning of 2026

Commercial applications of quantum computers

- **Oracle Cloud Infrastructure** and **American Binary**: announced a post-quantum encrypted VPN solution (*Ambit Client*) available on Oracle's cloud marketplace
  - Secure defense and enterprise infrastructure against quantum threats
  - https://blogs.oracle.com/cloud-infrastructure/oracle-american-binary-post-quantum-solutions
- **Orange Business** and **Cisco**: announced post-quantum cryptography (PQC) secured WAN services, offering quantum-safe networking on a global scale
  - https://thequantuminsider.com/2026/02/10/orange-business-cisco-pqc-secured-network-services/
- **eMudhra Limited:** expanded its PQC advisory services to help enterprises transition to quantum-secure cryptography
  - https://scanx.trade/stock-market-news/stocks/emudhra-limited-expands-post-quantum-cryptography-advisory-services-for-global-enterprises/33387747

Post-Quantum Cryptography report

- Industry research report
    - Published in January 2026
    - 43 pages
- Main topic: **post-quantum cryptography is shifting from research to real production deployments**
    - It is not just a theoretical work anymore
- <u>Key highlights</u>
    - This is the moment for the adoption of post-quantum solutions
    - Post-quantum cryptography is moving beyond laboratory validation and proof-of-concept trials
    - Design post-quantum cryptography *migration strategies*, *prioritize high-risk systems* and long-lifecycle assets, and *align security architectures* with evolving standards and regulatory expectations
- [Post-Quantum Cryptography Industry Research Report 2026: PQC Transitions from Research Concept to Core Cybersecurity Pillar Amid Rising Quantum Computing Breakthroughs](#)
- [Post-Quantum Cryptography](#)

Implementation of Quantum Safe Ecosystem in India

- Report published in February 2026

- India is preparing to defend its digital infrastructure against the threat of quantum computing

- **National task force** outlining a roadmap to achieve post-quantum security by 2028

- The report details a **phased approach**

  - Phases:

    - 2028: Short-Term PQC/Hybrid Solution Pilots

    - 2030: Medium-Term PQC Migration

    - Long-Term PQC Default & Rating Framework

- https://quantumzeitgeist.com/post-quantum-security-quantum-computing-quantum-security/

Academic and technical progress

- *Adaptive Quantum-Safe Cryptography for 6G Vehicular Networks via Context-Aware Optimization*

  - https://arxiv.org/abs/2602.01342

- *PQC standards alternatives -- reliable semantically secure key encapsulation mechanism and digital signature protocols using the rank-deficient matrix power function*

  - https://arxiv.org/abs/2601.00332

- *Toward Quantum-Safe Software Engineering: A Vision for Post-Quantum Cryptography Migration*

  - https://arxiv.org/abs/2602.05759

Upcoming events and standardization

- Next events - progress in standards, deployments, and real-world PQC cases
  - https://pqca.org/
- **Eurocrypt 2026**
  - Rome, Italy, on 10-14 May 2026
  - https://pqca.org/event/eurocrypt-2026/
- Workshop on Quantum-Secure Networks and Systems (**QSNS 2026**)
  - On June 23-26 2026, Vilamoura, Algarve, Portugal
  - https://qubip.eu/qsns2026/

QSNS 2026

3rd Workshop on Quantum-Secure Networks and Systems

QUBIP   pq·react   PQ-NEXT   POSEIDON   QARC   Q-FENCE