QUBIP

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

POST QUANTUM NEWS

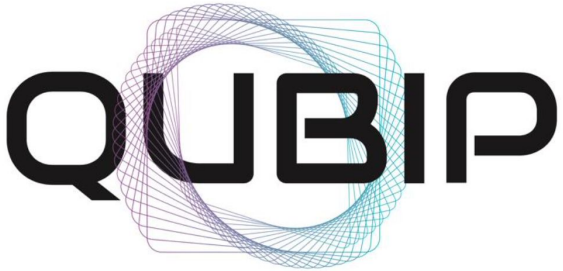
Updates

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



- 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

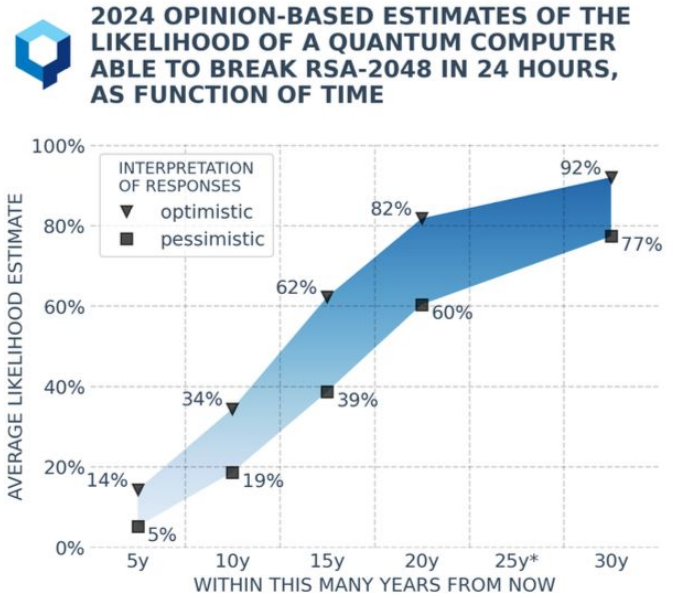
Overview

- How did 2024 Post Quantum research go?
  - Quantum threat timeline report 2024
  - IBM quantum roadmap from 2024 on
  - BSI study on quantum computer development
- New standard drafts
  - NIST SP 800-227
  - NIST IR 8547
- Other news
  - Accenture and QuSecure
  - QSNS workshop

How did 2024 Post Quantum research go?

Quantum Threat Timeline Report 2024

- Report by Global Risk Institute and evolutionQ
- The **quantum threat** may be closer than previously thought. In 2024:
  - Major advances in Quantum Error Correction (QEC)
  - Architectures other then superconducting systems show potential
  - New quantum leaders
  - New NIST's PQC standards published
- **Takeaways**:
  - Proactive quantum threat mitigation
  - Well-planned quantum-safe transition



https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/

IBM Quantum Roadmap from 2024 on

2024	2025	2026	2027	2029	2033+
Expand the utility of quantum computing	Demonstrate quantum-centric supercomputing	Automate and increase the depth of quantum circuits	Scale quantum computing	Deliver a fully error-corrected system	Deliver quantum-centric supercomputers with 1000's of logical qubits

- In 2025, IBM will demonstrate the **first quantum-centric supercomputer.**
- They will also enhance the quality, execution, speed, and parallelization of **quantum circuits**.
    - They will make **quantum computing easier to use** by abstracting quantum circuits into quantum functions and Qiskit patterns

https://www.ibm.com/roadmaps/quantum/

BSI Study on Quantum Computer Development

- Current state of affairs in the **theoretical aspects and physical implementation** of quantum computing
- **Takeaways**:
  - Quantum algorithms:
    - Shor's and Regev's algorithms are promising but are not yet efficient
    - New heuristic algorithms lack proofs of convergence
  - Quantum computers:
    - *Fault-tolerant quantum computers*: high performance, significant overhead
    - *NISQ (Noisy Intermediate-Scale Quantum)*: systems effective for small problems, unlikely to achieve cryptanalytic quantum advantage
- **Challenges**:
  - Diverse hardware platforms face unique scaling and performance issues
  - Secrecy in research and competition complicates predictions

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungstand_QC_V_2_1.html

New standard drafts

NIST SP 800-227

- NIST has introduced SP 800-227, “**Recommendations for Key-Encapsulation Mechanisms**”, to provide guidelines for their secure implementation
  - Published on Jan. 7th, public comments period will end on March 7th
  - The recommendations apply to all KEMs
- Conditions to use KEM securely:
  - The selected **KEM** is approved
  - The **devices** used to execute KEM algorithms are secured
  - The key-establishment process satisfies an application-appropriate notion of integrity
  - The **shared secret key** produced by the KEM is used in a secure way

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-227.ipd.pdf

NIST IR 8547

- NIST has published NIST IR 8547: "**Transition to Post-Quantum Cryptography Standards**" to describe the expected approach for the transition
  - Published on Nov. 12th, public comments period was closed on Jan. 10th
- Transition plan
- Traditional algorithms deprecation and disallowment dates

https://csrc.nist.gov/pubs/ir/8547/ipd

Digital signature algorithm family	Parameters	Transition
ECDSA [FIPS 186]	112 bits of security strength	Deprecated after 2030 Disallowed after 2035
	>= 128 bits of security strength	Disallowed after 2035
EdDSA [FIPS 186]	>= 128 bits of security strength	Disallowed after 2035
RSA [FIPS 186]	112 bits of security strength	Deprecated after 2030 Disallowed after 2035
	>= 128 bits of security strength	Disallowed after 2035

Digital signature algorithm family	Parameters	Transition
FInite Field DH and MQV [SP80056A]	112 bits of security strength	Deprecated after 2030 Disallowed after 2035
	>= 128 bits of security strength	Disallowed after 2035
Elliptic Curve DH and MQC [SP80056A]	112 bits of security strength	Deprecated after 2030 Disallowed after 2035
	>= 128 bits of security strength	Disallowed after 2035
RSA [SP80056B]	112 bits of security strength	Deprecated after 2030 Disallowed after 2035
	>= 128 bits of security strength	Disallowed after 2035

Other News

QSNS

2nd Workshop on Quantum-Secure Networks and Systems

- Second edition
  - First edition has been a success!
- Joint initiative of the **QUBIP** and **PQ-React** projects
- Co-located with the 30th IEEE Symposium on Computers and Communications, July 2-5, 2025, Bologna, Italy
- **Topic**: cybersecurity challenges of the quantum era from an engineering perspective
- Workshop Paper Submission: February 10th, 2025

https://qubip.eu/qsns2025/

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]