

Post Quantum Cryptography and the Internet of Things

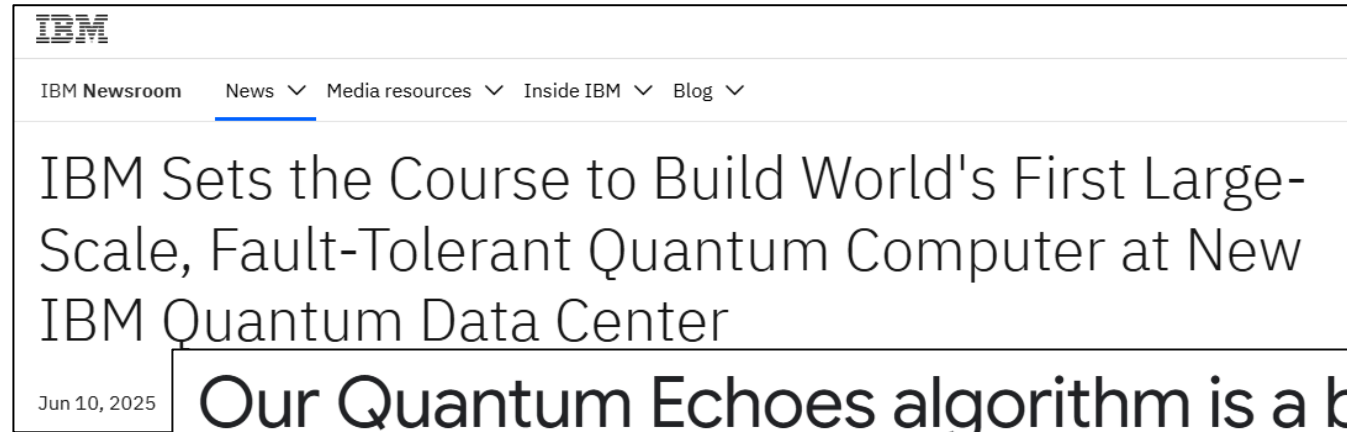
Lory Thorpe

IBM Research

Chair GSMA Post Quantum Telco Network Task Force

The Quantum Threat

- Quantum computing is both a revolutionary opportunity and a fundamental threat
- A sufficiently powerful quantum computer will be able to compromise the public key cryptography that currently underpins digital security

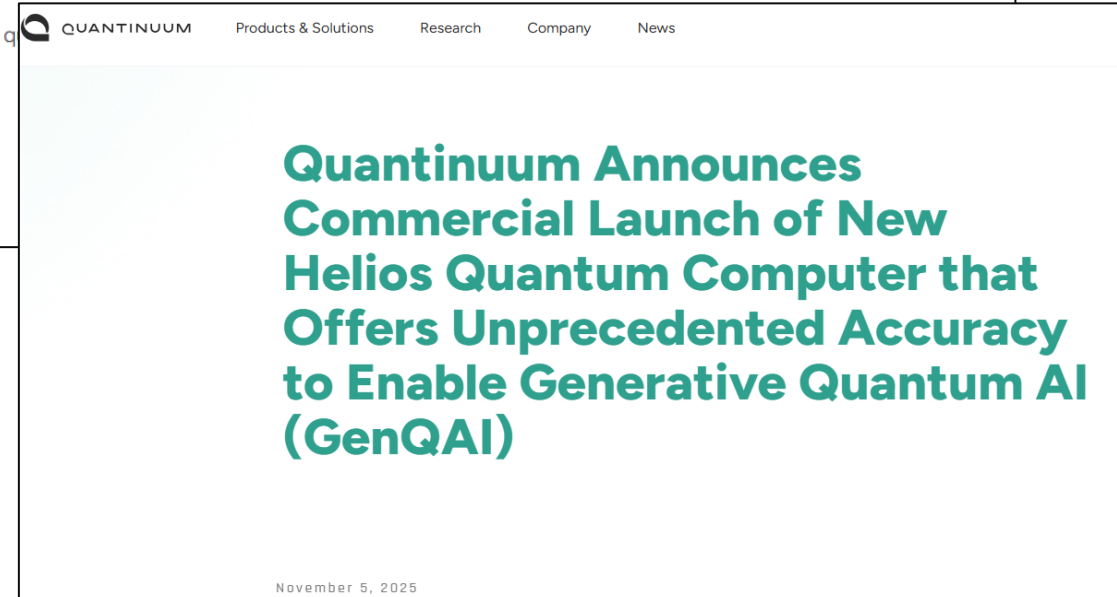


Our Quantum Echoes algorithm is a big step toward real-world applications for quantum computing

Oct 22, 2025
5 min read

Our Willow q hardware.

 **Hartmut Neven**
Founder and Lead,
Google Quantum AI



Security in the quantum era

Post Quantum Cryptography

Next generation cryptography algorithms, resistant to classical and quantum attacks

PQC standardization process (first set of NIST algorithms standardized in August 24)

Runs on classical computers!

Migration-PQC implementation

The migration to Quantum-safe affects:

- Cryptographic protocols, such as TLS and IPSec
- Software development and code
- Vendor products
- Software as a service
- Infrastructure, network, devices, etc.

and requires new capabilities such as cryptographic discovery & cryptographic agility



ML-KEM: Primary algorithm for Key encapsulation (to be used for key exchange)



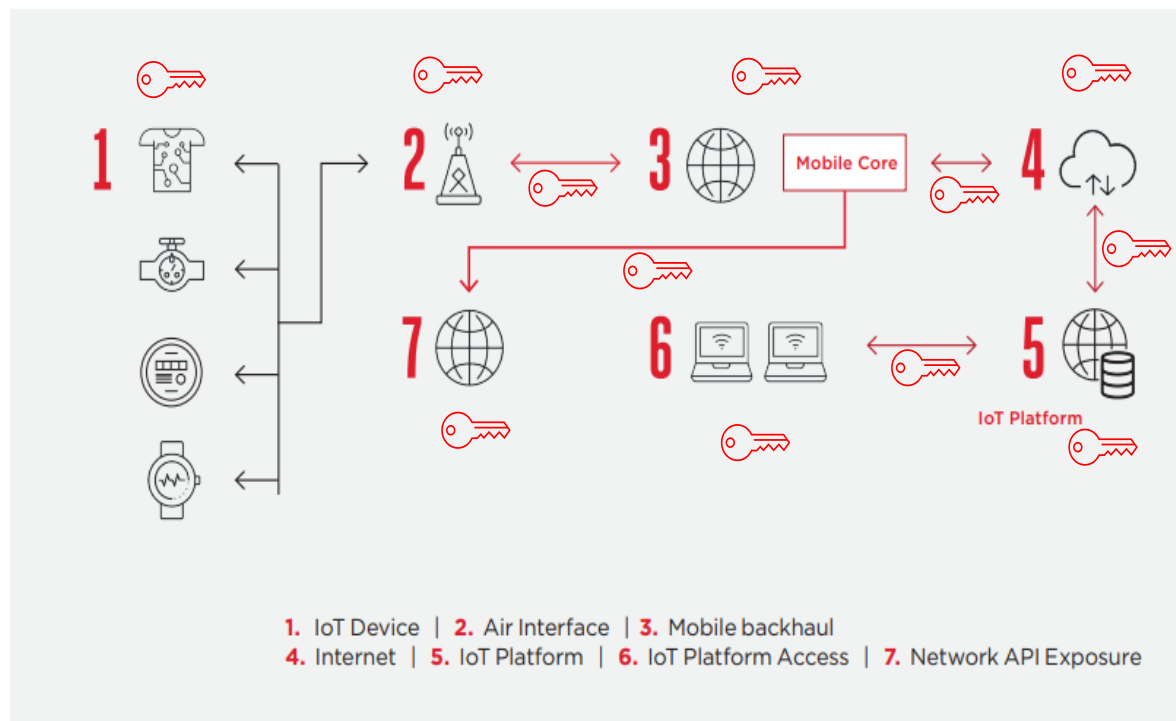
ML-DSA: Primary algorithm for digital signatures



SLH-DSA: Stateless hash-based algorithm for digital signatures

[NIST Releases First 3 Finalized Post-Quantum Encryption Standards | NIST](#)

What does this mean for IoT?



Harvest and access data, eavesdropping

Harvest and decrypt of stored data through compromise of secure communication protocols (man in the middle attacks)

Unauthorised device access and manipulation

Compromise data integrity, ability to alter the behaviour of the IoT device

Malware/ransomware/spyware attacks

Remote access of systems to exfiltrate information (for example, device location) through fraudulent authentication

Use the device as computation power (zombie device)

Malicious/invasive SW is installed, allowing attackers to take control of the IoT device authentication

Device spoofing

Add fraudulent devices to the IoT solution that disguises as a legitimate device

Access to adjacent systems connected to the IoT solution

Use the IoT solution as a gateway to infiltrate/compromise adjacent systems, including the network. Trigger malicious actions (i.e. door unlock)

Fraud and anomaly detection compromise

Undermine the effectiveness of anomaly or fraud detection to delay, subvert detection

Public key cryptography plays a critical role in maintaining the confidentiality, integrity and authenticity of IoT solutions.

Quantum Threats for IoT- What will a cybercriminal do?

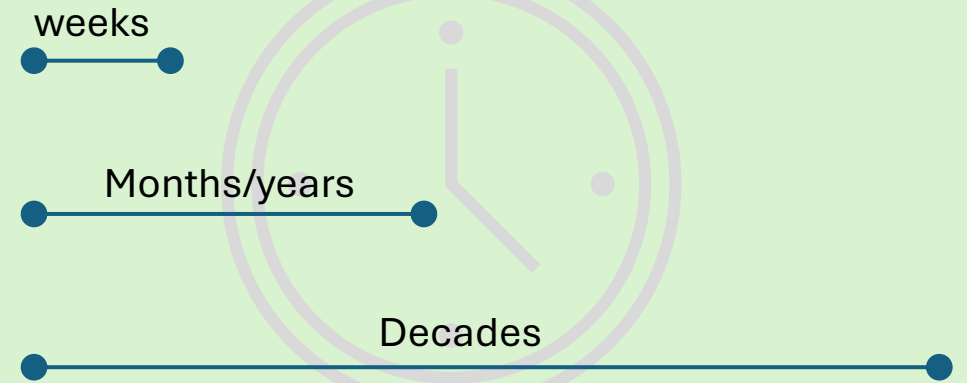
Widescale IoT adoption acceleration across industry, often involving sensitive data and critical systems, make IoT a valuable target for cybercriminals

PQC implementation in IoT-challenges and opportunities

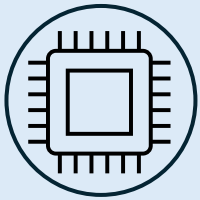
Sectors



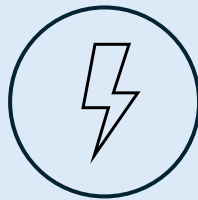
Device/Solution Lifecycle



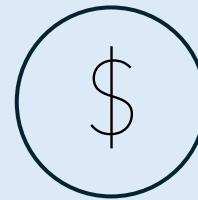
Resource Constraints



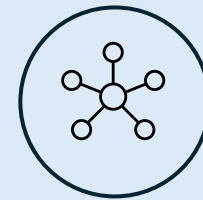
Memory and
processing power



Power supply



Cost



Connectivity

Recommendations

Pro-active preparation is essential for integrating post-quantum cryptography (PQC) into IoT systems to mitigate future security risks and reduce costs.



Post Quantum Cryptography in IoT



Collaboration between GSMA Post Quantum Telco Network Task Force and the 5G IoT Strategy Work Group, published in March 2025 ([PQ.04 Post Quantum Cryptography in IoT Ecosystem – IoT](#))

