Scan Me!

Post Quantum Cryptography

Securing Tomorrow's Infrastructure Against Quantum Threats

Saeed Othman

SYSTRA

Why Quantum Threats Matter

Quantum computing promises immense computational power, but it also poses a serious threat to today's digital security. Algorithms such as RSA and ECC, which protect online communication, banking, and infrastructure, rely on problems that are difficult for classical computers but easily solvable by quantum ones.

The emergence of large-scale quantum computers would render much of our current encryption obsolete, exposing sensitive information and critical systems to potential compromise. For industries and infrastructure with long life cycles, preparing for this shift now is essential to maintaining trust, safety, and operational resilience.

Why This Matters for High-Integrity Systems

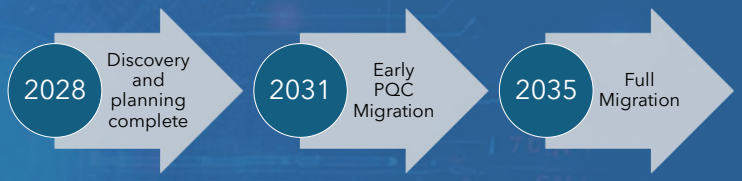
- Protects critical communication channels
- Reduces risk of cryptographic obsolescence
- Supports compliance with emerging assurance standards
- Enhances resilience for long-life assets

What can be done today?

- Implement data minimisation
  - Reduce the amount of data stored
- Adopt hybrid encryption
  - Combine post quantum and normal encryption techniques to achieve both efficient performance and strong security.
- Cryptographic Agility
  - Design systems to easily switch between cryptographic algorithms as new threats and standards emerge
- Regular security assessments
  - Conduct ongoing reviews and updates of security measures to ensure long-term data protection.

Government Timelines

NCSC Roadmap



NIST Roadmap

Emerging Quantum-Resistant Algorithms

Purpose	Classic Algorithms	Quantum Resistant Algorithms
Encryption & Key Exchange	RSA, ECC	**CRYSTALS-Kyber**
Digital Signatures	RSA, ECDSA	**CRYSTALS-Dilithium, Falcon**
Hash-Based Signatures	SHA-2, SHA-3	**SPHINCS+**
Security Basis	Integer Factorisation, Elliptic Curves	**Lattice / Hash-Based Problems**
Quantum Safe?	⊗	✓

Opportunities

- Early leadership in adoption and certification
- Development of new assurance frameworks
- Strengthened public trust in infrastructure

Challenges

- Complexity of migrating legacy systems
- Vendor readiness and toolchain updates
- Balancing performance and security