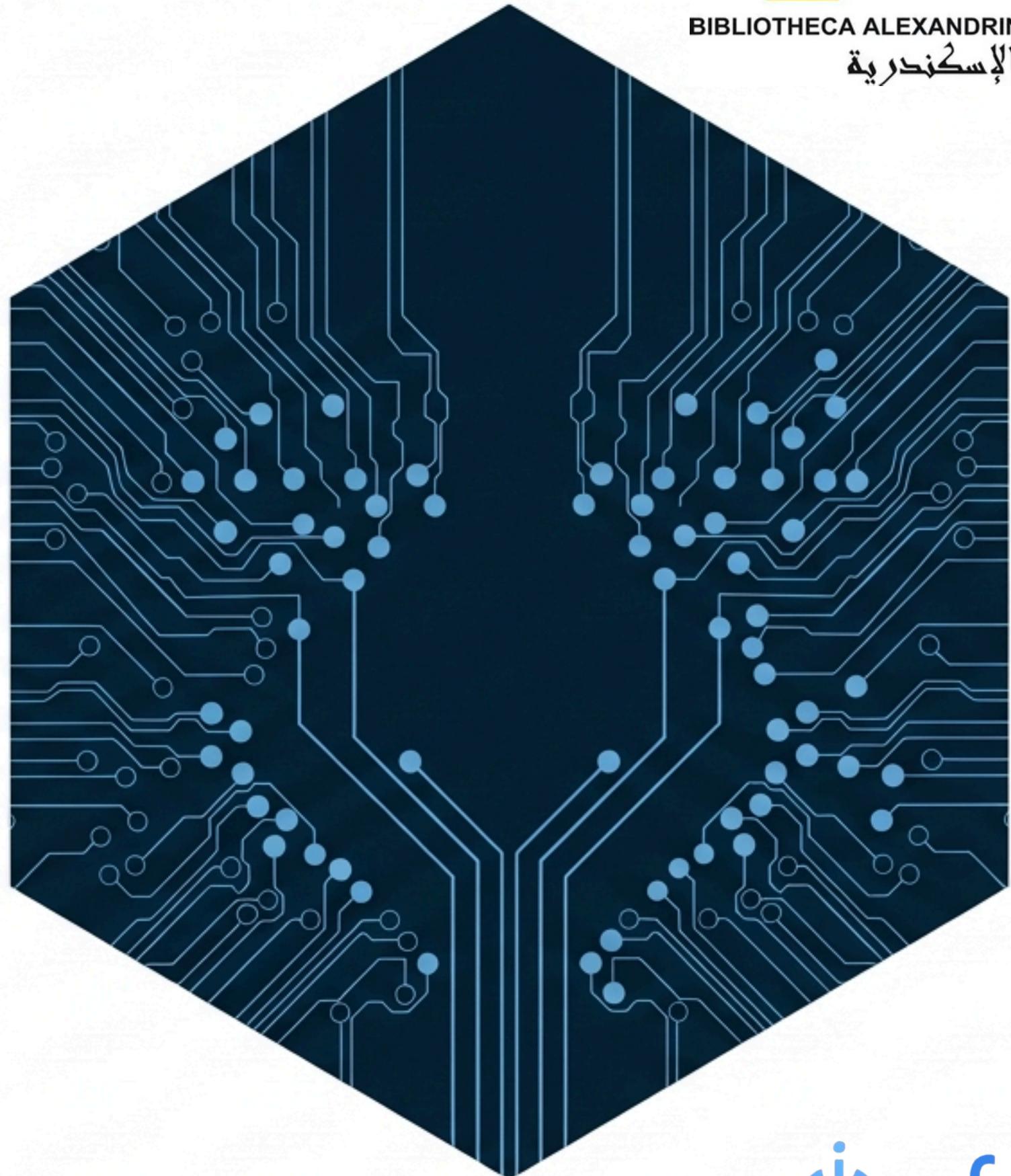


Post-Quantum Cryptography: Securing the Future

Navigating the Migration from
Classical to Quantum-Resistant
Standards

BASED ON CURRENT RESEARCH AND NIST 2024 STANDARDS



The Quantum Threat to Public-Key Infrastructure

Classical Security Vulnerabilities



Shor's Algorithm (1994): Breaks RSA factorisation and Elliptic Curve Cryptography (ECC) in polynomial time $O(n^3)$. Renders current PKI obsolete.

Impact: 2048-bit RSA breakable in hours.

Symmetric Key Weakening



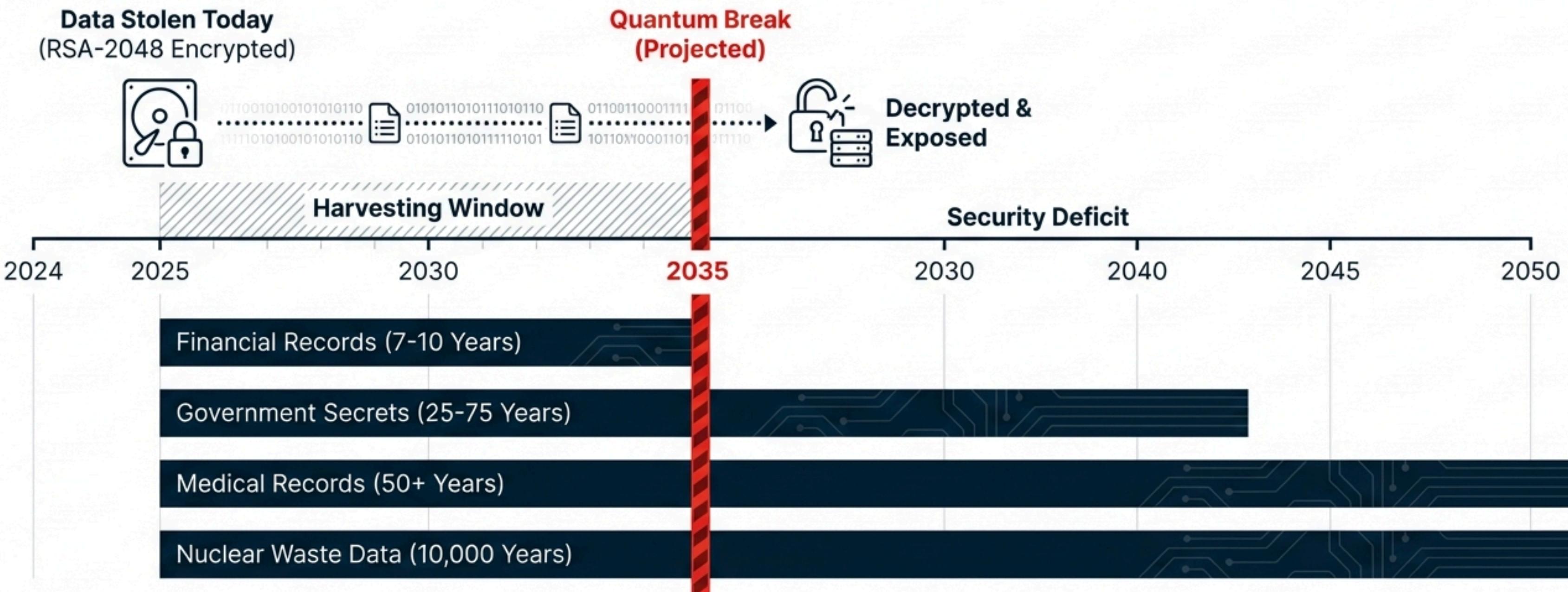
Grover's Algorithm (1996): Quadratic speedup for unstructured search. Reduces symmetric key security by half.

Impact: AES-128 effective security reduced to 64-bit.

Mitigation

AES-256 is required to maintain 128-bit quantum security.

The Immediate Crisis: Harvest Now, Decrypt Later



The Mathematical Foundations of PQC

The Standards

Lattice-Based (The Winner)

Learning With Errors (LWE).
Excellent performance, strong proofs.
Examples: Kyber, Dilithium.



Hash-Based (The Conservative)

Merkle trees.
Minimal assumptions.
Example: SPHINCS+.



Code-Based (The Veteran)

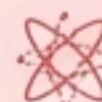
Error-correcting codes.
40+ years of confidence.
Examples: McEliece, HQC.



The Concerns

Multivariate

Rainbow (Broken 2022).
Research continues.



Isogeny-Based

SIKE (Broken 2022).
Security concerns.



The New Standards: NIST FIPS (August 2024)

Mandatory for US Government Use



FIPS 203

ML-KEM

Originally CRYSTALS-Kyber.
Primary Key Encapsulation
Mechanism.



FIPS 204

ML-DSA

Originally CRYSTALS-Dilithium.
Primary Digital Signature
Standard.



FIPS 205

SLH-DSA

Originally SPHINCS+.
Stateless Hash-Based
Signatures (Fallback).

Critical Infrastructure & Industrial IoT

Long Lifecycle Challenges

- Power Grid / SCADA: 30-50 year operational lifetime.
- Nuclear Facilities: Extreme security duration.
- Constraint: Limited CPU/memory makes 'heavy' crypto difficult.



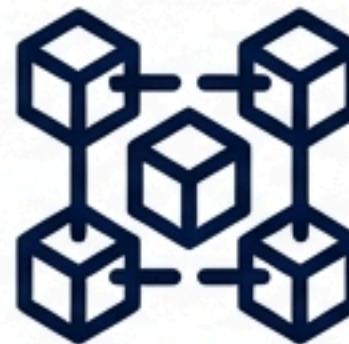
Financial Systems & The Digital Economy

Banking & Payments



7-10 year retention makes current ACH transfers vulnerable to “Harvest Now” attacks.

Blockchain & Crypto



Bitcoin/Ethereum rely on ECDSA signatures. Urgent need for quantum-resistant wallet addresses to prevent asset theft.

High-Frequency Trading

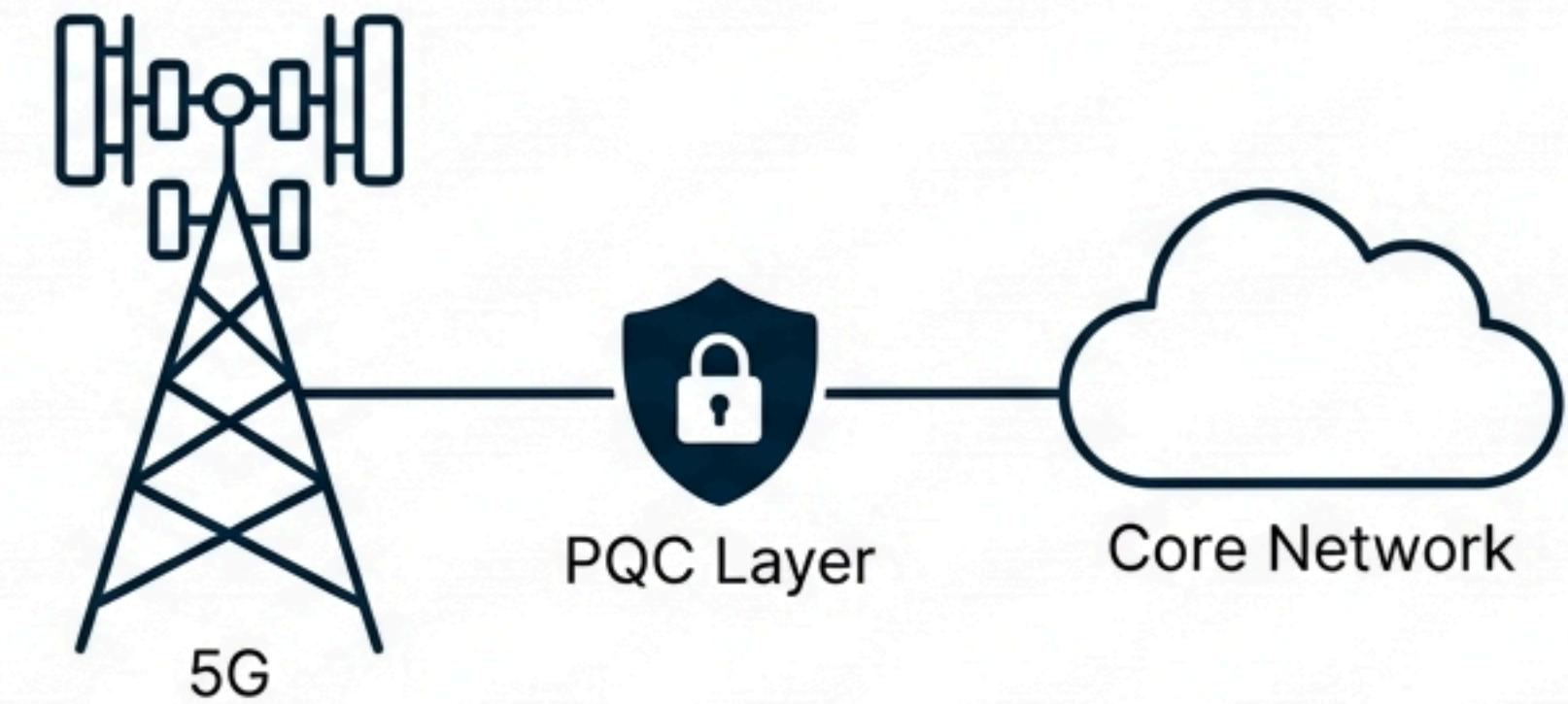


Requires data integrity speeds that PQC must match to maintain market stability.

Telecommunications & Open RAN Integration

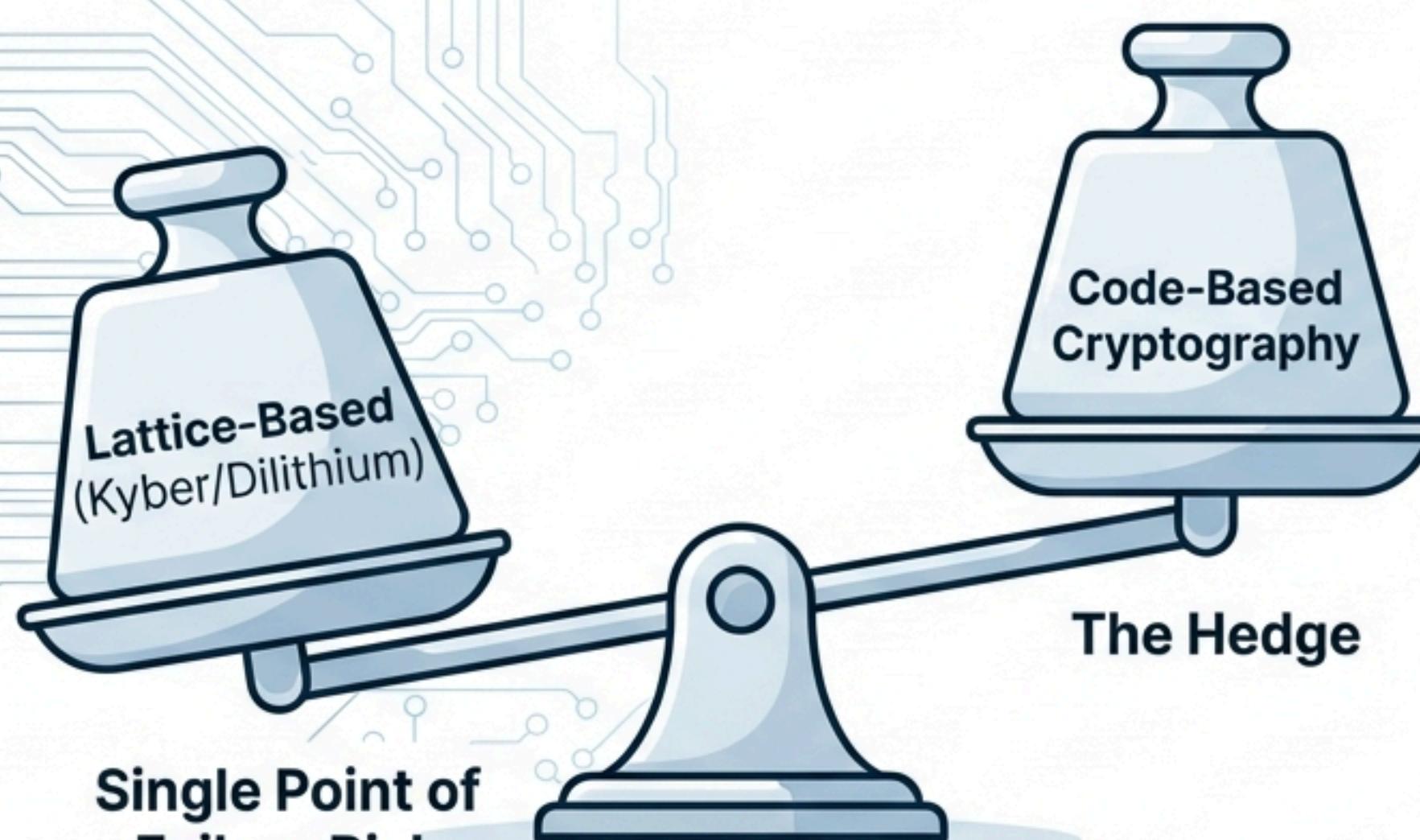
Integration Challenges & Requirements

- **Key Challenge:** Integrating PQC into Open RAN interfaces without latency degradation.
- **Application:** Protecting 5G/6G Backhaul and Fronthaul.
- **Government Requirement:** Classified communications need 25-75 year protection.



The Strategic Value of Mathematical Diversity in Inter Tight Deep Navy (#051C2C)

The **risk of a monoculture**: Do not rely solely on Lattice-based schemes.



Single Point of Failure Risk

- **Historical Confidence:** McEliece (1978) unbroken for 45+ years.
- **Security Foundation:** Syndrome Decoding Problem (NP-complete).
- **Independence:** Mathematically distinct from Lattice.

The Performance Bottleneck: HQC

Hamming Quasi-Cyclic - NIST Round 4 Candidate



High Security

Small keys, IND-CCA2 secure, based on well-understood error-correcting codes.



Low Speed

Significant performance bottleneck compared to Kyber. Standard implementations are much slower, limiting real-world enterprise adoption.



Research Breakthrough: OptHQC Optimization

OptHQC: Optimize HQC for High-Performance Post-Quantum Cryptography
(Dong, Feng, & Wang, Dec 2025)

3.6X

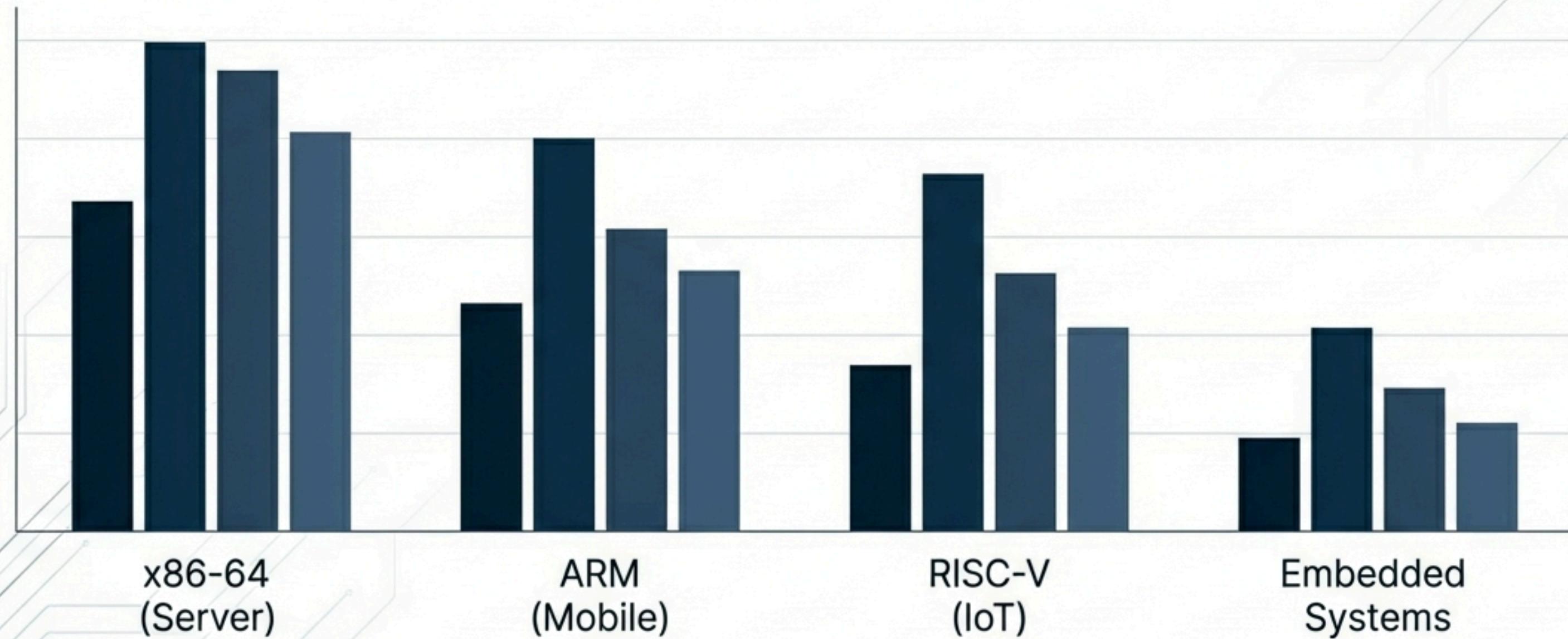
Speedup achieved in HQC operations

Methodology: Algorithm optimization for high-performance computing.

Result: Code-based cryptography becomes a viable, competitive alternative to Lattice schemes.

Real-World Performance Benchmarks

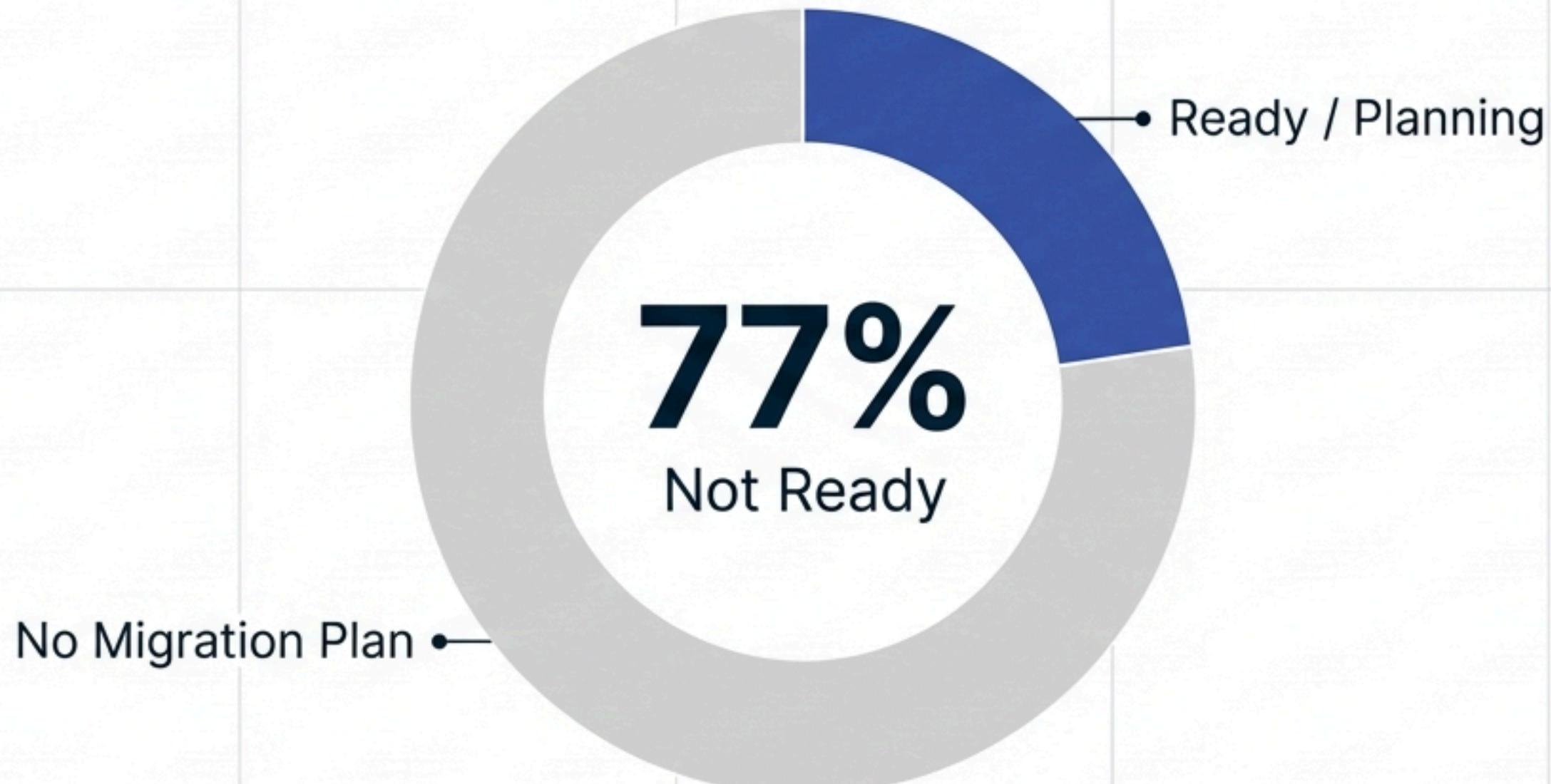
Testing PQC Across Heterogeneous Environments



Source: A Practical Performance Benchmark of Post-Quantum Cryptography (MDPI, May 2025)

The Readiness Gap

Are Enterprises Ready for Quantum-Safe Cybersecurity?

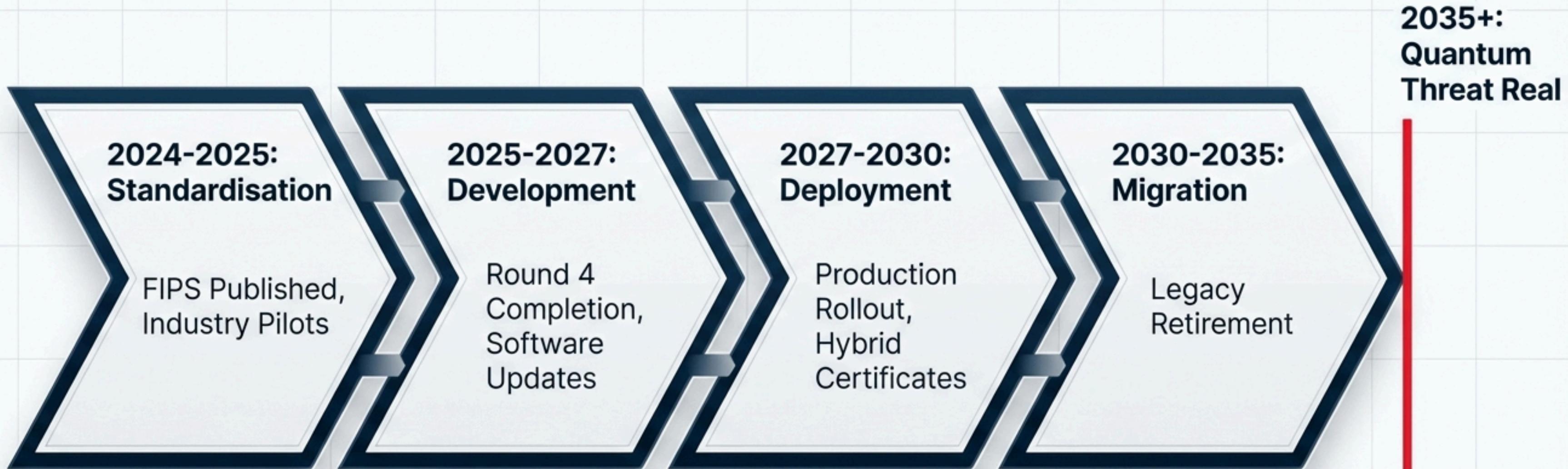


Survey of 500+ Organizations (arXiv, Sep 2025)

Key Barriers

- Legacy system complexity.
- IoT performance constraints.
- Certificate Authority (CA) infrastructure updates.

The Migration Roadmap (2024-2035)



The Window is Closing

We need crypto that outlasts the data.

1 Inventory

Identify long-lived data
(GDPR, HIPAA, Secrets).

2 Assess

Test crypto-agility and
hybrid implementations.

3 Adopt

Integrate FIPS 203, 204,
and 205 into procurement.

Migration takes 10-15 years. **The time to start is now.**