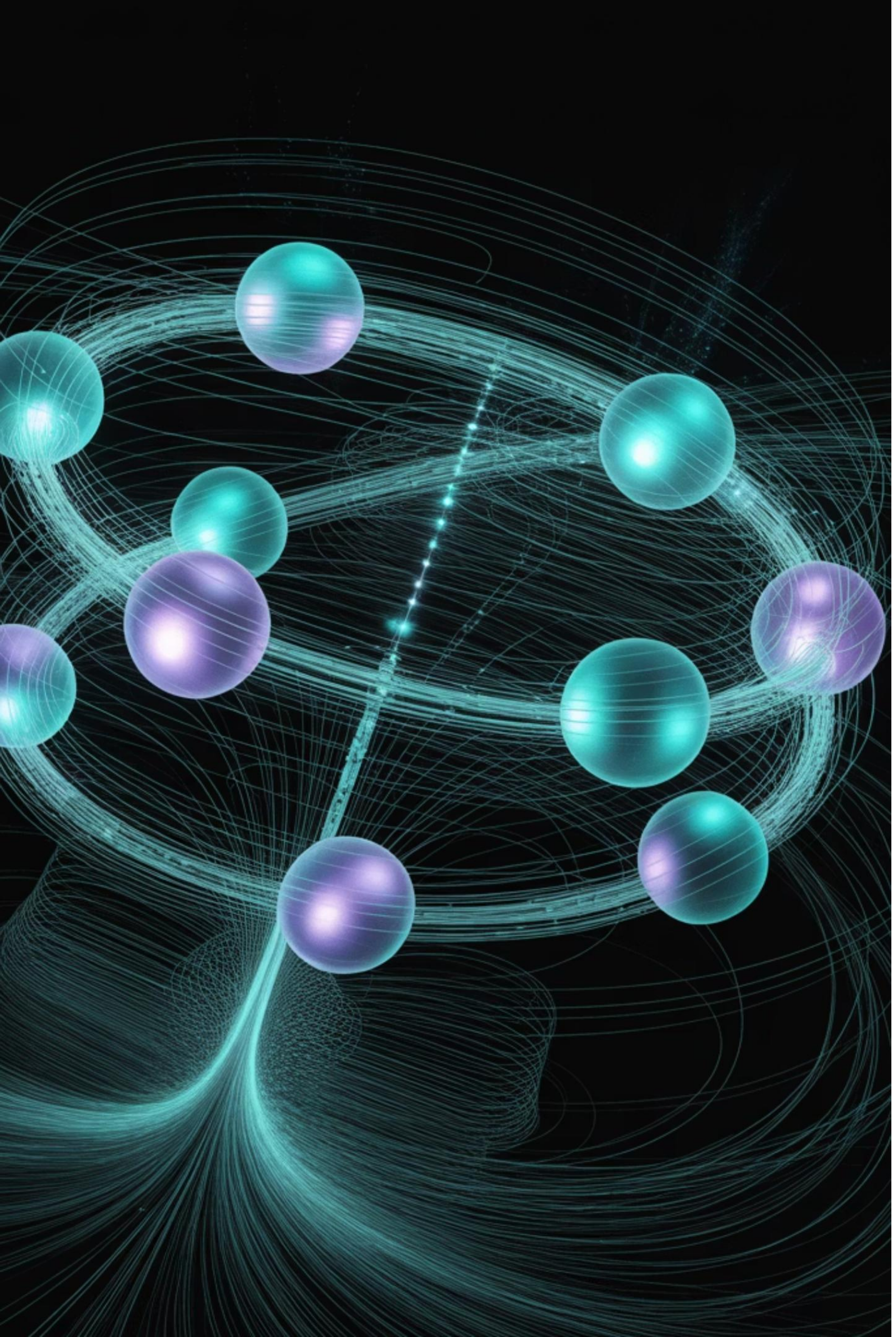


Quantum Technology & Cyber Security: Threats & Opportunities

A leadership challenge

The questions no one wants to ask

Cloud Trust

If quantum can break TLS, what happens to our trust in the cloud: our identity providers, secure channels, and zero trust assumptions?

Crypto Resilience

Is our cryptography genuinely future-ready, or just conveniently ignored?

Dependencies

When was the last time you truly audited *all* your cryptographic dependencies?

Future-Ready

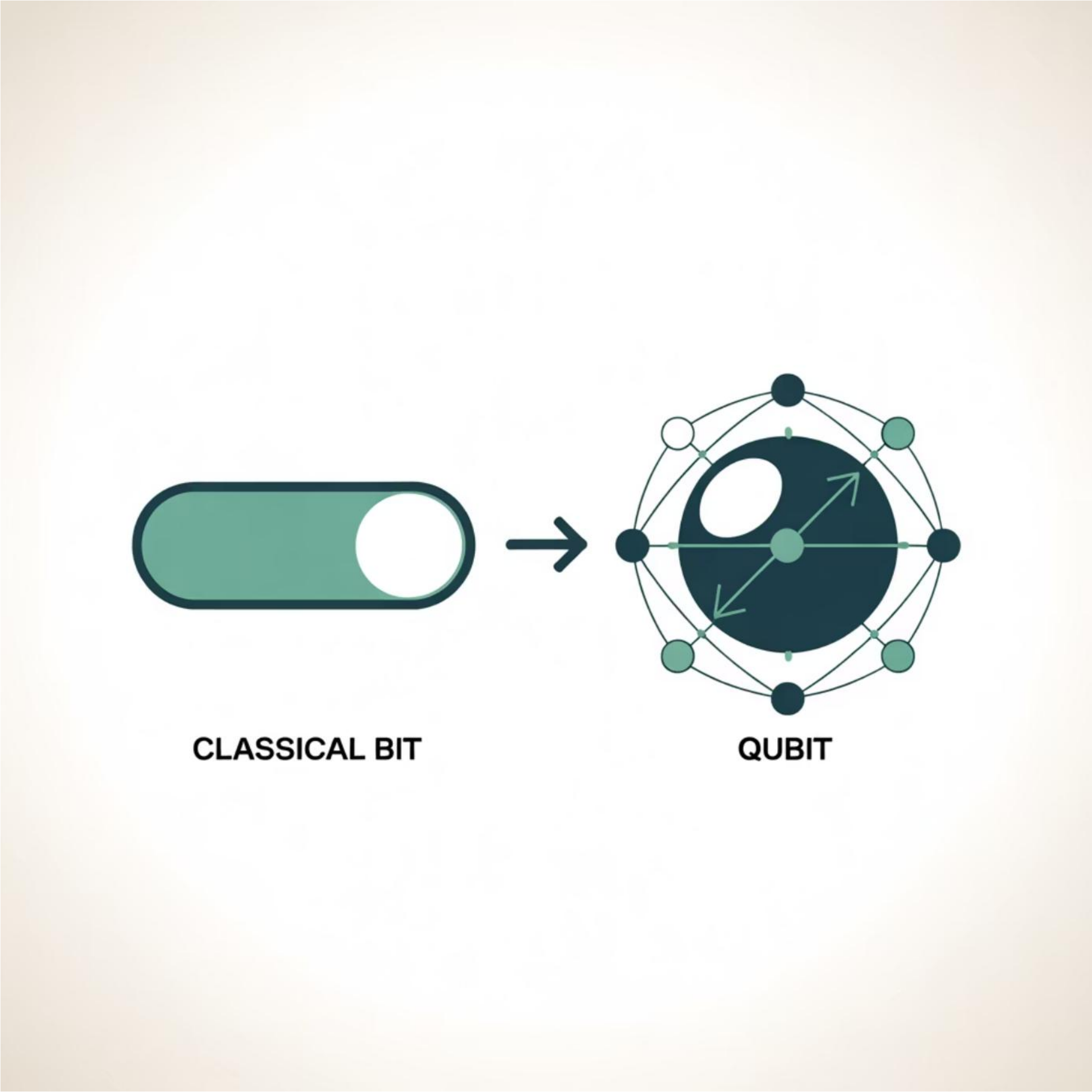
Are we building security for today, or for the quantum-enabled adversaries of tomorrow?

Your job as CISO: Turn uncertainty into action, prepare teams, vendors, and boards for what is coming.

Quantum technology is not just faster

Quantum technology represents a **fundamentally different paradigm**, not simply an acceleration of classical computers

- A **qubit** (quantum bit) is the basic unit of quantum information
- **Superposition** allows qubits to exist in multiple states simultaneously
- Qubits exist in multiple states simultaneously (2^n states for N qubits)
- **Entanglement** enables intrinsically linked computation across space
- **Decoherence** is the process by which a qubit loses its quantum state due to interference from its environment



Quantum technology myths vs reality

1

Myth #1: "Quantum technology can instantly crack any password"

Reality: Quantum computers don’t “guess” passwords instantly. For symmetric encryption (like AES), quantum computers provide only a quadratic speed-up, not an exponential one.

2

Myth #2: "Quantum technology replaces classical computing"

Reality: Quantum computers excel at certain specialised tasks, but they are not general-purpose replacements for classical systems.

3

Myth #3: "Quantum technology attacks are already everywhere"

Reality: While nation-states are harvesting encrypted data now (“harvest now, decrypt later”), there are no real-time quantum attacks yet. Cryptographically relevant quantum computers (CRQCs) are not expected until the 2030s at the earliest, though the timeline is uncertain.

Quantum technology threats to cyber security

Encryption & Key Exchange

RSA and ECC cryptosystems vulnerable to Shor's algorithm, potentially compromising secure communications.

Digital Signatures & Certificates

PKI infrastructure at risk, threatening the foundation of digital trust and authentication systems.

VPNs, TLS, SSH, HTTPS

Core security protocols require complete cryptographic overhaul to maintain confidentiality and integrity.

Stored Encrypted Data

Harvest Now, Decrypt Later risk: data with long-term value being harvested now for future decryption when quantum capabilities mature.

Quantum technology algorithms

Algorithm	Description & Target	Cybersecurity Implications
Shor's Algorithm	Provides exponential speedup for factoring large integers and solving discrete logarithm problems **Targets:** Public key cryptography (RSA, ECC)	• Completely breaks RSA and ECC encryption • Compromises digital signatures and certificates • Renders current PKI infrastructure obsolete • Requires fault-tolerant quantum computers with 1000s of logical qubits
Grover's Algorithm	Provides quadratic speedup for searching unsorted databases **Targets:** Symmetric cryptography (AES, hash functions)	• Effectively halves symmetric key security • 256-bit keys provide 128-bit equivalent security • AES-256 remains secure with current implementation • Mitigation: Double key sizes to maintain security levels

Post Quantum Cryptography (PQC) algorithms

Kyber

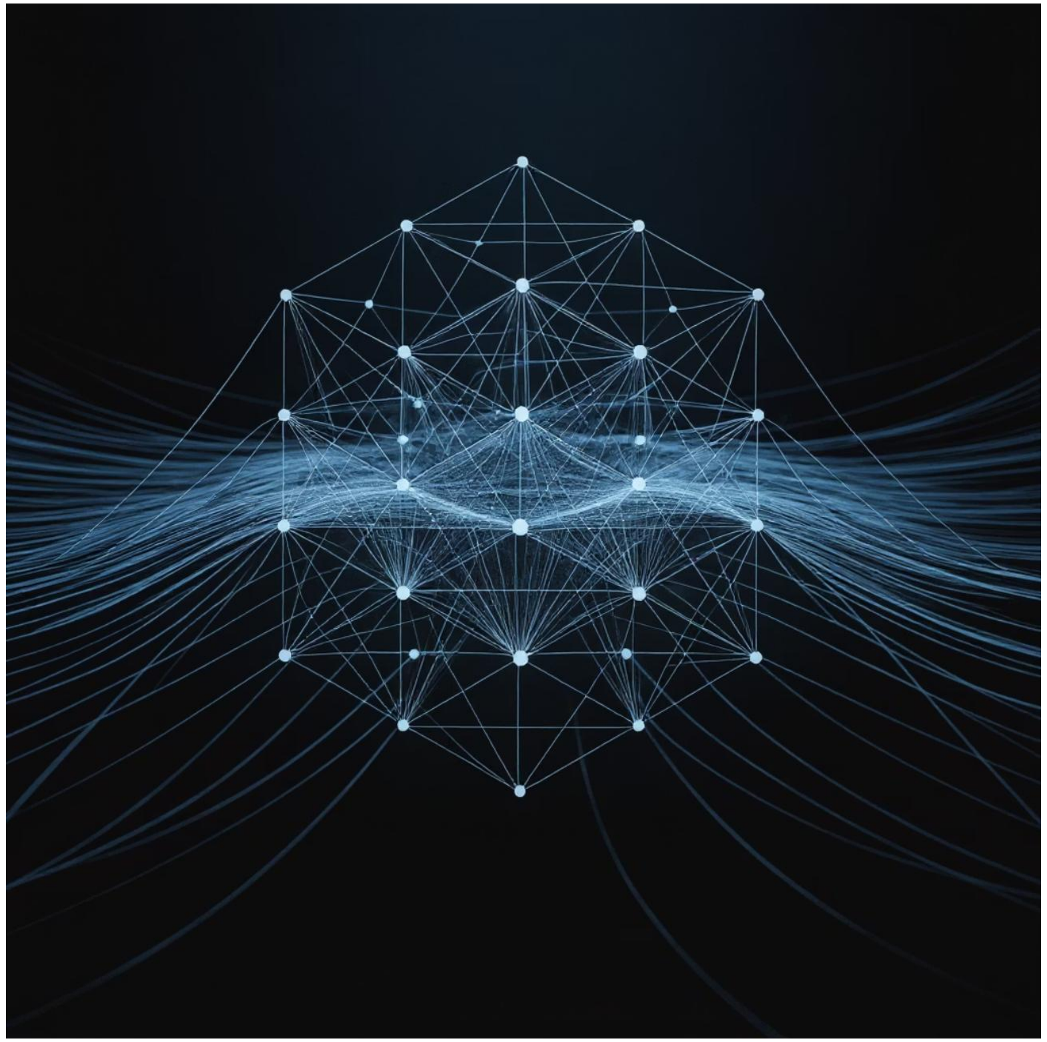
Key exchange mechanism replacing RSA/DH, based on lattice cryptography with strong quantum resistance properties.

Dilithium

Digital signature algorithm replacing RSA/ECC for authentication and integrity verification in a post-quantum environment.

Falcon

Lightweight, fast signature scheme optimised for IoT and mobile applications with constrained resources.



Challenges to cyber security

Timeline Uncertainty

Migration Complexity

Performance Impact

Lack of Visibility

Supply Chain Dependencies and Compliance

Resource Constraints

Cryptographic Obsolescence

Harvest Now, Decrypt Later

Risk categories

High Risk

Long-term sensitive data with 10+ year confidentiality requirements

- Financial records and transaction data
- Healthcare data and patient records
- Government secrets and classified information
- Intellectual property and trade secrets
- Legal documents and contracts

Medium Risk

Corporate communications and operational data

- Corporate communications and internal documents
- Customer databases and personal information
- Research data and development projects
- Business strategies and competitive intelligence
- Employee records and HR data

Low Risk

Short-term operational data with limited confidentiality needs

- Public communications and marketing materials
- Temporary operational data
- Non-sensitive system logs
- Public-facing application data
- Short-term cache and session data

Security benefits of quantum technology

1. **Quantum Key Distribution (QKD)**

   Secure key exchange that instantly detects eavesdropping, making communication virtually tamper-proof.

2. **True Quantum Randomness**

   Uses pure randomness (not software-based) to create keys that are unpredictable and unbreakable.

3. **Smarter Threat Detection**

   Boosts AI's ability to spot threats faster and more accurately, even those that are highly sophisticated.

4. **Strategic Cyber Advantage**

   Helps build future-proof, quantum-safe systems that give your organization a defensive edge.

The quantum technology transition

2024

NIST finalises PQC algorithms

2025

Early enterprise pilots: TLS, VPNs

2027

PQC adoption scales across infrastructure

2030

NSA & ASD deadline for quantum-safe systems

2035

Risk to legacy crypto becomes mainstream

⚠ The "crypto-agile window" is closing. Migration takes years; organisations must start preparing now to avoid rushed, costly implementations later.

Transitioning to quantum safe cryptography

Depending on an organisation's risk appetite and posture, the transition to quantum-safe cryptography can be evaluated using three key parameters:

1

Data Shelf-Life (X)

How long does your sensitive data need to remain confidential? Consider regulatory requirements, business value, and competitive advantage duration.

2

Migration Time (Y)

How long will it take to fully transition to quantum-safe cryptography? Include assessment, planning, implementation, and testing phases.

3

Quantum Timeline (Z)

When will cryptographically relevant quantum computers (CRQCs) become available? Current estimates suggest 2030s, but uncertainty remains.

Mosca's Theorem: X + Y > Z

If the sum of the data shelf-life and migration time exceeds the quantum timeline, your organisation is at risk and must act now to implement quantum-safe cryptography.

Transitioning to quantum cyber readiness: A white paper by CERT-In in collaboration with SISA https://www.sisainfosec.com/news-room/cert-in-and-sisa-unveil-whitepaper-on-quantum-cyber-readiness-to-future-proof-indias-digital-infrastructure/

Roadmap to quantum cyber readiness

1 Foundational Assessment & Strategic Planning

- Strong IDAM is still your #1 defence
- Know your sensitive data
- Risk Assessment & Cryptographic Inventory
- Governance & Stakeholder Alignment
- Stakeholder Engagement

2 Technology Readiness & Capability Building

- Hybrid Cryptography Adoption
- Testing & Vendor Collaboration
- Infrastructure Evaluation
- Automated Discovery Tools
- AI-Enhanced Risk Modelling

Be Proactive, Not Reactive

Lead, Don't Follow

Don't wait for mandates or incidents: they always come too late. Shape policy proactively rather than following industry hype.

Board-Level Risk

Bring quantum technology into strategic risk conversations at the highest level of the organisation.

Business Continuity

Treat crypto refresh as a critical business continuity function, not just a technical implementation.

The time to act is now. Start your quantum risk assessment, engage your vendors, and begin future-proofing your security architectures. Let's work together to build a quantum-resilient future.

THANK YOU


Fatime (Fatima) Hoblos
Cyber Security| Identity Access Management
| Identity Engineer| Identity Solutions Archit...