Quantum Computing's Impact on Global Security Infrastructure: Post-Quantum Cryptography Transition Analysis

Author: Driti Virani

Affiliation: Evergreen Valley High School, San Jose, CA

Mentor: Industry Expert, Confidential

Research Period: October 2025 - August 2026 (Expected)

Abstract

Quantum computing represents a discontinuous leap in computational capability that simultaneously undermines decades of cryptographic security while demanding wholesale transformation of global digital infrastructure. Unlike traditional computing threats that evolve incrementally, quantum computers equipped with Shor's algorithm can break RSA, ECC, and other public-key cryptosystems that secure internet communications, financial transactions, and classified government data.

This research examines the technical, economic, and geopolitical implications of transitioning global security infrastructure to quantum-resistant cryptographic systems before cryptographically-relevant quantum computers (CRQCs) emerge. Drawing on NIST's recently standardized post-quantum algorithms (CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+, FALCON), this study analyzes:

1. **Timeline Assessment:** When will CRQCs capable of breaking RSA-2048/ECC-256 realistically emerge? (Estimates: 10-30 years)
2. **Threat Analysis:** How does "harvest now, decrypt later" compress migration timelines?
3. **Technical Solutions:** Which NIST post-quantum algorithms address specific vulnerabilities?
4. **Migration Strategy:** Sector-specific roadmaps for finance, healthcare, defense, and critical infrastructure
5. **Geopolitical Implications:** Quantum arms race dynamics and intelligence gathering capabilities

Key Finding: Using Mosca's theorem ($X \leq Y + Z$), where X = data protection time, Y = migration time, and Z = CRQC emergence time, we demonstrate that organizations protecting data for 20+ years must begin quantum-safe migration immediately. The global migration cost is estimated at $25-100 billion, with financial services ($10-20B), government/defense ($15-25B), and critical infrastructure ($15-25B) bearing the largest burdens.

Methodology: Literature review of 30+ academic papers, NIST standardization documentation, industry reports from IBM/Google/IonQ, and policy frameworks from NSA, CISA, UNESCO, and OECD. Includes sector-specific case studies and cost-benefit analysis for enterprise migration.

1. Introduction

1.1 The Quantum Threat Landscape

On August 13, 2024, the National Institute of Standards and Technology (NIST) published the first three post-quantum cryptographic standards after an eight-year global competition (NIST, 2024). This milestone represents the cryptographic community's response to an existential threat: quantum computers capable of breaking the public-key cryptography that secures modern digital infrastructure.

The urgency stems from a mathematical breakthrough made three decades ago. In 1994, Peter Shor demonstrated that a sufficiently powerful quantum computer could factor large numbers exponentially faster than classical computers—a discovery that fundamentally undermines RSA encryption (Shor, 1994). Lov Grover's 1996 algorithm further showed quantum speedups for search problems, weakening symmetric cryptography (Grover, 1996).

Visual Element - Figure 1: Quantum Threat Timeline

```
2025: Current quantum computers (~1,000 noisy qubits)
        ↓
        20,000x gap
        ↓
2035–2040: Optimistic CRQC emergence (~20M noisy qubits OR ~4,000
logical qubits)
        ↓
2045–2055: Conservative CRQC emergence
        ↓
RSA-2048 broken → Financial systems compromised
                → Government secrets exposed
                → Internet trust model collapses
```

1.2 The "Harvest Now, Decrypt Later" Problem

Unlike traditional cybersecurity threats that require real-time exploitation, quantum computing introduces a temporal displacement attack vector. Adversaries are collecting encrypted data today—diplomatic cables, financial transactions, healthcare records, classified military communications—with the intent to decrypt them once quantum computers become available (Mosca, 2018).

This "store now, decrypt later" strategy collapses the timeline for action. Data encrypted today with 15-year secrecy requirements faces immediate risk if CRQCs emerge in

10-15 years. The window for migration is not “whenever quantum computers arrive” but “now.”

1.3 Research Question and Scope

Central Question: How do we transition global security infrastructure to quantum-resistant cryptographic systems before cryptographically-relevant quantum computers (CRQCs) emerge, and what are the technical, economic, and geopolitical implications of this transition?

Scope: - **Period Covered:** 2010-2025 (historical context) + 2025-2050 (forward-looking analysis)

Focus Areas: Technical (cryptography), Economic (migration costs), Policy (national security), Geopolitical (quantum arms race)

Target Output: 20-25 pages (full paper) OR 5-7 pages (executive summary for applications)

What Makes This Research Novel:

- Most research focuses on EITHER technical solutions OR policy implications. This study connects both.

- Emphasizes urgency and practical migration roadmaps, not just theoretical analysis

- Sector-specific analysis (finance, healthcare, defense, infrastructure) provides actionable insights

- Examines geopolitical dynamics often missing from technical cryptography papers

2. Methodology

2.1 Research Design

This study follows a structured literature review and analytical framework approach, synthesizing academic research, government policy documents, industry reports, and technical specifications from 2010-2025.

Data Collection Sources:

1. **Academic Papers:** Web of Science, IEEE Xplore, ACM Digital Library, arXiv, SpringerLink

2. **Government Publications:** NIST CSRC, NSA announcements, CISA guidelines, OECD reports

3. **Industry Technical Reports:** IBM Quantum roadmap, Google Quantum AI, IonQ/ Rigetti updates

4. **Policy Frameworks:** National Quantum Initiative Act (2018), EU Quantum Flagship, China quantum strategy

Selection Criteria: - Peer-reviewed research on quantum computing threats or post-quantum cryptography - Official government standards and policy documents - Industry technical documentation from quantum computing leaders - Publication date: 2010-2025 (with emphasis on 2020-2025 for recent developments)

2.2 Analytical Framework

Mosca's Theorem (Risk Assessment Model):

```
X ≤ Y + Z

Where:
X = Time data must remain secure
Y = Time required to migrate to PQC
Z = Time until CRQCs emerge

Conclusion: If X > Y + Z, start migrating NOW
```

Example Application: - X = 30 years (classified government data) - Y = 10 years (infrastructure migration time) - Z = 15 years (optimistic CRQC timeline) - **30 > 25 →** Must start migrating immediately

2.3 Key Sources

Foundational Papers: 1. Shor, P. W. (1994). "Algorithms for quantum computation: Discrete logarithms and factoring." 2. Grover, L. K. (1996). "A fast quantum mechanical algorithm for database search." 3. Mosca, M. (2018). "Cybersecurity in an era with quantum computers: Will we be ready?"

NIST PQC Standards: 4. NIST (2024). "Post-Quantum Cryptography Standardization: Selected Algorithms." 5. Alagic, G., et al. (2024). "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process."

Policy Documents: 6. NSA (2022). "Announcing the Commercial National Security Algorithm Suite 2.0." 7. CISA (2024). "Post-Quantum Cryptography Initiative." 8. European Commission (2023). "Quantum Technologies Flagship: Strategic Research Agenda."

Industry Reports: 9. IBM (2024). "IBM Quantum Development Roadmap." 10. Google Quantum AI (2023). "Quantum supremacy using a programmable superconducting

processor.” 11. National Academies (2019). “Quantum Computing: Progress and Prospects.”

3. Results

3.1 Timeline & Threat Assessment

Current State of Quantum Computing (2025): - **Largest quantum computers:** ~1,000 noisy qubits (IBM Condor) - **Required to break RSA-2048:** ~20 million noisy qubits OR ~4,000 logical qubits - **Gap:** 20,000x noisy qubits OR need quantum error correction breakthrough

CRQC Emergence Estimates: - **Optimistic:** 10-15 years (2035-2040) - **Conservative:** 20-30 years (2045-2055) - **Pessimistic:** 50+ years or never

Visual Element - Table 1: Data Sensitivity Lifecycles vs. Quantum Threat Horizon

Data Type	Required Protection Period	Threat Horizon	Action Required
Classified Government	30-50 years	Immediate	Migrate NOW
Healthcare Records	Lifetime + 50 years	Immediate	Migrate NOW
Financial Data	10-20 years	Urgent	Begin migration 2025-2027
Corporate Secrets	5-20 years	Moderate	Begin migration 2027-2030
Personal Communications	5-10 years	Low	Monitor and plan

3.2 Cryptographic Vulnerability Analysis

Quantum-Vulnerable Systems: - **RSA:** Public-key encryption (used in TLS, email, code signing) - **ECC/ECDSA:** Elliptic curve cryptography (used in TLS, Bitcoin, HTTPS) - **Diffie-Hellman:** Key exchange protocol (used in VPNs, TLS) - **DSA:** Digital Signature Algorithm

Why These Systems Break: Shor's algorithm exploits the mathematical structure of integer factorization and discrete logarithm problems, both of which underpin RSA and ECC. A quantum computer with sufficient qubits can solve these problems in **polynomial time**—meaning computation time grows slowly and predictably as the problem size increases (proportional to $(\log N)^3$), rather than exponentially. This transforms factoring from computationally infeasible (requiring billions of years on classical computers) to feasible (hours on a quantum computer), rendering 2048-bit RSA completely broken once CRQCs emerge.

Quantum-Resistant Systems: - **AES-256:** Symmetric encryption (Grover weakens to ~AES-128 equivalent, still secure) - **SHA-3:** Cryptographic hash (quantum-resistant) - **Lattice-based crypto:** NIST-selected PQC algorithms - **Hash-based signatures:** SPHINCS+

Key Insight: Grover's algorithm provides only quadratic speedup ($\sqrt{N}$), not exponential. Doubling symmetric key lengths (AES-128 → AES-256) compensates for quantum advantage. Public-key systems, however, face exponential quantum speedup and require complete replacement.

3.3 NIST Post-Quantum Cryptographic Standards

After an 8-year global competition evaluating 82 initial submissions, NIST selected 4 algorithms for standardization in 2024:

Visual Element - Table 2: NIST-Selected PQC Algorithms

Algorithm	Type	Security Basis	Public Key Size	Signature/ Ciphertext Size	Speed	Best Use Case
CRYSTALS-Kyber	Key Encapsulation	Lattice (MLWE)	800-1,600 bytes	700-1,500 bytes	Fast (<1ms)	TLS, VPN, key exchange
CRYSTALS-Dilithium	Digital Signature	Lattice (MLWE)	1,300-2,600 bytes	2,400-4,600 bytes	Fast	General signatures, code
SPHINCS+	Digital Signature	Hash-based	32-64 bytes	8,000-50,000 bytes	Slow (10-100ms)	Long-term archives, root CAs
FALCON	Digital Signature	Lattice (NTRU)	~900 bytes	600-1,200 bytes	Fast	IoT, embedded systems

3.3.1 Understanding Lattice-Based Cryptography (MLWE)

CRYSTALS-Kyber and CRYSTALS-Dilithium (2 of the 4 NIST-selected algorithms) are based on the **Module Learning With Errors (MLWE)** problem—the mathematical foundation that makes them quantum-resistant.

The Core Idea: "Learning With Errors"

Imagine trying to solve a system of linear equations (like high school algebra), but each equation has small random "noise" added to it. Without noise, solving for the secret is easy—just use Gaussian elimination. With carefully calibrated noise, the problem becomes exponentially hard, even for quantum computers.

Think of it like **static on a radio signal**: a little interference makes it exponentially harder to extract the original message. The noise must be calibrated perfectly—too little and it's solvable (insecure), too much and legitimate users can't decrypt (unusable).

Why MLWE Resists Quantum Attacks:

Problem Type	Example	Quantum Attack	Status
Factoring	RSA	Shor's algorithm (polynomial time)	❌ Broken
Discrete Log	ECC	Shor's algorithm (polynomial time)	❌ Broken
Lattice (MLWE)	Kyber/ Dilithium	No known efficient algorithm	✅ Secure

Key insight: Quantum computers excel at problems with exploitable mathematical structure (like factoring and discrete logarithms). Lattice problems have no known structure for quantum algorithms to exploit—the noise transforms a structured problem into an unstructured search.

Why We Trust MLWE: - **20+ years of study:** Security assumptions have withstood extensive cryptanalysis (Regev, 2005; Peikert, 2016) - **NIST validation:** Kyber and Dilithium selected after 8-year global competition evaluating 82 algorithms - **Practical performance:** Fast operations (<1ms) and reasonable key sizes (1-2 KB) - **Caveat:**

Future quantum algorithms *might* break these assumptions, but no evidence suggests this is likely

3.3.2 Performance Trade-offs and Implementation Challenges

Performance Trade-offs: 1. **Key/Signature Size:** PQC keys are 3-10x larger than RSA/ECDSA (problem for IoT, satellites) 2. **Computational Speed:** PQC operations are 2-5x slower in some cases 3. **Bandwidth Consumption:** Increased data transmission requirements 4. **Implementation Complexity:** Side-channel vulnerabilities (timing attacks on lattice crypto)

Implementation Challenges: - **Backward Compatibility:** Legacy systems cannot be easily upgraded - **Hardware Constraints:** Embedded devices lack resources for larger keys - **Unknown Quantum Algorithms:** Future breakthroughs might break lattice assumptions - **Standardization Fragmentation:** China developing separate PQC standards

3.4 Sector-Specific Migration Analysis

3.4.1 Financial Services

Current Cryptography: - SWIFT network: RSA-2048 signatures - Payment processors: TLS with RSA/ECDHE - Stock exchanges: ECDSA for high-frequency trading - ATM networks: RSA for PIN verification - Blockchain: ECDSA signatures (Bitcoin, Ethereum)

Quantum Threat: - “Harvest now, decrypt later” on financial transactions - Fraudulent transactions if signatures forged - Cryptocurrency theft (private keys exposed) - SWIFT interception (espionage, manipulation)

Migration Roadmap: - **2025-2028 (Phase 1):** Pilot hybrid PQC/RSA in development environments - **2028-2030 (Phase 2):** Deploy hybrid Kyber+RSA in production TLS - **2030-2033 (Phase 3):** Replace ATMs and POS terminals with PQC-capable hardware - **2033-2035 (Phase 4):** Sunset classical crypto, full PQC migration - **2035+ (Phase 5):** Maintain crypto agility, monitor for new threats

Estimated Costs: - Global banking: $10-20 billion - Hardware replacement (ATMs, HSMs): $8-12 billion - Software updates: $3-5 billion - Training and compliance: $1-2 billion

3.4.2 Healthcare

Current Cryptography: - Electronic Health Records (EHR): TLS with RSA - Medical devices: RSA/ECC for firmware updates - Telemedicine: TLS for video consultations - Health insurance: HIPAA-compliant encryption (RSA/AES)

Quantum Threat: - Patient privacy violations if EHRs decrypted retroactively - Medical device hacking (pacemakers, insulin pumps) - Insurance fraud if claims data exposed - HIPAA violations with massive fines

Migration Roadmap: - **2025-2028 (Phase 1):** Update EHR systems to support hybrid PQC - **2028-2032 (Phase 2):** Replace medical devices on normal refresh cycles - **2032-2040 (Phase 3):** Full PQC migration (long timeline due to device lifecycles) - **2040+ (Phase 4):** Legacy devices air-gapped or decommissioned

Estimated Costs: - US healthcare: $5-10 billion - Medical device replacement: $3-5 billion - EHR software updates: $1-2 billion - Compliance and training: $1-3 billion

3.4.3 National Defense

Current Cryptography: - Classified communications: NSA Suite B (ECC-384, AES-256) - Nuclear command & control: Classified encryption (likely RSA/ECC) - Military satellite communications: Quantum-vulnerable key exchange - Intelligence gathering: RSA/ECC for secure data transmission

Quantum Threat: - Adversaries harvesting classified communications NOW for decryption in 10-15 years - Diplomatic cables exposed retroactively (decades of negotiations) - Nuclear C2 systems compromised (catastrophic risk) - Intelligence sources revealed (human assets in danger)

Migration Roadmap: - **Already underway (classified programs):** NSA CNSA 2.0 mandates PQC migration - **2025-2028:** Deploy PQC for Top Secret systems - **2028-2030:** Deploy PQC for Secret systems - **2030-2033:** Deploy PQC for Confidential and Unclassified systems

NSA CNSA 2.0 Timeline: National security systems must transition to PQC by 2035, with Top Secret systems prioritized for immediate migration.

Estimated Costs: - US Department of Defense: $10-15 billion - Intelligence agencies: $5-10 billion - Allied nations (NATO): $10-20 billion

3.4.4 Critical Infrastructure

Current Cryptography: - Power grids: SCADA systems with RSA/ECC authentication - Water treatment: Industrial control systems (often unencrypted or weak crypto) - Transportation: Traffic control, railway signaling with legacy crypto - Telecommunications: 5G networks with ECC-based security

Quantum Threat: - Cyberattacks using quantum computers to disrupt infrastructure - Espionage (foreign adversaries map critical systems) - Physical damage (manipulate SCADA to cause equipment failure) - Cascading failures (power + water + transport)

Migration Roadmap: - **2025-2030 (Phase 1):** Segment networks, deploy PQC at edge devices - **2030-2040 (Phase 2):** Replace core systems during normal refresh cycles - **2040-2050 (Phase 3):** Full migration (extremely long timeline)

Estimated Costs: - US critical infrastructure: $15-25 billion - Power grid: $5-10 billion - Water/wastewater: $2-5 billion - Transportation: $3-5 billion - Telecommunications: $5-10 billion

4. Discussion

4.1 Geopolitical Implications

Quantum Arms Race: - **United States:** $1.2B National Quantum Initiative, IBM/Google leadership - **China:** $10B+ investment, claims quantum supremacy (photonic computer, 2020) - **European Union:** €1B Quantum Flagship program - **Question:** Does quantum advantage translate to geopolitical power?

Intelligence Implications: - Adversaries collecting encrypted communications TODAY for future decryption - Past diplomatic negotiations could be exposed retroactively - Espionage capabilities amplified once CRQCs emerge

Export Controls: - US ECRA restricts quantum computing technology exports - China restricts quantum tech exports (2023) - Dual-use dilemma: Research vs. weaponization

Standardization Politics: - NIST vs. Chinese PQC standards (potential fragmentation) - Trust issues: Are algorithms backdoored? (No evidence, but concern) - Need for global interoperability vs. national security concerns

4.2 Economic Impact

Global Migration Cost Estimate: $25-100 billion

Breakdown by Sector: - Financial services: $10-20 billion - Healthcare: $5-10 billion - Government/defense: $15-25 billion - Critical infrastructure: $15-25 billion - Enterprise/SMBs: $20-30 billion

Cost Drivers: 1. Hardware replacement (ATMs, HSMs, embedded devices) 2. Software updates (TLS libraries, cryptographic APIs) 3. Training and certification (developers, security teams) 4. Compliance and auditing 5. Opportunity cost (delayed features, diverted engineering resources)

4.3 Key Findings

Finding 1: Timeline Compression Mosca's theorem demonstrates that organizations protecting data for 20+ years must begin migration immediately. The "harvest now,

decrypt later" threat means encrypted data collected today is at risk once CRQCs emerge.

Finding 2: No Single Solution Different sectors require different algorithms: - **Finance:** CRYSTALS-Kyber for TLS, CRYSTALS-Dilithium for signatures - **Healthcare:** Hybrid PQC for long device lifecycles - **Defense:** SPHINCS+ for long-term classified data - **IoT:** FALCON for constrained devices

Finding 3: Hybrid Cryptography Essential Migration will require 5-10 years of hybrid classical+PQC systems for backward compatibility. Organizations cannot flip a switch—they must support both old and new cryptography simultaneously.

Finding 4: Geopolitical Fragmentation Risk If US and China standardize different PQC algorithms, the internet could fragment into incompatible security zones, undermining global commerce and communication.

Finding 5: Cost vs. Risk Trade-off $25-100B migration cost is massive but pales compared to potential losses from quantum-enabled data breaches (estimated trillions in IP theft, financial fraud, national security damage).

5. Recommendations

5.1 For Governments

1. **Mandate PQC Timelines:** Set sector-specific deadlines (e.g., financial services by 2030)
2. **Fund Migration Support:** Provide grants/loans for SMBs unable to afford migration
3. **Harmonize Standards:** Work with international partners to prevent fragmentation
4. **Quantum Literacy:** Fund educational programs for policymakers and the public

5.2 For Enterprises

1. **Conduct Crypto Inventory:** Map all uses of cryptography in systems
2. **Prioritize Data Sensitivity:** Start with systems protecting 20+ year data
3. **Pilot Hybrid Systems:** Test PQC+classical crypto in non-production environments
4. **Build Crypto Agility:** Design systems that can swap algorithms without major rewrites

5.3 For Researchers

1. **Improve PQC Performance:** Optimize algorithms for embedded devices and IoT
2. **Side-Channel Resistance:** Harden implementations against timing attacks

3. **Post-Quantum Security Proofs:** Strengthen confidence in lattice-based assumptions
4. **Migration Tools:** Develop automated tools for crypto inventory and replacement

5.4 For Developers

1. **Use Crypto Libraries:** Never implement cryptography from scratch
2. **Enable Algorithm Negotiation:** Design protocols that can upgrade to PQC
3. **Monitor NIST Updates:** Stay current with emerging standards
4. **Test Hybrid Deployments:** Validate PQC compatibility with existing systems

6. Limitations

Limitation 1: Timeline Uncertainty CRQC emergence estimates range from 10-50+ years. If quantum error correction breakthroughs occur sooner than expected, timelines compress further.

Limitation 2: Evolving Standards NIST will continue standardizing additional algorithms. This research focuses on the first 4, but future algorithms may supersede them.

Limitation 3: Cost Estimates Migration cost estimates ($25-100B) are based on industry projections and could vary significantly depending on adoption speed and technological advances.

Limitation 4: Geopolitical Assumptions Analysis assumes US-China strategic competition continues. Geopolitical shifts could alter quantum technology sharing and standardization dynamics.

Limitation 5: No Primary Data This research relies on secondary sources (published papers, government reports, industry documentation). Future work should include primary data from enterprise pilots and government migration programs.

7. Conclusion

Quantum computing represents a paradigm shift in cybersecurity—not an incremental threat but a discontinuous leap that undermines the cryptographic foundations of modern digital infrastructure. The transition to post-quantum cryptography is not a question of “if” but “when,” and for many organizations, the answer is “now.”

Mosca's theorem provides a clear framework: if data must remain secure for longer than the migration time plus the time until CRQCs emerge, migration must begin immediately. For classified government data, healthcare records, and long-term financial instruments, this threshold has already been crossed.

The $25-100 billion global migration cost is substantial but necessary. The alternative—waiting for quantum computers to emerge before acting—risks catastrophic breaches that could expose decades of encrypted communications, financial transactions, and national security secrets.

Success requires coordinated action across governments, enterprises, researchers, and developers. NIST has provided the algorithmic foundation with CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+, and FALCON. Now begins the harder work: deploying these algorithms at scale, ensuring backward compatibility, training the workforce, and maintaining crypto agility for future threats.

The quantum future is uncertain, but the need to prepare is not. The organizations that act now will be protected. Those that wait may find their encrypted data—collected today, decrypted tomorrow—has become a liability they can never recover from.

Appendices

Appendix A: NIST PQC Algorithm Technical Details

A.1 CRYSTALS-Kyber (Key Encapsulation Mechanism)

Purpose: Secure key exchange (replaces RSA/ECDH in TLS)

Security Basis: Module Learning With Errors (MLWE) problem

Security Levels: - Kyber-512: AES-128 equivalent - Kyber-768: AES-192 equivalent - Kyber-1024: AES-256 equivalent

Key Characteristics: - Public key: ~800-1,600 bytes (vs RSA-2048: 256 bytes) - Ciphertext: ~700-1,500 bytes - Fast operations: <1ms on modern CPUs - Well-studied, high confidence

Use Cases: - TLS 1.3 key exchange (HTTPS) - VPN protocols (WireGuard, OpenVPN) - Secure messaging (Signal, WhatsApp) - Email encryption (PGP/GPG replacement)

A.2 CRYSTALS-Dilithium (Digital Signatures)

Purpose: Authenticate messages and code (replaces RSA/ECDSA signatures)

Security Basis: Module Learning With Errors (MLWE) + Fiat-Shamir transform

Security Levels: - Dilithium2: NIST Level 2 (~AES-128) - Dilithium3: NIST Level 3 (~AES-192) - Dilithium5: NIST Level 5 (~AES-256)

Key Characteristics: - Public key: ~1,300-2,600 bytes - Signature: ~2,400-4,600 bytes (vs ECDSA: 64 bytes) - Fast signing and verification - Deterministic (no randomness needed)

Use Cases: - Code signing (software updates) - Document signing (PDFs, contracts) - Blockchain/cryptocurrency signatures - TLS certificate authentication

A.3 SPHINCS+ (Hash-Based Signatures)

Purpose: Ultra-conservative signatures relying only on hash function security

Security Basis: Cryptographic hash functions (SHA-256, SHAKE-256)

Key Characteristics: - Public key: 32-64 bytes (small!) - Signature: 8,000-50,000 bytes (HUGE!) - Slow signing (~10-100ms) - Stateless (safe for multiple uses)

Advantages: - Only relies on hash function security (most conservative) - No complex math assumptions (lattices, number theory) - Long-term security confidence

Use Cases: - Firmware updates (signature size doesn't matter) - Certificate authorities (root CA signatures) - Long-term document archival - Backup/fallback signatures

A.4 FALCON (Fast Fourier Lattice-Based Compact Signatures)

Purpose: Compact signatures for constrained devices

Security Basis: NTRU lattices

Security Levels: - FALCON-512: NIST Level 1 (~AES-128) - FALCON-1024: NIST Level 5 (~AES-256)

Key Characteristics: - Public key: ~900 bytes - Signature: ~600-1,200 bytes (smallest PQC signature!) - Fast operations - Complex implementation (floating-point arithmetic)

Challenges: - Implementation complexity (more error-prone) - Side-channel vulnerabilities (timing attacks) - Less mature than Dilithium

Use Cases: - IoT devices (limited bandwidth) - Embedded systems - Mobile devices - Satellite communications

Appendix B: Mosca's Theorem Application Examples

Example 1: Classified Government Data - X = 50 years (Top Secret documents) - Y = 10 years (government infrastructure migration) - Z = 15 years (optimistic CRQC timeline) - **50 > 25** → Must start NOW

Example 2: Healthcare Records - X = 80 years (patient lifetime + 30 years) - Y = 15 years (medical device replacement cycles) - Z = 20 years (conservative CRQC timeline) - **80 > 35** → Must start NOW

Example 3: Financial Transactions - X = 10 years (credit card fraud prevention) - Y = 5 years (payment system upgrades) - Z = 15 years (optimistic CRQC timeline) - **10 < 20** → Can wait 5-10 years (but should plan now)

Example 4: Personal Emails - X = 5 years (typical email sensitivity) - Y = 2 years (email provider upgrades) - Z = 15 years (optimistic CRQC timeline) - **5 < 17** → Low urgency (but providers should upgrade proactively)

Appendix C: Quantum Computing Technical Primer

C.1 How Quantum Computers Work

Classical computers use **bits** (0 or 1). Quantum computers use **qubits** that can be in superposition (both 0 and 1 simultaneously).

Quantum Phenomena Exploited: 1. **Superposition:** Qubits exist in multiple states at once 2. **Entanglement:** Qubits influence each other instantaneously 3. **Interference:** Quantum states can amplify correct answers and cancel incorrect ones

C.2 Shor's Algorithm (RSA Breaking)

RSA security depends on factoring large composite numbers into their prime factors. For RSA-2048, this means factoring a 2048-bit number (617 decimal digits) into two primes.

Classical Factoring: - **Best algorithm:** General Number Field Sieve (GNFS) - **Time required:** Sub-exponential—faster than brute force but still infeasible - **For RSA-2048:** Estimated ~1 billion CPU-years - Even with all computers on Earth: Would take centuries - **Conclusion: Computationally infeasible**

Shor's Algorithm (Quantum): - **Time required:** Polynomial time—grows slowly as numbers get larger - **For RSA-2048:** ~8 hours with sufficient quantum hardware - **Hardware needed:** ~4,000 **logical** qubits (error-corrected) - Current technology (2025): ~1,000 noisy qubits - Gap: ~20,000x more qubits needed (requires ~20M physical qubits with current error rates) - **Timeline:** Feasible in 10-30 years once quantum error correction matures

The Key Insight: The shift from billions of years (classical) to hours (quantum) is a **discontinuous leap**—not incremental improvement but fundamental transformation. This is why RSA must be replaced entirely, not just strengthened. Shor's algorithm exploits the mathematical structure of factoring using quantum superposition and interference

C.3 Grover's Algorithm (Symmetric Crypto Weakening)

Symmetric encryption (like AES) can be broken by brute force—trying every possible key until finding the correct one.

Classical vs. Quantum Brute Force: - **Classical:** Must try ~2^n keys (where n = key length) - AES-128: 2^128 ≈ 340 undecillion attempts (infeasible) - **Grover's algorithm:** Reduces to ~2^(n/2) attempts using quantum search - AES-128: 2^64 ≈ 18 quintillion attempts (borderline) - AES-256: 2^128 ≈ 340 undecillion attempts (still secure)

Impact on AES Security:

Key Length	Classical Security	Quantum Security (Grover)	Status
AES-128	2^128 operations	2^64 operations	Borderline (64-bit security)

Key Length	Classical Security	Quantum Security (Grover)	Status
AES-256	2^256 operations	2^128 operations	✅ Secure (128-bit security)

The Solution: Simply **double key lengths** to compensate for Grover's square-root speedup. AES-256 becomes the standard for quantum-resistant symmetric encryption. Unlike RSA/ECC, symmetric crypto doesn't need replacement—just longer keys.

Key Difference from Shor's Algorithm: - **Shor:** Exponential speedup → RSA completely broken (catastrophic threat) - **Grover:** Quadratic speedup → AES weakened but manageable (easily fixed by doubling key length)

Appendix D: Sector Migration Cost Breakdown

D.1 Financial Services ($10-20 billion)

Cost Category	Estimate	Notes
Hardware Replacement (ATMs, HSMs)	$8-12B	~500K ATMs globally @ $16-24K each
Software Updates (Core Banking)	$2-3B	TLS libraries, payment processors
Compliance & Auditing	$500M-1B	PCI-DSS, SOX requirements
Training & Certification	$500M-1B	Developer training, security teams

D.2 Healthcare ($5-10 billion)

Cost Category	Estimate	Notes
Medical Device Replacement	$3-5B	Pacemakers, insulin pumps, imaging
EHR Software Updates	$1-2B	Epic, Cerner, proprietary systems
HIPAA Compliance	$500M-1B	Privacy audits, breach prevention
Training	$500M-1B	Clinical staff, IT teams

D.3 Government/Defense ($15-25 billion)

Cost Category	Estimate	Notes
Classified Systems	$10-15B	Top Secret / SCI networks
Unclassified Systems	$3-5B	.mil domains, civilian agencies

Cost Category	Estimate	Notes
Allied Coordination	$2-5B	NATO, Five Eyes interoperability

D.4 Critical Infrastructure ($15-25 billion)

Cost Category	Estimate	Notes
Power Grid	$5-10B	SCADA, smart meters, substations
Water/Wastewater	$2-5B	Industrial control systems
Transportation	$3-5B	Traffic control, railway signaling
Telecommunications	$5-10B	5G networks, fiber backbones

Appendix E: Interview Questions for Industry Mentor

E.1 Background & Context

1. What is your experience with post-quantum cryptography? (if not confidential)
2. How serious does industry consider the quantum threat? What timeline are you planning for?
3. What are the biggest challenges you foresee in PQC migration?
4. Should I focus more on technical analysis (algorithms) or policy implications (migration strategies)?
5. Are there specific sectors or use cases you think I should prioritize?

E.2 Technical Deep Dive

1. I estimated CRQCs will emerge in 10-20 years. Does this align with industry assessment?
2. What data does the industry consider at risk from “harvest now, decrypt later” attacks?
3. What are the practical limitations of NIST algorithms in consumer devices (iPhones, MacBooks)?
4. How does industry evaluate side-channel vulnerabilities in PQC implementations?
5. What is the impact of PQC to your services?
6. What is your biggest challenge in supporting PQC?
7. How does PQC impact your HSM strategy?

E.3 Strategic & Policy

1. I developed migration roadmaps for finance, healthcare, defense, and infrastructure. Are these realistic?
2. Are my cost estimates ($25-100B globally) reasonable?
3. How do export controls affect global PQC adoption?
4. Should PQC be a global standard or allow national variations?
5. What skills should I develop to work on quantum-safe cryptography in the future?

Appendix F: Bibliography (Extended)

Quantum Computing Fundamentals: 1. Shor, P. W. (1994). “Algorithms for quantum computation: Discrete logarithms and factoring.” *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124-134. 2. Grover, L. K. (1996). “A fast quantum mechanical algorithm for database search.” *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 212-219. 3. Mosca, M. (2018). “Cybersecurity in an era with quantum computers: Will we be ready?” *IEEE Security & Privacy*, 16(5), 38-41. 4. Preskill, J. (2018). “Quantum Computing in the NISQ era and beyond.” *Quantum*, 2, 79.

Post-Quantum Cryptography: 5. NIST (2024). “Post-Quantum Cryptography Standardization: Selected Algorithms.” National Institute of Standards and Technology. 6. Alagic, G., et al. (2024). “Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process.” NIST IR 8413. 7. Bernstein, D. J., & Lange, T. (2017). “Post-quantum cryptography.” *Nature*, 549(7671), 188-194. 8. Chen, L., et al. (2016). “Report on Post-Quantum Cryptography.” NIST IR 8105.

NIST PQC Algorithms: 9. Bai, S., et al. (2024). “CRYSTALS-Kyber Algorithm Specifications And Supporting Documentation.” NIST PQC Round 4. 10. Ducas, L., et al. (2024). “CRYSTALS-Dilithium Algorithm Specifications And Supporting Documentation.” NIST PQC Round 4. 11. Bernstein, D. J., et al. (2024). “SPHINCS+: Stateless Hash-Based Signatures.” NIST PQC Round 4. 12. Fouque, P.-A., et al. (2024). “FALCON: Fast-Fourier Lattice-based Compact Signatures over NTRU.” NIST PQC Round 4.

Lattice Cryptography: 13. Peikert, C. (2016). “A decade of lattice cryptography.” *Foundations and Trends in Theoretical Computer Science*, 10(4), 283-424. 14. Regev, O. (2009). “On lattices, learning with errors, random linear codes, and cryptography.” *Journal of the ACM*, 56(6), 1-40.

Policy & National Security: 15. NSA (2022). “Announcing the Commercial National Security Algorithm Suite 2.0.” National Security Agency. 16. CISA (2024). “Post-Quantum Cryptography Initiative.” Cybersecurity and Infrastructure Security Agency. 17. European Commission (2023). “Quantum Technologies Flagship: Strategic Research Agenda.” 18. National Quantum Initiative Act (2018). Public Law 115-368.

Industry Reports: 19. IBM (2024). “IBM Quantum Development Roadmap.” IBM Quantum Computing. 20. Google Quantum AI (2023). “Quantum supremacy using a programmable superconducting processor.” *Nature*, 574, 505-510. 21. Gartner (2024). “Hype Cycle for Quantum Computing, 2024.” 22. National Academies (2019). “Quantum Computing: Progress and Prospects.” National Academies Press.

Migration & Implementation: 23. Cloudflare (2024). “Experimenting with Post-Quantum Cryptography in TLS.” Cloudflare Blog. 24. Google (2023). “CECPQ2: Post-Quantum Key Agreement in Chrome.” Google Security Blog. 25. Sikeridis, D., Kampanakis, P., & Devetsikiotis, M. (2020). “Post-Quantum Authentication in TLS 1.3: A Performance Study.” *NDSS 2020*.

Economic & Geopolitical: 26. Atlantic Council (2023). “The Geopolitics of Quantum Computing.” 27. RAND Corporation (2022). “The Commercial and National Security Implications of Quantum Computing.” 28. Gheorghiu, V., & Mosca, M. (2019). “Benchmarking the quantum cryptanalysis of symmetric, public-key and hash-based cryptographic schemes.” arXiv:1902.02332.

Additional Technical Resources: 29. NIST SP 800-208: “Recommendation for Stateful Hash-Based Signatures” 30. ETSI Quantum-Safe Cryptography Specifications 31. IETF PQC Working Group Drafts

Appendix G: Technical Glossary

Complexity Terms: - **Polynomial time:** Algorithm runtime grows slowly (n^2, n^3); considered efficient - **Exponential time:** Runtime doubles with each bit; quickly infeasible (2^128 = 340 undecillion operations) - **Sub-exponential:** Faster than exponential, slower than polynomial; still infeasible for large inputs - **NP-hard:** No known efficient algorithm; lattice problems (basis for PQC) are NP-hard

Cryptographic Systems: - **Public-key crypto:** Two keys (public + private); RSA/ECC vulnerable to Shor's algorithm; Kyber/Dilithium quantum-resistant - **Symmetric crypto:** One shared key; AES-128 weakened to 64-bit security (Grover); AES-256 remains secure - **Digital signatures:** Proves message authenticity; RSA/ECDSA vulnerable; Dilithium/SPHINCS+/FALCON quantum-safe

Quantum Terms: - **Qubit:** Quantum bit in superposition (0 and 1 simultaneously); enables quantum parallelism - **Logical qubit:** Error-corrected qubit (~1,000-10,000 physical qubits each) - **CRQC:** Cryptographically-Relevant Quantum Computer; ~4,000 logical qubits needed to break RSA-2048 - **Quantum supremacy:** Quantum computer solves problem classical can't (achieved 2019; not yet cryptographically relevant)

Post-Quantum Algorithms: - **Lattice crypto:** Security based on hard problems in high-dimensional grids; basis for Kyber/Dilithium/FALCON - **Learning With Errors (LWE):** Solving noisy linear equations; exponentially hard even for quantum computers - **Hash-based signatures:** Security relies only on hash functions (SHA-256); ultra-conservative (SPHINCS+)

Security Levels: - **64-bit security:** 2^64 ≈ 18 quintillion operations (borderline; AES-128 under Grover) - **128-bit security:** 2^128 ≈ 340 undecillion operations (very secure; AES-256 under Grover) - **256-bit security:** 2^256 operations (overkill but future-proof)

Acknowledgments

This research was conducted under the mentorship of an Apple Director (name confidential) whose expertise in cryptographic systems and enterprise security architecture provided invaluable guidance. I am grateful to Dr. Natasha Mancuso, EdD (Foothill College, Stanford Global Studies Fellow) for her mentorship on academic research methodology developed during my AI in Education research, which informed the analytical framework for this study.

I thank the NIST Post-Quantum Cryptography team for their publicly accessible documentation and the cryptography research community for maintaining open-access publications that enabled this independent research.

All errors and omissions remain my own.

Author Bio

Driti Virani is a high school senior (Class of 2026) at Evergreen Valley High School in San Jose, California. As CEO and founder of TeachNova, an AI-powered education platform reaching 200+ educators across 5+ countries, she bridges technology and social impact. Her research interests span AI in education, post-quantum cryptography, and the ethical implications of emerging technologies. She serves as Senior Programmer for her FTC robotics team (2x Control Award winner, Motivate Award 2025) and Vice President of Physics and Astronomy clubs. She is an AP Scholar with Distinction and National French Contest Gold Medalist (2025).

Contact: viranidriti@gmail.com **Website:** https://driti.page **Research Portfolio:** https://driti.page/research.html

END OF PAPER