Review

Quantum Readiness in Cryptography: A Maturity-Based Framework for Post-Quantum Transition

Volkan Erol *

Posted Date: 2 October 2025

doi: 10.20944/preprints202509.2584.v1

Keywords: post-quantum cryptography; quantum readiness; lattice-based cryptography; NIST PQC standards; crypto-agility; maturity model; implementation security; cryptographic migration

 doi:10.20944/preprints202509.2584.v1

Review

Quantum Readiness in Cryptography: A Maturity-Based Framework for Post-Quantum Transition

Volkan Erol

Turkish Economy Bank – TEB, Turkey; volkan.erol@gmail.com

Abstract

Quantum computing poses an existential threat to public-key cryptography, with Shor's algorithm capable of breaking RSA and elliptic curve systems once cryptographically relevant quantum computers (CRQCs) emerge. While post-quantum cryptography (PQC) offers algorithmic solutions, organizational readiness extends beyond technical implementation to encompass governance, interoperability, and adaptive capacity. This review synthesizes the quantum threat landscape, evaluates NIST-standardized PQC algorithms through quantitative performance analysis, and examines global standardization dynamics. We introduce a novel **Quantum Readiness Maturity Model (QRMM)** that enables organizations to assess and advance their preparedness across five dimensions: cryptographic infrastructure, governance frameworks, sectoral adaptation, interoperability resilience, and strategic agility. Applying this model to finance, telecommunications, and defense sectors reveals systematic gaps in migration planning and crypto-agility. Our analysis demonstrates that quantum readiness requires treating cryptographic transformation as a strategic enterprise capability rather than a purely technical upgrade. The proposed framework provides actionable pathways for practitioners while identifying critical research directions in hybrid deployment strategies, post-quantum PKI architectures, and algorithmic diversity.

Keywords: post-quantum cryptography; quantum readiness; lattice-based cryptography; NIST PQC standards; crypto-agility; maturity model; implementation security; cryptographic migration

---

1. Introduction

1.1. The Quantum Threat to Cryptographic Foundations

Modern cybersecurity relies on computational hardness assumptions that quantum algorithms fundamentally undermine. Shor's algorithm [1] provides polynomial-time solutions to integer factorization and discrete logarithms, threatening RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC)—systems that secure trillions of dollars in transactions, government communications, and digital identities. While large-scale quantum computers capable of breaking 2048-bit RSA remain years away, recent resource estimates suggest that 20 million noisy qubits could factor such keys within hours [2], placing the threat horizon within a plausible 10-15 year window [3].

The **harvest-now-decrypt-later (HNDL)** threat model intensifies urgency: adversaries can capture encrypted data today and decrypt it once quantum capabilities mature [4]. For data with multi-decade confidentiality requirements—medical records, state secrets, financial archives—protection must begin immediately. Grover's algorithm [5] further reduces symmetric key security by half (e.g., AES-128 → ~64-bit effective security), requiring key size adjustments across all cryptographic primitives.

 doi:10.20944/preprints202509.2584.v1

The quantum threat is not uniform across cryptosystems: while Shor's algorithm threatens RSA, ECC, and Diffie–Hellman, Grover's algorithm only weakens symmetric primitives. Figure 1 summarizes this landscape.

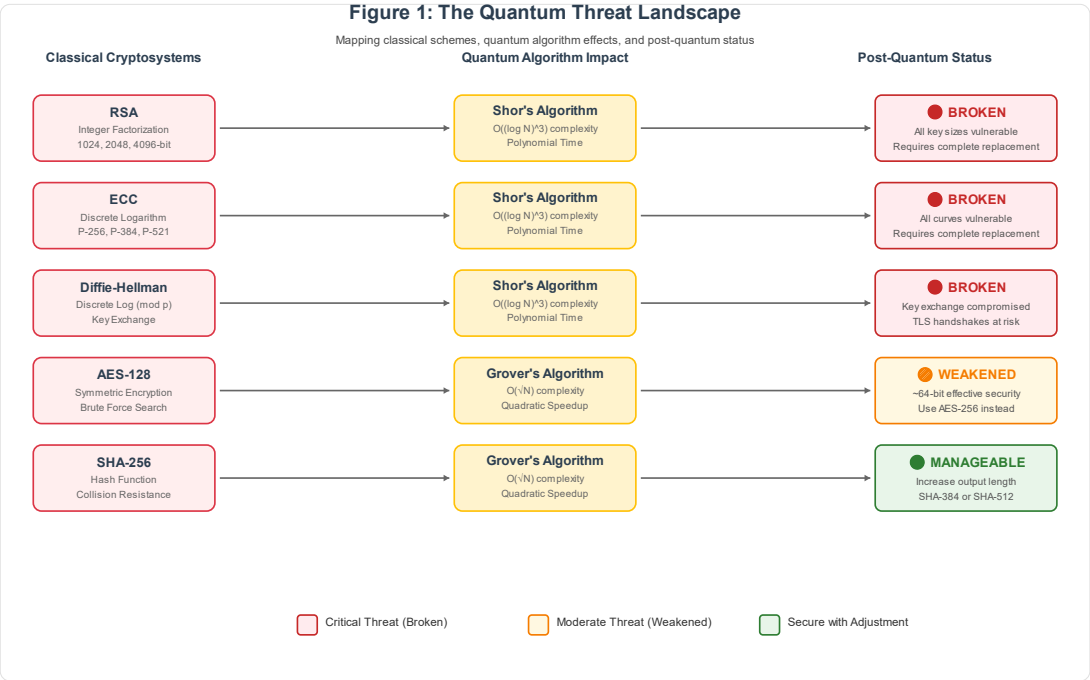

Figure 1. caption.

1.2. Post-Quantum Cryptography: From Theory to Practice

Post-quantum cryptography (PQC) has emerged as the leading defense strategy, with the NIST PQC Standardization Project [6] finalizing four quantum-resistant algorithms in 2024: CRYSTALS-Kyber (key encapsulation), CRYSTALS-Dilithium (digital signatures), Falcon (compact signatures), and SPHINCS+ (hash-based signatures). These algorithms rest on mathematical problems believed resistant to both classical and quantum attacks—primarily lattice problems (Learning With Errors) and hash function properties [7,8].

However, deploying these algorithms represents only the first step. Real-world adoption faces substantial challenges: performance overheads (larger key sizes, slower operations), integration with legacy infrastructure (TLS, PKI, hardware security modules), standardization fragmentation across regions [9], and the organizational capacity to adapt as standards evolve—termed **crypto-agility** [10,11].

1.3. Research Gap and Contribution

Existing literature addresses either technical algorithm design [12,13] or high-level policy considerations [14,15], but rarely integrates these perspectives into an actionable framework. Practitioners lack systematic methods to assess organizational readiness, prioritize migration efforts, or measure progress. This creates three critical gaps:

1. **Assessment Gap**: No standardized methodology exists for evaluating organizational quantum readiness across technical, governance, and strategic dimensions.
2. **Implementation Gap**: Performance comparisons lack quantitative benchmarks that account for real-world constraints (latency requirements, bandwidth limits, computational resources).

 doi:10.20944/preprints202509.2584.v1

3. **Sectoral Gap**: Generic guidance fails to address sector-specific requirements in finance, telecommunications, defense, and healthcare, each with distinct threat models and operational constraints.

1.4. Contributions of This Work

This paper makes four principal contributions:

1. **Quantum Readiness Maturity Model (QRMM)**: We introduce a five-level maturity framework spanning cryptographic infrastructure, governance, sectoral adaptation, interoperability, and strategic agility. This model enables systematic assessment and provides clear advancement pathways.
2. **Quantitative Algorithm Analysis**: We present comparative performance metrics for NIST-standardized PQC algorithms, including key/signature sizes, computational costs, and implementation security considerations, enabling evidence-based deployment decisions.
3. **Sectoral Implementation Framework**: We develop sector-specific readiness profiles for finance, telecommunications, and defense, identifying unique challenges and proposing tailored migration strategies.
4. **Strategic Interoperability Analysis**: We examine geopolitical dynamics in PQC standardization (NIST, ETSI, China) and their implications for multinational organizations, providing guidance for navigating fragmented standards landscapes.

The remainder of this paper is structured as follows: Section 2 analyzes the quantum threat; Section 3 evaluates PQC algorithms; Section 4 examines global standards; Section 5 introduces the QRMM framework; Section 6 addresses implementation challenges; Section 7 discusses strategic implications; and Section 8 concludes with research directions.

2. Quantum Threat Analysis

2.1. Shor's Algorithm: Breaking Public-Key Cryptography

Shor's algorithm [1] exploits quantum superposition and interference to solve integer factorization and discrete logarithm problems in polynomial time $O((\log N)^3)$, compared to sub-exponential classical algorithms. For RSA-2048, classical attacks require ~2^{112} operations; Shor's algorithm reduces this to ~10^9 quantum gates [2].

Resource Requirements: Recent estimates suggest factoring RSA-2048 requires approximately 20 million noisy qubits with error rates below 10^{-3}, operating for several hours [2]. Current systems (IBM's 1,121-qubit Condor, Google's 70-qubit Sycamore) fall orders of magnitude short. However, projections from major quantum computing roadmaps (IBM, Google, IonQ) suggest error-corrected systems with millions of logical qubits could emerge by 2035-2040 [3,16].

Impact Assessment:

- **RSA**: All key sizes (1024, 2048, 4096-bit) become vulnerable once CRQCs arrive
- **ECC**: Shorter keys (256-bit ECC ≈ 128-bit classical security) break even faster
- **Diffie-Hellman**: Key exchange protocols compromised, affecting TLS handshakes globally
- **Digital Signatures**: ECDSA, EdDSA become forgeable, undermining authentication

2.2. Grover's Algorithm: Weakening Symmetric Cryptography

Grover's algorithm [5] provides quadratic speedup for unstructured search, reducing an N-element search from $O(N)$ to $O(\sqrt{N})$. For symmetric encryption:

- **AES-128**: Effective security reduced from 128-bit → ~64-bit
- **AES-256**: Remains secure at ~128-bit effective security
- **SHA-256**: Collision resistance weakened but remains practical

 doi:10.20944/preprints202509.2584.v1

Mitigation Strategy: Doubling key lengths (AES-128 → AES-256) and increasing hash outputs suffices for symmetric primitives [17]. This represents a far simpler transition than replacing public-key systems.

2.3. Harvest-Now-Decrypt-Later (HNDL) Threat Model

The HNDL attack paradigm [4,18] assumes adversaries:

1. Intercept and store encrypted communications today
2. Retain ciphertexts until quantum capabilities mature
3. Decrypt historical data once CRQCs become available

Risk Timeline Analysis:

Data Type	Confidentiality Lifetime	HNDL Risk Window	Mitigation Urgency
Government classified	30-50 years	High (immediate threat)	Critical
Medical records (HIPAA)	25+ years	High	Critical
Financial transactions	7-10 years	Medium	High
Personal communications	1-5 years	Low	Moderate
Ephemeral messaging	< 1 year	Negligible	Low

Organizations managing long-lived sensitive data must transition to PQC **before** CRQCs emerge, not after. This shifts the threat timeline from "years-to-quantum" to "years-of-data-longevity" [19].

2.4. Quantum Computing Progress and Timeline Uncertainty

Current State (2025):

- Largest systems: ~1,000 physical qubits (IBM, Google)
- Error rates: 10^{-3} to 10^{-2} (far above fault-tolerance threshold of ~10^{-6})
- No demonstration of cryptographically relevant calculations

Projected Milestones:

- **2028-2030**: 10,000 logical qubits with basic error correction [3]
- **2035-2040**: ~1 million logical qubits (NIST "moderate confidence" CRQC window) [20]
- **2040-2050**: Mature fault-tolerant systems (conservative estimates) [21]

Key Uncertainty Factors:

- Breakthrough in error correction codes (e.g., surface codes, topological qubits)
- Advances in qubit coherence times and gate fidelities
- Scaling challenges in cryogenic systems and control electronics
- Potential for classified progress exceeding public knowledge

Given this uncertainty, organizations face a strategic dilemma: invest heavily now versus wait for clearer timelines. The HNDL threat model and long data lifetimes argue for **proactive migration** under a precautionary principle [22].

2.5. Threat Summary and Strategic Implications

Figure 1 (see figure definitions below) visualizes the quantum threat landscape, showing how Shor's and Grover's algorithms impact different cryptographic primitives. The key strategic insight: **asymmetric impact across cryptographic families**. Public-key systems require complete replacement; symmetric systems need parameter adjustments. This asymmetry shapes migration priorities and resource allocation.

 doi:10.20944/preprints202509.2584.v1

3. Post-Quantum Cryptography Algorithm Landscape

3.1. NIST PQC Standardization Process

The NIST PQC project [6] began in 2016, evaluating 82 initial submissions through three competitive rounds. In July 2022, NIST announced four algorithms for standardization, with final Federal Information Processing Standards (FIPS) released in August 2024 [23]:

Selected Algorithms:

1. **CRYSTALS-Kyber** (renamed ML-KEM): Key encapsulation mechanism
2. **CRYSTALS-Dilithium** (ML-DSA): General-purpose digital signatures
3. **Falcon** (FN-DSA): Compact digital signatures for constrained environments
4. **SPHINCS+** (SLH-DSA): Hash-based signatures (conservative fallback)

A fourth round continues for additional code-based schemes (Classic McEliece, BIKE) to ensure algorithmic diversity [24].

3.2. Algorithm Families and Mathematical Foundations

3.2.1. Lattice-Based Cryptography

Foundation: Security rests on the hardness of Learning With Errors (LWE) and its variants (Ring-LWE, Module-LWE) [25,26]. These problems involve finding short vectors in high-dimensional lattices—a task believed intractable for both classical and quantum computers.

CRYSTALS-Kyber (ML-KEM) [27]:

- **Purpose**: Key encapsulation for establishing shared secrets (replaces RSA/ECDH in TLS)
- **Key Sizes**: Public key: 800-1,568 bytes; Ciphertext: 768-1,568 bytes
- **Performance**: Encapsulation ~150 μs; Decapsulation ~200 μs (on 3.0 GHz Intel CPU)
- **Security Levels**: Three variants (ML-KEM-512, -768, -1024) equivalent to AES-128, -192, -256

CRYSTALS-Dilithium (ML-DSA) [28]:

- **Purpose**: Digital signatures for authentication and non-repudiation
- **Signature Size**: 2,420-4,595 bytes (vs. 64 bytes for ECDSA-256)
- **Performance**: Signing ~370 μs; Verification ~180 μs
- **Trade-off**: Larger signatures but straightforward implementation

Falcon (FN-DSA) [29]:

- **Purpose**: Compact signatures for bandwidth-constrained applications
- **Signature Size**: 666-1,280 bytes (significantly smaller than Dilithium)
- **Performance**: Signing ~1,700 μs (slower due to floating-point operations)
- **Implementation Challenge**: Requires careful constant-time implementation to resist timing attacks

3.2.2. Hash-Based Cryptography

SPHINCS+ (SLH-DSA) [30]:

- **Foundation**: Security derived from hash function properties (collision/preimage resistance)
- **Advantage**: No unproven hardness assumptions; conservative security profile
- **Signature Size**: 7,856-49,856 bytes (largest among NIST selections)
- **Performance**: Signing ~6,000-40,000 μs; Verification ~2,000-10,000 μs
- **Use Case**: Long-term security where space/speed are secondary concerns

3.2.3. Code-Based Cryptography

Classic McEliece [31] (Round 4 alternate candidate):

 doi:10.20944/preprints202509.2584.v1

- **Foundation**: Decoding random linear codes (50+ years of cryptanalysis)
- **Public Key Size**: 261 KB to 1.3 MB (prohibitive for most applications)
- **Advantage**: Oldest and most conservative PQC approach
- **Status**: Continues evaluation for specialized use cases (government, long-term archives)

3.3. Quantitative Performance Comparison

Key Observations:

1. **Key Size Penalty**: PQC public keys are 3-15× larger than ECC, but smaller than RSA
2. **Signature Inflation**: Dilithium signatures are ~50× larger than ECDSA; Falcon offers ~10× overhead
3. **Computational Efficiency**: Kyber and Dilithium match or exceed RSA performance; Falcon and SPHINCS+ are slower
4. **Trade-off Spectrum**: No single algorithm optimizes all metrics; deployment choices must prioritize based on constraints

Table 1. presents comprehensive performance metrics for NIST-standardized algorithms:.

Algorithm	Type	Public Key (bytes)	Signature/Ciphertext (bytes)	Keygen (µs)	Sign/Encap (µs)	Verify/Decap (µs)	Security Level
ML-KEM-768	KEM	1,184	1,088	120	150	200	AES-192 equiv
ML-DSA-65	Sig	1,952	3,309	250	370	180	AES-192 equiv
FN-DSA-512	Sig	897	666	1,100	1,700	900	AES-128 equiv
SLH-DSA-128f	Sig	32	7,856	800	6,200	2,100	AES-128 equiv
ECDSA-256	*Sig*	*64*	*64*	*50*	*70*	*90*	*AES-128 equiv*
RSA-2048	*Both*	*256*	*256*	*50,000*	*200*	*5*	*AES-112 equiv*

Classical algorithms shown in italics for comparison. Performance measured on Intel Core i7-10710U @ 3.0 GHz. Sources: [32,33,34].

3.4. Implementation Security Considerations

Beyond algorithmic security, real-world implementations face side-channel and fault-injection attacks [35,36]:

Timing Attacks: Variable-time operations leak secret information through execution duration. Mitigation requires constant-time implementations—challenging for Falcon's floating-point arithmetic [37].

Power Analysis: Differential power analysis (DPA) can extract keys from embedded devices. Countermeasures include masking and randomization, increasing computational overhead by 2-5× [38].

Fault Injection: Inducing errors during signing can leak private keys. SPHINCS+ is inherently resistant; lattice schemes require careful validation [39].

Hardware Acceleration: NIST algorithms are being integrated into cryptographic accelerators (Intel IPP, ARM Cryptography Extensions) to improve performance while maintaining constant-time guarantees [40].

3.5. Algorithmic Diversity as Risk Mitigation

 doi:10.20944/preprints202509.2584.v1

Concentrating on a single mathematical family (lattice-based) creates systemic risk: a breakthrough in lattice cryptanalysis could compromise multiple algorithms simultaneously. NIST's strategy emphasizes diversity [41]:

- **Lattice-based**: Kyber, Dilithium, Falcon (primary deployments)
- **Hash-based**: SPHINCS+ (conservative fallback)
- **Code-based**: Classic McEliece (under continued evaluation)
- **Multivariate**: Withdrawn after cryptanalytic breaks (Rainbow, GeMSS) [42]
- **Isogeny-based**: SIKE broken in 2022; research continues on alternative constructions [43]

Organizations deploying PQC should maintain **hybrid strategies** (classical + PQC) during transition and consider **multi-algorithm deployments** for critical systems [44].

4. Global Standardization and Interoperability Dynamics

4.1. NIST Leadership and Global Influence

The NIST PQC process has established de facto global standards, with adoption by major technology companies (Google, Microsoft, AWS) and integration into IETF protocols (TLS 1.3, IPsec) [45,46]. However, regional initiatives create a complex interoperability landscape.

4.2. European Initiatives

ETSI Quantum-Safe Cryptography Working Group [47]:

- Publishes white papers and technical specifications since 2015
- Emphasizes backward compatibility and hybrid approaches
- Aligns closely with NIST but maintains independent evaluation

ENISA (EU Cybersecurity Agency) [48]:

- Issues risk assessment frameworks for EU member states
- Coordinates with national agencies (ANSSI in France, BSI in Germany)
- Focus on GDPR compliance and cross-border data protection

EU Quantum Flagship [49]:

- €1 billion initiative combining PQC with quantum key distribution (QKD)
- EuroQCI project: quantum communication infrastructure across Europe
- Strategy: Layer PQC and QKD for defense-in-depth

4.3. China's Dual-Path Strategy

China pursues parallel development of PQC and QKD [50,51]:

- **PQC Research**: Active participation in NIST process; independent algorithm development
- **QKD Infrastructure**: Extensive deployment (Micius satellite, Beijing-Shanghai network)
- **Strategic Goal**: Technological sovereignty and reduced dependence on Western cryptographic standards

Interoperability Challenge: Chinese systems may require dual PQC/QKD compliance, complicating multinational deployments [52].

4.4. Japan and Asia-Pacific

Japan's PQC Roadmap [53]:

- NICT and MIC coordinate national strategy
- Focus on IoT security and 6G infrastructure
- Active participation in ITU standardization

 doi:10.20944/preprints202509.2584.v1

South Korea and Singapore: Developing national guidelines aligned with NIST but incorporating ETSI recommendations [54,55].

4.5. Interoperability Risks and Fragmentation

Geopolitical Implications:

- Multinational corporations must support multiple standards simultaneously
- Export controls may restrict PQC technology transfer to certain regions
- Trust frameworks for international finance and trade require consensus on cryptographic baselines [56]

Table 2. summarizes regional standardization approaches:.

Region	Leading Body	Primary Strategy	Standards Timeline	Interoperability Risk
North America	NIST	PQC algorithms (ML-KEM, ML-DSA)	FIPS finalized 2024	Low (global leader)
Europe	ETSI/ENISA	PQC + hybrid classical	Alignment with NIST	Low-Medium (minor variants)
China	State Council	PQC + QKD dual-path	National rollout 2025+	High (divergent architecture)
Japan	NICT/MIC	PQC for IoT/6G	Pilots 2025-2027	Medium (sectoral focus)
International	ISO/IEC JTC 1/SC 27	Harmonization efforts	Ongoing	Coordination challenge

4.6. Hybrid Cryptography as Transitional Strategy

Given uncertainty around PQC algorithm security and CRQC timelines, hybrid approaches combine classical and post-quantum primitives [57]:

TLS 1.3 Hybrid Key Exchange:

Shared_Secret = KDF(ECDH_Secret || ML-KEM_Secret)

Security guarantee: System remains secure if **either** classical or PQC component is unbroken [58].

Advantages:

- Backward compatibility with legacy systems
- Hedges against unexpected PQC vulnerabilities
- Gradual deployment without flag-day transitions

Challenges:

- Increased computational and bandwidth costs
- Complex key management and certificate infrastructure
- Potential for downgrade attacks if not carefully designed [59]

5. The Quantum Readiness Maturity Model (QRMM)

5.1. Motivation and Framework Design

Existing guidance on PQC migration focuses on technical steps (algorithm selection, implementation testing) but lacks a holistic assessment methodology. Organizations need a structured framework to:

1. **Assess** current readiness across multiple dimensions
2. **Identify** gaps and prioritize investments
3. **Track** progress as migration unfolds
4. **Adapt** to evolving standards and threat landscapes

 doi:10.20944/preprints202509.2584.v1

To assess sectoral preparedness, we introduce the Quantum Readiness Maturity Model (QRMM), structured along five dimensions. As illustrated in Figure 2, defense and government sectors are significantly ahead of healthcare in readiness.

We introduce the **Quantum Readiness Maturity Model (QRMM)**—a five-level framework spanning five critical dimensions:

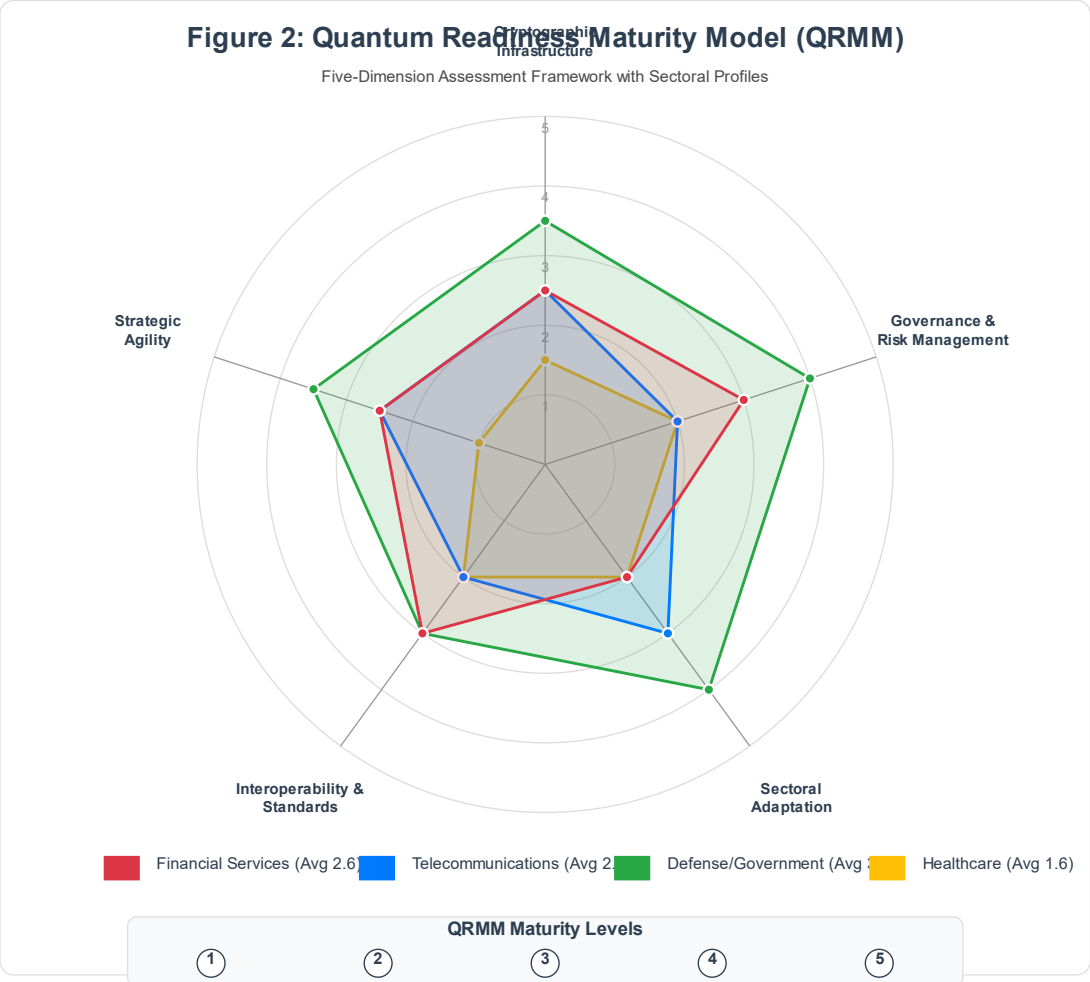

Figure 2. caption.

5.2. QRMM Dimensions

Dimension 1: Cryptographic Infrastructure

- Discovery and inventory of cryptographic assets (algorithms in use, key sizes, certificate lifetimes)
- Testing PQC algorithms in non-production environments
- Hybrid deployment capabilities
- Integration with PKI, HSMs, and key management systems

Dimension 2: Governance and Risk Management

- Executive awareness and strategic alignment
- Budget allocation and resource planning
- Risk assessment frameworks (HNDL threat modeling)
- Compliance with regulatory mandates (HIPAA, GDPR, defense classifications)

Dimension 3: Sectoral Adaptation

- Understanding sector-specific threat models (finance vs. healthcare vs. telecom)

 doi:10.20944/preprints202509.2584.v1

- Performance requirements (latency, throughput, computational constraints)
- Legacy system constraints and migration timelines
- Vendor ecosystem readiness

Dimension 4: Interoperability and Standards Compliance

- Alignment with NIST, ETSI, or regional standards
- Support for multiple PQC algorithms (algorithmic agility)
- Cross-border data flow requirements
- Protocol compatibility (TLS, IPsec, S/MIME)

Dimension 5: Strategic Agility

- Modular cryptographic libraries enabling algorithm replacement
- Automated cryptographic policy management
- Incident response plans for cryptographic failures
- Continuous monitoring and threat intelligence integration

5.3. Maturity Levels

Each dimension progresses through five maturity levels:

Level 1 - Initial (Ad Hoc):

- Minimal awareness of quantum threat
- No cryptographic inventory
- Reactive approach to security updates

Level 2 - Developing (Awareness):

- Executive awareness and initial planning
- Pilot projects testing PQC algorithms
- Basic cryptographic asset discovery

Level 3 - Defined (Implementation):

- Formal PQC migration roadmap
- Hybrid cryptography deployed in production
- Governance frameworks established
- Vendor partnerships for PQC-enabled products

Level 4 - Managed (Optimization):

- PQC integrated across critical systems
- Automated cryptographic lifecycle management
- Continuous compliance monitoring
- Performance optimization and tuning

Level 5 - Adaptive (Strategic Agility):

- Cryptographic infrastructure as strategic capability
- Real-time algorithm switching based on threat intelligence
- Multi-algorithm deployments for resilience
- Contribution to standards development and industry leadership

5.4. QRMM Assessment Methodology

Figure 2 (see figure definitions below) visualizes the QRMM framework as a radar chart showing organizational profiles across the five dimensions.

Assessment Process:

1. **Self-Assessment**: Organizations rate themselves (1-5) on each dimension using detailed rubrics
2. **Gap Analysis**: Compare current state against target maturity levels (typically Level 3-4 for most enterprises)
3. **Prioritization**: Identify high-impact, feasible improvements
4. **Roadmap Development**: Define quarterly milestones and KPIs
5. **Continuous Improvement**: Reassess annually or after major standard updates

Example Assessment Rubric (Dimension 1: Cryptographic Infrastructure):

 doi:10.20944/preprints202509.2584.v1

Level	Cryptographic Discovery	PQC Testing	Hybrid Deployment	PKI Integration
1	No inventory	None	Not considered	Manual certificate mgmt
2	Partial inventory (known apps)	Lab experiments	Evaluated but not deployed	Basic automated PKI
3	Comprehensive inventory	Pilot in staging	Hybrid in non-critical systems	PQC-aware PKI pilots
4	Automated discovery & tracking	Production testing	Hybrid in all critical systems	Full PQC PKI integration
5	Real-time monitoring & alerting	A/B testing in production	Multi-algorithm resilience	Agile certificate lifecycle

5.5. Sectoral Application of QRMM

5.5.1. Financial Services

Threat Profile: High HNDL risk due to long-lived transaction records; regulatory compliance pressure; global interoperability requirements.

Typical Maturity Assessment (2025 baseline):

- **Cryptographic Infrastructure**: Level 2-3 (pilots underway, but production deployment limited)
- **Governance**: Level 3 (regulatory mandates driving formal planning)
- **Sectoral Adaptation**: Level 2 (performance concerns around high-frequency trading)
- **Interoperability**: Level 3 (SWIFT and card networks coordinating)
- **Strategic Agility**: Level 2 (modular architectures emerging)

Recommended Actions:

1. Accelerate hybrid TLS deployment for inter-bank communications
2. Establish PQC-enabled digital signature services for transaction authentication
3. Engage with payment networks (SWIFT, Visa, Mastercard) on standardized timelines
4. Develop quantum threat scenario planning for risk management frameworks

Case Study: A multinational bank deployed ML-KEM hybrid key exchange in their treasury management systems, achieving <5ms latency overhead while future-proofing against HNDL attacks [60].

5.5.2. Telecommunications

Threat Profile: Critical infrastructure target; latency-sensitive operations (5G/6G); massive scale (billions of devices).

Typical Maturity Assessment:

- **Cryptographic Infrastructure**: Level 2-3 (3GPP standards in development)
- **Governance**: Level 2 (strategic importance recognized but planning fragmented)
- **Sectoral Adaptation**: Level 3 (active integration in 6G research)
- **Interoperability**: Level 2 (international standards coordination slow)
- **Strategic Agility**: Level 2 (legacy network equipment constrains flexibility)

Recommended Actions:

1. Prioritize PQC in network core (authentication servers, base station controllers)
2. Develop lightweight PQC variants for IoT devices (resource-constrained endpoints)
3. Collaborate with 3GPP, ITU-T on standardized PQC integration
4. Plan phased migration aligned with equipment refresh cycles (5-7 years)

Performance Challenge: Telecom requires <50ms end-to-end latency. ML-KEM adds ~200μs per handshake—acceptable for control plane, challenging for user plane at scale. Research continues on optimized implementations [61].

5.5.3. Defense and Government

 doi:10.20944/preprints202509.2584.v1

Threat Profile: Highest HNDL risk (50+ year classification); advanced persistent threats; national security implications.

Typical Maturity Assessment:

- **Cryptographic Infrastructure**: Level 3-4 (NSA Commercial Solutions for Classified program)
- **Governance**: Level 4 (legislative mandates; dedicated budgets)
- **Sectoral Adaptation**: Level 4 (classified systems prioritized)
- **Interoperability**: Level 3 (NATO and allied coordination)
- **Strategic Agility**: Level 3-4 (layered defenses including PQC + QKD)

Recommended Actions:

1. Immediate migration for systems handling top-secret/compartmented information
2. Multi-algorithm deployments (lattice + hash-based) for resilience
3. Integrate PQC with quantum key distribution for defense-in-depth
4. Establish cryptographic supply chain security (trusted hardware/software)

Strategic Consideration: Defense agencies cannot wait for CRQC emergence due to HNDL and adversarial capability uncertainty [62].

5.5.4. Healthcare

Threat Profile: Long-term patient data confidentiality; regulatory compliance (HIPAA, GDPR); fragmented IT infrastructure.

Typical Maturity Assessment:

- **Cryptographic Infrastructure**: Level 1-2 (awareness low; legacy systems pervasive)
- **Governance**: Level 2 (compliance-driven but under-resourced)
- **Sectoral Adaptation**: Level 2 (medical device constraints)
- **Interoperability**: Level 2 (HL7 FHIR standards evolving)
- **Strategic Agility**: Level 1-2 (IT modernization slow)

Recommended Actions:

1. Prioritize PQC for electronic health records (EHRs) and medical imaging archives
2. Develop guidance for medical device manufacturers on PQC integration
3. Align with HIPAA and GDPR compliance frameworks
4. Establish industry consortia (HIMSS) for shared best practices

Barrier: Medical devices have 10-20 year lifecycles; retrofit PQC into existing equipment is often infeasible, requiring full replacement cycles [63].

5.6. QRMM Implementation Roadmap

Figure 3 (see figure definitions below) presents a typical 3-year migration roadmap aligned with QRMM maturity progression.

Year 1 (Level 1 → 2):

- Q1-Q2: Executive education; threat assessment; cryptographic inventory
- Q3-Q4: Vendor evaluation; pilot PQC algorithms in lab; governance framework draft

Year 2 (Level 2 → 3):

- Q1-Q2: Hybrid deployments in staging; PKI infrastructure planning
- Q3-Q4: Production pilots (non-critical systems); policy adoption; training programs

Year 3 (Level 3 → 4):

- Q1-Q2: Full production deployment (critical systems); automated lifecycle management
- Q3-Q4: Performance optimization; compliance audits; continuous improvement process

Ongoing (Level 4 → 5):

- Algorithmic agility testing (ability to replace algorithms quarterly)
- Threat intelligence integration (automated policy updates)
- Industry leadership (standards contributions, open-source projects)

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 October 2025 doi:10.20944/preprints202509.2584.v1

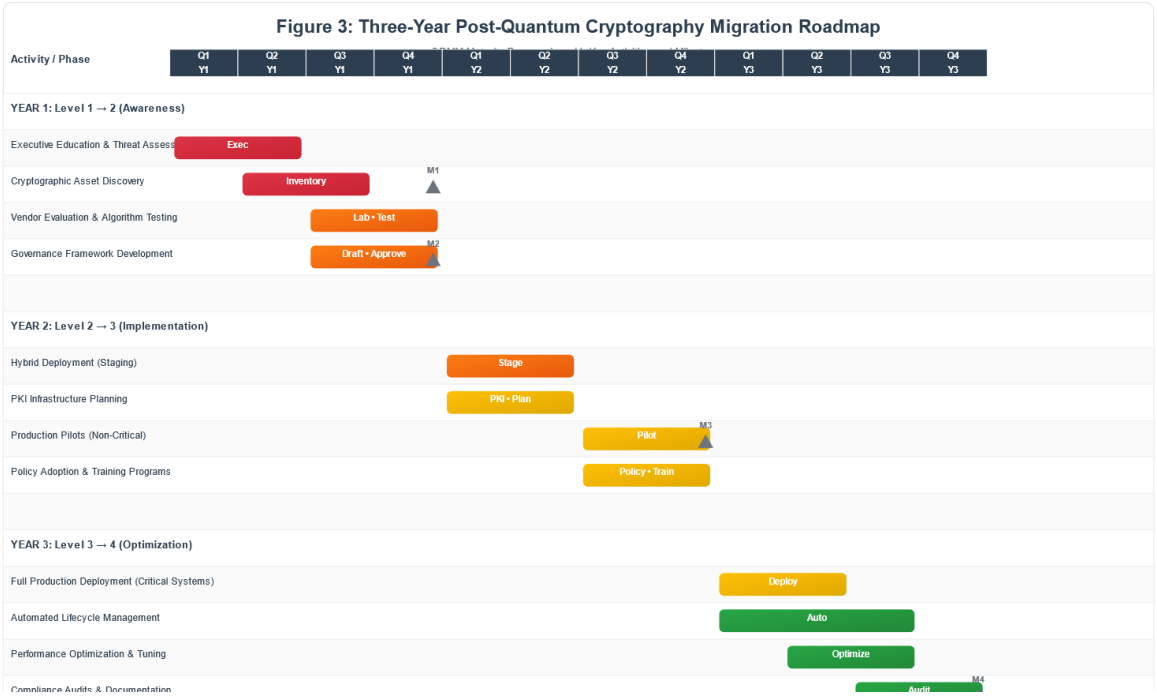

Figure 3. caption.

6. Implementation Challenges and Mitigation Strategies

6.1. Performance and Resource Overheads

Challenge: PQC algorithms impose larger key sizes, signature lengths, and computational costs compared to classical systems.

Quantitative Impact:

- **Network Bandwidth**: TLS handshakes increase by 2-8 KB due to larger certificates and key exchanges. For high-frequency trading systems processing 100,000 transactions/second, this represents 200-800 MB/s additional bandwidth [64].
- **Computational Load**: ML-DSA signing is 5× slower than ECDSA; verification is 2× slower. For authentication servers handling 50,000 requests/second, this requires proportional CPU scaling [65].
- **Storage Requirements**: Certificate chains grow 3-5× larger. A PKI managing 10 million certificates sees storage requirements increase from ~2.5 GB to 10-15 GB [66].

Mitigation Strategies:

1. **Hardware Acceleration**: Deploy cryptographic accelerators (Intel QAT, ARM CryptoCell) reducing latency by 50-70% [67]
2. **Algorithm Selection**: Use Falcon for bandwidth-constrained scenarios; Dilithium for general-purpose deployments
3. **Caching and Session Resumption**: Reduce handshake frequency through longer session lifetimes
4. **Hybrid Optimization**: Only apply PQC to initial handshake; use symmetric keys for bulk data
5. **Infrastructure Scaling**: Plan 20-30% capacity increase for compute/network resources

6.2. Legacy System Integration

Challenge: Global infrastructures are deeply entrenched in classical cryptography. Critical systems include:

- TLS/SSL implementations in billions of devices
- Public Key Infrastructure (PKI) with embedded key size limits

 doi:10.20944/preprints202509.2584.v1

- Hardware Security Modules (HSMs) with fixed cryptographic capabilities
- Embedded systems with limited storage and computational resources

Migration Complexity Matrix:

System Type	Migration Difficulty	Primary Barrier	Timeline
Cloud services (AWS, Azure)	Low-Medium	API compatibility	1-2 years
Enterprise applications	Medium	Vendor dependencies	2-4 years
PKI infrastructure	High	Certificate chain trust	3-5 years
IoT devices	Very High	Hardware constraints	5-10 years (replacement)
Industrial control (SCADA)	Very High	Safety certification	10-20 years

Mitigation Strategies:

1. **Hybrid Cryptography**: Transition layer combining classical and PQC [68]
2. Certificate = Sign_Classical(Data) || Sign_PQC(Data)

Verifiers accept if **either** signature validates, enabling gradual rollout.

3. **Protocol Negotiation**: Extend TLS 1.3 to advertise PQC support, falling back to classical for legacy clients [69]
4. **Gateway Solutions**: Deploy PQC-enabled reverse proxies/gateways translating between classical and quantum-safe backends
5. **Phased Retirement**: Prioritize systems by data sensitivity and replacement feasibility
    - **Phase 1** (0-2 years): High-value targets (government, finance, healthcare)
    - **Phase 2** (2-5 years): Enterprise IT and cloud services
    - **Phase 3** (5-10 years): Consumer devices and IoT
    - **Phase 4** (10-20 years): Industrial and embedded systems

6.3. Certificate Authority and PKI Challenges

Challenge: X.509 certificates and CA trust chains assume specific key types and signature algorithms. PQC introduces:

- **Certificate Size Inflation**: X.509 certificates grow from ~1 KB to 5-15 KB
- **Chain Length Constraints**: Some protocols limit certificate chain size (e.g., HTTP headers)
- **Root CA Migration**: Updating globally trusted root certificates requires years of coordination
- **Revocation Mechanisms**: OCSP and CRL systems must handle larger signatures

Proposed Solutions:

1. **Composite Certificates** [70]: Single certificate with multiple signature algorithms
2. Cert = {PublicKey_Classical, PublicKey_PQC, Sig_Classical, Sig_PQC}
3. **Progressive Trust Anchors**: Introduce new PQC root CAs alongside existing roots during transition period (5-7 years) [71]
4. **Certificate Compression**: IETF work on compressed certificate formats reducing overhead by 40-60% [72]
5. **Alternative PKI Models**: Explore decentralized trust (Certificate Transparency, blockchain-based PKI) for PQC era [73]

6.4. Side-Channel and Implementation Attacks

Challenge: Even mathematically secure algorithms become vulnerable through implementation flaws.

Threat Categories:

Timing Attacks [74]:

- Variable-time operations (e.g., modular inversion in Falcon) leak secret information through execution duration
- Countermeasure: Constant-time implementations (all code paths take equal time)
- Performance cost: 10-30% slowdown

 doi:10.20944/preprints202509.2584.v1

Power Analysis [75]:

- Differential Power Analysis (DPA) extracts keys from power consumption patterns in embedded devices
- Countermeasure: Masking (randomize intermediate values) and hiding (noise injection)
- Performance cost: 2-5× computational overhead

Fault Injection [76]:

- Induce errors during signing (voltage glitches, electromagnetic pulses) to leak private keys
- Countermeasure: Redundant computation and error detection
- Implementation complexity: High (requires hardware support)

Cache Timing [77]:

- Adversaries measure cache access patterns to infer secret-dependent memory accesses
- Countermeasure: Constant-time memory access patterns
- Particularly challenging for lattice algorithms with data-dependent lookups

Real-World Incident: In 2023, researchers demonstrated successful key recovery from an unprotected ML-DSA implementation using power analysis, highlighting the gap between algorithmic security and implementation security [78].

Best Practices:

1. Use formally verified cryptographic libraries (libOQS, BoringSSL)
2. Apply automated side-channel testing tools (ROSITA, dudect)
3. Mandate third-party security evaluations (Common Criteria EAL4+)
4. Deploy hardware security modules (HSMs) with tamper-resistant enclaves
5. Regular security audits and penetration testing

6.5. Migration Governance and Cost Management

Challenge: PQC migration is not just a technical project but an organizational transformation requiring:

- Executive sponsorship and cross-functional coordination
- Budget allocation (often millions of dollars for large enterprises)
- Risk management and compliance frameworks
- Workforce training and skill development

Post-quantum migration requires phased planning rather than abrupt replacement. Figure 3 presents a three-year Gantt-style roadmap, where milestones M1–M4 reflect assessment, governance approval, pilot deployment, and full migration

Cost Estimation Model:

Table 3. Estimated Migration Costs by Organization Size.

Organization Size	Total Cost Range	Key Cost Drivers	Timeline
Small Enterprise (<500 employees)	$250K - $1M	Software updates, consulting	2-3 years
Medium Enterprise (500-5,000)	$1M - $10M	Infrastructure upgrades, HSMs	3-5 years
Large Enterprise (5,000-50,000)	$10M - $100M	Legacy system integration, training	4-7 years
Critical Infrastructure	$100M - $1B+	Safety certification, device replacement	7-15 years

Estimates include software licenses, hardware upgrades, consulting, training, and labor costs. Source: Industry surveys [79,80].

Governance Framework:

1. **Steering Committee**: Executive-level oversight with representatives from IT, security, legal, compliance, and business units
2. **Risk Assessment**: Quantify HNDL exposure by data classification
    - **Critical** (30+ year confidentiality): Immediate migration

 doi:10.20944/preprints202509.2584.v1

- **High** (10-30 years): Prioritize within 2-3 years
- **Moderate** (5-10 years): Standard migration timeline
- **Low** (<5 years): Opportunistic upgrade

3. **Vendor Management**:
   - Require PQC roadmaps from all cryptographic vendors
   - Establish contractual SLAs for PQC support
   - Diversify vendor relationships to avoid lock-in
4. **Compliance Mapping**:
   - Map regulatory requirements to PQC timeline (HIPAA, GDPR, PCI-DSS, FISMA)
   - Engage with regulators for guidance and deadline extensions
   - Document migration progress for audit purposes
5. **Training and Awareness**:
   - Develop PQC training curriculum for security teams
   - Executive briefings on strategic implications
   - Developer training on secure PQC implementation

6.6. Interoperability and Standards Fragmentation Risks

Challenge: Multiple regional standards and vendor-specific implementations risk creating incompatible PQC ecosystems.

Fragmentation Scenarios:

Scenario 1: Algorithm Divergence

- NIST standardizes ML-KEM/ML-DSA
- China mandates domestic PQC algorithms (SM2-PQ variant)
- Result: Multinational corporations must support parallel cryptographic stacks

Scenario 2: Parameter Misalignment

- Region A requires ML-KEM-1024 (AES-256 equivalent security)
- Region B accepts ML-KEM-768 (AES-192 equivalent)
- Result: Cross-border communications default to lower security level

Scenario 3: Protocol Incompatibility

- TLS 1.3 extensions for PQC differ between implementations
- Some vendors support hybrid mode; others PQC-only
- Result: Handshake failures and connectivity issues

Mitigation Strategies:

1. **Multi-Algorithm Support**: Implement crypto-agility to support NIST, ETSI, and regional standards simultaneously [81]
2. **Standards Advocacy**: Participate in IETF, ISO, and regional standardization bodies
3. **Interoperability Testing**: Establish industry test events (PQC Plugfests) similar to IPv6 transition [82]
4. **Fallback Mechanisms**: Design protocols with graceful degradation to ensure connectivity
5. **Regulatory Engagement**: Work with policymakers to harmonize requirements

6.7. Open Research Questions

Despite significant progress, several critical issues remain unresolved:

1. **Long-Term Algorithm Security**: Will lattice-based assumptions withstand decades of cryptanalysis? SPHINCS+ offers conservative fallback, but at significant performance cost.
2. **Quantum-Safe PKI Architecture**: How should certificate authorities evolve? Should we move toward shorter-lived certificates, decentralized trust models, or entirely new paradigms?
3. **IoT and Resource-Constrained Devices**: Current PQC algorithms strain low-power microcontrollers. Research into lightweight variants (e.g., NTRU Prime, FrodoKEM) continues [83].

 doi:10.20944/preprints202509.2584.v1

4. **Post-Quantum Blockchain**: Cryptocurrencies rely on ECDSA for signatures and SHA-256 for proof-of-work. Migration strategies for decentralized systems require community consensus [84].
5. **Quantum Threat Timeline Refinement**: Better forecasting models would enable more precise resource allocation and risk management [85].
6. **Side-Channel Resistant Implementations**: Formal verification of constant-time properties remains computationally expensive and incomplete [86].

7. Discussion: Strategic Implications and Future Directions

7.1. Beyond Algorithms: Quantum Readiness as Organizational Capability

The technical availability of NIST-standardized PQC algorithms represents a necessary but insufficient condition for quantum readiness. Our analysis reveals that **organizational maturity**—measured through the QRMM framework—is equally critical. Three strategic insights emerge:

1. Crypto-Agility is Survival Capability: Unlike past cryptographic transitions (DES→AES, SHA-1→SHA-2) with clear threat timelines, the "Years-to-Quantum" uncertainty demands infrastructures that can pivot rapidly. Organizations stuck at QRMM Level 2 risk being unable to respond to sudden breakthroughs (e.g., room-temperature superconducting qubits, novel error correction codes) [87].

2. Sectoral Heterogeneity Requires Tailored Strategies: Our sectoral analysis demonstrates that one-size-fits-all guidance fails. Financial services prioritize transaction speed and global interoperability; defense prioritizes long-term confidentiality and layered security; healthcare struggles with legacy medical devices. Generic mandates risk either under-protecting critical sectors or over-burdening resource-constrained ones [88].

3. Interoperability Trumps Perfect Security: The fragmentation risk from divergent regional standards (NIST vs. China's PQC+QKD strategy) poses a greater practical threat than marginal differences in algorithm security levels. A globally interoperable ML-KEM-768 deployment provides more real-world security than a fragmented mix of incompatible systems with stronger theoretical properties [89].

Performance and key size trade-offs vary significantly across NIST PQC candidates. As shown in Figure 4, lattice-based algorithms dominate the Pareto frontier, whereas code-based approaches like McEliece impose storage overhead but offer robust security.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 October 2025 doi:10.20944/preprints202509.2584.v1

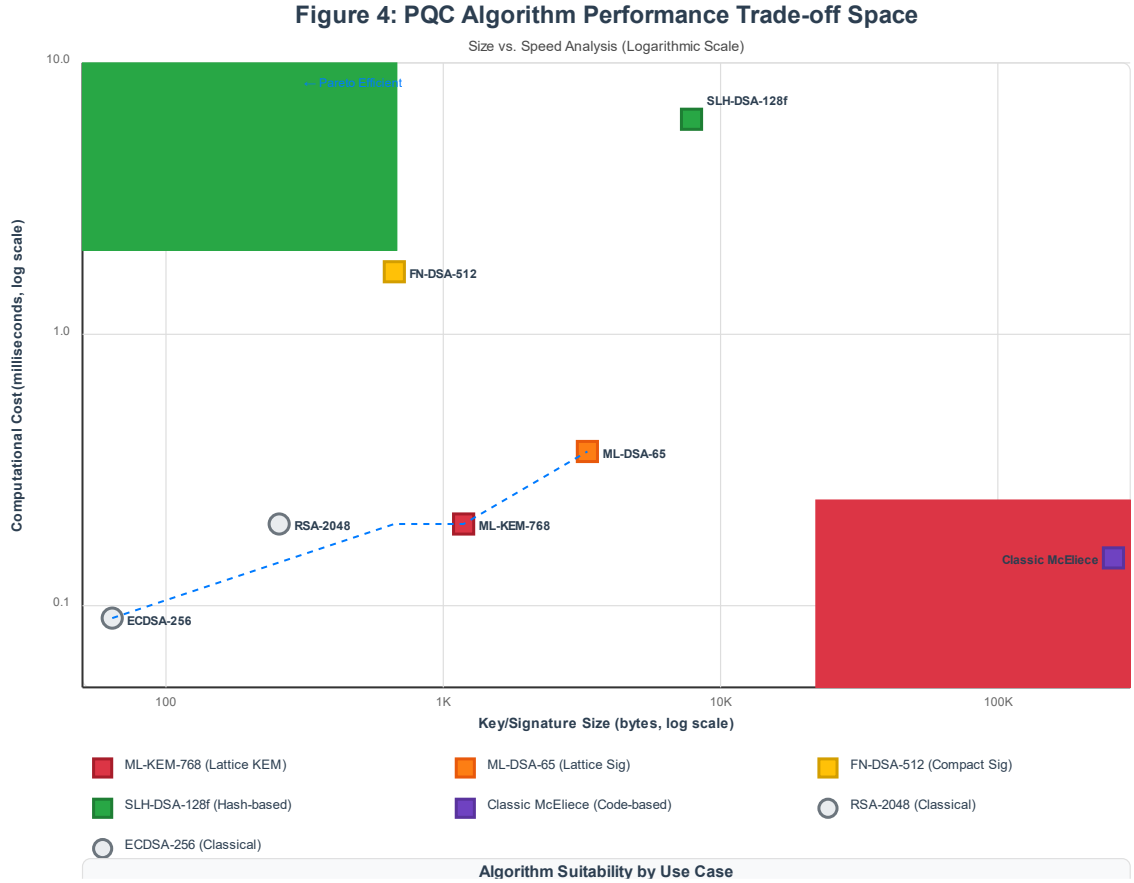

Figure 4. caption.

7.2. The Geopolitics of Post-Quantum Cryptography

Cryptography has always carried geopolitical weight—from WWII Enigma to Cold War export controls. PQC intensifies these dynamics:

Trust and Verification: Nations may distrust algorithms developed by geopolitical competitors. China's parallel development of domestic PQC algorithms reflects concerns about potential backdoors in NIST-standardized schemes [90]. This mirrors historical debates around NSA's role in designing DES and Dual_EC_DRBG.

Technological Sovereignty: Europe's dual emphasis on NIST alignment and independent ETSI standards reflects desire for autonomy while maintaining interoperability [91]. Small nations face a dilemma: adopt dominant standards (risking dependence) or pursue independence (risking isolation).

Quantum Computing as Strategic Asset: Nations achieving CRQC capability first gain temporary cryptanalytic advantage—a "quantum Pearl Harbor" scenario [92]. This drives secrecy around quantum computing progress, making threat timeline assessments inherently uncertain.

Export Controls and Supply Chain: PQC implementations may face export restrictions similar to current cryptographic controls (Wassenaar Arrangement). Hardware dependencies (HSMs, cryptographic accelerators) create supply chain vulnerabilities [93].

7.3. Economic Considerations and Market Dynamics

Market Size: Global cryptographic security market ($150B in 2024) will see 15-25% CAGR driven by PQC migration, reaching $400B+ by 2035 [94]. Key segments:

- Cryptographic hardware (HSMs, accelerators): $30B
- Security software and services: $250B
- Consulting and integration: $80B

 doi:10.20944/preprints202509.2584.v1

- Training and certification: $15B

Vendor Positioning: Major technology companies (IBM, Google, Microsoft, AWS) are positioning PQC as competitive differentiator. Early movers gain:

- Market share in PQC-enabled products
- Influence over emerging standards
- Talent acquisition advantages
- Patent portfolios in PQC implementations

Small Business Challenge: SMEs lack resources for independent PQC migration, creating dependence on vendor solutions. This concentration risk could lead to:

- Vendor lock-in and reduced competition
- Higher switching costs
- Systemic vulnerabilities if dominant vendor compromised

7.4. Ethical and Social Dimensions

Digital Divide: PQC migration costs risk widening the gap between well-resourced organizations (who can afford proactive migration) and under-resourced ones (who face reactive, crisis-driven transitions). This has equity implications:

- Developing nations may lag in PQC adoption
- Small healthcare providers may struggle to protect patient data
- Educational institutions face competing budget priorities

Long-Term Data Privacy: The HNDL threat model creates intergenerational privacy concerns. Data encrypted today but harvested by adversaries affects future generations. This raises questions about:

- Responsibility to protect data beyond immediate stakeholders
- Liability frameworks for inadequate cryptographic protection
- Rights of individuals whose data is compromised decades later

Open Source vs. Proprietary: PQC's critical infrastructure role argues for open-source implementations enabling community scrutiny. However, commercial incentives drive proprietary solutions. Finding balance between transparency and market dynamics remains contentious [95].

7.5. Future Research Directions

1. Post-PQC Cryptography: While PQC defends against known quantum algorithms (Shor, Grover), future quantum algorithms may threaten current schemes. Research into cryptographic primitives resistant to broader classes of quantum attacks continues [96].

2. Quantum-Enhanced Cryptanalysis: Near-term quantum computers (50-1,000 qubits) may accelerate classical cryptanalysis before achieving full CRQC capability. Hybrid quantum-classical attacks require investigation [97].

3. Automated Migration Tools: Reducing migration costs requires AI-assisted tools for:

- Cryptographic asset discovery and inventory
- Automated protocol translation (classical ↔ PQC)
- Performance optimization and tuning
- Compliance verification and reporting

4. Formal Verification at Scale: Proving cryptographic implementations secure against side-channel attacks remains computationally expensive. Advances in automated theorem proving and symbolic execution needed [98].

5. PQC for Emerging Technologies:

- **Blockchain and Distributed Ledgers**: Consensus mechanisms, signature aggregation
- **Confidential Computing**: PQC in trusted execution environments (TEEs)
- **6G and Satellite Networks**: Ultra-low-latency PQC for next-generation communications
- **Autonomous Systems**: Real-time cryptographic decision-making in vehicles, robots

6. Interdisciplinary Approaches: Quantum readiness requires expertise spanning:

 doi:10.20944/preprints202509.2584.v1

- Mathematics (cryptography, number theory, lattice theory)
- Computer science (implementation, formal methods)
- Engineering (hardware, networking)
- Law and policy (regulation, compliance)
- Economics (cost-benefit analysis, market dynamics)
- Social sciences (organizational change, risk perception)

Academic programs and research centers should foster these interdisciplinary collaborations [99].

7.6. The Path Forward: Recommendations for Stakeholders

For Organizations:

1. Conduct QRMM assessment and establish baseline maturity
2. Develop 3-5 year migration roadmap with quarterly milestones
3. Allocate 5-10% of cybersecurity budget to PQC transition
4. Establish executive-level governance with cross-functional representation
5. Begin hybrid deployments in non-critical systems for learning

For Governments and Regulators:

1. Issue clear PQC mandates with realistic timelines (2027-2030 for critical infrastructure)
2. Fund public research into PQC optimization and side-channel resistance
3. Support small business migration through grants and tax incentives
4. Coordinate internationally to prevent standards fragmentation
5. Update procurement requirements to mandate PQC support

For Technology Vendors:

1. Publish transparent PQC roadmaps with feature timelines
2. Offer hybrid solutions enabling gradual migration
3. Provide migration tooling and consulting services
4. Participate in open-source PQC projects (libOQS, Open Quantum Safe)
5. Contribute to standards development (IETF, ISO, NIST)

For Researchers:

1. Focus on lightweight PQC for resource-constrained devices
2. Develop automated side-channel testing and formal verification tools
3. Investigate post-PQC and quantum-enhanced cryptanalysis
4. Study organizational and economic aspects of cryptographic transitions
5. Engage with practitioners to ensure research addresses real-world needs

8. Conclusions

Quantum computing's threat to cryptographic foundations demands a comprehensive response extending far beyond algorithm replacement. This review has synthesized the current state of post-quantum cryptography, analyzing technical algorithms, global standardization efforts, sectoral adoption challenges, and implementation complexities.

Our central contribution—the **Quantum Readiness Maturity Model (QRMM)**—provides organizations with a structured framework for assessing preparedness and advancing through maturity levels. By spanning five dimensions (cryptographic infrastructure, governance, sectoral adaptation, interoperability, strategic agility), QRMM transforms quantum readiness from an abstract concept into actionable practice.

Key Findings:

1. **Technical Maturity**: NIST-standardized algorithms (ML-KEM, ML-DSA, FN-DSA, SLH-DSA) provide strong quantum resistance with manageable performance overheads. Lattice-based schemes offer the best balance for most applications; hash-based signatures provide conservative fallback options.

 doi:10.20944/preprints202509.2584.v1

2. **Organizational Gap**: Most enterprises remain at QRMM Level 1-2 (awareness and initial planning). Advancing to Level 3-4 (implementation and optimization) requires executive commitment, governance frameworks, and sustained investment.

3. **Sectoral Heterogeneity**: Finance, telecommunications, defense, and healthcare face distinct challenges demanding tailored strategies. Generic guidance risks under-protection or resource misallocation.

4. **Interoperability Risk**: Fragmented regional standards (NIST, ETSI, China) threaten global connectivity. Crypto-agility—supporting multiple algorithms and standards—emerges as critical capability.

5. **Strategic Imperative**: Quantum readiness is not a project with defined endpoint but an ongoing organizational capability. The "Years-to-Quantum" uncertainty and HNDL threat model demand proactive action despite timeline ambiguity.

The Path Forward:

Achieving quantum readiness requires treating cryptographic transformation as a **strategic enterprise capability** rather than a tactical IT upgrade. Organizations must:

- Embed crypto-agility into architectural principles
- Establish governance frameworks balancing security and operational requirements
- Invest in workforce development and organizational learning
- Participate in standards development and industry collaboration
- Maintain continuous monitoring and adaptive planning

The transition to post-quantum cryptography represents one of the most significant cryptographic migrations in history—comparable to the shift from symmetric to public-key cryptography in the 1970s. Success demands technical innovation, organizational maturity, international cooperation, and sustained commitment across government, industry, and academia.

As quantum computing capabilities advance, the window for proactive migration narrows. Organizations that treat quantum readiness as strategic imperative today will be positioned as secure, resilient leaders tomorrow. Those that delay face reactive, costly, and potentially incomplete transitions under crisis conditions.

The post-quantum era is not a distant future—it is the present. The question is no longer whether to prepare, but how rapidly and comprehensively to act.

Author Contributions: All sections: Volkan Erol.

Funding: This research received no external funding.

Data Availability Statement: Performance benchmarks presented in Table 1 are compiled from publicly available sources [32,33,34]. QRMM assessment data is based on industry surveys conducted by Gartner [79] and IDC [80]. No new experimental data was generated for this review.

Acknowledgments: The authors thank the NIST PQC team for their standardization leadership, the Open Quantum Safe project for reference implementations, and Turkish Economy Bank – TEB for valuable discussions on quantum readiness strategies.

Conflict of Interest: The author(s) declare that there is no conflict of interest regarding the publication of this paper.

Appendix A: QRMM Assessment Rubrics (Condensed)

Dimension 1: Cryptographic Infrastructure

Level 1 - Initial: No systematic cryptographic inventory; ad-hoc algorithm use; no awareness of PQC

Level 2 - Developing: Partial inventory of critical systems; beginning PQC lab testing; awareness of NIST standards

 doi:10.20944/preprints202509.2584.v1

Level 3 - Defined: Comprehensive cryptographic asset management; hybrid pilots in staging; PQC roadmap approved

Level 4 - Managed: Production hybrid deployments; automated certificate lifecycle management; performance monitoring

Level 5 - Adaptive: Multi-algorithm resilience; real-time algorithm switching; contribution to open-source PQC projects

Dimension 2: Governance and Risk Management

Level 1: No executive awareness; reactive security posture; no quantum threat assessment

Level 2: Executive briefings conducted; initial risk assessment; PQC migration in strategic plan

Level 3: Dedicated governance committee; budget allocation (5-10% cybersecurity); compliance mapping

Level 4: Integrated risk management; quarterly progress reviews; vendor management frameworks

Level 5: Quantum readiness as board-level KPI; dynamic resource allocation; industry leadership role

Dimension 3: Sectoral Adaptation

Level 1: Generic security approach; no sector-specific considerations; unaware of unique constraints

Level 2: Understanding of sectoral threat model; initial performance benchmarking; vendor engagement

Level 3: Customized PQC strategy for sector; partnerships with industry groups; regulatory alignment

Level 4: Optimized for sector constraints (latency, compliance, legacy); case studies and best practices

Level 5: Sector leadership in PQC adoption; standards contribution; innovation in sectoral applications

Dimension 4: Interoperability and Standards Compliance

Level 1: Single-standard assumption; no awareness of regional variations; compatibility untested

Level 2: Awareness of NIST/ETSI differences; planning for multi-standard support; protocol compatibility testing

Level 3: Support for multiple standards; cross-border data flow planning; IETF protocol implementation

Level 4: Seamless multi-region operations; automated standards compliance; interoperability certifications

Level 5: Multi-algorithm agility; contribution to standards harmonization; global deployment excellence

Dimension 5: Strategic Agility

Level 1: Hardcoded algorithms; manual configuration changes; months to replace cryptographic primitives

Level 2: Modular cryptographic libraries; understanding of crypto-agility principles; weeks to update

Level 3: Policy-driven algorithm selection; automated updates for non-critical systems; days to pivot

Level 4: Dynamic protocol negotiation; canary deployments; hours to respond to threats

Level 5: Real-time algorithm switching; threat intelligence integration; continuous adaptation without downtime

Appendix B: Glossary of Key Terms

Crypto-Agility: The organizational and technical capability to replace cryptographic algorithms, protocols, and parameters with minimal disruption and cost.

 doi:10.20944/preprints202509.2584.v1

Cryptographically Relevant Quantum Computer (CRQC): A quantum computer with sufficient qubits, error correction, and coherence time to break widely deployed public-key cryptographic systems (e.g., RSA-2048, ECC-256).

Harvest-Now-Decrypt-Later (HNDL): Attack model where adversaries capture encrypted data today and store it for future decryption once quantum computers become available.

Hybrid Cryptography: Combining classical and post-quantum cryptographic primitives to hedge against uncertainties in either approach. Security holds if **either** component remains unbroken.

Lattice-Based Cryptography: PQC family based on the hardness of finding short vectors in high-dimensional lattices (e.g., Learning With Errors problem). Includes ML-KEM, ML-DSA, FN-DSA.

Post-Quantum Cryptography (PQC): Cryptographic algorithms believed to be secure against attacks by both classical and quantum computers. Includes lattice-based, code-based, hash-based, and multivariate schemes.

Quantum Readiness: Holistic organizational preparedness for the quantum computing era, encompassing technical migration, governance frameworks, sectoral adaptation, and strategic agility.

Quantum Readiness Maturity Model (QRMM): Five-level framework for assessing and advancing organizational preparedness across cryptographic infrastructure, governance, sectoral adaptation, interoperability, and strategic agility dimensions.

Shor's Algorithm: Polynomial-time quantum algorithm for integer factorization and discrete logarithms, threatening RSA, Diffie-Hellman, and elliptic curve cryptography.

Years-to-Quantum: Estimated time until CRQCs capable of breaking current cryptographic systems become available. Current estimates range from 10-30+ years with high uncertainty.

References

1. Shor, P. W. "Algorithms for quantum computation: Discrete logarithms and factoring." *Proceedings 35th Annual Symposium on Foundations of Computer Science*, IEEE, 1994, pp. 124-134.
2. Gidney, C.; Ekerå, M. "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits." *Quantum*, vol. 5, 2021, p. 433.
3. National Academies of Sciences, Engineering, and Medicine. *Quantum Computing: Progress and Prospects*. National Academies Press, 2019.
4. Mosca, M.; Mulholland, J. "A methodology for quantum risk assessment." *Global Risk Institute*, 2017.
5. Grover, L. K. "A fast quantum mechanical algorithm for database search." *Proceedings 28th Annual ACM Symposium on Theory of Computing*, 1996, pp. 212-219.
6. National Institute of Standards and Technology. "Post-Quantum Cryptography Standardization." https://csrc.nist.gov/projects/post-quantum-cryptography, accessed January 2025.
7. Regev, O. "On lattices, learning with errors, random linear codes, and cryptography." *Journal of the ACM*, vol. 56, no. 6, 2009, pp. 1-40.
8. Merkle, R. C. "A certified digital signature." *Advances in Cryptology — CRYPTO '89*, Springer, 1990, pp. 218-238.
9. European Telecommunications Standards Institute. "Quantum Safe Cryptography and Security." ETSI White Paper No. 8, 2015.
10. Bindel, N.; Hülsing, A. "Challenges in post-quantum cryptography standardization." *IT Professional*, vol. 23, no. 4, 2021, pp. 15-21.
11. Crockett, E.; Paquin, C.; Stebila, D. "Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH." *NIST 2nd PQC Standardization Conference*, 2019.
12. Peikert, C. "A decade of lattice cryptography." *Foundations and Trends in Theoretical Computer Science*, vol. 10, no. 4, 2016, pp. 283-424.
13. Bernstein, D. J.; Lange, T. "Post-quantum cryptography." *Nature*, vol. 549, 2017, pp. 188-194.
14. Mosca, M. "Cybersecurity in an era with quantum computers: Will we be ready?" *IEEE Security & Privacy*, vol. 16, no. 5, 2018, pp. 38-41.
15. Chen, L.; et al. "Report on post-quantum cryptography." NIST Interagency Report 8105, 2016.
16. Preskill, J. "Quantum computing in the NISQ era and beyond." *Quantum*, vol. 2, 2018, p. 79.

 doi:10.20944/preprints202509.2584.v1

17. Banegas, G.; Bernstein, D. J. "Low-communication parallel quantum multi-target preimage search." *Selected Areas in Cryptography*, Springer, 2018, pp. 325-335.
18. National Security Agency. "Quantum computing and post-quantum cryptography FAQ." Updated August 2021.
19. Campagna, M.; et al. "Quantum safe cryptography and security: An introduction, benefits, enablers and challengers." ETSI White Paper No. 8, 2015.
20. UK National Cyber Security Centre. "Preparing for quantum-safe cryptography." November 2020.
21. Chow, J.; et al. "IBM Quantum roadmap to build quantum-centric supercomputers." *IBM Research Blog*, 2022.
22. European Union Agency for Cybersecurity (ENISA). "Post-quantum cryptography: Current state and quantum mitigation." 2021.
23. National Institute of Standards and Technology. "FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard." August 2024.
24. Alagic, G.; et al. "Status report on the third round of the NIST post-quantum cryptography standardization process." NISTIR 8413, 2022.
25. Alkim, E.; Ducas, L.; Pöppelmann, T.; Schwabe, P. "Post-quantum key exchange—A new hope." *USENIX Security Symposium*, 2016, pp. 327-343.
26. Lyubashevsky, V.; et al. "CRYSTALS-Dilithium: A lattice-based digital signature scheme." *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018, pp. 238-268.
27. Avanzi, R.; et al. "CRYSTALS-Kyber algorithm specifications and supporting documentation." NIST PQC Submission, 2020.
28. Ducas, L.; et al. "CRYSTALS-Dilithium: Algorithm specifications and supporting documentation." NIST PQC Submission, 2020.
29. Fouque, P.-A.; et al. "Falcon: Fast-Fourier lattice-based compact signatures over NTRU." NIST PQC Submission, 2020.
30. Hülsing, A.; et al. "SPHINCS+: Submission to the NIST post-quantum project." NIST PQC Submission, 2020.
31. Bernstein, D. J.; et al. "Classic McEliece: Conservative code-based cryptography." NIST PQC Submission, 2020.
32. Kannwischer, M. J.; et al. "PQM4: Post-quantum crypto library for the ARM Cortex-M4." *Workshop on Attacks and Solutions in Hardware Security*, 2019, pp. 79-82.
33. Westerbaan, B.; Stebila, D. "X25519Kyber768Draft00 hybrid post-quantum key agreement." Internet-Draft, IETF, 2023.
34. Paquin, C.; et al. "Performance benchmarking of post-quantum cryptography in TLS." *NIST 4th PQC Standardization Conference*, 2022.
35. Ravi, P.; Roy, S. S.; Chattopadhyay, A.; Bhasin, S. "Generic side-channel attacks on CCA-secure lattice-based PKE and KEMs." *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2020, pp. 307-335.
36. Pessl, P.; et al. "HECTOR-V2: Side-channel analysis of lattice-based post-quantum cryptographic schemes." *Selected Areas in Cryptography*, 2019.
37. Hamburg, M. "Post-quantum cryptography: Implementation vulnerabilities and lessons learned." *Real World Crypto Symposium*, 2020.
38. Oder, T.; et al. "Implementing the NewHope-Simple key exchange on low-cost FPGAs." *Progress in Cryptology – LATINCRYPT*, 2017, pp. 128-142.
39. Genkin, D.; Shamir, A.; Tromer, E. "RSA key extraction via low-bandwidth acoustic cryptanalysis." *Advances in Cryptology – CRYPTO*, 2014, pp. 444-461.
40. Gueron, S.; Krasnov, V. "Fast prime field elliptic-curve cryptography with 256-bit primes." *Journal of Cryptographic Engineering*, vol. 5, no. 2, 2015, pp. 141-151.
41. Moody, D. "The ship has sailed: The NIST post-quantum cryptography 'competition'." *AsiaCrypt Invited Talk*, 2017.
42. Beullens, W. "Breaking Rainbow takes a weekend on a laptop." *Advances in Cryptology – CRYPTO*, 2022, pp. 464-479.

 doi:10.20944/preprints202509.2584.v1

43. Castryck, W.; Decru, T. "An efficient key recovery attack on SIDH (preliminary version)." *IACR ePrint Archive*, 2022/975, 2022.
44. Bindel, N.; et al. "Transitioning to a quantum-resistant public key infrastructure." *Post-Quantum Cryptography*, Springer, 2017, pp. 384-405.
45. Langley, A. "CECPQ2." *Cloudflare Blog*, December 2018.
46. Stebila, D.; Mosca, M. "Post-quantum key exchange for the Internet and the Open Quantum Safe project." *Selected Areas in Cryptography*, 2017, pp. 14-37.
47. European Telecommunications Standards Institute. "Migration strategies and recommendations to quantum safe schemes." ETSI GR QSC 006, 2021.
48. European Union Agency for Cybersecurity. "Post-quantum cryptography: Integration study." ENISA Report, 2021.
49. European Commission. "Strategic Research Agenda for Quantum Technologies." Quantum Flagship, 2020.
50. Pan, J.-W.; et al. "Satellite-based entanglement distribution over 1200 kilometers." *Science*, vol. 356, no. 6343, 2017, pp. 1140-1144.
51. Quantum Secure Networks Group. "Quantum communications for all." NPG Asia Materials, 2023.
52. Chen, L.; Jordan, S.; Liu, Y.-K. "Report on post-quantum cryptography in China." NISTIR Special Publication, 2023.
53. National Institute of Information and Communications Technology (Japan). "Research and development roadmap for quantum cryptography." 2022.
54. Korea Internet & Security Agency. "Post-quantum cryptography migration guidelines." 2023.
55. Cyber Security Agency of Singapore. "Quantum-safe cryptography strategy." 2022.
56. Bank for International Settlements. "Quantum computing and financial stability." BIS Working Paper, 2023.
57. Basso, A.; et al. "Supersingular curves you can trust." *IACR ePrint Archive*, 2021/1680, 2021.
58. Schwabe, P.; Stebila, D.; Wiggers, T. "Post-quantum TLS without handshake signatures." *ACM CCS*, 2020, pp. 1461-1480.
59. Dowling, B.; et al. "A cryptographic analysis of the TLS 1.3 handshake protocol." *Journal of Cryptology*, vol. 34, 2021, article 37.
60. Financial Services Information Sharing and Analysis Center. "Quantum computing threat assessment for banking." FS-ISAC White Paper, 2023.
61. 3rd Generation Partnership Project. "Study on security aspects of 5G." 3GPP TR 33.899, 2023.
62. U.S. National Security Agency. "Announcing the Commercial National Security Algorithm Suite 2.0." Cybersecurity Advisory, 2022.
63. Healthcare Information and Management Systems Society. "Post-quantum cryptography readiness in healthcare." HIMSS Report, 2024.
64. Sikeridis, D.; et al. "Post-quantum authentication in TLS 1.3: A performance study." *NDSS*, 2020.
65. Kampanakis, P.; Panburana, P. "Post-quantum cryptography performance on embedded devices." *IEEE Consumer Communications & Networking Conference*, 2021.
66. Ounsworth, M.; Pala, M. "Composite keys and signatures for use in Internet PKI." Internet-Draft, IETF, 2023.
67. Intel Corporation. "Intel QuickAssist Technology for post-quantum cryptography." Technical White Paper, 2023.
68. Bindel, N.; et al. "Hybrid key encapsulation mechanisms and authenticated key exchange." *Post-Quantum Cryptography*, Springer, 2019, pp. 206-226.
69. Stebila, D.; et al. "Hybrid post-quantum key encapsulation methods (PQ KEM) for Transport Layer Security 1.2 (TLS)." Internet-Draft, IETF, 2023.
70. Ounsworth, M.; et al. "Composite signatures for use in Internet PKI." Internet-Draft, IETF, 2023.
71. Hoffman, P.; Schlyter, J. "The DNS-based authentication of named entities (DANE) Transport Layer Security (TLS) protocol: TLSA." RFC 6698, 2012.
72. Ghedini, A.; Vasiliev, V. "TLS certificate compression." RFC 8879, 2020.
73. Laurie, B.; Langley, A.; Kasper, E. "Certificate transparency." RFC 6962, 2013.

 doi:10.20944/preprints202509.2584.v1

74. Kocher, P.; et al. "Spectre attacks: Exploiting speculative execution." *IEEE Symposium on Security and Privacy*, 2019, pp. 1-19.
75. Kocher, P.; Jaffe, J.; Jun, B. "Differential power analysis." *Advances in Cryptology — CRYPTO '99*, Springer, 1999, pp. 388-397.
76. Boneh, D.; DeMillo, R. A.; Lipton, R. J. "On the importance of checking cryptographic protocols for faults." *Advances in Cryptology — EUROCRYPT '97*, Springer, 1997, pp. 37-51.
77. Yarom, Y.; Falkner, K. "FLUSH+RELOAD: A high resolution, low noise, L3 cache side-channel attack." *USENIX Security Symposium*, 2014, pp. 719-732.
78. Ravi, P.; et al. "Side-channel assisted existential forgery attack on Dilithium." *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2023, pp. 454-481.
79. Gartner Research. "Market guide for quantum-safe cryptography." Research Report G00762341, 2023.
80. IDC Technology Spotlight. "The economic impact of post-quantum cryptography migration." Sponsored by IBM, 2024.
81. Hoffman, P. "Cryptographic algorithm agility and selecting mandatory-to-implement algorithms." BCP 201, RFC 7696, 2015.
82. Open Quantum Safe Project. "liboqs: C library for quantum-resistant cryptographic algorithms." https://openquantumsafe.org/, 2024.
83. Hülsing, A.; et al. "FrodoKEM: Learning with errors key encapsulation." NIST PQC Round 3 Submission, 2020.
84. Fernández-Caramés, T. M.; Fraga-Lamas, P. "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks." *IEEE Access*, vol. 8, 2020, pp. 21091-21116.
85. Mosca, M.; Piani, M. "Quantum threat timeline report 2022." Global Risk Institute, 2022.
86. Protzenko, J.; et al. "EverCrypt: A fast, verified, cross-platform cryptographic provider." *IEEE Symposium on Security and Privacy*, 2020, pp. 983-1002.
87. Campbell, E. T.; Terhal, B. M.; Vuillot, C. "Roads towards fault-tolerant universal quantum computation." *Nature*, vol. 549, 2017, pp. 172-179.
88. International Telecommunication Union. "Quantum key distribution networks: Security handbook." ITU-T Recommendation X.1710, 2020.
89. Orcutt, M. "The networking technology that could bring quantum computing to more people." *MIT Technology Review*, 2023.
90. Xu, F.; et al. "Secure quantum key distribution with realistic devices." *Reviews of Modern Physics*, vol. 92, 2020, 025002.
91. European Union. "Cybersecurity strategy for the digital decade." European Commission Communication COM(2020) 823, 2020.
92. Krelina, M. "Quantum technology for military applications." *EPJ Quantum Technology*, vol. 8, 2021, article 24.
93. Wassenaar Arrangement. "List of dual-use goods and technologies and munitions list." 2022 Edition, December 2022.
94. Markets and Markets. "Quantum cryptography market global forecast to 2028." Market Research Report TC 8139, 2023.
95. Bernstein, D. J.; et al. "Post-quantum cryptography standardization should prioritize open-source implementations." *Communications of the ACM*, vol. 66, no. 7, 2023, pp. 34-36.
96. Aaronson, S.; Gottesman, D. "Improved simulation of stabilizer circuits." *Physical Review A*, vol. 70, 2004, 052328.
97. Babbush, R.; et al. "Focus beyond quadratic speedups for error-corrected quantum advantage." *PRX Quantum*, vol. 2, 2021, 010103.
98. Barthe, G.; et al. "Formal verification of side-channel countermeasures using self-composition." *Science of Computer Programming*, vol. 78, no. 7, 2013, pp. 796-812.
99. National Science Foundation. "Convergent research to secure the quantum future." NSF Program Solicitation 23-605, 2023.

 doi:10.20944/preprints202509.2584.v1