Quanta Security Whitepaper

Technical Research Position on Post-Quantum Security Infrastructure for Emerging Digital Systems

---

Abstract

The imminent transition from classical cryptographic security models toward post-quantum resilient systems represents one of the most urgent unresolved challenges in modern digital infrastructure. Advances in quantum computation are steadily approaching thresholds where currently deployed asymmetric cryptographic standards—particularly RSA, ECC, and related public-key systems—may become computationally vulnerable under sufficiently capable fault-tolerant quantum machines.

While full-scale cryptographically relevant quantum computers remain under active development, the strategic threat is immediate because adversaries may already engage in harvest-now, decrypt-later operations: intercepting encrypted data today for future decryption once quantum capability matures.

Quanta Security is positioned as a research-driven initiative focused on investigating practical post-quantum defensive architectures that address not only algorithm replacement but also the deeper systems challenge: secure migration, layered trust continuity, hybrid deployment, and resilience under evolving attack models.

This paper outlines the urgency of the post-quantum transition, identifies critical unresolved technical domains, and proposes a research direction aimed at operationally deployable security frameworks rather than isolated algorithmic substitution.

---

1. Introduction

Digital trust today depends heavily on mathematical assumptions whose hardness is tied to classical computational limits.

Current internet-scale security depends primarily on:

- integer factorization hardness
- discrete logarithm hardness
- elliptic curve discrete logarithm hardness

These assumptions underpin:

- TLS certificate systems
- VPN infrastructures
- cloud identity systems
- digital signatures
- secure financial messaging
- critical infrastructure authentication
- software update verification chains

The emergence of scalable quantum algorithms fundamentally changes this landscape.

Most notably:

Peter Shor demonstrated that quantum computation can efficiently solve integer factorization and discrete logarithm problems under quantum conditions via what is widely known as Shor's algorithm.

This creates direct future vulnerability for:

- RSA
- ECDSA
- Diffie-Hellman
- elliptic-curve key exchange systems

The consequence is not theoretical long-term concern alone—it is an infrastructure migration race already underway.

---

2. Why the Threat Is Immediate Before Quantum Arrival
2.1 Harvest-Now, Decrypt-Later Risk

Sensitive encrypted traffic intercepted today may remain strategically valuable for years.

Examples include:

- government archives
- medical records
- financial transaction trails
- intellectual property

- research data
- strategic communication archives

Any data whose confidentiality horizon exceeds quantum arrival time is already exposed.

This creates immediate urgency because delayed migration increases cumulative future exposure.

2.2 Cryptographic Migration Is Slower Than Algorithm Discovery

Replacing cryptography at scale is not equivalent to patching software.

Migration requires:

- certificate ecosystem redesign
- protocol negotiation redesign
- hardware compatibility validation
- firmware signing changes
- key lifecycle redesign
- identity continuity assurance

Historically, cryptographic migrations take many years across global infrastructure.

Therefore quantum-safe deployment must begin before universal standards fully mature.

---

3. Limitations of Current Post-Quantum Adoption

Recent standardization efforts are important but incomplete.

National Institute of Standards and Technology has advanced post-quantum cryptographic standardization through lattice-based and hash-based candidate selection.

Important standardized directions include:

- CRYSTALS-Kyber
- CRYSTALS-Dilithium
- SPHINCS+

However algorithm standardization alone does not solve operational deployment complexity.

---

4. Research Gap: System-Level Post-Quantum Security Remains Underdeveloped

The dominant current focus globally remains algorithm-centric.

This leaves major unresolved domains:

4.1 Hybrid Cryptographic Trust Models

During migration, systems must often operate with:

- classical cryptography
- post-quantum cryptography
- hybrid trust validation simultaneously

This introduces attack surfaces such as:

- downgrade negotiation
- mixed trust ambiguity
- certificate path inconsistency
- signature validation fragmentation

Research is needed for mathematically consistent hybrid trust orchestration.

4.2 Key Management Under Expanded Post-Quantum Sizes

Many post-quantum schemes introduce substantial increases in:

- public key size
- signature size
- memory requirements
- transmission overhead

Operational consequences include:

- TLS latency impact
- constrained device incompatibility
- embedded deployment barriers
- cloud handshake amplification

Research must target compression-aware secure deployment models.

4.3 Cloud-Native Quantum Safe Security Layers

Modern infrastructure increasingly depends on several cloud service providers.

Yet post-quantum readiness at cloud-native orchestration layers remains fragmented.

Critical unresolved areas:

- quantum-safe service mesh authentication
- secure container identity rotation
- PQ-safe API trust exchange
- distributed key orchestration across ephemeral workloads

---

5. Quanta Security Research Direction

Quanta Security proposes research centered on deployable post-quantum security architecture, not merely isolated cryptographic substitution.

The core philosophy:

> **"Security migration must preserve operational continuity while raising resistance against both classical and emerging quantum attack surfaces."**

---

6. Proposed Technical Research Domains

6.1 Adaptive Hybrid Cryptographic Gateways

Research target:

Design gateways capable of dynamically selecting:

- classical secure channels
- hybrid channels
- full PQ channels

based on endpoint capability, trust policy, and latency constraints.

Potential components:

- cryptographic negotiation intelligence
- policy-aware handshake engines
- downgrade resistance enforcement

6.2 Quantum-Resilient Certificate Lifecycle Models

Research target:

Investigate certificate systems capable of handling:

- dual signatures
- staged root transitions
- long-lived trust continuity

Current PKI assumptions may become structurally inadequate during migration.

6.3 Lightweight PQ Security for Resource-Constrained Systems

Critical domain:

IoT and embedded systems remain highly exposed.

Research challenge:

Deploy lattice-safe or hash-safe mechanisms under:

- limited CPU
- constrained RAM
- strict power budgets

This domain remains globally under-addressed.

6.4 Secure Data Longevity Models

Sensitive archives require long-term confidentiality.

Research area:

Develop layered encryption rotation models designed for:

- delayed cryptographic upgrades
- future-proof archival protection
- quantum-safe staged re-encryption pipelines

---

7. Why Immediate Research Investment Is Necessary

Waiting for mature universal deployment standards introduces systemic risk.

By the time quantum capability reaches disruptive thresholds:

- infrastructure replacement will still be incomplete
- legacy systems will remain exposed
- sensitive data loss becomes irreversible

The time required for safe migration exceeds the warning time likely available once quantum breakthroughs become operationally meaningful.

This makes research funding urgent now.

---

8. Strategic Importance Beyond Commercial Security

Post-quantum readiness impacts:

- national digital sovereignty
- healthcare systems
- financial continuity
- critical infrastructure resilience
- secure education systems
- industrial IP protection

This is not solely a cybersecurity upgrade.

It is future trust preservation.

---

9. Position of Quanta Security

Quanta Security aims to contribute in the following role:

- applied post-quantum systems research
- practical deployment architecture design
- migration strategy frameworks
- future security testing models

The objective is to bridge:

academic theory → deployable infrastructure

rather than remain confined to theoretical cryptographic evaluation.

---

10. Conclusion

The quantum threat is often misunderstood because the visible attack capability has not yet fully arrived.

However cryptographic transitions operate on long time horizons.

Therefore, the research window is already open.

The institutions, research groups, and technical initiatives that begin serious work now will shape secure digital trust for the next several decades.

Quanta Security seeks to participate in this foundational stage through focused research into practical post-quantum defensive systems.