Assignment 7.1: Quantum-Ready Risk Management Plan

Joshua A. Wortz

University of San Diego

CSOL-530

Cameron Carter, MS

06/22/2025

Introduction

Quantum computing promises revolutionary capabilities in processing power by harnessing the principles of quantum mechanics, such as superposition and entanglement. While these innovations could fuel scientific breakthroughs, they pose a substantial threat to existing encryption protocols that form the backbone of global cybersecurity. As quantum capabilities advance, widely used cryptographic algorithms like RSA may become obsolete, exposing sensitive data to unprecedented vulnerabilities. This paper assesses the threat posed by quantum computing to RSA encryption, examines two emerging quantum-resistant cryptographic strategies, and proposes a multi-phase roadmap for organizations to transition to quantum-safe infrastructure.

Quantum Computing and the Breakdown of RSA Encryption

RSA encryption, which is built upon the computational difficulty of factoring large prime numbers, has been a cornerstone of secure communication for decades. Its security relies on the fact that classical computers would require an impractically long time to break the encryption using brute-force methods. However, quantum computing fundamentally alters this dynamic.

Shor's algorithm, a quantum algorithm developed in 1994, can factor large integers in polynomial time—something classical computers cannot feasibly achieve. When quantum computers become sufficiently robust, Shor's algorithm will be capable of breaking RSA encryption, potentially decrypting protected data almost instantaneously (Emmanni, 2023). This renders RSA and similar asymmetric cryptographic schemes, such as Elliptic Curve Cryptography (ECC), critically vulnerable in a post-quantum world. The implications are especially concerning for stored, long-term sensitive data, which could be harvested today and

decrypted later when quantum capabilities mature—commonly referred to as the "store now, decrypt later" threat.

Evaluating Post-Quantum Cryptographic Strategies

To counteract these emerging risks, the cybersecurity community is actively pursuing post-quantum cryptographic (PQC) methods. Two of the most promising strategies are lattice-based cryptography and quantum key distribution (QKD).

Lattice-Based Cryptography

Lattice-based cryptography is based on complex mathematical problems such as the Learning With Errors (LWE) problem, which is believed to be resistant to both classical and quantum attacks. This family of cryptographic methods includes encryption schemes, digital signatures, and even fully homomorphic encryption, which enables computation on encrypted data without decryption (Emmanni, 2023). NIST has shortlisted lattice-based candidates as part of its Post-Quantum Cryptography Standardization Project, indicating strong global momentum toward adoption (NIST, 2023).

Quantum Key Distribution (QKD)

QKD utilizes principles of quantum mechanics to create secure communication channels. Unlike traditional key exchange protocols, which are vulnerable to interception, QKD detects any eavesdropping attempts due to the quantum property of measurement disturbance. The BB84 protocol is one such method that allows two parties to detect and prevent man-in-the-middle attacks with near certainty. While QKD offers theoretically unbreakable encryption, its practical

deployment faces challenges such as the need for dedicated optical infrastructure and limited range (LevelBlue, 2024).

Multi-Phase Roadmap to Quantum-Resistant Security

Phase 1: Assessment and Awareness (Year 1)

Organizations begin by evaluating their exposure to quantum threats and preparing stakeholders.

- **Goal**: Identify critical cryptographic dependencies and raise awareness.
- **Activities**: Conduct a risk assessment, inventory encryption assets, classify data sensitivity, and initiate staff training.
- **Deliverables**: Risk analysis report, asset inventory, and internal training modules.

Phase 2: Strategic Planning and Pilot Testing (Years 2–3)

In this phase, organizations explore quantum-resistant alternatives in controlled environments.

- **Goal**: Test post-quantum cryptographic (PQC) options.
- **Activities**: Form a transition team, test NIST candidate algorithms, and evaluate vendor capabilities.
- **Deliverables**: Pilot results, vendor assessments, and transition strategy recommendations.

Phase 3: Infrastructure Modernization (Years 3–5)

With proven strategies, the infrastructure is upgraded to support post-quantum resilience.

- **Goal**: Enable cryptographic agility and align systems and vendors with PQC readiness.

- **Activities**: Implement hybrid classical-PQC solutions, update key management systems, and negotiate vendor compliance.
- **Deliverables**: PQC-enabled systems, contract updates, and new architecture documentation.

Phase 4: Organization-Wide Deployment (Years 5–7)

The final phase ensures enterprise-level implementation and monitoring.

- **Goal**: Complete rollout and embed quantum-safe practices into operations.
- **Activities**: Deploy PQC organization-wide, implement monitoring tools, and update response plans.
- **Deliverables**: Full deployment documentation, security audit logs, and updated incident response protocols.

Conclusion

Quantum computing represents a double-edged sword, offering extraordinary computational potential while posing a threat to dismantle the foundations of modern encryption. RSA, once a paragon of digital security, is now at risk due to quantum algorithms like Shor's. In response, lattice-based cryptography and quantum key distribution offer viable paths to secure the future. However, success requires more than technical solutions; it demands a phased, organization-wide commitment to adapt and evolve. By acting now, organizations can ensure resilience in the coming quantum age and preserve trust in their digital infrastructures.

References

Emmanni, P. S. (2023). *The impact of quantum computing on cybersecurity*. *Journal of Mathematical & Computer Applications*, 2(2), 1–4. https://doi.org/10.47363/JMCA/2023(2)140

LevelBlue. (2024). *Quantum computing and cybersecurity: Preparing for a new age of threats*. Retrieved from https://levelblue.com/blogs/security-essentials/quantum-computing-and-cybersecurity-preparing-for-a-new-age-of-threats

National Institute of Standards and Technology (NIST). (2023). *Post-quantum cryptography standardization*. Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography