Information Systems Student Research Journal

Innovation Snapshot DOI: ISSN:

Q Secure

John Wesley Cook
The University of Alabama

Jessica Dodson
The University of Alabama

Overview

Quantum computing is a computational paradigm that leverages quantum-mechanical principles such as superposition and entanglement to solve problems significantly faster than classical computers (NIST, 2022). While quantum computing promises breakthroughs in medicine, logistics, and artificial intelligence, it also threatens the foundation of modern security. Algorithms such as RSA and ECC, which are widely used in banking, e-commerce, and government systems, will become obsolete once quantum computers mature (The Times, 2024).

Q Secure is a conceptual framework designed to help financial institutions transition to post-quantum cryptography (PQC) and safeguard sensitive customer data from emerging quantum threats. Developed for the AIS SCLC 2025 Post-Quantum Computing Security Challenge, Q Secure won 1st place amongst 20+ teams with a prize of $2,000. Our project tackled the critical question: How can organizations proactively adapt to a world where current encryption methods will no longer be secure?

The Aim

Our project was driven by a central concern: Financial systems are uniquely vulnerable to quantum computing's ability to break encryption. Payment processors, authentication systems, and fraud detection models all rely on algorithms that could soon be compromised.

Our aim was to:

- Identify quantum-resistant algorithms suitable for financial systems.
- Develop a phased migration strategy that balances security with operational continuity.
- Estimate the financial costs and risks associated with adopting PQC.
- Emphasize crypto-agility—the ability to update cryptographic methods as standards evolve.

By focusing on these goals, our project provides a practical model for how the financial sector can prepare for the post-quantum world.

The Process

Our process combined technical research with risk analysis and migration planning. From the NIST PQC Standardization Initiative, three key algorithm categories emerged.

- Lattice-based algorithms (Kyber, NTRU, Dilithium): Strong resistance to both classical and quantum attacks; suitable for key exchange and digital signatures (NIST, 2022).
- Hash-based algorithms (SPHINCS+, XMSS): Provide robust integrity verification for digital authentication, though at the cost of larger signature sizes (Simpson, 2025).
- Code-based algorithms (BIKE, Classic McEliece): Exceptionally resistant to decryption, making them ideal for long-term data encryption, though sometimes impractical for real-time applications (The Times, 2024).

Our framework directly integrates these algorithms: Kyber for key exchange, Dilithium for signatures, and BIKE for encryption. These choices were guided by NIST recommendations and strike a balance between performance, scalability, and security.

Migration Strategy

We designed a four-phase roadmap for transitioning from current RSA/ECC systems to PQC:

1. Security Assessment: Identify vulnerable RSA/ECC systems, prioritize risks, and ensure PCI-DSS/GDPR compliance.
2. Pilot Deployment: Introduce Kyber, Dilithium, and BIKE on non-critical systems, monitoring latency and throughput with Splunk and Elastic Stack.
3. Phased Migration: Transition high-priority systems in waves, supported by hybrid cryptography and IBM QRadar threat monitoring.
4. Enterprise Integration: Update compliance policies, train employees, and implement crypto-agility for future standards (NIST, 2022).

Cost Estimates

Transition costs were projected between $141,000 and $920,000, including hardware upgrades, software development, and employee training. While substantial, this investment is necessary to protect financial infrastructure against future quantum threats (Forbes Tech Council, 2025).

Reflections

This project emphasized that preparing for quantum disruption requires more than technology—it requires planning, adaptability, and people. Adaptability matters because algorithms considered secure today may be broken by new advances tomorrow (Forbes Tech Council, 2025). Employee readiness is also critical, as training and certification ensure employees can securely manage PQC systems and minimize human error. Broader implications also became clear: while our focus was finance, the same framework can be applied to healthcare, defense, and cloud computing.

Looking toward the future, tools like quantum key distribution (QKD) and ongoing regulatory guidance from NIST will help shape the security landscape. By developing Q Secure, we learned that proactive planning today is the key to safeguarding trust, stability, and innovation in the digital economy of tomorrow.

More Information

More information about the authors:

John Wesley Cook: https://www.linkedin.com/in/johnwesleycook/

Jessica Dodson: https://www.linkedin.com/in/jessicadodson03/

Declaration of AI Statement

Artificial intelligence tools were used to assist in the preparation of this document. Specifically, AI was used to help summarize our project deliverables, refine technical language, integrate references, and ensure clarity and consistency in presenting our research. All ideas, arguments, and project results remain those of the authors.

References

Forbes Tech Council. (2025). Quantum-safe infrastructure: Tough challenges and expert solutions. Forbes. Retrieved from https://www.forbes.com/councils/forbestechcouncil/2025/01/24/quantum-safe-infrastructure-tough-challenges-and-expert-solutions/

Khodadad Kashi, A., & Kues, M. (2025). Frequency-bin-encoded entanglement-based quantum key distribution in a reconfigurable frequency-multiplexed network. *Light: Science & Applications, 14,* Article 49. Retrieved from https://www.nature.com/articles/s41377-024-01696-8

NIST. (2022). Post-quantum cryptography. U.S. Department of Commerce. Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography

Simpson, J. (2025). The quantum security revolution: A CISO's guide to post-quantum cryptography. *LinkedIn.* Retrieved from https://www.linkedin.com/pulse/quantum-security-revolution-cisos-guide-post-quantum-justin-simpson-q2fke

The Times. (2024). Battle begins to stop quantum computers smashing cyber defences. The Times. Retrieved from https://www.thetimes.co.uk/article/battle-begins-to-stop-quantum-computers-smashing-cyber-defences-rzmlwqw7f