Frontiers in Computer Science and Artificial Intelligence
DOI: 10.32996/fcsai
Journal Homepage: www.al-kindipublisher.com/index.php/fcsai

FCSAI
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Quantum-Resilient Cryptographic Protocols for U.S. Data Security

Md Rasheduzzaman Labu
Department of Information Assurance and Cybersecurity, Gannon University, Erie, Pennsylvania, USA
Corresponding Author: Md Rasheduzzaman Labu, **Email:** sourcerweb@gmail.com

| ABSTRACT

As quantum computing technology advances, its capability to undermine widely adopted cryptographic systems presents a significant challenge to modern cybersecurity. This paper presents a strategic roadmap that shall help companies and industries in the USA understand how to proactively manage the risks associated with quantum-enabled attacks. The study proposes a quantum-resistant cryptographic framework, *STL-QCRYPTO*, which is targeted at bringing industry-specific methodologies for implementing quantum-safe security measures. The proposed framework guarantees long-term protection against the transformative impact of quantum computing. Emphasizing practical ways of deploying quantum-safe systems, this study gives active insight into mitigating emerging quantum cyber risks. The roadmap provides industries with the necessary tools to safeguard against key security threats that may emerge in the quantum era through a structured timeline and targeted recommendations.

| KEYWORDS

Quantum-Resilient Cryptography; Data Security; Data breaches; STL-QCRYPTO; Quantum computing

| ARTICLE INFORMATION

ACCEPTED: 15 November 2025 **PUBLISHED:** 30 November 2025 **DOI:** 10.32996/fcsai.2025.4.2.6

Introduction

The current generation in the USA is living through a very special era of innovation where digital advancement is taking huge leaps into their everyday lives, changing the way they perform daily tasks. From cloud technology to artificial intelligence and now quantum computing, things are moving more quickly than ever (Ganesan et al., 2024). With each development comes new opportunities, opening doors for industries to change, human experiences to evolve, and complex global problems to be solved. Quantum computing is leading the way into the future, offering innovations such as advanced AI systems and new material discoveries, among other areas of much quicker drug development. Quantum Computing also opens up avenues for environmental probing, using advanced quantum sensors to dive deeper than ever (Tariq et al., 2024). These are far from the next steps of technological evolution; these are landmarks in a journey toward a smarter, more connected world.

This research paper proposes a comprehensive strategic framework for mitigating quantum attacks in an industrial environment, and such a framework was organized into three different strategic levels, namely foundational, intermediate, and advanced. These strategic levels were presented according to priority order, based on the urgency of implementation and the complexity of execution involved. The pathway presented here is relatively easy to understand and very clear for an organization looking to identify ways to improve its defenses against quantum threats. It also describes the incremental adoption process in which an organization can adopt and implement each step of the strategic transition level. This paper also explores, for each level, potential industrial use cases that give insight into how each might be applied in the real world. Finally, we note the regulatory considerations industries need to address for compliance with relevant legal and policy frameworks to be achieved when putting quantum attack mitigation strategies into practice.

Copyright: © 2025 the Author(s). This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) 4.0 license (https://creativecommons.org/licenses/by/4.0/). Published by Al-Kindi Centre for Research and Development, London, United Kingdom.

Problem Statement

Sood (2024), argues that while impressive, these developments also bring major challenges. As we realize the transformative technologies, complexities abound that only can be mastered by balanced innovation with security and ethics. The arrival of fully operational quantum systems-especially one with a few hundred error-free systems offers a serious threat to digital cybersecurity as we know it today. Sodiya et al. (2024), posited that a major point of concern is the level of vulnerability these techniques would be once deployed out of mathematical problems that have been too hard to solve classically, such as factorization. This vulnerability became highlighted when Peter Shor developed a quantum algorithm that could break cryptographic systems based on classic mathematics, including RSA encryption. Shor's construction underlined the urgent need for remediation of such weaknesses; thus, the need for the development of quantum-resistant cryptography began to take hold globally. As quantum technology advances, the need for organizations to implement quantum-safe strategies of encryption becomes increasingly important in light of this threat (Tobke et al., 2023).

Allgyer et al. (2024), asserted that even though quantum computing has yet to reach the level where functional, scalable quantum computers are commercially accessible in the USA, IT practitioners cannot afford to overlook the potential risks they present. Proactive cybersecurity adoption: it's a question of when, not if. Just imagine this: if sensitive data were stolen today, it would still be encrypted and secure. At least for now. But when those quantum systems get sophisticated enough someday, that same data could be decrypted, making it unsecured and exposed. Andreou (2024), indicated that quantum computers can crack lots of cryptographic algorithms currently in use, putting sensitive information that needs long-term protection at risk. Enterprises should start deploying quantum-resistant encryption strategies now. Action today is a key component to ensuring the security of vital data in the quantum era.

Background of the Study

Figure 1 depicts the trends of data breach incidents and exposed record volume in the US from 2005 to 2020. There is an upward trend, with the data breaches increasing gradually from 157 in 2005 to peak at 1,632 in 2017 and a slight decline to 1,001 in 2020. Exposed records are more spasmodic; huge spikes occurred in 2009, 2017, and 2018. During these three years, the exposed records reached their peak at 197.61 million, 471.23 million, and 164.68 million records, respectively (Anand et al., 2024). These ups and downs in breach frequency indicate that the number of breaches is growing, while the number of records exposed differs from one breach to another. Amazingly, though the number of breaches reported in 2020 went down, records exposed were at an enormous scale, which means the nature and potential severity of cybersecurity threats change with time (Anand et al., 2024).

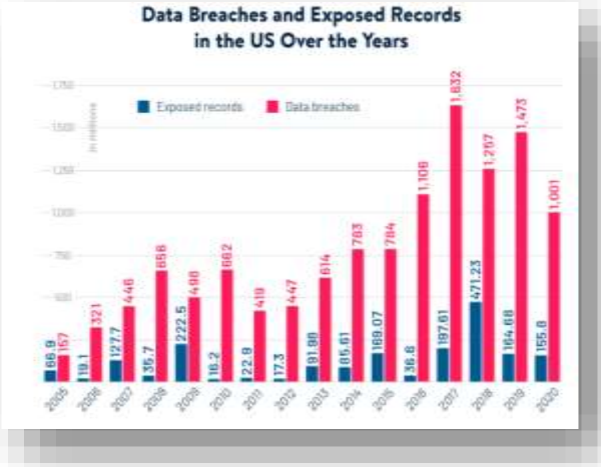

Figure 1: Exhibits Data Breaches &Exposed Records Over the Years

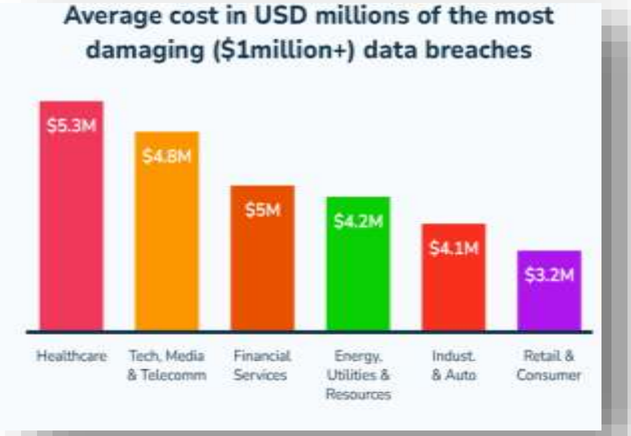

Figure 2: Displays the Average Cost of the Data Breaches

Figure 2 shows the average cost of the most damaging ($1 million+) data breaches by industry. The industries with the highest averages are Healthcare at $5.3 million, Tech, Media, and Telecom with an average cost of $4.8 million, and Financial Services at $5 million. In comparison, Energy, Utilities, and Resources are at $4.2 million, Industrial and Auto at $4.1 million, and Retail and Consumer at $3.2 million (Anand et al., 2024). That would therefore mean that data breaches in healthcare translate into much higher financial penalties owing to the sensitive nature of the data concerning patients and the great overall potential for damages.

The trends in the graphs above depict the increasing threat of data breaches in the U.S., with both incidents and the volume of records exposed seeing growth over the years. These reflect the increasingly sophisticated nature of cyberattacks and growing vulnerabilities in existing security systems. Events like those in 2017 and 2018, where records exposed increased many-fold, make clear the fact that even a single breach can become a catastrophe (Ganesan et al., 2024). With the advent of quantum computing, all these vulnerabilities are suspected to increase, because most of the cryptographic protocols in use today can be broken by a quantum system. There is therefore an urgent need for quantum-resilient cryptographic protocols that can safeguard sensitive data against a future quantum-enabled attack. Proactively adopting those advanced measures will be crucial for long-term security infrastructure for the data of the U.S. and for mitigating risks due to ever-powerful cyber threats (Brattain & Bardeen, 2024).

Research Objectives

The principal objective of this research project is to investigate and develop resilient cryptographic strategies that can combat different kinds of quantum computing attacks against sensitive information security in the United States. The study aims to pinpoint vulnerabilities in the current encryption techniques, which quantum computers can exploit in particular by investigating the implications of quantum algorithms on commonly deployed cryptographic protocols. The research will also look into existing quantum-resistant algorithms and their effectiveness, scalability, and integration into current cybersecurity frameworks. By focusing on the real-world solutions that exist and a concrete roadmap for implementing quantum-safe encryption, this paper aims to help policymakers, organizations, and security experts tackle the imminent challenges in securing data in the quantum era.

Related Works

Quantum-resistant security controls have been explored for some time in many areas, such as their implementation on specific platforms or applications, enhancing the efficiency of the algorithms, and other related aspects. The works are reviewed in the following subsections, sorted by the type of security controls.

Secure Boot

Halak et al. (2024), presented a post-quantum secure boot authentication proposal based on the hash-based signature XMSS. They implemented this solution on a secure SoC that embeds RISC-V cores. The XMSS verification hardware was controlled by the Signature Verification Unit, which was divided into four stages for secure boot through AXI interfaces. Therein, several hash calculations were performed, which were of paramount importance in most of the operation steps of XMSS verification. This optimization was done about the parallel computation of the WOTS chains, which could be reused when implementing the XMSS key and signature generation functions.

Muhammad (2024), developed a secure boot mechanism in another study using hash-based signatures, corresponding to both stateful and stateless categories. They chose the LMS signature scheme as the stateful option and SPHINCS+ as the stateless option and compared them against the traditional RSA scheme. Their results, considering the LMS implementation on an FPGA board, showed that hardware implementations of hash-based signatures are less efficient compared to RSA. Wagner et al. studied the impact of stateful and stateless hash-based signatures (LMS and XMSS, SPHINCS+, respectively) on secure boot mechanisms, considering also RSA and ECDSA. The authors here proposed a flexible hardware-software design able to support both signature types depending on hardware specifications.

Secure Access

Secure access allows control of entry to systems, netw

orks, or resources by reducing the associated risks of unauthorized users or devices. Extended Access Control enables attribute-based access control using smart cards. Chua et al. (2024), provided a quantum-resistant variant of the EAC protocol, called PQ-EAC, which uses the post-quantum digital signature schemes Dilithium, Falcon, and SPHINCS+, with the post-quantum KEM Kyber. They chose NIST's security level 3 for digital signatures and level 5 for the KEM. Hybrid schemes for both classical and post-quantum methods were also recommended in the study, as they can easily support existing systems while being prepared for future steps. Several experiments have been conducted by them to assess a variety of PQEAC performances in more practical scenarios between chip and terminal. While their verification of the Dilithium signature took 86ms, our secure access with Dilithium takes 100ms. However, considering that the verification method and the security level differ, the performance and memory usage are remarkably close to the results found by them.

Secure Update

To protect connected vehicles and devices, integrating quantum-resilient solutions into over-the-air (OTA) updates for automotive and IoT systems is essential. Randaliev et al. (2023), highlighted the importance of quantum-resistant security for IoT devices with long lifespans. They assessed the SUIT standard for IoT software updates in a post-quantum context, concentrating on digital signatures. Using the open-source SUIT implementation in RIOT, the study tested various post-quantum signature schemes on popular IoT hardware platforms such as ARM Cortex-M, RISC-V, and ESP32. The results estimated the real-world effects of transitioning from pre-quantum to post-quantum signatures on low-power, microcontroller-based IoT devices. Similarly, Bos et al. implemented the Dilithium algorithm in the AUTOSAR Adaptive Platform to secure OTA updates on the NXP S32G processor, focusing on reducing the impact on the update process while enhancing quantum resilience.

Strategic Planning & Deployment: Steps Toward Quantum-Safe Security

According to Tariq et al. (2024), the quantum threat to present security frameworks is significant and demands an urgent, "act-now" response from all industries. As these classical security infrastructures are too complex, proper countermeasures in case of potential quantum attacks must employ strategic and tactically well-planned approaches. Recognizing that security today usually is in integrated frameworks, we have developed a quantum-safe security framework that provides early mitigation against future risks, putting organizations on course for a changing threat landscape. Speaking generically, there are two main kinds of cryptography: symmetric and asymmetric cryptography.

Asymmetric Cryptography

Asymmetric cryptography relies on a complicated mathematical operation. The most common ones used include RSA. The basis of the security of RSA lies in the difficulty of factoring big numbers into their prime factors; this is considered infeasible today. In contrast with symmetric methods, which are fast but provide weak security, asymmetric cryptography is much slower. Its keys need to be much larger to provide equivalent protection. In the case of the factorization method being discovered quickly, it will require even larger primes, hence lengthening the computational requirements and reducing efficiency even more (Sood, 2024). Asymmetric systems involve two keys: one public key encrypts the data while another private key decrypts it, making asymmetric systems less efficient to implement globally in today's world of high-speed digitization. Figure 3 shows a basic diagram of encryption and decryption in asymmetric cryptography.

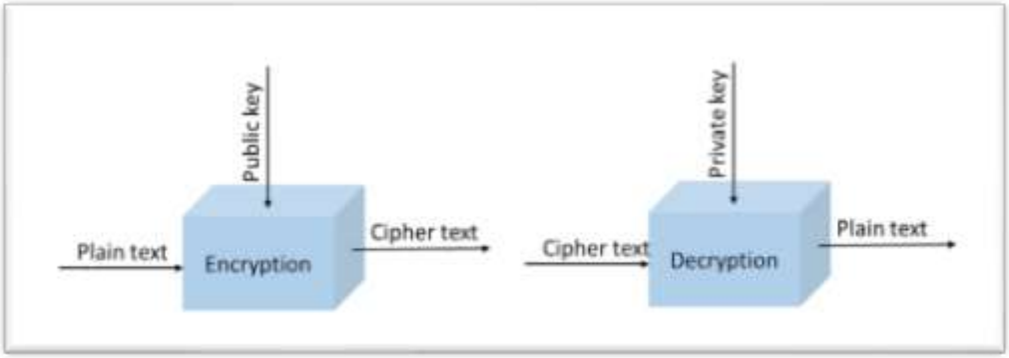

Figure 3: Depicts Encryption & Decryption in Asymmetric Cryptography

Symmetric Cryptography

As per Sodiya et al. (2024), symmetric cryptography involves the use of the same secret key by both the sender and the receiver. The key has to be shared between them through a secure, authenticated channel. Ideally, the key will be generated from a pseudorandom number generator, though true randomness remains something of a problem. It is very important to choose a high-entropy random number generator; this can lead to very good security. Symmetric cryptography usually includes better performance and shorter key lengths for the same level of security than asymmetric schemes. One of the most widely used and most secure symmetric algorithms is AES or Advanced Encryption Standard; hence, AES supports a key length of 128, 192, and 256 bits for encryption and decryption, as depicted in Figure 4.

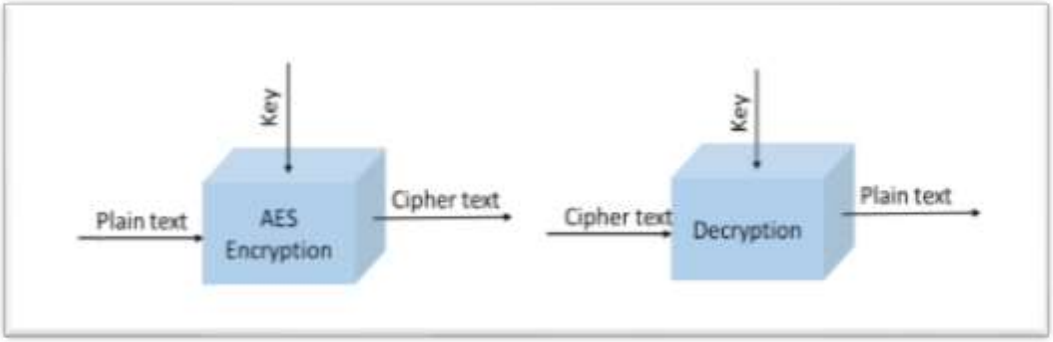

Figure 4: Showcases Encryption & Decryption in Symmetric Cryptography

From a strategic viewpoint, this research project established three different levels to facilitate the shift from traditional security approaches to quantum-safe solutions within the cybersecurity domain. These allow for the implementation of a phased plan that an organization can start working on regarding quantum-resistant measures without complete interference with ongoing operations. This shall facilitate dealing with the current vulnerabilities, planning for medium-term upgrades, and preparing for long-term quantum advances accordingly. The framework provided will enable one to respond to quantum threats in an emergent manner through proactive and holistic approaches. By adopting this multi-level strategy, businesses get future-proofed against the fast-changing technological landscape.

Strategic Transition Levels (STL)

In developing our strategic roadmap to implement quantum-safe security, we define the "Strategic Transition Level" framework that focuses on three imperative levels of defense. **STL-I**-Foundational level emphasizes securing the system with asymmetric cryptography in preparation for quantum attacks. **STL-2**-Intermediate and **STL-3**-advanced transition levels introduce more sophisticated measures of security, especially using symmetric cryptography approaches to protect against emergent quantum attacks. The approach of tiering creates a robust and adaptive framework for a defense that can comprehensively safeguard against the threat landscape of quantum, which is constantly evolving.

A. Strategic Transition Level I-(STL-I):

Recently, NIST came out with its first post-quantum cryptography standards and called for action by industries. With time, the research fraternity continued the design and evaluation of classical cryptographic algorithms with resistance to quantum attacks, with lattice-based and hash-based algorithms most prevalent. In its latest announcement, NIST standardized three cryptographic algorithms to keep post-quantum cryptography resistant against attacks from both classical and quantum computers (Bishwas & Ken, 2024). With quantum computers currently not being powerful enough to break through today's security systems, Moody spoke to the importance of proactive preparation against some sort of quantum threat in the future.

B. Strategic Transition Level 2-(STL-2)

Halak et al. (2024), postulated that the STL-2 strategy concentrates on a hybrid quantum-classical approach, with Quantum Random Number Generators (QRNGs) playing a paramount role. Contrasting with the classical random number generator, which relies on some type of deterministic algorithm or physical process, the QRNG exploits principles from quantum mechanics to generate truly random numbers. Within this STL-2 strategy, combining keys that come from QRNGs with classical symmetric-key cryptographic algorithms like AES results in much stronger protection against post-quantum attacks. This hybrid approach significantly raises the bar in terms of security by further developing protection against possible quantum threats compared to what has been achieved with the STL-I approach. Additionally, it enables businesses to migrate select parts of applications to quantum step by step without losing performance in current systems.

C. Strategic Transition Level 3 (STL-3)

The approach of STL-3 is a very intricate process for adoption and involves high investment in migrating infrastructure. A feasibility analysis should, therefore, be thoroughly performed to capture system weaknesses and, where necessary, smoothly prioritize the shift from classical to quantum solutions (De Roure & Santos, 2024). Detailed planning will be necessary for a smooth, efficient transition, and implementation. It provides an exceptionally robust defense against current and emerging quantum threats, ensuring an exceptionally high level of security assurance.

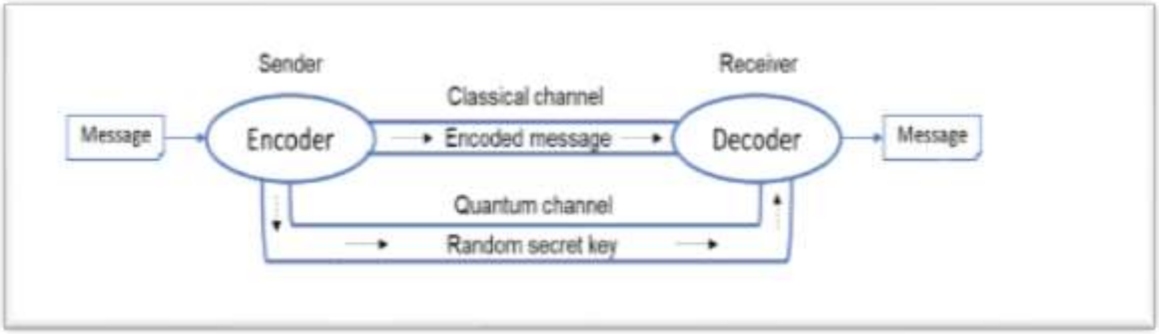

Figure 5: Portrays the Quantum Key Distribution

Figure 6 displays the strategic framework and its equivalent levels for transitioning from a classical security ecosystem to a quantum-secure surrounding.

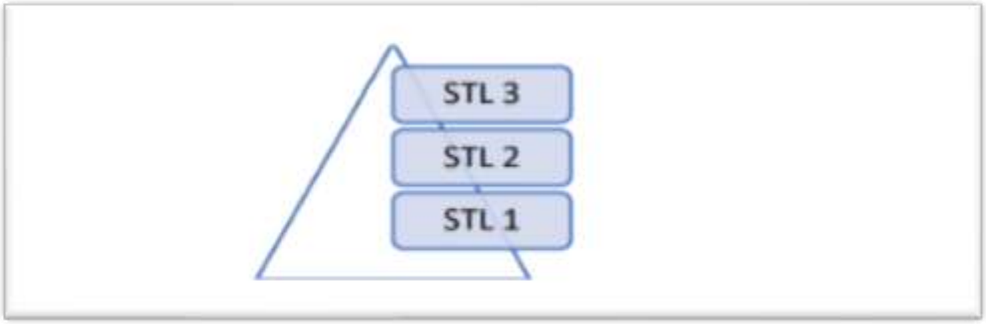

Figure 6: Depicts the Strategic Transition Level Framework

Proposed Framework for Quantum-Resilient Technology

The proposed QCRYPTO system framework is a seven-step strategic roadmap tailored to assist organizations in implementing quantum-resistant cryptography. There is progressive building at each stage to ensure systematic and impactful transitioning to quantum-resilient security. The framework includes:

- **Quest:** This phase launches the quantum threats and opportunities for exploration by industries, hence focusing on the current landscape as well as emerging quantum technologies (Asimiyu, 2024).
- **Commence:** Concentrates on the identification of vulnerabilities within classical cryptography systems that are prone to quantum attacks, the bedrock of focused mitigation (Asimiyu, 2024).
- **Review:** Revolves around assessing the current infrastructure of an organization and its local risk due to quantum exposure, identifying priorities where the most critical areas are those that are operational and in urgent need of improvement because of the quantum threat (Asimiyu, 2024).
- **Yield**: The gradual integration of quantum-resistant solutions allows for seamless compatibility to take place with existing systems, therefore fostering a culture of innovation and adaptability within an organization (Ganesan et al., 2024).
- **Pivot:** The architecture is strategically transformed, embedding the organization with quantum-resistant cryptographic algorithms of a higher order; second, the security protocols are enhanced at critical touchpoints (Ganesan et al., 2024).
- **Transcend:** This stage involves the scalability of quantum-resilient security measures across all digital assets for holistic protection, positioning an organization for the future in the handling of quantum advancements (Ganesan et al., 2024).
- **Observe**: The solution must be continuously monitored and tested post-implementation for any sort of security gaps. Updates and patches must be performed on a timely basis, not only for growing technology but also for newly emerging threats, so that the solution is resilient and stands effective against emerging cyber threats (Ganesan et al., 2024).

The proposed systematic Framework progression enables organizations to safeguard their existing systems while future-proofing their operations in the rapidly advancing quantum landscape, ensuring sustained resilience and a competitive edge. Figure 7 presents a Strategic Roadmap for the QCRYPTO framework the integration of the QCRYPTO and STL frameworks results in a strategic solution named "STL-QCRYPTO," and is shown in Figure 8.

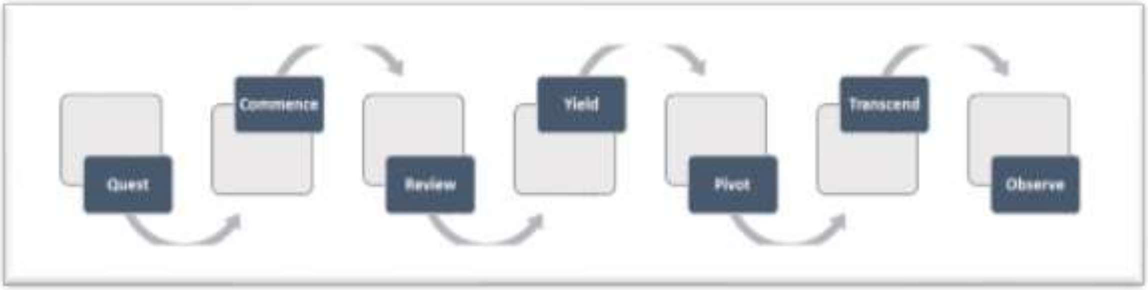

Figure 7: Exhibits the Strategic QCRYPTO System Framework

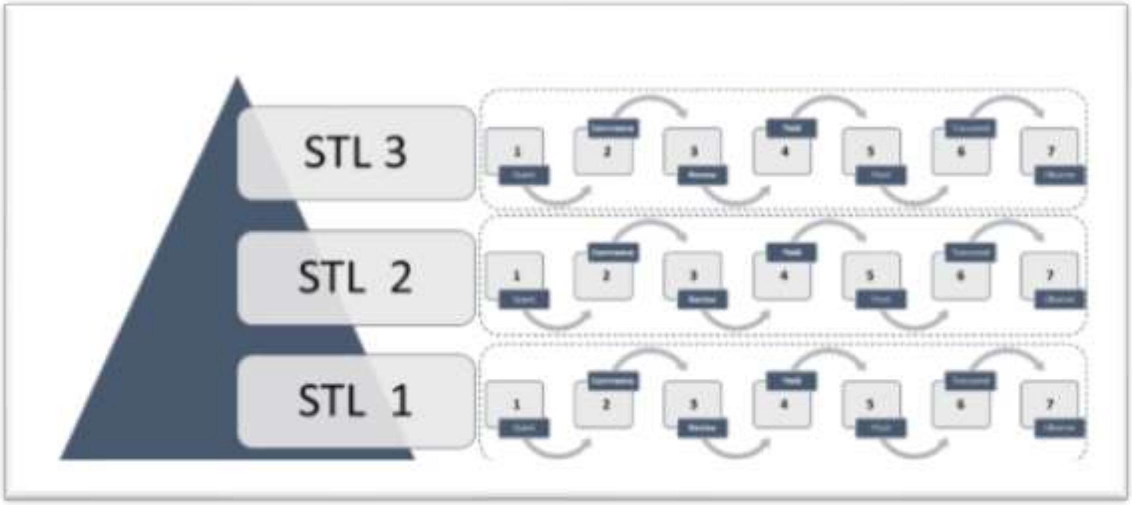

Figure 8: Depicts the Consolidated STL-QCRYPTO

Implementation Strategy

✓ **Cloud-based PQC adoption:** Leverage cloud AWS, and Azure, which are already well into developing quantum-resistant cryptography. The organizations can offload the infrastructure costs to such providers.

✓ **Quantum-Safe VPNs and TLS-**Employ quantum-safe VPNs for remote access and TLS for web communications.

✓ **End-to-End Encryption:** PQC Implementation algorithms like CRYSTALS-Kyber for secure communications using software-based solutions that minimize hardware Investment.

✓ **Hybrid Cryptographic Models**: Implementation can be performed by using a hybrid approach combining classical and post-quantum cryptography to maintain backward compatibility while progressively adopting PQC.

✓ I**nvest in PQC-compatible HSMs:** Investment in HSM and encryption modules for supporting post-quantum algorithms like CRYSTALS-Dilithium and FALCON.

✓ **Network Layer Security:** Firewalls, routers, and VPNs should be upgraded to support PQC standards. The mid-size organizations might also need to invest in network hardware capable of dealing with more elaborate cryptographic Operations.

✓ **Progressive Hardware Upgrades:** Adopt a phased approach to replacing vulnerable hardware with quantum-resistant components, focusing on key systems first.

Conclusion

To sum up, quantum computing presents a plethora of opportunities mixed with great challenges for industries globally. Further advancements in the area of quantum technologies are going to bring enormous transformations for fields like artificial intelligence, materials science, and healthcare. The strategic roadmap presented in this paper is practically able to guide organizations and industries proactively toward the quantum threat. It also arranges mitigation strategies into three tiers of systematically implemented controls: Foundational, Intermediate, and Advanced. The framework thus enables organizations to prioritize their respective actions based on preparedness, resource availability, and solution complexity. This structured yet adaptive and dynamic approach means that at every level of scale, even foundational measures enhance quantum resilience, whereas advanced strategies deliver comprehensive, future-ready defenses.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Allgyer, W., White, T., & Youssef, T. A. (2024). Securing the Future: A Comprehensive Review of Post-Quantum Cryptography and Emerging Algorithms. *SoutheastCon 2024*, 1282-1287.

[2] Anand, A., & Hassabnis, A. (2024, June). Qcrypt: Leveraging Post-Quantum Cryptography for Enhanced Security of Data at Rest. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-9). IEEE.

[3] Andreou, A., Mavromoustakis, C. X., Markakis, E. K., Mastorakis, G., Pallis, E., & Bourdena, A. (2024). Exploring Quantum-Resistant Cryptography Solutions for Health Data Exchange. In *Intelligent Technologies for Healthcare Business Applications* (pp. 19-47). Cham: Springer Nature Switzerland.

[4] Asimiyu, Z. (2024). Quantum-Resistant Cybersecurity for Critical Infrastructure: Preparing for the Post-Quantum Era in National Defense.

[5] Aydeger, A., Zeydan, E., Yadav, A. K., Hemachandra, K. T., & Liyanage, M. (2024, October). Towards a quantum-resilient future: Strategies for transitioning to post-quantum cryptography. In *2024 15th International Conference on Network of the Future (NoF)* (pp. 195-203). IEEE.

[6] Brattain, W., & Bardeen, J. (2022). Quantum and the Cybersecurity Imperative. *Dig tal Debates*, 15.

[7] Bishwas, A. K., & Sen, M. (2024). Strategic Roadmap for Quantum-Resistant Security: A Framework for Preparing Industries for the Quantum Threat. *arXiv preprint arXiv:2411.09995*.

[8] Ganesan, K. S., Gupta, S., Kandele, S., Kumar, S., Maddipati, H. C., Sahu, R. A., & Saraswat, V. (2024). Quantum-Resilient Security Controls. In *Proceedings of Recent Advances in Quantum Computing and Technology* (pp. 12-19).

[9] Halak, B., Gibson, T., Henley, M., Botea, C. B., Heath, B., & Khan, S. (2024). Evaluation of performance, energy, and computation costs of quantum-attack resilient encryption algorithms for embedded devices. *IEEE Access*.

[10] De Roure, D., & Santos, O. (2023). NLP, the BB84 quantum cryptography protocol, and the NIST-approved Quantum-Resistant Cryptographic Algorithms. *Authorea Preprints*.

[11] Radanliev, P., De Roure, D., & Santos, O. (2023). Red Teaming Generative AI/NLP, the BB84 quantum cryptography protocol, and the NIST-approved Quantum-Resistant Cryptographic Algorithms. *arXiv preprint arXiv:2310.04425*.

[12] SaberiKamarposhti, M., Ng, K. W., Chua, F. F., Abdullah, J., Yadollahi, M., Moradi, M., & Ahmadpour, S. (2024). Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data. *Heliyon*, *10*(10).

[13] Singamaneni, K. K., & Muhammad, G. (2024). A novel integrated quantum-resistant cryptography for secure scientific data exchange in ad hoc networks. *Ad Hoc Networks*, *164*, 103607.

[14] Sodiya, E. O., Umoga, U. J., Amoo, O. O., & Atadoga, A. (2024). Quantum computing and its potential impact on US cybersecurity: A review: Scrutinizing the challenges and opportunities presented by quantum technologies in safeguarding digital assets. *Global Journal of Engineering and Technology Advances*, *18*(2), 049-064.

[15] Sood, N. (2024). Cryptography in Post Quantum Computing Era. *Available at SSRN 4705470*.

[16] Tariq, L., Atta, A., Farooq, U., Anwar, N., Asim, M., & Tabassum, N. (2024). Quantum-Inspired Cryptography Protocols for Enhancing Security in Cloud Computing Infrastructures. *STATISTICS, COMPUTING AND INTERDISCIPLINARY RESEARCH*, *6*(1), 19-31.

[17] Többe, L., Grote, O., & Ahrens, A. (2023, May). A Practical Approach to Quantum Resilient Cloud Usage Obtaining Data Privacy. In *2023 International Interdisciplinary PhD Workshop (IIPhDW)* (pp. 1-4). IEEE.