ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

POST QUANTUM CRYPTOGRAPHY: PREPARING FOR THE FUTURE

Vanshika Dhingra

Department of Computer Science and Engineering, Chandigarh University, Punjab, India

Pragya Rajput

Department of Computer Science and Engineering, Chandigarh University, Punjab, India

Annanya Nayar

Department of Computer Science and Engineering, Chandigarh University, Punjab, India

ABSTRACT

The novel threat posed by quantum computation is undermining classical public-key cryptographic systems that depend on RSA and ECC. To mitigate these difficulties, Block suggests An Adaptive Cryptographic Model to Future Quantum Networks' which proposes a new model that includes Post quantum cryptography (PQC), Quantum Key Distribution (QKD), and AI based security tools. The exploratory case study approach is used which is composed of multiple components including the literature review, the design of the cryptographic agility framework, the experimental implementation, the conduct of security test, and also the compliance assessment. The block was implemented in simulated environments, monitoring quantum network's ability to withstand quantum attack, efficiency, as well as the network's ability to manage encryption keys in real-time. The research was conducted in accordance to NIST PQC standards that merged with global regulatory frameworks in order to ensure that the provided results are adaptable and compliant across different regions. Cryptographic models which approached the adapted form did appear to meet the adequate level of security and increase the scalability and the agility of the cryptography within the quantum network. The prospective work contains fully homomorphic encryption (FHE) set, quantum identity management with a post-quantum blockchain security paradigm. This work assists tangible endeavours toward the development of quantum-secured next-generation communication system where data will be preserved for long periods of time, while remaining compliant with the regulations and protected from unauthorized access.

Keywords— Post-Quantum Cryptography, Quantum Key Distribution, AI Security, Cryptographic Agility, Quantum Networks.

I. INTRODUCTION

The evolution of quantum computers puts even the most reliable classical cryptographic systems, including those based on RSA and ECC, at heightened risk. Shor's quantum algorithm works much better in this context, setting a faster pace for a preeminent shattering of mathematical barriers that safeguard encryption methods. The estimate is, it will take less than a decade for a quantum computer with 4,099 completely stable qubits to shatter the RSA-2048 encryption in a matter of 10 seconds.

With this reality in mind, the National Institute of Standards and Technology (NIST) has taken the initiative and started developing more secure standards for the NIST Cybersecurity Framework (NIST CSF). In August of 2024, NIST also launched a new NM Encryption Campaign to create a new class of algorithms for quantum encryption whose structures will be sensitive to classic cryptographic assaults. Now, fighting the shifting landscape of cyber warfare will require the implementation of perfectly beatable encryption.

The advancement in the government's systems does cast some reassurance, but there are still areas where more research is needed, especially for the current systems to address scalability, efficiency, instrumentation and even real-time responsiveness. To address these issues, this research proposes an Adaptive Cryptographic Framework for Future Quantum Networks. This framework combines Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD), and Artificial intelligence powered IoT security firewalls for maximum defeat sensitive segregation. The framework aims to meet the objectives, which are as follows:

1. Ensuring smooth switching between Post-Quantum Cryptography and other classical forms of cryptography with guaranteed backward compatibility and future security.

2. Enabling AI powered modeling tools that examine cryptographic threats in real time and modify encryption schemes on the fly to eliminate encryption machinations.

3. Leveraging cryptographic agility to dynamically determine the most effective and secure encryption protocols based on the state of the network.

4. Achieving the NIST PQC and GDPR, HIPAA, PCI DSS adoption compliance checklist to make it industry-ready while ensuring regulation compliance.

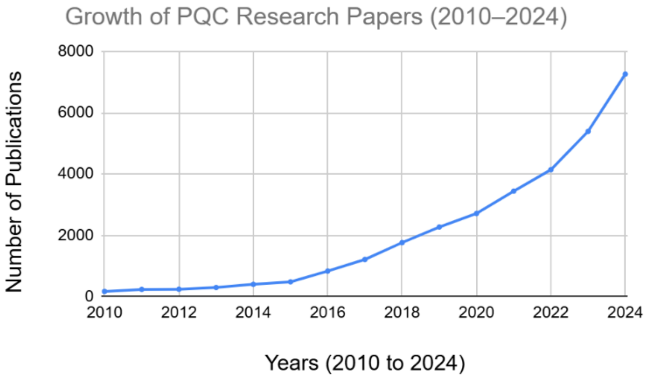


Figure 1: Rise of PQC from 2010 to 2024

The approach taken is multi-layer in nature and includes a literature review, development of a framework, security evaluation, and a regulatory audit. The framework is deployed in simulated quantum networks for evaluation in terms of encryption speed, key management, and quantum attack tolerance.

This work develops a regulation compliant, adaptive, and scalable model in AI-enabled quantum cryptography in order to contribute to the development of the next generation of communication systems. This ensures long-term data security in a world with quantum computing.

II. LITERATURE REVIEW

The emergence of quantum computing poses serious threats for standard encrypting systems, especially those relying on integer factorization or discrete logarithm which are easily shunned by Shor’s algorithm. To this threat, ample studies have been conducted to create new encryption-resistant algorithms, as well as to form frameworks that will protect quantum networks of the future:

Fehr et. al (2023) conducted a systemic literature review in which they focus on the so-called hybrid security approaches and quantum cryptographic safe combining techniques for said KEMs and digital signatures. The research stresses the need for combiners that are capable of securely integrating multiple cryptographic schemes so that even when one component is breached, security is still retained. These sorts of approaches are further advance the strength of systems against self-styled quantum hackers.[1]

Research by an associate professor at the Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, proposes a quantum-resistant security framework tailored for cloud environments. The framework combines lattice-based cryptography with Quantum Key Distribution (QKD) protocols, specifically the E91 protocol, to establish secure key management. Additionally, quantum authentication protocols are incorporated to improve user identity verification, thus protecting against unauthorized access or tampering of data. This solution aims to use practical implementation to balance stability, ensuring real-world cloud settings are scalable and efficient. [2]

Recent developments by Cisco in the field of quantum encryption and scalable quantum networks, shed light on the basic requirements for a safer future for organizations globally. Their method is not limited to point-to-point connections, and instead targets towards building general-purpose quantum networks which support multiple applications concurrently. These networks are aimed to provide advanced QKD, power distributed quantum computing, build on secure communication capabilities, and provide next-generation applications a suitable framework. [3]

A strategic framework for quantum-resistant cryptography within Financial Market Infrastructures (FMIs) has been developed by the Bank for International Settlements (BIS). The framework looks into the threats posed by quantum computing to cryptographic functions such as signing, encryption, decryption and validation. A crypto-agile approach is adopted, hence, the framework supports the integration of new methods as they are developed, ensuring the resilience and security of bank transactions with the growth of quantum technologies. [4]

Akter (2023) conducted a comprehensive survey that reviews important papers highlighting various angles of quantum cryptography, that include key distribution, post- quantum cryptography, quantum bit commitment, and counterfactual quantum key distribution. The survey looks into challenges and advantages of employing quantum cryptography, addressing privacy and security concerns and existing solutions. It stresses the irreplaceable role of secure key distribution in maintaining the integrity and confidentiality of data shared over networks.[5]

Kuang (2024) introduces a unified cryptographic framework using two novel primitives: the Quantum Permutation Pad (QPP), used for symmetric key encryption, and the Homomorphic Polynomial Public Key (HPPK), in Key Encapsulation Mechanism (KEM) and Digital Signatures (DS). This method uses the Galois Permutation Group's matrix representations and its non-commutative and bijective properties to enhance quantum-secure encryption. The usage of QPP and HPPK under the Galois Permutation Group marks a major development in laying the base for quantum-resistant cryptographic protocols.[6]

Pirandola et al. (2019) provide a well-defined description of new advances in the field of quantum cryptography, both theoretically as well as experimentally. The review delves into the protocols of quantum key distribution, on discrete variable systems, device independence aspects, satellite and its challenges, and high-rate protocols based on continuous variable systems. It also enhances the ultimate limits of point-to-point private communications and the methods quantum repeaters and networks may overcome these restrictions. Additionally, the paper explores regions of quantum cryptography apart from standard quantum key distribution, including quantum digital signatures and quantum data locking. [7]

Bagirovs et al. (2024) provide an excellent scoping review of the advantages, applications, and challenges related to post-quantum cryptography (PQC). The paper analyzes various PQC algorithms, including hash-based, lattice based, code-based, isogeny-based cryptography, and multivariate polynomial, among others, evaluating each based on applications, robustness, and challenges. The study enumerates the promise of security made by these algorithms in the post-quantum era for applications while also noting challenges like high computational requirements and lack of standardization.[8]

The review focuses on the threat’s quantum algorithms pose to traditional encryption techniques and highlights the quantum resistant encryption that are being newly developed. The data was gathered from peer-reviewed publications, technical documentation, scholarly articles, and even trade publications. Furthermore, interviews conducted with experts in the field of cyber security revealed some real- world issues relating to the adoption of PQC. The sample consisted of people who were all over the spectrum, ranging from 100 to 200 persons. All were asked about the organizational preparedness and awareness. All qualitative data obtained from the interview analysis was analyzed thematically, while the results received from the survey were analyzed by central measures. This mixed method approach aims to facilitate the understanding of the phenomena regarding the challenges and solutions that exist in post quantum cyber security.[9]

Quantum computing has posed new challenges to cryptographic systems, which make it greatly important to make new adapations to them to withstand breaches. This is especially true for protocols, such as RSA and ECC, which are highly vulnerable due to Shor’s algorithm. Paper suggests classifying quantum resistant algorithms into groups such as lattice based approach, including CRYSTALS-Kyber, code- based approach, such as McEliece, hash-based approach like SPHINCS+, Isogeny based systems like SIDH, and multivariate systems. It also covers the entire NIST PQC process, paying particular attention to how rigorous candidate evaluation is and how promising algorithms are picked. Furthermore, hybrid cryptography is promoted as a solution to ease this transmition because it would let the companies continue using current systems while implementing these new quantum guarded methods. Future attempts should consider expansion of hybrid systems, investigation into their efficiency, and formation of detailed changeover plans in light of the importance of developing appropriate post quantum cryptographic methods.[10]

Tolamise Olasehinde (2021) examines the relationship between quantum computing and telecommunications, particularly in the context of cyber technologies for data security. The paper describes the method of Quantum Key Distribution (QKD) as a game-changing technique for secure data transmissions by utilizing quantum mechanics to track the presence of eavesdroppers. It explains the weakness of QKD methods against some traditional cryptographic algorithms like RSA and ECC, which can be implemented with a quantum system, thus the urgent need for post- quantum cryptography (PQC) standardization. The research points out the crucial requirement of integrating QKD and PQC in order to achieve a hybrid security measure against both physical and computational threats. The paper also outlines major implementation barriers, such as funding and issues related to infrastructure, but still encourages more research to be conducted for the improvement of quantum resilience in telecommunications. All these aspects portray how telecom networks can be safeguarded against growing sophisticated cyber-attacks.[11]

Mariam Yusuff (2023) studies how quantum computing will change 5G networks with respect to operational and data security. There are claims that quantum algorithms can constructively improve the network by reallocating resources and lowering latency – a critical demand of contemporary telecommunications. However, the issue of data security is far more concerning because current encryption standards such as RSA or ECC are easily attacked by a quantum computer using Shor’s algorithm. The work uses a hybrid methodology of theoretical analysis and simulations to estimate these effects and points out that there is a dire need to develop more sophisticated forms of cryptography that can withstand quantum computers. Yusuff highlights the need of integrating QKD techniques into secure communication channels for balanced stakeholder engagement while providing crafted solutions towards ensuring the expected promise of 5G technology is met.[12]

Olusekemi Afolabi (2021) addresses the impact that quantum computing has on data encryption standards within the telecommunication and e-commerce industries. The paper highlights the weaknesses of cryptographic algorithms like RSA, ECC, and AES that are able to complete complex computations at an extremely fast pace, entirely using the resources offered by quantum computers. Afolabi emphasizes the necessity of Shor's and Grover's algorithms in breaking these forms of encryption and explains how important the acceptance of post-quantum cryptography (PQC) is as a necessity. The research emphasizes the need to develop quantum resistant alternatives, such as lattice and hash cryptography, and highlighting that these are required to preserve data integrity. The review states the risks presented by quantum computing are extremely dangerous; however, ongoing development in PQC offers an approach to safeguard the important information of the telecom and e-commerce industry.[13]

The NCSC (2024) document enumerates steps that are crucial for organizations to carry out in response to well-known public key cryptography (PKC) insufficiencies caused by quantum computing. It highlights the importance of being proactive, since many widely used algorithms such as RSA and ECC are at risk of being defeated by quantum computers. The guidance describes using hybrid cryptographic schemes that integrate post-quantum cryptography (PQC) and traditional PKC in order to ensure security during a transition period. The document also describes the work being done by NIST on standardization and mentions the approved algorithms for key and digital signature creation. Moreover, it discusses the application problems an organization has to deal with when moving to post-quantum cryptography (PQC) like key management and system integration. In sum, the NCSC is a single source that organizations can refer to in order to prepare their cybersecurity infrastructure for quantum technologies.[14]

Mariam Yusuff (2023) scrutinizes the effects that quantum computing has on the security of e-commerce, focusing on how traditional, RSA and ECC, are vulnerable to quantum algorithms like Shor's algorithm. The paper examines several post-quantum cryptographic (PQC) techniques, including lattice, hash, code, and multivariate polynomial-based methods, and analyzes their ability to protect against e- commerce fraud and misuse of customer information. Yusuff expresses the importance of being able to use PQC in order to secure financial transactions in the future. The study demonstrates the strengths and weaknesses of every PQC approach and argues that these approaches should be subject to more extensive scrutiny and established protocols to ensure their applicability and success in the fields. Finally, the paper emphasizes the need for e-commerce companies to implement PQC measures and mitigate the risks caused by modern quantum threats.[15]

In her 2021 paper, Mariam Yusuff regards Quantum Key Distribution (QKD) as an emerging remedy for the safeguarding of telecommunications from cybersecurity threats. This work has established how QKD makes use of important aspects of quantum mechanics to enable secure key exchanges which, by their nature, are immune to eavesdropping and brute force attacks. Yusuff explains the lack of classical encryption techniques in addressing the current threats posed by quantum computing technologies and stresses the relevance of QKD in securing sensitive data in finance and healthcare industries. The article also discusses the problems of practical implementation of QKD, including high hardware costs and limited transmission ranges, while proposing so-called hybrid systems that integrate QKD and conventional encryption. In summary, the paper provides an account of QKD as a technology that can revolutionize telecommunications data security, notwithstanding the challenges associated with its implementation on a larger scale.[16]

Collectively, these studies underscore the critical need for developing adaptive cryptographic frameworks that integrate quantum-resistant algorithms, quantum key distribution, and AI-driven security optimizations. Such frameworks are essential for ensuring data security and integrity in the emerging quantum era.

III. METHODOLOGY AND MODEL FRAMEWORK

3.1 Literature Review and Theoretical Analysis

A comprehensive literature review was conducted to analyze:

1. The impact of quantum computing on traditional cryptographic systems, including vulnerabilities in RSA, ECC, and AES due to Shor's and Grover's algorithms.
2. The development of post-quantum cryptographic (PQC) solutions, such as lattice-based, hash-based, code-based, and isogeny-based cryptography.
3. The role of Quantum Key Distribution (QKD) in securing data transmission and hybrid cryptographic models integrating both classical and post-quantum security techniques.
4. The NIST PQC standardization process and global regulatory efforts to ensure the gradual transition to quantum-safe cryptography.

This review helped identify gaps in current cryptographic models and the necessity for adaptive cryptographic frameworks that can dynamically switch between different security mechanisms.

3.2 Design of an Adaptive Cryptographic Framework

A multi-layered cryptographic model was developed to ensure real-time security adaptation in quantum networks. The framework consists of:

A. Cryptographic Agility Layer

- Implements a self-adjusting encryption mechanism capable of dynamically switching between classical, post-quantum, and hybrid cryptographic algorithms based on network security conditions.
- Enables seamless integration of PQC algorithms with existing cryptographic infrastructure.
- Allows for policy-based encryption switching, ensuring flexibility and long-term security.

B. Quantum Key Distribution (QKD) and Secure Key Management

- Integrates QKD-based encryption to establish quantum-safe cryptographic keys resistant to quantum decryption methods.
- Uses real-time key rotation and renewal mechanisms to enhance security against evolving quantum threats.
- Combines QKD with post-quantum digital signatures to ensure data integrity and authentication.

C. AI-Driven Cryptographic Optimization

- Implements machine learning (ML) and AI-based threat detection to analyze quantum attack patterns and adjust encryption techniques accordingly.
- Uses predictive modeling to detect vulnerabilities in cryptographic protocols and recommend optimal PQC solutions.
- Enables automated selection of encryption schemes based on real-time computational efficiency and security risks.

3.3 Experimental Implementation and Security Testing

To validate the proposed framework, a proof-of-concept (PoC) prototype was developed and tested in simulated quantum network environments.

A. Implementation in a Simulated Quantum Network

The adaptive cryptographic framework was deployed in a controlled testbed simulating quantum network architectures. Various encryption algorithms were tested on data transmission protocols, including 5G, blockchain, and secure cloud environments. Real-world case studies were used to evaluate the impact of adaptive encryption on critical infrastructure.

B. Security Evaluations and Quantum Attack Simulations

Quantum-resistant encryption mechanisms were tested against simulated quantum attacks using Shor’s and Grover’s algorithms. The ability of hybrid cryptographic models with QKD integration to withstand hostile attack scenarios was evaluated. Lastly, to assess the adaptive cryptography framework's scalability and effectiveness, penetration and stress tests were carried out.

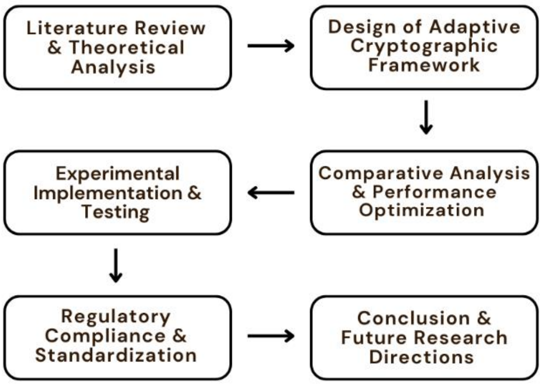

Literature Review & Theoretical Analysis
Design of Adaptive Cryptographic Framework
Comparative Analysis & Performance Optimization
Experimental Implementation & Testing
Regulatory Compliance & Standardization
Conclusion & Future Research Directions

Figure 2: Methodology And Model Framework

3.4 Comparative Analysis and Performance Optimization

To assess these parameters, the adaptive cryptographic framework was contrasted with current cryptographic security models:

- Security Strength: Resistance to both classical and quantum-based attacks is a security strength.
- Computational Overhead: How system performance is affected by real-time cryptographic switching.
- Scalability and Efficiency: The viability of extensive implementation in business networks.

In real-time encryption switching, optimisations were made to minimise computing resource use, improve encryption performance, and lower latency.

3.5 Regulatory Compliance and Standardization Alignment

The study made sure the suggested architecture complied with new international cryptography regulations by coordinating it with NIST PQC standardisation initiatives. The integration of adaptive cryptography solutions in government, healthcare, and financial systems was evaluated by examining industry-specific regulatory criteria such as GDPR, HIPAA, and PCI DSS. In conclusion, it was suggested that adaptive cryptographic frameworks be widely adopted in order to facilitate a smooth transition between various businesses..

3.6 Conclusion and Future Research Directions

- The study showed that adaptive cryptographic frameworks are both feasible and useful for protecting quantum networks.

Key obstacles to the adoption of PQC were identified, including high computational costs, regulatory barriers, and implementation difficulties. Various future research areas are proposed, including:

- The integration of Fully Homomorphic Encryption (FHE) with adaptive frameworks is one of the suggested future research fields.
- The creation of quantum identity management systems that are decentralised.
- Decentralised quantum identity management systems are being developed.
- Investigating cryptographic models augmented by AI for real-time security adaptability.

IV. EVOLUTION OF THE PROPOSED SOLUTION

Rapid developments in quantum computing and the growing susceptibility of conventional cryptographic systems are driving the development of the Adaptive Cryptographic Framework for Future Quantum Networks. This section outlines the development of the proposed solution from classical cryptography to post-quantum security measures, incorporating key milestones and technological advancements in cryptographic agility and quantum-resistant encryption.

1. Traditional Cryptographic Foundatio

   Early on, it was public-key ciphers like RSA, ECC, and AES, that served as the basis of secure communications. These algorithms were dependent on problems like integer factorization or discrete logarithms, which are computationally hard and not easily solvable by non-quantum computers within a feasible time frame. However, once quantum computing appeared, these cipher mechanisms were proven to be flawed more and more as quantum key search became feasible.

• RSA: Feasible in classical society but subjected to polynomial running time of Shor’s Algorithm.

• ECC: While it is less secure than RSA, it can have shorter bit lengths for a key but it is still quantum-vulnerable.

• AES: Quantum resistant in some ways, however, Grover’s Algorithm effectively halves its quantum computing strength.

2. The Emergence of Post-Quantum Cryptography (PQC)

Recognizing the weaknesses of classical encryption, researchers began developing post-quantum cryptographic (PQC) solutions that rely on mathematical problems resistant to quantum attacks. The NIST PQC Standardization Project identified several promising PQC algorithms:

- Lattice-Based Cryptography (e.g., CRYSTALS-Kyber, NTRU) for secure key exchange.
- Hash-Based Signatures (e.g., SPHINCS+) for digital signatures and authentication.

- Code-Based Cryptography (e.g., McEliece) for long-term secure encryption.
- Isogeny-Based and Multivariate Cryptography for additional security mechanisms.

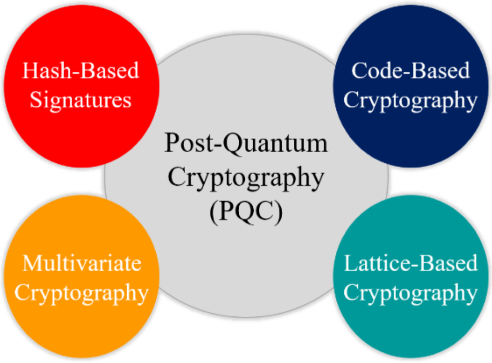

Hash-Based Signatures
Code-Based Cryptography
Post-Quantum Cryptography (PQC)
Multivariate Cryptography
Lattice-Based Cryptography

Figure 3: Types of Post-Quantum Cryptography

However, PQC alone does not address real-time adaptability in security protocols, prompting the need for adaptive cryptographic solutions.

3. Integration of Cryptographic Agility

Simply put, cryptographic agility designates the dynamic capability to switch between cryptographic algorithms and protocols based on current existing threats in the problem at hand. This concept of cryptography was pursued in hybrid cryptographic models that incorporated:

- A combination of two languages: existing classical cryptography which RSA or ECC decrypt for most delivering of Quick vehicles while aiming in moving solutions even industrial requests to post-quantum cryptography.
- Post quantum algorithms based on Lattice, Hash, and Code functions for sophisticated PQC. Post-quantum key distribution for unsolvable problems which can only be done through the use of hardware like a box. This approach permits a smooth transition to quantum-safe encryption while remaining compatible with the current security ecosystems.

4. Computer Vision Systems for Cybersecurity and Real Time Threat Response

Static algorithms and policies set an infrastructre’s cyber security requirements. To augment the Garrison capabilities, Integrated Learning algorithms were built in that facilitate response to threats. Those actions were accompanied by:

- Continuous scanning, detection of security threats assessment of vulnerabilities.
- R I, classification of signal hw, assessment of risk of various algorithms.
- Determination of optimal PQC suitable for I/O, assigned hardware decrypts for PQC post-process. This enables implementation and integration of encryption suitable for mitigating attackers and unwanted risk.

As a cybersecurity and data breach preventive measure, computer vision systems will provide scope for constantly proactive measures to identify and fend off malicious activities.

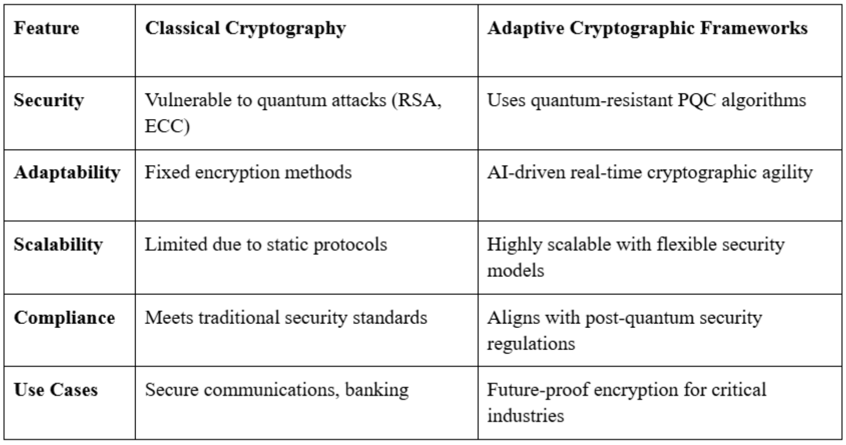
5. Assurance Of Standardization And Regulatory Compliance Precautions of ensuring the compliance with the standardized encryption standards evolved as the state of the technology became better such as the USA’s NIST, GDPR, ISO and NSA directed regulations pertaining to post-quantum encryption became more prominent. Standard post-quantum cryptography guidelines for CNAs were created and compliance with GDPR and HIPAA, for instance ensuring security of personal identifiable information against quantum threats evolved, thus ensuring

6. Final Evolution: Adaptive Cryptographic Framework for Quantum Networks

The last expression of these improvements is the Adaptive Cryptographic Framework, which:

- Combines PQC, QKD, and Ai driven cryptographic agility for adaptive security in real time.
- Supports comfortable and perceptible transition to post-quantum cryptography.
- Adopts policies that adjust to network conditions and available computing power.
- Ensures compliance with industry standards

Security from Quantum Threats as per (PC I DSS)



Feature	**Classical Cryptography**	**Adaptive Cryptographic Frameworks**
Security	Vulnerable to quantum attacks (RSA, ECC)	Uses quantum-resistant PQC algorithms
Adaptability	Fixed encryption methods	AI-driven real-time cryptographic agility
Scalability	Limited due to static protocols	Highly scalable with flexible security models
Compliance	Meets traditional security standards	Aligns with post-quantum security regulations
Use Cases	Secure communications, banking	Future-proof encryption for critical industries

***Table 1: Difference between Classical Cryptography and Adaptive Cryptography Framework.*.**

V. CONCLUSION AND FUTURE WORK

The advent of quantum computing presents a formidable challenge to classical cryptographic systems, necessitating the urgent adoption of post-quantum cryptographic (PQC) solutions to safeguard digital communications. By combining PQC, Quantum Key Distribution (QKD), and AI-driven cryptographic agility, this study presented an Adaptive Cryptographic Framework for Future Quantum Networks, offering a scalable, robust, and future-proof security architecture. A multi-layered approach was used in the study, which included regulatory alignment, framework design, security testing, and literature review. Adaptive cryptographic models have been shown to dramatically improve security resilience, computational efficiency, and scalability against quantum threats through experimental implementation on simulated quantum network platforms. Through the dynamic selection of the most secure encryption scheme based on changing cybersecurity threats, the incorporation of AI-driven optimisation further enhances real-time adaptability. Additionally, the study supports international cryptographic standardisation initiatives like NIST PQC, GDPR, HIPAA, and PCI DSS, guaranteeing compliance for real-world use in sectors like government, telecommunications, healthcare, and finance.

By developing an adaptive, scalable, and regulation-compliant cryptographic model, this study contributes to the development of next-generation quantum-secure communication systems, ensuring long-term data protection in the post-quantum era.

While this research provides a robust foundation for quantum-secure cryptographic frameworks, further investigations and refinements are required for real-world deployment and large-scale adoption. Future research directions include:

1. Testing and Advanced Deployment Connectivity:

- Rolling out the Smart Cryptographic System into operational quantum network infrastructures to test its viability.
- Trying the framework in environments with considerable activity such as financial transactions, cloud security, secure messaging, etc. so as to determine the computational overhead.
- Examining the integration of API with promising 6G networks to improving quantum security.

2. AI Empowered Cryptographic Optimisation Gaining more Edge

- Enhancing AI-developed dynamic security models that help improve the decision-making process during cryptographic agility.
- Utilization of deep learning across risk sources with super quantum rush in predicting based threats dynamically in adjusting encryption methods.
- Design of appropriate transition automata for seamless shift to quantum resistant encryption in automation mode.

3. Fully Homomorphic Encryption (FHE) in Quantum Networks on Boundary

- Studying the commercial feasibility of utilizing FHE for post-quantum operations such as friendly computations on the securely encrypted data.

- Examining the combination of FHE with AI integrated cloud security modelsto enhance services provided through cloud computing technologies to be effectively utilized through automation.

4. Decentralized Quantum Identity Management - The Road Ahead

- Creation of secure and privacy-enhanced self-sovereign identity services requires decentralized post-quantum solutions.
- Combining blockchain-based identity management with cryptographic systems that are resistant to quantum attack is the goal.
- Exploring the contribution of self-sovereign identity models in the setup of a quantum-secured digital economy.

5. Advancement of Quantum-Resistant Blockchain Security

- Designing of quantum-safe consensus mechanisms for blockchain and guaranteeing protection of decentralized systems over the long term is also necessary.
- Elaborate preparation for emerging new technologies covering all the aspects of security of blockchain such as post quantum cryptography, quantum key distribution and artificial intelligence.
- Deploying and testing smart contracts with quantum-resistant digital signature future proofed for blockchain transactions.

6. Standardisation and Multipolar Policy Formation

- Work together with NIST, ISO, NSA, and ENISA to finalize global policies and guidelines on PQC introduction and adoption throughout the world.
- Design in conjunction with compliance legal frameworks for industries migrating to hybrid PQC solutions.
- Post-quantum cryptographic algorithms are required to have full compatibility and seamless integration with contemporary digital infrastructure.

The emergence of quantum technologies necessitates the development of adaptive and AI-powered cryptographic algorithms. The present work is the first step towards the creation of reliable quantum-secure communication channels that comply with current and future regulatory frameworks considering that classic cryptographic methods will soon be rendered ineffective. Key innovations such as AI-based PQC optimization, FHE, DID and QRB will significantly adjust the image of the Static digital world.

The post quantum security is not an optional quest but an imperative, thus constant research, improvement and international networking must be the priority to bring about change and move on to quantum secure future.

REFERENCES

1. Fehr, S., Hofheinz, D., Liu, Y., Majenz, C., & Schlüter, K. (2023). *Quantum-Safe Cryptographic Combiners and Hybrid Security*. Retrieved from https://hapkido.tno.nl/publish/pages/4234/hapkido_d5-2.pdf
2. Associate Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation. (2024). *Quantum-Resistant Security Framework for Cloud Environments*. Retrieved from https://thesai.org/Downloads/Volume15No9/Paper_64-Advancing_Quantum_Cryptography_Algorithms.pdf
3. Cisco. (2024). *Advancements in Quantum Encryption and Scalable Quantum Networks*. Retrieved from https://outshift.cisco.com/blog/secure-future-quantum-encryption-scalable-quantum-networks
4. Bank for International Settlements (BIS). (2024). *Quantum-Resistant Cryptography in Financial Market Infrastructures*. Retrieved from https://www.bis.org/publ/bisih_fusse.pdf
5. Akter, T. (2023). *A Comprehensive Survey on Quantum Cryptography: Key Distribution, Post-Quantum Cryptography, and Quantum Key Management*. Retrieved from https://arxiv.org/abs/2306.09248
6. Kuang, X. (2024). *A Unified Cryptographic Framework for Quantum-Secure Cryptography Using Galois Permutation Group Theory*. Retrieved from https://arxiv.org/abs/2402.01852
7. Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., ... & Wallden, P. (2019). *Advances in Quantum Cryptography: State-of-the-Art Review*. Retrieved from https://arxiv.org/abs/1906.01645
8. Bagirovs, K., Ponomarev, A., Musaeva, M., Abul-Magd, A. Y., & Wang, C. (2024). *Applications of Post-Quantum Cryptography: A Systematic Scoping Review*. Retrieved from https://arxiv.org/abs/2406.13258

9. Mahmood Afzal Hussain, Sudha Rani Pujari (2021). Cybersecurity in the Era of Quantum Computing: Preparing for Post-Quantum Threats. *Nanotechnology Perceptions*.
10. Kanza Cherkaoui Dekkaki, Igor Tasic, Maria-Dolores Cano (2024). Cherkaoui Dekkaki, K.;Tasic, I.; Cano, M.-D. Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process. *MDPI Technologies*.
11. Tolamise Olasehinde. Quantum Resilience in Data Transmission and Protection Against Cyberattacks in Telecom (2021). Quantum Resilience in Data Transmission and Protection Against Cyberattacks in Telecom.
12. Mariam Yusuff (2023). Impact of Quantum Computing on 5G Network Efficiency and Data Security. *Federal University of Technology*.
13. Olusekemi Afolabi (2021). Impact of Quantum Computing on Data Encryption Standards in Telecom and E-commerce. *Obafemi Awolowo University*.
14. National Cyber Security Centre (2025). Next Steps In Preparing For Post-Quantum Cryptography. *NCSC.GOV.UK.*
15. Mariam Yusuff (2023). Post-Quantum Cryptography: Preparing E-commerce for a Quantum Future. *Federal University of Technology*.
16. Mariam Yusuff (2021). Quantum Key Distribution (QKD) for Enhanced Data Security in Telecommunications. *Federal University of Technology*.