OPEN ACCESS

Global Journal of Research in Humanities & Cultural Studies

ISSN: 2583-2670 (Online)

Volume 05 | Issue 01 | Jan.-Feb. | 2025

Journal homepage: https://gjrpublication.com/gjrhcs/

Review Article

Post-Quantum Cryptography: A Comprehensive Review of Methods, Applications, and Challenges in a Quantum-Powered Future

*Ms. Amruthalakshmi [1], Dr. Anant Kumar Kulkarni [2], Mrs. Shilpakala K [3]

[1]Research Scholar, Srinivas University, Mangaluru, Karnataka, India
[2]Professor and Head, Department of Mathematics, Srinivas Institute of Technology, Mangaluru, Karnataka, India
[3]Assistant Professor, Department of Mathematics, Srinivas Institute of Technology, Mangaluru, Karnataka, India

DOI: 10.5281/zenodo.14807779 **Submission Date: 03 Jan. 2025 | Published Date: 05 Feb. 2025**

***Corresponding author: Ms. Amruthalakshmi**

Research Scholar, Srinivas University, Mangaluru, Karnataka, India

Abstract

It is true that most areas are undergoing a revolution through quantum computing but heavily in cryptography. Potentially safe cryptographic systems could be broken if quantum attacks are successful in breaching those systems, which may then compromise both the confidentiality and integrity of information. Shor's and Grover's algorithms break widely used encryption algorithms such as RSA and ECC since it reduces the time complexity of the computation but gives some advantage in power to an adversary who has a quantum device. Thus, post-quantum cryptography is now the urgent requirement today, as it is expected to be one of the cryptography streams that will withstand both classical attacks as well as quantum attacks. That, however, takes into account a thorough review on need that this should consider in order to move into PQC by considering methodologies and the applications accompanied with challenges involved. Some key methods of cryptography include listing cryptographic inventories on already available assets with their respective dependencies, followed by data classification to indicate what should really be transferred while at risk assessment to note vulnerability from attack perspective of quantum attack. Such techniques prove important in terms of being a part of the framework, so one gets to define the process structure as a migration procedure. Finally, case studies involve real-life scenarios, as those demonstrate that methods suggested have good feasibility and security in maintaining secrecy for the protected information. PQC is being applied in many areas, including enterprise security, government systems, and financial services. Hybrid cryptographic systems are being used by businesses to transition smoothly without compromising the operational integrity. Governments, responsible for protecting classified information, are embracing PQC to ensure long-term data protection against emerging quantum threats. Financial institutions also encourage the adoption of PQC to abide by very stringent regulations and protect sensitive information and transactions from customers. Such applications showcase the ubiquitous nature of PQC in a quantum-powered future.

In addition, promising prospects on the PQC adoption, however, include challenges. Its migration process would be complex since it would incorporate interoperability with legacy systems and increased computational demands and an ever-evolving quantum threat landscape. However, a way to consistently and reliably achieve widespread industries' adoption lies in efforts like the NIST PQC standardization initiative that closes this gap more between classical and post-quantum methods. Hybrid cryptographic solutions and emerging trends continue to bridge the gap between classical and post-quantum methods, thereby assuring a smoother transition. It isn't strictly a technology in itself but will be an imperative in organizations seeking asset protection when such time comes when wide deployment of quantum computing is inevitable. Overall, it is thus to propose review adoption-encouragement of parties into collaboration even while continuing research on achieving the real strengths of quantum resilience in systems to be able to cryptograph.

Key words: Quantum computing, post-quantum cryptography (PQC), Cryptographic systems, Quantum threats, Hybrid cryptographic solutions, NIST PQC standardization, Data security, Encryption algorithms.

1. Introduction

Cryptography is the best modern-day security because it can assure integrity and authenticity along with its proof of privacy for digital communication and transactions. As of now, its base algorithms, RSA, ECC, and AES have provided thus far a powerful defense, which would likely push away classical computing threats, but perhaps the sheer advent of quantum computing is likely to destroy their underlying foundational structures. Quantum algorithms, like Shor's (1994) and Grover's (1997), are the most efficient known methods for solving problems such as integer factorization, discrete logarithms, etc., which serve as the foundation for the security of traditional cryptographic techniques [7], [6].

Quantum computation threatens more than a theoretical attack. Practical concerns make it possible for a sufficiently powerful quantum computer to decrypt sensitive communications, financial transactions and classified information currently protected by classical cryptographic algorithms. It provides post-quantum cryptography, that is an interdisciplinary field, the development of quantum-resistant algorithms. PQC is distinct from its classical counterpart since it relies on mathematical problems that, theoretically, would not be breakable even when a quantum computer is built which contains lattice-based cryptography and multivariate polynomial equations, as well as hash-based construction [9] (2020), [12] (2016).

Going to PQC is inevitable. It remains challenging. Migration should be smooth and requires a very complex landscape of technological, operational, and regulatory considerations. In this process, the National Institute of Standards and Technology (NIST) has led the standardization process for PQC algorithms [1] (2016). Since the beginning of its launch, NIST PQC has identified a few candidates that could be promising candidates: CRYSTALS-KYBER for key encapsulation and CRYSTALS-Dilithium for digital signatures likely to be used as building blocks of quantum-resistant cryptographic systems [17] (2023).

This article discusses critical methodologies which underpin PQC migration to include cryptographic inventorying, data classification, and risk assessment. Cryptographic inventorying is the process of cataloging the existing cryptographic assets in a computer system including keys, certificates, and protocols for identification of dependencies and vulnerabilities [3] (2022), [8] (2019). Data classification will be prioritizing assets as per their sensitivity and potential impact in the event of compromise, thereby allowing organizations to allocate resources effectively [5] (2021). Risk assessment will evaluate the quantum threat in present systems towards defining strategies for targeted migration [4] (2024).

Applied fields of PQC are very practical in enterprise security, government systems, and finance. Enterprises apply hybrid cryptographic solutions for an optimal balance between security performance and the transition period [19] (2023). Governments apply PQC for protecting classified information which ensures long term data confidentiality. Financial institutions apply quantum resistant algorithms for protecting sensitive customer data that helps them to abide by very stringent regulatory standards of a financial sector [10] (2020) and [13] (2019).

There are also a few challenges associated with the adoption of PQC. For example, the legacy systems can interoperate with each other and increase computing. Therefore, the changing nature of the quantum threat end. However, it also draws attention to some mitigating elements, such as standardization, and emerging trends - hybrid cryptographic approach - that helps to overcome those challenges [2] (2018), [19] (2023), thus making this a proactive systematic approach for handling the complexities related to PQC migration and to protect assets against the threats of a quantum era.

This paper synthesizes current research, methodologies, and practical applications in the field to provide a comprehensive analysis of PQC. It advocates collaborative efforts among researchers, industry stakeholders, and policymakers for the challenges at hand and toward the full realization of the promise of post-quantum cryptographic systems in securing a quantum-powered future.

2. Methods for PQC Migration

2.1 Cryptographic Inventorying

First off, the method for migration is through cryptographic inventorying. This process will entail a detailed and extensive listing of all cryptographic assets within an organization. Such assets include algorithms, keys, certificates, and protocols currently employed. An example of manual inventorying is labor-intensive but allows a granular control and deeper understanding of the cryptographic landscape. Automatically, sophisticated scanning tools can utilize such capabilities in order to abbreviate the inventorying process with greater efficiency and precision. Key among the results of this strategy is the identification of dependencies and vulnerabilities in the cryptographic infrastructure and opening space for further migration work [3] (2022), [8] (2019)).

2.2 Data Classification

The next critical process during the PQC migration process is data classification. This process deals with the grouping of data assets according to the sensitivity of information and the resultant impact of breach. For example, financial records and proprietary intellectual property may be prioritized as critical assets because they are of vital importance. Classifying risk to datasets appropriately enables organizations to plan their migration and resource allocation better. This would systemically safeguard the most sensitive data at the earliest time possible against threats of quantum threats. [5] (2021) [13] (2019).

2.3 Risk Assessment

One of the excellent cornerstones for PQC migration is one based on the proper risk assessment. Organizations need to conduct a quantum risk assessment methodology on any existing cryptographic system using dependency graph and vulnerability models, among other techniques. By evaluating these vulnerabilities, decision-makers will be in a position to determine systems most vulnerable to attacks by a quantum, hence establishing specific strategies toward their migration. Risk assessments also allow resource allocation to critical vulnerabilities, thus ensuring a smooth transition to a quantum-secure infrastructure with minimum disruption [4] (2024), [9] (2020).

3. Applications of PQC

3.1 Enterprise Security

Quantum cryptography has served many applications for enterprise security. Firms have adopted quantum-resistant algorithms for their critical infrastructure protection and other secret information. Hybrids that marry both classical cryptosystems and post-quantum cryptosystems are a step-effective way through which security gives way to efficiency for enterprises. The enterprises can, therefore, sustain a continuity of their operations as they begin using the quantum-resistant algorithms. As an enterprise goes on with its ever-increasing dependence on digital ecosystems, it is likely to include PQC in the pantheon of its security tools [3] (2022); [19] (2023).

3.2 Government Systems

Government systems is another area where PQC must be implemented. The national security agencies depend on quantum-resistant algorithms to store secret information and protect the communication channels. As government data must be kept secret for a long time, PQC plays a crucial role in protecting national interest. Governments are interested in establishing quantum-resistant cryptographic standards to strengthen their cyber security framework against potential quantum attacks [8] (2019), [10] (2020).

Financial Sector

An integrated role for PQC exists within the financial business when it comes to the security of banking operations and their payment systems. The large volumes of sensitive data defined financial organizations in as far as customer data and transaction history were concerned, which have made them desirable goals for hackers. Introducing PQC algorithms mainly keeps up with harsh regulations but fundamentally enhances the general level of safety connected to operations. With advancements in quantum computing, there is a need for a quantum-resistant cryptography system to ensure trust and reliance in financial service systems [9] (2020), [13] (2019).

Challenges and Emerging Trends

One of the main challenges in migrating to PQC is interoperability between classical and post-quantum systems. The company operates in complex interlocking IT ecosystems. Legacy systems run alongside modern infrastructure. Integration and compatibility become crucial at the time of transition [19] (2023).

Next comes the issue of additional computational and storage demands of PQC algorithms. Most post-quantum algorithms require more extended key sizes and more computational power, which can be one of the reasons for the upgradation of current hardware and software systems [4] (2024), [17] (2023).

Standardization efforts will be crucial to making PQC adoption easier. The NIST PQC standardization process is one such effort aimed at making post-quantum algorithms worldwide accepted, implemented consistently and reliably across different implementations. As such standards mature, they will provide a strong foundation for organizations to build on [1] (2016), [12] (2016).

Hybrid approaches seem to be relatively promising on the horizon of PQC. Hybrid schemes do, by definition, include a classical cryptosystem together with quantum-resistant algorithms hence form the kind of an intermediate system connecting pure security requests and performance-based requirements. It is hybrid hybrid solutions which will provide companies with levers to secure continuity of operations even after transition is made from unreliable insecure cryptographic building blocks towards the secure ones [19] (2023); [6] (1997).

Conclusion

Traditional cryptographic systems have been put to test with the advent of the quantum computing era, and the weaknesses have come forward. The review is basically requesting the organizations to move immediately toward post-quantum cryptography. Organizations have various systematic methods that provide effective vulnerabilities in cryptographic infrastructures, such as cryptographic inventorying, data classification, and risk assessment. The applications of PQC in enterprise security, government systems, and the financial sector reveal how important it is to protect sensitive data in order to maintain operational resilience.

However, the vast complexities in alteration are brought forth by interoperability, resource intensiveness, and dynamicity issues in quantum threats. Hybrid methodologies and standardization of frameworks adopted will promise good prospects for having security before migration, during, and after the process also. Research engagement with diverse ranges of stakeholders further becomes a big need for advancing PQC methods, their maturity along with the challenges for the latest emerging issues at the doorstep.

Conclusion: Transition to PQC is a strategic need rather than simply a technical one. Organizations should be actively guarding their assets, evolving over time so that they will be better positioned against threats and ensuring that the systems of cryptography could live as long as possible in the quantum world.

References

1. *National Institute of Standards and Technology (NIST) PQC Standardization Process.*
2. *ETSI TR 103 616: Quantum-Safe Cryptographic Schemes.*
3. *IBM® Cryptographic Inventory for Post-Quantum Migration.*
4. Hasan, K.F., et al., "A Framework for Migrating to Post-Quantum Cryptography," IEEE Access, 2024.
5. *CARAF: A Framework for Crypto-Agility Risk Assessment.*
6. Grover, L.K., "Quantum Mechanics Helps in Searching an Unsorted Database," Physical Review Letters, 1997.
7. Shor, P.W., "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994.
8. *Netherlands National Communications Security Agency PQC Migration Handbook.*
9. Bernstein, D.J., et al., "Post-Quantum Cryptography: The State of the Art," Springer, 2020.
10. *Australian Cyber Security Centre (ACSC) Protective Security Policy Framework.*
11. *IEEE Standard for Public-Key Cryptography.*
12. Chen, L., et al., "Report on Post-Quantum Cryptography," NIST IR 8105, 2016.
13. *Payment Card Industry Data Security Standard (PCI DSS).*
14. Rivest, R.L., Shamir, A., Adleman, L., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, 1978.
15. *Australian Prudential Regulation Authority (APRA) CPS 234.*
16. Diffie, W., Hellman, M., "New Directions in Cryptography," IEEE Transactions on Information Theory, 1976.
17. *Falcon and CRYSTALS-Dilithium: NIST-Approved PQC Algorithms.*
18. *Office of Management and Budget (OMB) Memorandum on Quantum Computing Risk.*
19. *Hybrid Cryptosystems for Secure Transition to PQC.*
20. *Secure Communication Protocols in the Quantum Era.*

CITATION

Amruthalakshmi, Kulkarni, A. K., & Shilpakala K. (2025). Post-Quantum Cryptography: A Comprehensive Review of Methods, Applications, and Challenges in a Quantum-Powered Future. In Global Journal of Research in Humanities & Cultural Studies (Vol. 5, Number 1, pp. 63–66). https://doi.org/10.5281/zenodo.14807779