IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Study on Quantum Cryptography vs Post-Quantum Cryptography:

[1] Murali Mohan Kumar A, [2] K Chandra Sekhar,
[1] Associate Professor [2] Associate Professor
[1] Master of Computer Applications, [2] Master of Computer Applications
[1], Mother Theresa Institute of Computer Applications (MCA), Palamaner, Chittoor, India
[2], Mother Theresa Institute of Computer Applications (MCA), Palamaner, Chittoor, India

Abstract: The emergence of quantum computing presents a formidable challenge to contemporary cryptographic techniques, potentially compromising the security of digital communications worldwide. Two dominant strategies have evolved in response: Quantum Cryptography grounded in the principles of quantum mechanics, and Post-Quantum Cryptography (PQC), which reinforces classical cryptography against quantum threats. This paper provides an in-depth comparative study of both paradigms, analyzing their theoretical foundations, operational mechanisms, practical applicability, and limitations. Through this analysis, we explore how these approaches can jointly contribute to robust and future-proof cryptographic security.

Index Terms **Quantum Cryptography, Post-Quantum Cryptography, Quantum Key Distribution, Quantum Computing, Cryptographic Security, PQC, Quantum Threats**

I Introduction

In the contemporary digital ecosystem, the protection of data privacy, integrity, and authenticity is primarily ensured through well-established cryptographic protocols. These conventional systems, such as RSA, Elliptic Curve Cryptography (ECC), and DSA, are rooted in the computational hardness of specific mathematical challenges. However, advancements in quantum computing threaten to dismantle these defenses, prompting the need for a paradigm shift in cryptographic design and application.

Quantum computing exploits quantum phenomena such as superposition and entanglement to perform calculations that are infeasible for classical computers. Algorithms like Shor's and Grover's demonstrate the ability to break widely used encryption methods, compromising current digital security. This threat landscape necessitates the exploration of novel cryptographic methodologies resilient to quantum capabilities.

Two leading approaches have emerged:

1. Quantum Cryptography, which achieves secure communication based on the physical laws of quantum mechanics rather than computational difficulty.
2. Post-Quantum Cryptography (PQC), which involves developing new mathematical cryptographic algorithms designed to withstand quantum-level attacks while maintaining compatibility with classical systems.

Our study systematically compares these two paths, highlighting their theoretical and practical implications for future information security.

II. Background

2.1. Conventional Cryptography The issues used in conventional cryptography are too complex for current classical computers to solve computationally. The intractability of the elliptic curve discrete logarithm problem is the foundation of ECC, whereas the difficulty of factoring big numbers is the foundation of RSA. Although they constitute the cornerstone of contemporary secure communications, these schemes lack quantum resilience.

2.2. Quantum Computing Threat Quantum algorithms have the potential to compromise existing encryption schemes. Shor's algorithm can factor large numbers efficiently, breaking RSA and ECC, while Grover's algorithm can reduce the brute-force effort against symmetric encryption by a square root factor, necessitating stronger symmetric keys.

III. The use of quantum cryptography

3.1. The Basic Idea Quantum cryptography secures data exchange by taking use of the quantum nature of particles. It is based on the Heisenberg Uncertainty Principle and the No-Cloning Theorem, which guarantee that any attempt to intercept quantum data changes its state and can be detected.

3.2. Distribution of Quantum Keys (QKD)

• BB84 Protocol: BB84, which was proposed by Bennett and Brassard in 1984, generates and securely distributes encryption keys using quantum bits, or qubits.

• Ekert developed the E91 Protocol, which generates keys using entangled particles and improves security by using quantum correlations.

.3.3. Advantages

• Intrinsic eavesdropping detection mechanisms
• Based on immutable laws of physics
• Potential for absolute (information-theoretic) security

3.4. Limitations

• Requires specialized infrastructure (e.g., quantum channels, photon detectors)
• Sensitive to transmission distance and environmental noise
• Currently limited to key distribution, not full data encryption

IV. Post-Quantum Cryptography (PQC)

4.1. Fundamental Idea PQC includes cryptographic methods that are safe from quantum and conventional assaults. These algorithms don't depend on quantum characteristics and can be run on conventional hardware.

4.2. Algorithms and Categories

• Lattice-based Cryptography: Contains programs such as Kyber and NTRU, which are renowned for their effective operation and robust security presumptions.

• McEliece is a well-known example of code-based cryptography, which provides good security but has issues with big key sizes.

• Hash-based cryptography: XMSS and SPHINCS+ are two examples that work well for digital signatures. Multivariate polynomial cryptography is based on the solution of systems of nonlinear equations over finite fields.

.SIKE is a well-known example of isogeny-based cryptography, which makes use of the characteristics of elliptic curve isogenies.

4.3. Benefits

• Easily implemented in current digital ecosystems Backward compatibility with traditional communication protocols; adaptability and affordability with regard to hardware requirements

4.4. Difficulties Some techniques require huge key/signature sizes; security is predicated on mathematical hypotheses that have not been confirmed; as quantum research advances, there may be unanticipated flaws.

V. Evaluation via Comparison

A feature Quantum Encryption Quantum mechanics is the foundation of post-quantum cryptography. Complexity of mathematics, Infrastructure Quantum hardware is needed. operates on traditional systems, Level of Security Information-theoretic Security of computation, Important Use Case Distribution of keys Complete encryption and signatures Implementation Physical constraints Scalable and broadly applicable, Exposure to Potential Future Findings minimal (based on
physics) Moderate (based on math)

VI. Conclusion

To mitigate the vulnerabilities brought up by quantum computing, two essential tactics are quantum cryptography and post-quantum cryptography. Despite the fact that quantum cryptography provides physics-based, verifiable security, it is limited by infrastructure and technological limitations. On the other hand, PQC is compatible with existing digital frameworks and works realistically, but it is still theoretically susceptible to future advances in quantum algorithms.

It is better to think of these paradigms as complementing rather than as competing solutions. Next-generation cyber security is probably going to be built on a hybrid security paradigm that combines the physical guarantees of quantum cryptography with The useful adaptability of PQC. To protect the world's digital infrastructure and preserve confidence in secure communications as the quantum age draws near, proactive investment in both technologies is crucial.

References

[1] Bennett, C. H., & Brassard, G. (1984). *Quantum cryptography: Public key distribution and coin tossing*. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175–179.
[2] Shor, P. W. (1994). *Algorithms for quantum computation: Discrete logarithms and factoring*. Proceedings of the 35th Annual Symposium on Foundations of Computer Science, IEEE, 124–134.
[3] Grover, L. K. (1996). *A fast quantum mechanical algorithm for database search*. Proceedings of the 28th Annual ACM Symposium on Theory of Computing, 212–219.
[4] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). *Quantum cryptography*. Reviews of Modern Physics, 74(1), 145–195. https://doi.org/10.1103/RevModPhys.74.145
[5] National Institute of Standards and Technology (NIST). (2023). *Post-Quantum Cryptography Standardization Project*.
[6] Chen, L. et al. (2016). *Report on Post-Quantum Cryptography*. NISTIR 8105. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105
[7] Pirandola, S. et al. (2020). *Advances in quantum cryptography*. Advances in Optics and Photonics, 12(4), 1012–1236. https://doi.org/10.1364/AOP.361502
[8] Lu, Y. et al. (2022). *Satellite-based quantum key distribution: Progress and challenges*. npj Quantum Information, 8(1), 1–11. https://doi.org/10.1038/s41534-022-00553-6
[9] Bernstein, D. J., Buchmann, J., & Dahmen, E. (Eds.). (2009). *Post-Quantum Cryptography*. Springer. https://doi.org/10.1007/978-3-540-88702-7