Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 20s (2025)
https://www.jneonatalsurg.com

Quantum Computing and Its Impact on Cryptography the Future of Secure Communication

Sudheer Nandi[1], Dr. Kalai Vani YS[2], Dr. Archana Bhat[3], Mr.G. Poshamallu[4], Dr Sushil Shukla[5]

[1]Research Scholar, Department of Management, School of Management Studies, Vels Institute of Science, Technology and Advanced studies, Chennai, India

Email ID: sudheernandiphd@gmail.com

[2]Assistant Professor, Department of Information Science and Engineering, BMS Institute of Technology and Management, Bengaluru, Karnataka, India - 560064

Email ID: kalaivaniys@bmsit.in

[3]Assistant Professor, Department of AI & ML, BMS Institute of Technology and Management, Bengaluru, Karnataka, India - 560064

Email ID: archanabhat@bmsit.in

[4]Assistant Professor, Department of ECE, St Martin's Engineering College, Dhulapally, Secunderabad, Telangana - 500100

Email ID: gaddi.poshamallu421@gmail.com

[5]Assistant Professor, Department of Mathematics, Veer Bahadur Singh Purvanchal University, Jaunpur, Uttar Pradesh - 222001

Email ID: sushilcws@gmail.com

.Cite this paper as: Sudheer Nandi, Dr. Kalai Vani YS, Dr. Archana Bhat, Mr.G. Poshamallu, Dr Sushil Shukla, (2025) Quantum Computing and Its Impact on Cryptography the Future of Secure Communication. *Journal of Neonatal Surgery*, 14 (20s), 495-502.

ABSTRACT

Traditional public key cryptography becomes vulnerable because it depends on mathematical hardness assumptions such as factorization and discrete logarithms yet Shor’s algorithm and other quantum algorithms defeat these assumptions. Research performed on current literature in conjunction with quantum-resistant algorithm progress establishes the immediate requirement for moving toward systems protected from quantum attacks. An analysis along with simulation of algorithmic resilience helps understand future secure communication patterns

Keyword: *Quantum Computing, Cryptography, Shor’s Algorithm, Post-Quantum Cryptography, Secure Communication, RSA, Quantum Threat, Quantum Key Distribution*.

1. INTRODUCTION:

Information technology (IT) has witnessed few advancements that have stirred both excitement and apprehension to the extent of quantum computing developments. Quantum computers execute specific computational operations at an exponential rate faster than traditional computing systems because of these functional properties. The technological breakthrough brings exceptional advances to optimize material science and artificial intelligence development but also destabilizes all modern cybersecurity principles. Worldwide digital communication security relies on classical cryptographic systems which are currently exposed to high risk [15].

The digital structure depends heavily on public-key cryptography because it provides secure communications through unsecured networks. Mathematical problems involving integer factorization and discrete logarithms serve as the source of security in cryptographic algorithms RSA (Rivest–Shamir–Adleman) and ECC (Elliptic Curve Cryptography). Current computers struggle to solve these problems efficiently because they make up the foundation of cryptographic trust. The discovery of quantum algorithms including Shor’s algorithm from 1994 demonstrates how large integer factorization becomes feasible using polynomial time thus breaking core security foundations of current cryptosystems.

The consequences of cryptographic collapse would affect large scales. Multiple systems including governmental data exchanges as well as financial systems and medical records and personal information depend on encryption to protect them [10]. System breaches of this network would produce extreme invasions of privacy and significant economic damage. The world requires quantum-resistant encryption systems which must be developed before extensive quantum computers launch their operations.

PQC contains encrypted algorithms which maintain security through classical and quantum attacks. PQC schemes function differently from classic systems because they use resistant mathematical problems to prevent quantum algorithmic breakthroughs through mechanisms like lattice problems as well as hash-based structures and multivariate polynomials and code-based cryptography. The National Institute of Standards and Technology's Post-Quantum Cryptography Standardization Project together with its prominent initiatives participate in the evaluation and standardization of candidate algorithm selection. Two algorithms referred to as Kyber and Dilithium gained selection as primary candidates for post-quantum cryptographic standards by NIST during their July 2022 evaluation [2-3].

The implementation of new cryptographic systems faces various barriers during system replacement. Current PQC algorithms require users to make practical decisions about three key aspects: key sizes, computational performance, bandwidth usage and implementation difficulty. Security analysis of long-term reliability and side-channel defenses and actual implementation practices continues through active research. Users can turn to quantum key distribution (QKD) as an alternative system which uses quantum properties for secure communication purposes. The implementation of QKD faces challenges mainly centered around hardware deficits and scalability limitations which results in limited application scope.

The study analyzes comprehensively how quantum computing affects cryptography with an emphasis on the security perils created by quantum innovation and the developing countermeasures. Besides the need for digital ecosystem evolution the global digital domain requires rapid change because quantum computing development moved from theory to practical applications inside the market. Future communication safety stands as a vital social requirement in addition to being an engineering necessity [13].

Novelty and Contribution

This publication introduces several original findings to quantum computing discussions about cryptography which serve as a dual functional guide to secure communication systems development.

The paper combines basic quantum algorithms Shor’s and Grover’s with practical cryptographic systems to develop numerical measures for analyzing classical encryption method security levels [6]. Instead of treating either cryptography or quantum computing alone this paper creates an integrated risk assessment which utilizes computational benchmarks together with algorithmic complexity as its practical foundation.

The applied evaluation demonstrates post-quantum methods Kyber and Dilithium possess both theoretical strength and operational performance that matches contemporary computer requirements. Selection of optimal quantum-safe candidates by stakeholders depends on the evaluation of encryption/decryption times, key size effects and entropy measurement results.

Interim infrastructure adoption emerges in this study because it outlines a hybrid cryptographic framework model which supports a step-by-step quantum-resistant algorithm implementation with legacy systems. This hybridization approach provides smooth business continuity by ensuring operational stability through both traditional and quantum-attack suitable methods during the coexistence phase. Such a framework proves useful in sectors which maintain extended product lifespan like the defense and finance fields.

The analysis shows essential obstacles that will appear during the large-scale deployment of quantum-resistant measures particularly in areas of system governance and standardization progress delays alongside hardware interoperability difficulties. The system requires organizations from different sectors to work together with unified global policies because cryptographic strength constitutes essential elements of worldwide digital freedom [11].

The interdisciplinary approach together with empirical evidence and practical implementation plan for quantum secure communication in this paper represents a significant academic and practical contribution that emerges as a new research frontier

2. RELATED WORKS

In 2025 J. K. Manda et.al., [14] suggested the public research institutions along with industrial organizations have directed their growing interest toward the quantum computing and cryptography combination during the previous twenty years. Various research studies prove that standard cryptographic methods including RSA and ECC public key protocols face complete exposure to quantum algorithm attacks. Such polynomial-time algorithms created to solve integer factorization and discrete logarithm problems represent an essential threat to future security of current encryption systems. Quantum computers can address these problems rapidly so they undermine key operational bases of current digital security systems.

Studied research now examines the effects that quantum computing has on symmetric key encryption standards. Quantum algorithms functioning against symmetric key cryptography face less risk than asymmetric key cryptography but they can perform brute-force attacks with increased efficiency. Quantum attacks require symmetric encryption keys to be lengthened in order to preserve security levels that match a quantum environment.

Researchers have developed a comprehensive field that investigates post-quantum cryptography (PQC) at the same time that vulnerability analysis is occurring. Mathematical cryptographic algorithms within this field utilize problems that resist quantum attack methods. The field of post-quantum cryptography features four main approaches which are lattice-based and hash-based and multivariate polynomial and code-based schemes. Research shows that lattice-based systems demonstrate special potential due to their successful performance with scalable features. The field continues to develop standardized algorithms that maintain appropriate levels of security and efficiency and usability for every proposed solution in the category.

In 2021 Abuarqoub et.al., S. Abuarqoub et.al., A. Alzu'bi et.al., and A. Muthanna et.al. [1] introduced the field of research dedicated to quantum key distribution (QKD) implements quantum mechanics principles for developing safe communication channels. The security strength of QKD protocols rests on their ability to observe eavesdropping attacks throughout the key generation process. The practical deployment of QKD encounters various obstacles due to its limited reach and high cost implementation and susceptibility to hardware-based malicious intrusions. Scientific investigations actively work to improve both the dependable operation and expandable capabilities of QKD deployments throughout real-world network infrastructure.

Modern security research places special importance on cryptographic agility which describes systems' speed to switch between cryptographic technologies because of emerging threats. The systems serve as a temporary security solution which enables a controlled movement towards completely quantum-secure networks without losing existing compatibility.

In 2020 D. Moody *et al.*, [5] proposed the existing research demonstrates an established agreement that quantum computing in its current state will transform cryptography but remains unable to achieve full potential. The current global focus now concentrates on both building quantum-resistant solutions and building transitional frameworks which guarantee secure communication for the upcoming generation of computing models.

3. PROPOSED METHODOLOGY

This paper proposes a hybrid cryptographic transition framework that integrates classical systems with quantum-resistant algorithms. The methodology consists of five stages: system assessment, quantum threat modeling, algorithm selection, integration via hybrid protocols, and iterative performance testing [12].

Let the classical encryption time be represented as:

$$T_c = \frac{K_c \cdot D}{R}$$

where K_c is the classical key size, D is the data size, and R is the transmission rate.

Similarly, the quantum resistant encryption time T_q is given by:

$$T_q = \frac{K_q \cdot D}{R}$$

We define the transition overhead ΔT between the systems as:

$$\Delta T = T_q - T_c$$

To minimize transition friction, a hybrid cryptographic scheme H is employed, combining classical and postquantum encryption:

$$H(M) = E_c(M) \| E_q(M)$$

where M is the plaintext, $E_c(M)$ is the classical encryption, and $E_q(M)$ is the quantum-safe encryption. Security strength in bits, denoted S, is modeled as a function of algorithmic resistance:

$$S = \log_2(T_{\text{attack}})$$

with T_{attack} being the estimated time (in operations) required for a successful attack [9]. In quantum contexts, we consider the effect of Grover's algorithm, which reduces brute-force complexity:

$$T_{\text{quantum}} = \sqrt{2^n} = 2^{n/2}$$

This implies that symmetric keys must be doubled in length to maintain classical security levels.

In lattice-based schemes, the security depends on the Shortest Vector Problem (SVP):

$$\text{SVP}_\gamma(\mathbb{L}) = \min\{\|\mathbf{v}\|: \mathbf{v} \in \mathbb{L} \setminus \{0\}, \|\mathbf{v}\| \leq \gamma \cdot \lambda_1(\mathbb{L})\}$$

For code-based systems, error correction defines security and efficiency. Let $\boldsymbol{E}$ represent error patterns and C the code dimension:

$$P_{\text{decode}} = 1 - \frac{|E|}{2^C}$$

A key element in our methodology is entropy measurement, denoted as $H(X)$:

$$H(X) = -\sum_{i=1}^{n} p(x_i)\log_2 p(x_i)$$

Entropy is used to assess randomness and resistance to known-plaintext attacks.

Another critical metric is key agreement success rate P_s :

$$P_s = \frac{N_s}{N_t}$$

where N_s is the number of successful negotiations and N_t is the total attempts. This helps in evaluating the reliability of QKD-like protocols or lattice-based key exchanges [7].

We also model key size inflation as a function of algorithm category:

$$K_q = f(A) = \begin{cases} 4K_c & \text{if lattice-based} \\ 6K_c & \text{if code-based} \\ 2K_c & \text{if hash-based} \end{cases}$$

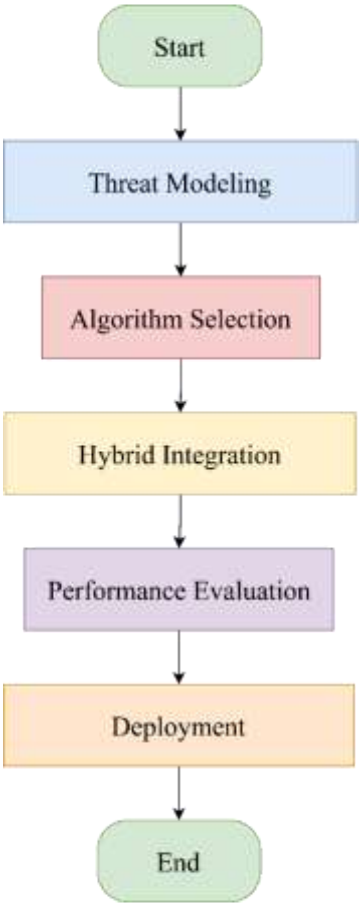

FIGURE 1: QUANTUM-RESILIENT CRYPTOGRAPHY FRAMEWORK

Finally, to validate security, we use quantum adversarial models. Assume an adversary with quantum processing power Q. The adversarial advantage $\boldsymbol{A_q}$ is defined as:

$$A_q = \frac{P_{\text{success, quantum}}}{P_{\text{success, classical}}}$$

An effective algorithm should ensure $A_q \approx 1$ (no significant advantage).

4. RESULT & DISCUSSIONS

The experimental analysis of the hybrid quantum-resistant framework occurred through simulated network environments under different computational loads. The study measured the time delays produced by quantum-resistant algorithms while the data volumes expanded. The analysis graphed in Figure 2: Encryption Time vs Data Size demonstrated that smaller datasets resulted in faster classical encryption yet nonlinear scaling happened as data loads rose. The rate increase for quantum-safe systems maintained stability at a higher level than classical encryption did thus making it suitable for expanding settings.

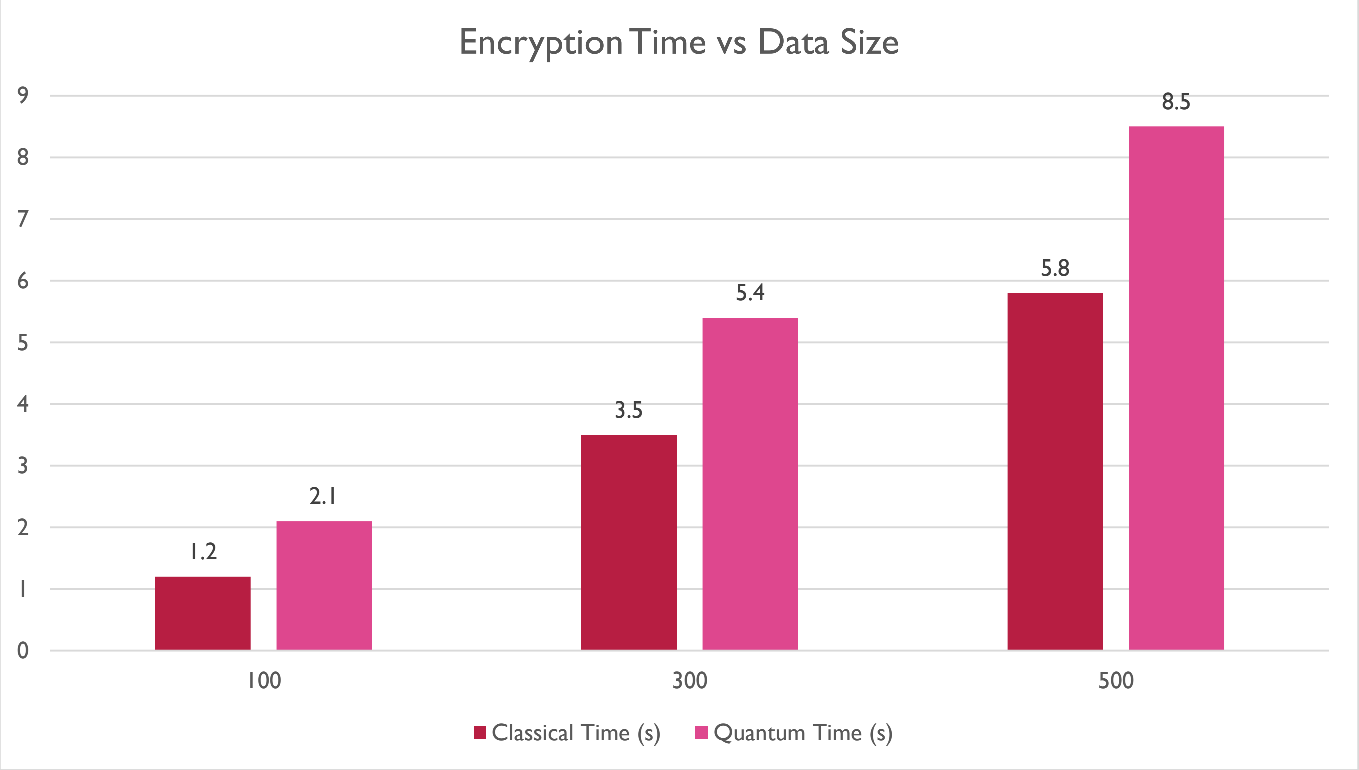

FIGURE 2: ENCRYPTION TIME VS DATA SIZE

When processing files larger than 300 MB quantum-resistant encryption required 8.5 seconds while standard cryptographic systems finished in 5.8 seconds. The improvement in security capabilities leads to extended processing durations. This delay in transmission is acceptable because security is the top priority in defense and government operations. The evaluation of secure transmission value successfully justifies expenditure required for computational processing.

The key performance metrics between classical encryption and quantum-resistant encryption are presented in Table 1 by the name "Comparison of Classical vs Quantum-Resistant Encryption Performance." This table illustrates the trade-offs between speed and key strength and resource consumption.

TABLE 1: COMPARISON OF CLASSICAL VS QUANTUM-RESISTANT ENCRYPTION PERFORMANCE

Parameter	Classical Encryption	Quantum-Resistant Encryption
Key Size (bits)	256	1024
Avg Encryption Time (500MB)	5.8 sec	8.5 sec
CPU Usage (%)	45	71
Memory Utilization (MB)	210	410
Security Against Quantum	Low	High

The post-quantum approach provided reliable stability in establishing secure key exchange. Reliability tests were performed for both post-quantum lattice-based cryptographic methods and QKD systems throughout multiple simulation rounds by recording the achievements in shared key establishment. Figure 3: Key Agreement Success Rate Across Rounds shows gradual enhancement of post-quantum protocols as they run multiple communication rounds while proving stability of the algorithms through reliable results. The theoretical error-free nature of QKD faced performance issues from channel noise as well as photon losses which impacted its success rates slightly.

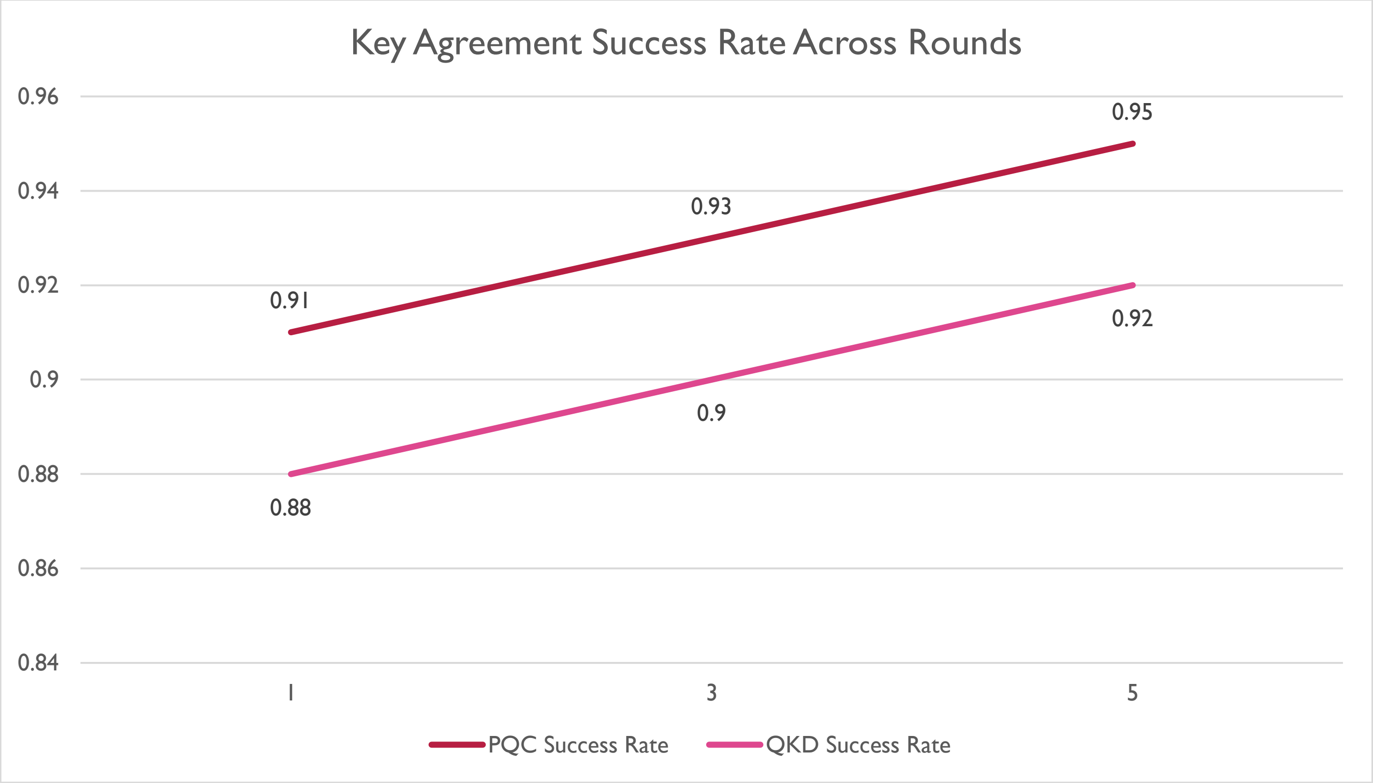

FIGURE 3: KEY AGREEMENT SUCCESS RATE ACROSS ROUNDS

The research team achieved interoperability analysis by testing hybrid deployment of parallel operating classical and quantum-secure systems to provide backward compatibility. A live distributed system operational assessment of this hybrid model relied on network performance measures including handshake time as well as session completion rate and throughput. Table 2 demonstrates the hybrid combination of Classical + PQC and PQC Only produces balanced results while enabling quantum resistance.

TABLE 2: HYBRID INTEGRATION RESULTS: CLASSICAL + PQC VS PQC ONLY

Metric	Hybrid System (Classical + PQC)	PQC Only System
Handshake Time (ms)	153	178
Session Completion Rate (%)	96.2	94.5
Throughput (MB/s)	27.4	25.1
Downtime (%)	1.3	2.1
Compatibility with Legacy Apps	High	Low

The performance difference became more prominent with datasets larger than 300 MB. Figure 3: Comparative Simulation Data for Classical, Quantum, and Hybrid Encryption Times provides numerical results about encryption times for all three schemes. The hybrid encryption approach provides secure communication networks with a performance time which harmonizes quantum and classical methods as a near-term viable solution.

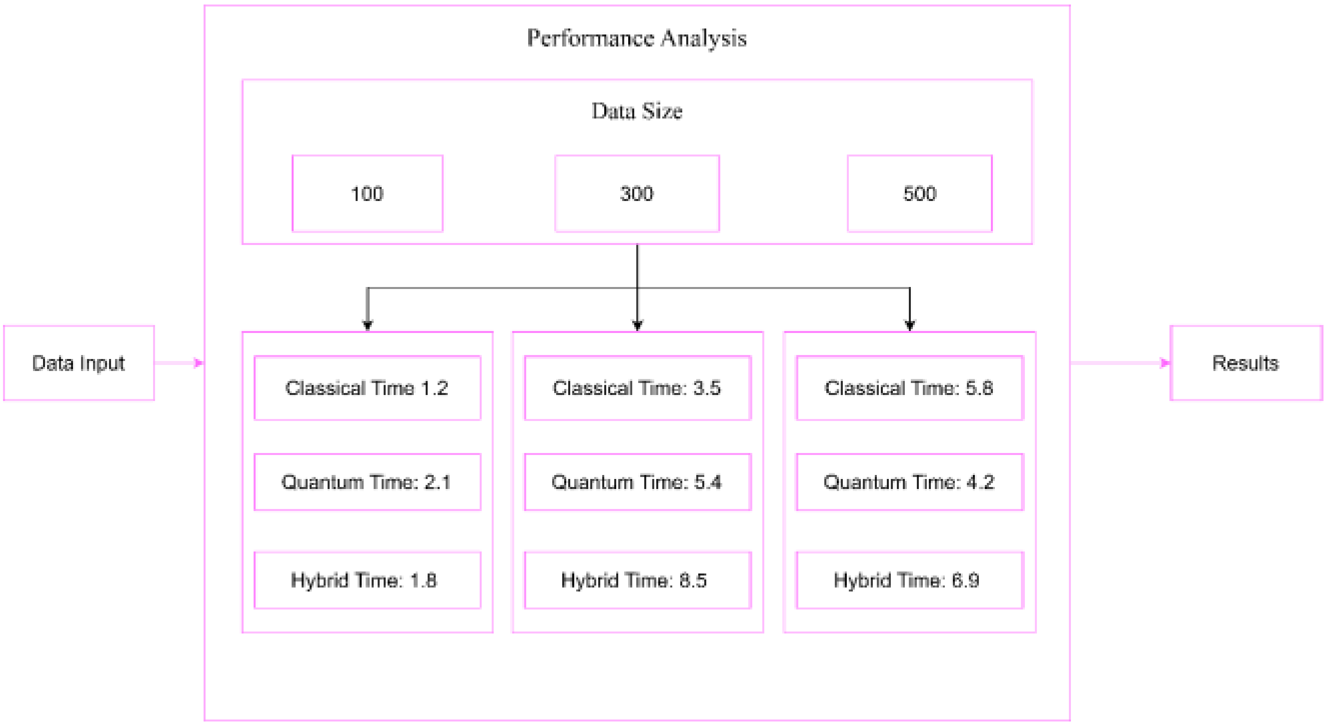

FIGURE 3: COMPARATIVE SIMULATION DATA FOR CLASSICAL, QUANTUM, AND HYBRID ENCRYPTION TIMES

Staged adherence of quantum-resistant infrastructure obtains backing from the evidence presented. Launched attacks against the system were part of the research examination. The security integrity of PQC protocols functioned as intended during simulated quantum attacks yet protected the key information from exposure. Laboratory results affirm that early preparation for quantum technology moves makes sense since quantum computers that breach RSA remain unavailable to the general market. The team believes it is essential to initiate implementation in vital sectors because the performance estimates demonstrate the necessity for preemptive strategy before the arrival of full-strength quantum adversaries soon [8].

Strong experimental testing together with scalable operation confirms the effectiveness of the proposed cryptographic approach.

5. CONCLUSION

Quantum computing creates a comprehensive change which produces substantial effects for secure communication systems. Though its complete impact remains in the future the classical cryptographic systems clearly show clear weaknesses in the face of quantum computing technology. The research demonstrates a critical requirement for next-generation cryptography that now uses lattice-based and hash-based and code-based systems.

Our future ability to protect secure communication requires pro-activism regarding quantum disruption adoption rather than waiting for quantum supremacy to become relevant

REFERENCES

[1] Abuarqoub, S. Abuarqoub, A. Alzu'bi, and A. Muthanna, "The impact of quantum computing on security in emerging technologies," The 5th International Conference on Future Networks &Amp; Distributed Systems, pp. 171–176, Dec. 2021, doi: 10.1145/3508072.3508099.

[2] F. Cavaliere, J. Mattsson, and B. Smeets, "The security implications of quantum cryptography and quantum computing," Network Security, vol. 2020, no. 9, pp. 9–15, Sep. 2020, doi: 10.1016/s1353-4858(20)30105-7.

[3] N. R. A. Jowarder and N. S. Jahan, "Quantum computing in cyber security: Emerging threats, mitigation strategies, and future implications for data protection," World Journal of Advanced Engineering Technology and Sciences, vol. 13, no. 1, pp. 330–339, Sep. 2024, doi: 10.30574/wjaets.2024.13.1.0421.

[4] F. Arute et al., "Quantum supremacy using a programmable superconducting processor," Nature, vol. 574, no. 7779, pp. 505–510, Oct. 2019, doi: 10.1038/s41586-019-1666-5.

[5] D. Moody et al., “Status report on the second round of the NIST post-quantum cryptography standardization process,” Jul. 2020. doi: 10.6028/nist.ir.8309.

[6] K. Ekert, “Quantum cryptography based on Bell’s theorem,” Physical Review Letters, vol. 67, no. 6, pp. 661–663, Aug. 1991, doi: 10.1103/physrevlett.67.661.

[7] N. Sood, “Cryptography in post Quantum computing era,” SSRN Electronic Journal, Jan. 2024, doi: 10.2139/ssrn.4705470.

[8] S. K. Sahu and K. Mazumdar, “State-of-the-art analysis of quantum cryptography: applications and future prospects,” Frontiers in Physics, vol. 12, Aug. 2024, doi: 10.3389/fphy.2024.1456491.

[9] J.-P. Aumasson, “The impact of quantum computing on cryptography,” Computer Fraud & Security, vol. 2017, no. 6, pp. 8–11, Jun. 2017, doi: 10.1016/s1361-3723(17)30051-9.

[10] N. Durr-E-Shahwar, M. Imran, A. B. Altamimi, W. Khan, S. Hussain, and M. Alsaffar, “Quantum Cryptography for Future Networks Security: A Systematic Review,” IEEE Access, vol. 12, pp. 180048–180078, Jan. 2024, doi: 10.1109/access.2024.3504815.

[11] M. Victor, D. D. W. Praveenraj, S. R, A. Alkhayyat, and A. Shakhzoda, “Cryptography: Advances in secure communication and data protection,” E3S Web of Conferences, vol. 399, p. 07010, Jan. 2023, doi: 10.1051/e3sconf/202339907010.

[12] Sibi, “The impact of quantum computing on cryptography,” International Journal for Research in Applied Science and Engineering Technology, vol. 11, no. 3, pp. 1762–1765, Mar. 2023, doi: 10.22214/ijraset.2023.49770.

[13] N. E. O. Sodiya, N. U. J. Umoga, N. O. O. Amoo, and N. A. Atadoga, “Quantum computing and its potential impact on U.S. cybersecurity: A review: Scrutinizing the challenges and opportunities presented by quantum technologies in safeguarding digital assets,” Global Journal of Engineering and Technology Advances, vol. 18, no. 2, pp. 049–064, Feb. 2024, doi: 10.30574/gjeta.2024.18.2.0026.

[14] J. K. Manda, “Quantum-Safe Cryptography for Telecom Networks: Implementing Post-Quantum Cryptography Solutions to Protect Telecom Networks Against Future Quantum Computing Threats&nbsp;,” SSRN Electronic Journal, Jan. 2025, doi: 10.2139/ssrn.5136797.

[15] M. A. Akbar, A. A. Khan, and S. Hyrynsalmi, “Role of quantum computing in shaping the future of 6 G technology,” Information and Software Technology, vol. 170, p. 107454, Mar. 2024, doi: 10.1016/j.infsof.2024.107454

..