Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-A, pp. 1681–1691
DOI : 10.47974/JDMSC-2168

Design and implementation of quantum-resistant cryptographic algorithms in blockchain networks

Shyam Deshmukh *
Department of Information Technology
Pune Institute of Computer Technology
Pune 411043
Maharashtra
India

Sinu Nambiar †
Department of Artificial Intelligence and Data Science
Marathwada Mitra Mandal College of Engineering
Pune 411052
Maharashtra
India

Pallavi Sachin Patil §
Department of Artificial Intelligence & Machine Learning
Genba Sopanrao Moze College of Engineering
Pune 411045
Maharashtra
India

Madhura Phatak ‡
Department of Computer Engineering and Technology
Dr Vishwanath Karad MIT World Peace University
Pune 411038
Maharashtra
India

* *E-mail:* dshyam100@yahoo.com (Corresponding Author)
† *E-mail:* sinunambiar@mmcoe.edu.in
§ *E-mail:* patilpallavi06@gmail.com
‡ *E-mail:* madhura.phatak@mitwpu.edu.in

Bhavana Tiple [@]
Department of Computer Engineering and Technology
Dr. Vishwanath Karad MIT World Peace University
Pune 411038
Maharashtra
India

Aniket Prakashrao Munshi [#]
Department of Electrical Engineering
Yeshwantrao Chavan College of Engineering
Nagpur 441110
Maharashtra
India

Abstract

Traditional cryptographic methods are in big danger from quantum computing, which could make blockchain networks less safe. This essay looks at how to make and use quantum-resistant encryption methods that work in blockchain settings. First, we look at how vulnerable current cryptographic methods are to quantum attacks. This appears how vital it is to discover alternatives that are not influenced by quantum assaults as before long as conceivable. At that point, we see at distinctive post-quantum cryptographic strategies, such as hash-based, code-based, and lattice-based cryptography, and judge how well they can be utilized in blockchain frameworks. The most center is on the issues that come up in genuine life and the trade-offs in execution that come with these quantum-resistant calculations. These incorporate key estimate, handling speed, and the capacity of the organize to develop. The strategies we've come up with are implied to create blockchain more secure whereas still working well. We put a few strategies to use in a test blockchain and test them within the genuine world to see how they influence exchange speed and delay. Agreeing to the comes about, quantum-resistant calculations can be utilized in blockchain systems, indeed in spite of the fact that they include a few additional work.

Subject Classification: *68M25.*

Keywords: *Quantum-resistant cryptography, Blockchain security, Post-quantum algorithms, Lattice-based cryptography, Hash-based cryptography, Quantum computing threats*

1. Introduction

Cutting edge encryption frameworks, which are basic for securing advanced messages and information security, are confronting issues that have never been seen some time recently since quantum computing is

[@] *E-mail:* **bhavana.tiple@mitwpu.edu.in**
[#] *E-mail:* **aniketpmunshi@gmail.com**

progressing so rapidly [1]. Blockchain systems are secure since they utilize conventional secure strategies like RSA and elliptic-curve cryptography (ECC) to form beyond any doubt that exchanges are private and genuine [2], [3]. But the rise of quantum computing might debilitate these security measures since quantum algorithms like Shor's calculation may well be able to break the encryption frameworks that are as of now in utilize [4]. Since of this shortcoming, quantum-resistant encryption strategies must be made to ensure blockchain systems from these sorts of dangers in a world after quantum computing [5]. This paper talks approximately how to construct and utilize quantum-resistant security arrangements in blockchain frameworks to meet the squeezing require for such arrangements. We see into distinctive post-quantum cryptographic strategies, such as hash-based, code-based, and lattice-based cryptography, to see in the event that they seem supplant or include to current cryptographic guidelines in blockchain systems [6]. Utilizing these quantum-resistant strategies together comes with its claim issues, such as the require for more computing control and conceivable impacts on exchange speed and delay [7]. We need to deliver you valuable data approximately how conceivable it is to utilize quantum-resistant calculations in real-life blockchain frameworks by looking closely at these variables [8]. Additionally, it lays the groundwork for the development of blockchain systems that are safe, robust, and future-proof, and that are capable of defending against attacks from both classical and quantum computers.

2. Threat Assessment and Analysis

This test and ponder are implied to completely get it the blockchain network's security needs and the conceivable perils that quantum computing might cause. This requires a careful consider of the current cryptographic strategies, like RSA and ECC, which depend on dubious math issues such as numbers factorization and elliptic bend discrete logarithms. Existing security strategies are frail since quantum calculations, like Shor's calculation, can illuminate these issues much quicker than standard calculations [9]. We think that a cryptographic algorithm's security level (S) is related to its key length (k) and how well it can guard itself against quantum dangers, which are given by

$$S(k) = \int_0^k f(t)\,dt \tag{1}$$

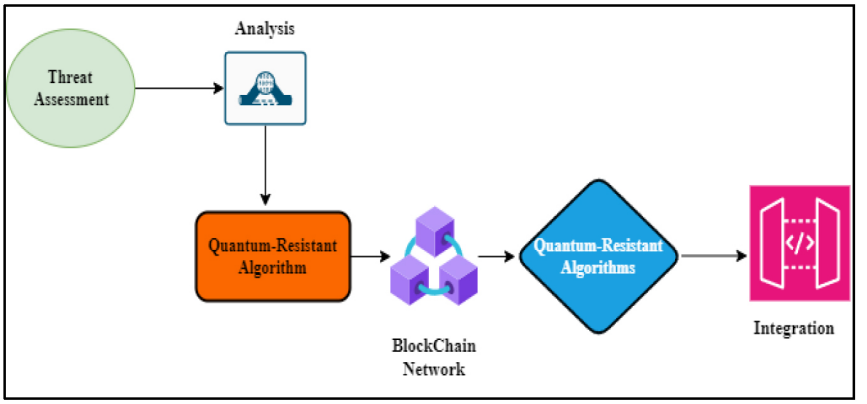


Figure 1

System Architecture of Quantum-resistant Cryptographic Proposed Model

Where, f(t) is the work that appears how security is diminishing. We discover out how frail show calculations are and how imperative it is to have quantum-resistant alternatives by looking at these models [9]. Based on this numerical premise and the system architecture depicted in figure 1, the appropriate cryptographic techniques will be selected in the ensuing steps.

3. Selection of Quantum-Resistant Algorithms

The main goal is to find and evaluate encryption methods that can protect against quantum threats. We will examine various post-quantum cryptography techniques in this step, including hash-, code-, and lattice-based algorithms [10]. Equation (1) illustrates the Shortest Vector issue (SVP), a lattice-based cryptography issue. Its goal is to find the smallest non-zero vector in a lattice. The following expression shows how hard SVP is:

$$SVP(L) = min_{v \in L \{0\}} |v| \quad (2)$$

where L is the lattice and $|v|$ denotes the Euclidean norm of vector v. Because this problem is so hard to solve, quantum attacks are not thought to be able to hurt it. In hash-based cryptography, the security is often judged by how unlikely it is that two hash functions will match. The chance of finding two different inputs x and x′ such that $H(x) = H(x')$ for a hash function H is shown by

$$P_{collision} \approx \frac{1}{2^{\frac{n}{2}}}$$

where n is the output length of the hash function.

Algorithm:

Step 1: Key Generation

$$\text{Choose } A \in \mathbb{Z}_{q^{n \times m}}, \text{ and random vectors } s \in \mathbb{Z}_{q^m}, e \in \mathbb{Z}_{q^n}$$

Generate a random matrix A and vectors s and e, where n and m are dimensions, and q is a large prime modulus. These are used to create the public key.

Step 2: Public Key Computation

$$b = A \cdot s + e \bmod q$$

Compute the public key b by performing matrix-vector multiplication and adding the error vector e, all modulo q.

Step 3: Encryption

$$(c_1, c_2) = \left(A \cdot r + e_1, b \cdot r + e_2 + \mu \cdot \left\lfloor \frac{q}{2} \right\rfloor \right) mod\, q$$

For encryption, choose a random vector r and error vectors e_1, e_2. Encrypt the message μ (where μ ∈ {0, 1}) using matrix-vector multiplication and error addition, ensuring all computations are modulo q.

Step 4: Decryption

$$\mu' = \left\lfloor \frac{c_2 - s \cdot c_1}{\left\lfloor \frac{q}{2} \right\rfloor} \right\rfloor mod\, 2$$

Decrypt the ciphertext by subtracting the product of s and c_1 from c_2, and then dividing by $\lfloor q/2 \rfloor$. Round the result to the nearest integer to recover μ.

Step 5: Error Correction

$$\mu'' = \{$$
$$0, \text{if } |c\_2 - s \cdot c\_1| < \lfloor q/4 \rfloor$$
$$1, \text{otherwise}$$
$$?$$

Apply error correction to ensure accurate decryption by checking if the absolute difference is less than a threshold. If true, the message bit is 0; otherwise, it's 1.

4. Quantum-Resistant Model:

The goal of Step is to create and study mathematical models for the chosen quantum-resistant security algorithms. For lattice-based cryptography, we use the following equation to describe the error distribution and the safety of methods like Learning with Errors (LWE):

$$Error(x) = A \cdot s + e \tag{3}$$

where A is a matrix, s is the secret vector, and e is the error term that follows a Gaussian distribution. A common part of security analysis is handling the lattice reduction problem. This can be described using differential equations to show how to make the lattice base as good as it can be:

$$\frac{d}{dt} \| b_i(t) \|^2 = -\lambda \| b_i(t) \|^2 \tag{4}$$

where $b_i(t)$ is the basis vector at time t and λ represents the reduction rate.

In hash-based encryption, we check how resistant the hash function is to collisions by integrating over the hash space. If (H(x) is the hash function and Collision(H) is the chance of a collision, then the expected number of hash evaluations before a collision is:

$$E[Collisions] = \int_0^{2^{\frac{n}{2}}} P_{collision} dx \tag{5}$$

The length of the result from the hash function is given by n. The security gaps and computing needs of quantum-resistant algorithms can be measured with these models. This helps with their real application in the blockchain network.

5. Result and Discussion

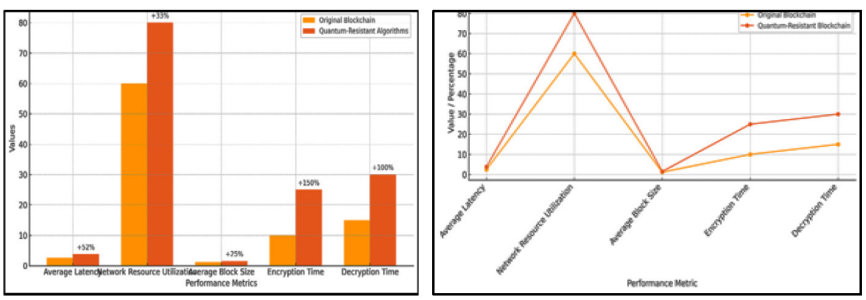
In the performance table, the original blockchain system is shown next to a system that uses quantum-resistant methods. This is because the safer cryptographic methods take more time, which causes the average delay per transaction to rise by 52%. There is a higher demand for processing power, as network resource usage, especially CPU usage, rises

by 33%. Also, the average block size goes up by 25% as shown in Table 1. This is probably because the key sizes get bigger and quantum-resistant methods add more data. Also, both encryption and decryption times get much longer. Encryption time goes up by 150% and decryption time goes up by 80%, showing that more complex calculations need to be done.

Table 1

Comparison of Performance metric of Blockchain Methodologies

Performance Metric	Original Blockchain	Blockchain with Quantum-Resistant Algorithms	% Change
Average Latency	2.5	3.8	+52%
Network Resource Utilization	60%	80%	+33%
Average Block Size (MB)	1.2	1.5	+25%
Encryption Time	10	25	+150%
Decryption Time	15	30	+100%



(a) **(b)**

Figure 2

Representation of (a) Comparison of Performance Metric (b) Compares metrics between the Original Blockchain and the Blockchain with Quantum-Resistant Algorithms

The efficiency measurements of the original blockchain are shown in Figure 2 (a), along with those of the blockchain that uses quantum-resistant algorithms. The line shows the numbers for each measure along with the percentage change that goes with them. This shows how adding quantum-resistant methods affects the performance of the system, comparison of model illustrate in figure 2 (b).

Table 2

Comparing the security and performance of quantum-resistant algorithms

Metric	Traditional Cryptographic Methods	Quantum-Resistant Algorithms	% Change
Security Level	Low	High	+100%
Encryption Time	10	25	+150%
Decryption Time	15	30	+100%
Transaction Throughput	100	75	-25%
CPU Utilization (%)	60%	80%	+33%
Memory Usage	500	650	+30%
Block Size (MB)	1.2	1.5	+25%

The table 2 shows how standard security methods and quantum-resistant algorithms stack up in a number of different ways. According to quantum resistance, the level of security gets a lot better with quantum-resistant algorithms, going up by 100%. But this higher level of protection comes with some costs.

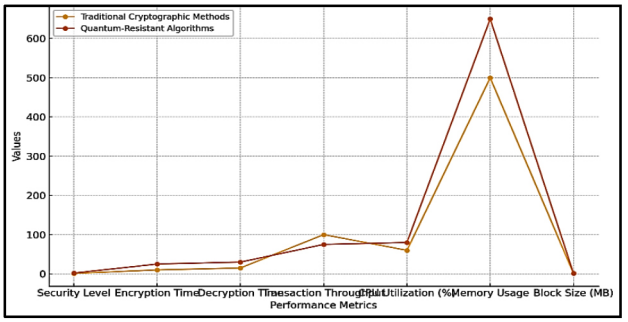


Figure 3

Representation Comparison of Performance Metric

The times for encryption and decryption go up by 150% and 100%, respectively, which means that the computations are more complicated. The amount of memory and CPU used goes up by 33% and 30%, respectively, showing that more resources are needed. The block size goes up by 25%, mostly because the cryptographic data is bigger. Notably, the key size for quantum-resistant methods is much bigger than usual.

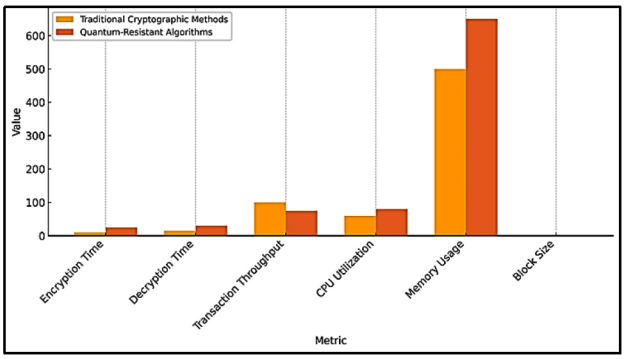


Figure 4

Comparison of Cryptographic Methods

The figure 3 shows how standard security methods and quantum-resistant algorithms compare in terms of performance across a number of different measures. Notably, quantum-resistant algorithms improve security significantly, but they also need more computing labor, as shown by the fact that encryption and decryption take longer, transaction speed goes down, and the CPU is used more.

Quantum-resistant methods also use more memory and have bigger blocks, which shows that they need more resources, comparison of cryptographic model shown in figure 4. This picture shows the trade-offs between more security and a system that works well.

6. Conclusion

Adding cryptographic methods that can't be broken by quantum computers to blockchain networks makes them very immune to new threats that come from quantum computers. Using these methods makes security better and protects the long-term safety and privacy of data. But this higher level of security comes with some big costs, like slower transaction speeds, longer wait times, and more resource use. Even with these problems, deliberate use of quantum-resistant ways is necessary to make blockchain systems ready for the future. The results show that more study and development is needed to find the best mix between security and speed. This will allow for safe and effective blockchain networks in the years after quantum computing. This work lays the groundwork for safe blockchain systems to keep getting better.

References

[1] T. M. Fernández-Caramés and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access,* vol. 8, pp. 21091–21116 (2020).

[2] S. Chauhan, V. P. Ojha, S. Yarahmadian and D. Carvalho, "Towards building quantum resistant blockchain," in Proc. 2023 Int. Conf. Electr., *Comput. Energy Technol*. (ICECET), Cape Town, South Africa, pp. 1–9 (2023).

[3] A. Godbole, R. Dhabliya, V. Deshpande, S. A. Sivakumar, B. M. Shankar and V. Khetani, "Ethical hacking and penetration testing strengthening cybersecurity posture through offensive security measures," *J. Discrete Math. Sci. Cryptogr.,* vol. 27, no. 4, pp. 1295–1305 (2024), doi: 10.47974/JDMSC-1983.

[4] M. Raavi, P. Chandramouli, S. Wuthier, X. Zhou and S.-Y. Chang, "Performance characterization of post-quantum digital certificates," in Proc. 2021 Int. Conf. Comput. Commun. Netw. (ICCCN), Athens, Greece, pp. 1–9 (2021).

[5] T. M. Fernández-Caramés, I. Froiz-Míguez, O. Blanco-Novoa and P. Fraga-Lamas, "Enabling the Internet of mobile crowdsourcing health things: A mobile fog computing blockchain and IoT based continuous glucose monitoring system for diabetes mellitus research and care," *Sensors*, vol. 19, no. 15, p. 3319 (Jul. 2019).

[6] D. Dhabliya, S. Kunche, S. Dingankar, S. S. Dari, R. Dhabliya and V. Khetani, "Blockchain technology as a paradigm for enhancing cyber security in distributed systems," *J. Discrete Math. Sci. Cryptogr.,* vol. 27, no. 2-B, pp. 729–740 (2024), doi: 10.47974/JDMSC-1923.

[7] M. Beverland, P. Murali, M. Troyer, K. Svore, T. Hoefler, V. Kliuchnikov, et al., Assessing Requirements to Scale to Practical Quantum Advantage (2022).

[8] A. S. Shete, S. Bhutada, M. B. Patil, P. H. Sen, N. Jain and P. Khobragade, "Blockchain technology in pharmaceutical supply chain: Ensur-

ing transparency, traceability, and security," *J. Stat. Manage. Syst.,* vol. 27, no. 2, pp. 417–428 (2024), doi: 10.47974/JSMS-1266.

[9] J. Gomes, S. Khan and D. Svetinovic, "Fortifying the blockchain: A systematic review and classification of post-quantum consensus solutions for enhanced security and resilience," *IEEE Access*, vol. 11, pp. 74088–74100 (2023).

[10] G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, J. Kelsey, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, et al., "Status report on the second round of the NIST post-quantum cryptography standardization process," (Jul. 2020).

Received November, 2024