Quantum-Resistant Blockchain: Enhancing Blockchain Security with ROUND5, A Lattice-based Cryptosystem

Md. Saiful Islam, *Mymensingh Engineering College, Mymensingh,2208, Bangladesh*

Puja Rani Saha, *Mymensingh Engineering College, Mymensingh,2208, Bangladesh*

Muhammed Muminul Hoque, *Mymensingh Engineering College, Mymensingh,2208, Bangladesh*

AKM Bahalul Haque, *.LUT University, Finland*

Tushar Kanti Saha, *Jatiya Kabi Kazi Nazrul Islam University, Trishal, Mymensingh, Bangladesh*

Ekram Hossain, *Mymensingh Engineering College, Mymensingh,2208, Bangladesh*

Abstract—

Traditional cryptographic techniques that form the basis of blockchain security are becoming more vulnerable to quantum attacks as a result of the development of quantum computing. With an emphasis on Round5 algorithm, this paper explores the use of quantum-resistant cryptographic algorithms to strengthen blockchain security systems. Round5 operates as an all-purpose, secure, low-complexity cryptosystem with guaranteed security levels against both classical and quantum threats that will be found sustaining technological evolution in the future; therefore, without such an adjustment, all blockchain improvements will be at risk in the future. Firstly, our study involves an in-depth understanding of how blockchain relies on cryptography for secure transactions and privacy. Second, it involves the potentially disruptive benefits of quantum computing and its ability to hack current cryptographic solutions. Finally, it involves the potential for ROUND5, a lattice-based cryptographic solution, to be integrated into a blockchain for better safety and operation. In this respect, we propose a quantum-resistant blockchain architecture to provide better safety without any drastic operational shortcomings. The quantum-resilient nature inspires confidence in this blockchain application for current and future technological use.

Blockchain is a decentralized, immutable, secure digital ledger used for safe and transparent record-keeping, constructed via transactions grouped into blocks that connect through cryptography [1]. Thus, "blockchain" is a collection of transactions grouped into blocks that connect in a chain through cryptography. The chains of blocks where each consecutive block connects to the one before [2] it allows for data integrity, since the longer the chain grows and the more transactions occur, the more challenging, if not impossible, it becomes to change what is already there.Blockchain technology, underpinning cryptocurrencies like Bitcoin [3] and Ethereum, has revolutionised numerous industries offering decentralized, transparent, and secure solutions.

However, the emergence of quantum computing poses a significant threat to the security of blockchain systems. Quantum computers, with their immense computational power, can potentially break the cryptographic algorithms that underpin the security of blockchain networks, such as RSA and ECC. This vulnerability necessitates the adoption of post-quantum cryptographic solutions to safeguard the future of blockchain technology.

Lattice-based cryptography emerges as a promising approach to post-quantum cryptography, offering strong security guarantees against quantum attacks. It relies on complex math problems related to lattice structures, like the Shortest Vector Problem (SVP) and the Learning With Errors (LWE) problem, which are difficult to solve even with powerful quantum computers [4]. These issues are immune to attacks by

XXXX-XXX © 2021 IEEE
Digital Object Identifier 10.1109/XXX.0000.0000000

quantum computers because they are computationally difficult to solve even with quantum algorithms like Shor's or Grover's. Lattice-based methods utilize complicated, multi-dimensional structures to facilitate encryption, digital signatures, and key exchange. Whereas standard cryptosystems rely on discrete logarithms or factorization for self-securing—both of which quantum computers can break in a matter of seconds—polynomially secure efforts based on lattices are better for a wide range of applications, easy to apply to low-resource devices yet still highly resilient with security assurances [5]. Lattice-based cryptography will ensure that communications function properly in a post-quantum realm due to its stability and improvements such as regularized lattices and speedup methods.

One such lattice-based cryptosystem, ROUND5, has gained significant attention due to its efficiency and security properties. By leveraging the power of lattice based mathematics, ROUND5 provides a robust solution to the quantum threat, ensuring the continued security and integrity of blockchain networks. Round5 is a post-quantum cryptography public key encryption and key encapsulation system, which is the next generation of blockchain security for an anticipated quantum computing threat. Its lattice architecture provides a secure, effective, and flexible response to upcoming security requirements in a quantum environment [6]. The NIST Post-Quantum Cryptography Standardization initiative includes Round 5. Its goal is to develop robust cryptographic defenses against risks posed by quantum computing. This system makes use of the complex General Learning with Rounding (GLWR) issue, which is well-known for being resistant to quantum attacks. It engages an ideal security efficiency balance with its adjustments to the Lindner Peikert (LP) scheme, but it is vulnerable to attack based on the comparatively easy Learning with Rounding (LWR) problem. Its adaptive architecture enables it to act as R5_CCA_KEM for Key Encapsulation Method and R5_CCA_PKE as it works with Public Key Encryption (PKE), meeting the security requirements needed to support blockchain transactions. Since Round5 is a finalist in the NIST PQC Standardization Project and is used in multiple programming languages, an international adoption pattern and similarly positive news suggest that this could be a feasible, effective PQC solution for blockchain security. As blockchain networks are vulnerable to emerging attacks, Round5 would be the best defense for any blockchain network since it's lightweight, accessible across multiple languages, and immune to quantum attacks. Round 5 seems critical to the safety and viability of blockchain technology in an unavoidable quantum era [7].

This research aims to delve deeper into the performance and security characteristics of ROUND5. We will analyze key metrics such as key size, execution time, and quantum security level to evaluate the practical feasibility of integrating ROUND5 into blockchain key encryption systems. Additionally, we will compare ROUND5 with other leading lattice-based cryptosystems to identify its strengths and weaknesses.By understanding how ROUND5 performs in terms of key generation, signature generation, and verification times, we can assess its suitability for various blockchain applications. Analyzing the key size of ROUND5 and comparing it to other post-quantum cryptosystems will provide insights into its storage and communication overhead. Furthermore, evaluating the estimated quantum security level of ROUND5 will help us understand its resilience against future quantum attacks. Through a comprehensive comparative analysis, we aim to identify the strengths and weaknesses of ROUND5 relative to other lattice-based cryptosystems. This will enable us to assess its potential to enhance the security and efficiency of blockchain networks. By addressing these research questions, we aim to provide valuable insights into the practical application of ROUND5 in blockchain technology, contributing to the development of a more secure and resilient digital future.

Background Theories

How Blockchain Works

The distributed and tamper-proof digital ledger named Blockchain verifies transactions securely through cryptographic algorithms together with consensus mechanisms. The cryptographic hash from the previous block exists in each block to protect data integrity and stop any unauthorized changes. Asymmetric cryptography enables secure identity verification through public and private keys. SHA-256 hash functions serve as data authentication tools which verify that stored information stays unchanged. Thus, private keys enable signature and decryption operations, but encryption and public key signature verification processes authenticate transactions. Blockchain data becomes immutable after its addition because network consensus through Proof of Work (PoW) or Proof of Stake (PoS) mechanisms is required to modify it [8]. Because validation occurs across multiple systems the approach offers robust security as well as complete transparency. The decentralized approach to validation makes blockchain a secure and transparent system.

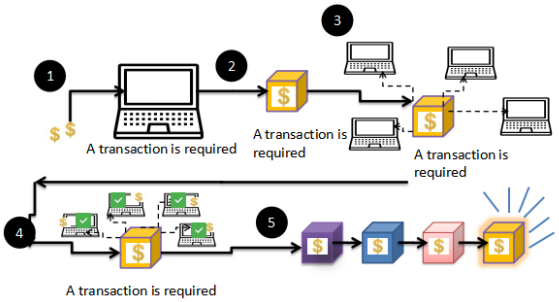

FIGURE 1: Working procedure of blockchain

Ahram [9] provides an extensive overview of the disruptive nature of blockchain across all realms in his article. From finance to health to any logistics with supply chain, he believes that blockchain is a transparent, secure, immutable way to record information that will only increase IoT and cloud-based expansion, smart contract viability, and better cybersecurity.

Quantum Computing

Quantum computing is a type of computing that uses quantum mechanical laws to compute information. Bits are the basic unit of information used in calculations by ordinary computers. A bit is either a 1 or a 0. Yet quantum computers use quantum bits—quantum or qubits. Due to the quantum property of superposition, a qubit can exist as 0 and 1 at the same time [10]. Furthermore, due to another quantum property called entanglement, qubits can become entangled so that the state of one qubit changes the state of the other qubit, regardless of distance. This makes it possible for quantum computers to process enormous volumes of data and carry out intricate computations at rates that greatly exceed those of classical computers [11]. This study [12] looks into the theory behind quantum algorithms and how they relate to classical complexity classes. It focuses on how time and space limitations affect the abilities of classical computers. In contrast to the exponential time needed by classical algorithms, it examines how quantum computation can provide more power, especially when solving problems like factoring in polynomial time and discrete logarithms [12].

Limitation Of Existing Blockchain Security

Despite its strong architecture and reliance on cryptographic principles, blockchain technology is not immune to vulnerabilities. This study examines[13], that traditional blockchain systems are based on cryptographic methods like RSA and ECC, which use the fact that it's difficult to compute problems like factoring large numbers or solving discrete logarithm problems. The development of quantum computing, capable of effectively cracking existing encryption schemes, poses a serious threat to these methods. The security features of current blockchain systems are particularly vulnerable to post-quantum attacks.

- RSA and ECC are vulnerable to Shor's algorithm

Shor's algorithm is a quantum computing technology that can effectively solve the mathematical challenges that secure popular cryptography schemes like RSA and ECC. ECC is based on the discrete logarithm problem over elliptic curves [14], whereas RSA depends on the difficulty of factoring large integers [15]. By significantly reducing the computational complexity of these issues, Shor's approach makes it possible for a strong enough quantum computer to crack their security in polynomial time. For instance, research by Singh and Sakk [16] explores the vulnerability of traditional cryptographic systems to quantum attacks and emphasizes the need for adopting post-quantum cryptography solutions to ensure data security in a quantum era.

- SHA-256 is vulnerable to Grover's algorithm

The core hash function used in blockchain security, SHA-256, faces a significant threat from Grover's algorithm. While classical computers require 2^{256} operations to perform a brute-force attack on SHA-256, Grover's algorithm allows quantum computers to reduce this effort to approximately 2^{128} operations [17]. In a quantum computing context, this reduces SHA-256's security strength by half, making it less resilient to preimage attacks. This technique risks the security of SHA-256-based blockchain protocols by enabling quantum computers to speed up preimage searches [18].

Mathematics of Round5

ROUND5 operates as a post-quantum cryptographic scheme that relies on the Ring Learning With Rounding (RLWR) problem which demonstrates efficient performance compared to the Learning With Errors (LWE) problem.The core mathematical equation of ROUND5 is:

$$b = \left\lfloor \frac{A \cdot s}{p} \right\rceil \mod q \tag{1}$$

where:

- A is a public random matrix (mod q),
- s is the secret key vector,

- p is a smaller modulus,
- $\lfloor \cdot \rceil$ denotes the rounding function,
- b is the resultant "noisy" output.

ROUND5 implements this equation from lattice-based cryptography to introduce rounding noise which creates a hard problem even for quantum computers in (1).It uses RLWR to establish post-quantum security through its ability to transform ciphertexts into indistinguishable random values which protect against classical and quantum attack methods.ROUND5 protects blockchain transactions with consensus mechanisms against quantum attacks which underscores its method for boosting network security.

Research Methodology

Proposed Scheme

By including the ROUND5 key encryption technique, Figure 2 illustrates how transactions flow across the network, the role of encryption, the consensus process, and inter-node secure communication. At the top of the diagram, the Blockchain Block Structure details how a secure transaction occurs and is stored within the quantum-resilient blockchain. Every blockchain contains two main sections which are the block header and block body. The header includes ROUND5-encrypted keys, which denote secure key exchange is quantum-resilient. The hash of the previous block is included to keep the blockchain's integrity by linking blocks together. Furthermore, the Merkle root exists in this header to allow for rapid validation of all transactions. The body of the block includes the encrypted transactions that ensure sensitive data is protected from unauthorized access.

In the middle of the diagram, the Consensus Mechanism operates as a vital component that validates transactions. When a user initiates a transaction, the network nodes authenticate it by securely exchanging ROUND5-encrypted messages. The blockchain receives transactions only after validator nodes validate them. A winning node is then selected to finalize the block, ensuring decentralization and tamper resistance.

On the right side of the diagram presents post-quantum communication channels through node communication framework to establish secure node-to-node interactions. The channels establish quantum-resistant security for message exchanges so that every network node maintains secure communication while remaining protected from quantum decryption attacks.

Finally, thetransaction floww demonstrates the user-driven transaction process that starts with encryption and network broadcast. The system adds validated transactions to blockchain blocks during the consensus process. The blockchain maintains its long-term viability in a post-quantum world through this approach which provides transparency and security and protects against quantum-based threats.

Experimental Result

Experimental set-up

ROUND5 performance results were achieved in a laboratory environment. Thus, this section will elaborate the hardware and software testing environment setup and reasoning for certain choices. Testing was performed on MacBook Pro 10.1. The processor speed is 2.6 GHz Intel Core i7. The operating system is macOS 10.14.1. The compilers compiling the ROUND5 code include GCC and Apple LLVM version 10.0.0 (clang-1000.11.45.5); the flags are -march=native, -mtune=native, -O3, -fomit-frame-pointer, -fwrapv. One note of concern in the experimental protocol is the decision to take minimum execution times for all operations out of the 10,000 iterations. Normally, median or average values are taken; however, it is this author's prerogative to determine that minimum execution times are the least amount of time each operation took from an algorithmic and non-external perspective due to situational circumstances such as system overhead or multitasking. For example, some operations such as storing the transposed matrices and allocating temporary results will significantly affect the subsequent memory footprint—therefore, reporting such results after a real-time execution will allow for a more accurate memory footprint.

Performance Analysis

Round5_CPA_KEM This section will consider the effectiveness of ROUND5's CPA-KEM performance through various figures, which ultimately demonstrate effectiveness across categories but better appreciation through the graphics [7]. Figure 3 concerns time performance related to all CPA-KEM operations and also related to security significance. It assesses the performance of ROUND5's CPA-KEM across NIST Levels 1, 3, and 5 for public key size, ciphertext size, and bandwidth requirements. A clear evaluation of the trade-off between resource usage and security level is made possible by this graphic portrayal. It reports on execution time for key pair generation, encapsulation,

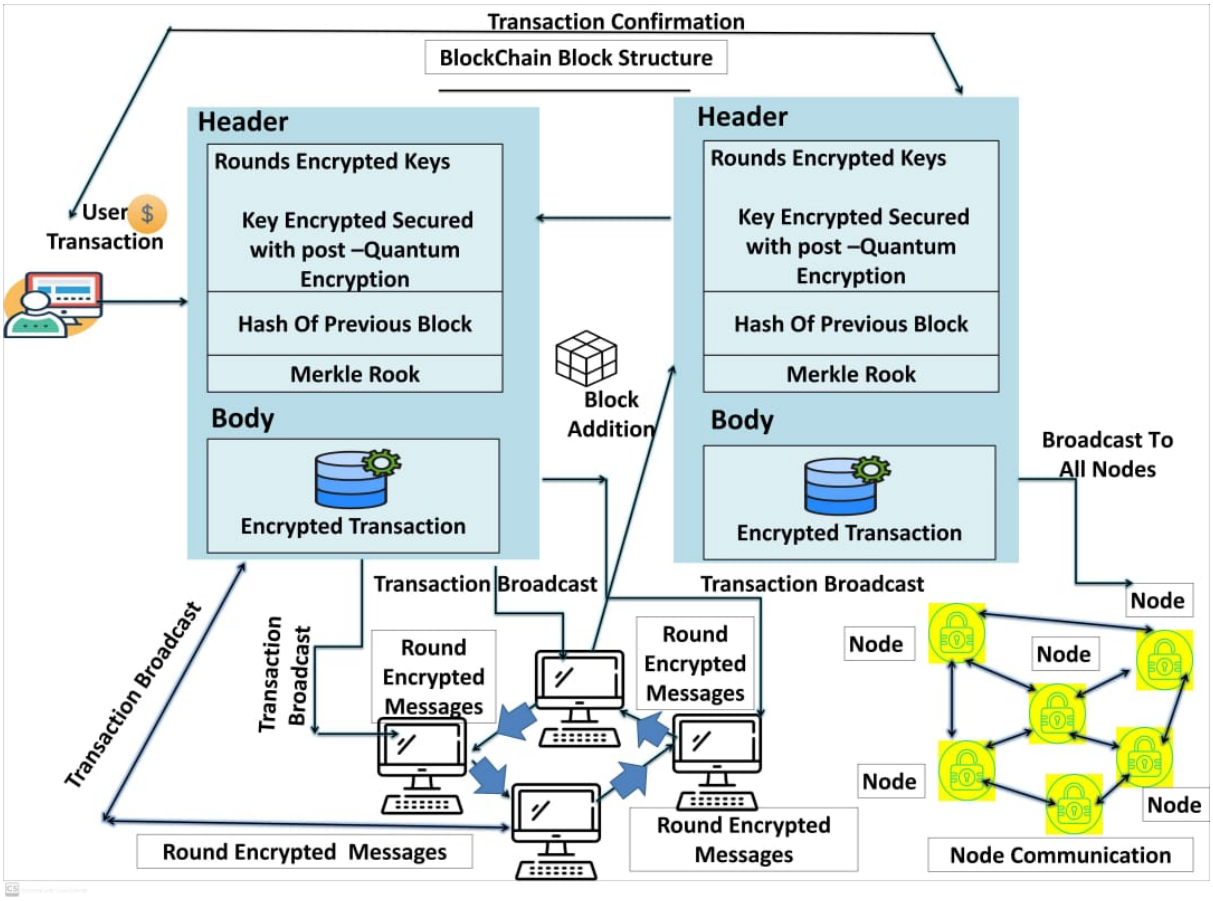

FIGURE 2: Quantum Resistant Blockchain with ROUND5 Key Encryption

and decapsulation across NIST levels 1, 3, and 5. Such an all-encompassing comparison allows a developer to understand computational performance relative to any level it chooses, which assists the developer in determining the best configuration for their needs. This straightforward graphical representation with such inclusive analysis makes ROUND5 applicable in any arena.

Round5_CCA_PKE This section employs a number of instructive figures to visually explore ROUND 5's CCA-PKE performance [7]. These numbers tell an powerful narrative about the effectiveness of the scheme at different security levels and use scenarios. Figure 3 will delve into the interplay between security level and performance for ROUND5's CCA-PKE. These figures analyze key size parameters, total bandwidth consumption, and public/ciphertext sizes across NIST post-quantum security levels 1, 3, and 5. This visual representation will be helpful for a clear understanding of the importance associated with selecting different security levels. It will empower developers to make informed choices for their specific applications. The relationship between security level and performance for ROUND 5's CCA-PKE will be examined in detail in Figure 4. The aggregate bandwidth usage as well as the public and ciphertext sizes for NIST post-quantum security levels 1, 3, and 5 will be examined in these numbers. Along with showing the matching key size requirements, this investigation will also show timing performance related to these unique CCA-PKE configurations.

Comparison with Other Lattice-based Post-Quantum Cryptosystems

Many cryptosystems have been developed as a result of the search for dependable and effective post-quantum cryptographic solutions. The lattice-based cryptosystem ROUND5 is notable for its potential flexibility and performance. Comparing it to other well-known lattice-based systems is crucial to comprehending its full potential. This part emphasizes critical parameters that characterise the stability and effective-

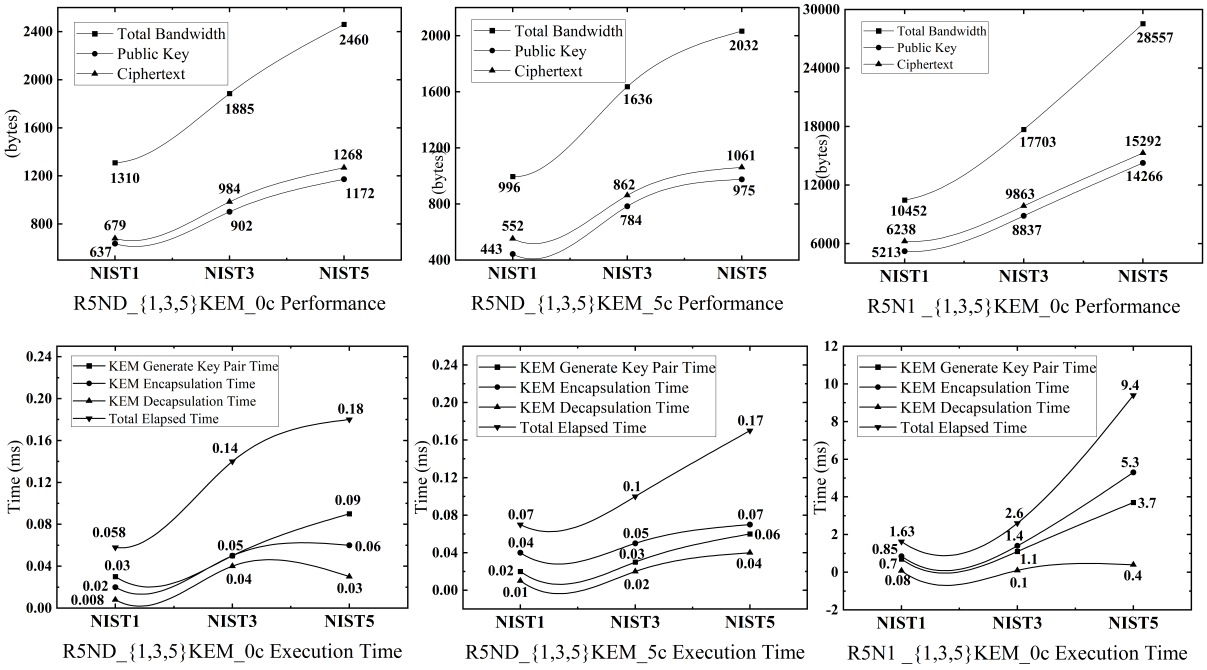

FIGURE 3: Round5_CPA_KEM Performance Analysis

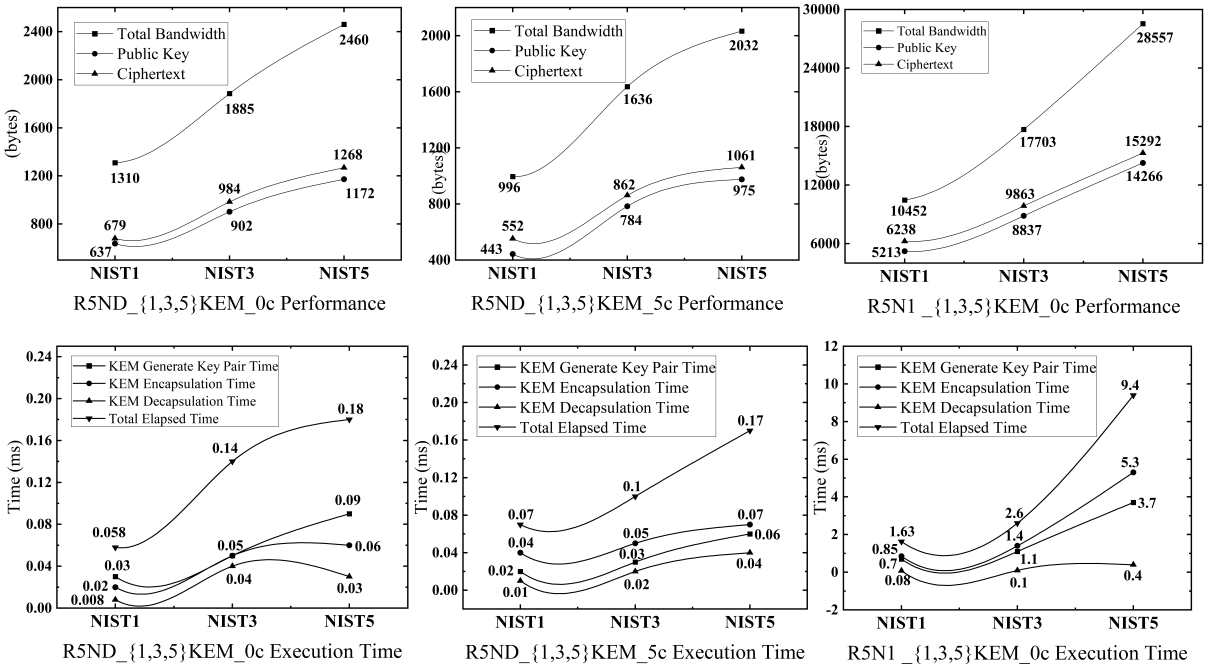

FIGURE 4: Round5_CCA_PKE Performance Analysis

ness of post-quantum cryptosystems and conducts a thorough comparative examination.

Security Considerations

To evaluate the robustness of a cryptosystem, two fundamental dimensions of security are considered:

- **Quantum Security:** This measures a system's ability to withstand attacks executed using quantum computing capabilities. For a cryptosystem to be future-proof, its resistance to quantum-based algorithms like Shor's must be established.
- **Classical Security:** Even in the current era dominated by classical computers, cryptographic systems must maintain high resilience against classical attacks to ensure their immediate reliability.

Key Size and Resource Efficiency

The size of keys and ciphertexts has a significant impact on the effectiveness of cryptosystems in practical applications:

- **Public Key Size:** In blockchain networks, where scalability and bandwidth efficiency are significant concerns, smaller public keys minimize storage and communication overhead.
- **Private Key Size:** Small private keys make safe storage and operational procedures like decryption and signing easier.

Figure 5 serves as an essential reference, offering a thorough comparison of ROUND5 against other post-quantum cryptosystems across several key dimensions that has been stated above.

Performance Metrics and Blockchain Applications

The effectiveness of time-sensitive cryptographic procedures is highlighted in Table 1, which explores ROUND5's operational performance in comparison to other cryptosystems. The following comparisons are especially helpful for blockchain nodes, which rely significantly on computing speed and dependability:

- **Key Generation Cycle:** This process entails creating a secure pair of public and private keys, which serves as a crucial foundation for establishing encrypted communication between blockchain nodes.
- **Encapsulation Cycle:** Encapsulation ensures the confidentiality of data by transforming a message into a ciphertext accessible only to the holder of the corresponding private key.
- **Decapsulation Cycle:** This operation retrieves the plaintext message from ciphertext, enabling secure access to encrypted blockchain transactions.

Cryptosystem	Key Generation (Cycles)	Performance Evaluation Hardware
NewHope-512 (CCA)	117,128	Intel Core i7-4770K
NewHope-1024 (CCA)	244,944	Intel Core i7-4770K
NTRUEncrypt (ntruhps701)	23,302,424	Intel Core i7-4770K
NTRUEncrypt (ntruhps4096821)	31,835,958	Intel Core i7-4770K
NTRU Prime (sntrup4591761)	940,852	Intel Xeon E3-1275 v3
NTS-KEM Level 5	229,357,286	16-core server with Intel Xeon E5-2667 v2
ROLLO-II 256	11,410,000	Intel Core i7-7820X
Round5 KEM	56,300	MacBook Pro 15.1 with Intel Core i7
RQC-III	1,820,000	Intel Core i7-7820X
SABER KEM	163,333	Intel Core i5-7200U

??

TABLE 1: Performance Comparison of Post Quantum Encryption Algorithms for Blockchain Nodes [19]

Cryptosystem	Decapsulation (Cycles)	Encapsulation (Cycles)
NewHope-512 (CCA)	206,244	180,648
NewHope-1024 (CCA)	437,056	377,092
NTRUEncrypt (ntruhps701)	3,642,966	1,256,210
NTRUEncrypt (ntruhps4096821)	4,920,436	1,856,936
NTRU Prime (sntrup4591761)	93,676	44,788
NTS-KEM Level 5	2,500,475	532,168
ROLLO-II 256	7,940,000	2,390,000
Round5 KEM	59,500	97,900
RQC-III	23,200,000	3,550,000
SABER KEM	215,733	196,705

TABLE 2: Performance Comparison of Post Quantum Encryption Algorithms for Blockchain Nodes [19]

Suitability for Blockchain Applications

Round5 Compact Keys, Swift Operations: A Blockchain-Friendly PQC Scheme

Blockchain technology security requires an approach shift to post-quantum cryptography (PQC) due to the impending threat of quantum computers. The quantum era's Shor's Algorithm has made traditional cryptographic primitives susceptible, which presents a serious security issue. ROUND5 shows promise as a blockchain application solution. The public and private key sizes of ROUND5 are clearly smaller than those of several other lattice-based PQC methods. When compared to previous lattice-based cryptosystems, research indicates key size reductions of between 30 and 50 blockchain nodes will need less storage, and there may be less communication overhead when sending keys throughout the network. Additionally, ROUND5 demonstrates faster execution times for important cryptographic activities, such as key generation, encapsulation, and decapsulation. ROUND5 achieves quantifiably faster execution times than several other PQC algorithms. This results in faster transaction processing times and better overall blockchain functionality. These

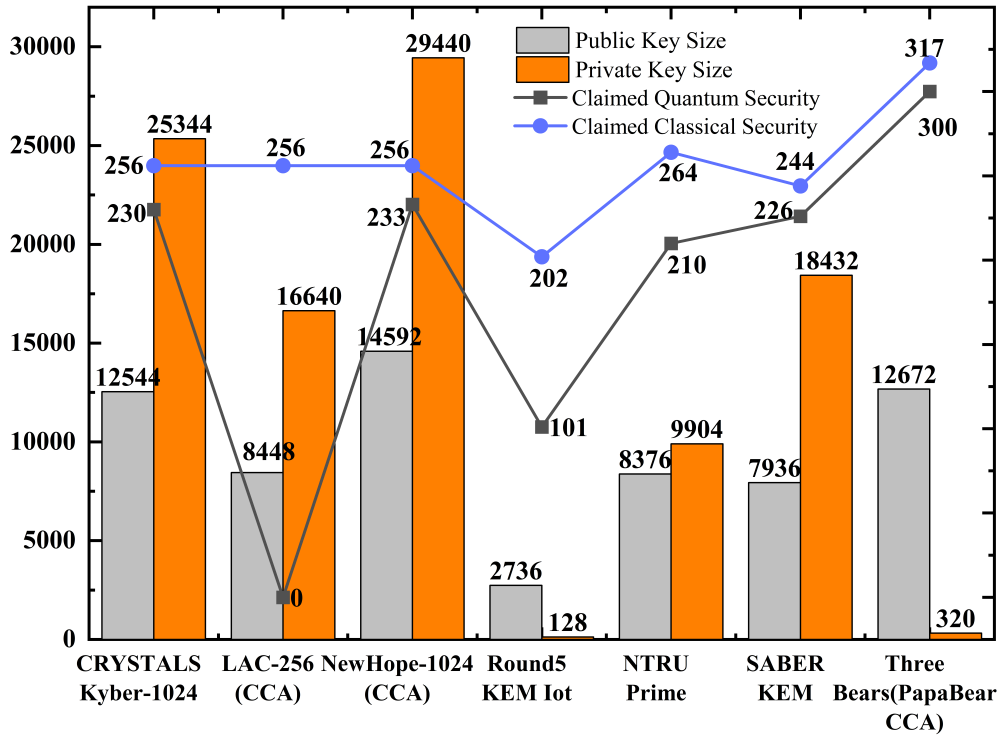

FIGURE 5: Comparison Between Different Lattice-Based Post-Quantum Cryptosystem [19]

qualities are in perfect harmony with fundamental aspects of blockchain design, especially scalability, which gains from smaller 43 key sizes.

Security and Efficiency in Balance: A Customizable Method

For blockchain applications, efficiency is essential, but security always comes first. These two factors are frequently forced to trade off by traditional cryptography primitives. However, ROUND 5 presents a more sophisticated strategy. Because it offers customizable security parameters, blockchain applications may be designed to strike a careful balance between security and performance, adjusting to the unique requirements of each implementation. This reconfigurability depends on ROUND5's lattice-based underlying mathematical structure. The blockchain application can be customized to attain the required security level by modifying certain parameters in the lattice structure. Higher security parameters provide a stronger protection against potential assaults, yet higher key size and potentially slower run times. Lower security parameters expose the application to more potential attacks, yet allow for lower key size and faster run times. This means that application developers and deployers can apply this malleability based upon their own specific attack profile to make the most educated guess. An attack profile is essentially determining what attacks could be posed against a blockchain application's security. For example, a public blockchain could be more vulnerable than a permissioned blockchain based upon the number of users—a public blockchain is open to everyone, yet a permissioned blockchain has a set number of trusted users, which means it could have fewer vulnerabilities based upon the stability of those interested in using the application. Thus, for ROUND5, the structure of this blockchain application would benefit from lower security parameters in this permissioned situation where speed of transaction is valued as an appropriate trade-off for better functionality. This follows the low-risk profile. Yet, it would be preferable to have a greater security priority and use stronger security parameters for ROUND5 in a public blockchain where vulnerabilities might not be too severe—some might even have malevolent intent. For any blockchain application security functioning in a post-quantum fu-

ture, ROUND5 can therefore be adaptable in either way.

ROUND5: Unveiling a Secure and Efficient Post-Quantum Architecture for Blockchains

The future of blockchain security is clouded by the impending threat of quantum computing. Shor's Algorithm exposes traditional cryptographic primitives, posing a threat to the complex network of trust that underpins blockchains. Nevertheless, ROUND5, a lattice-based post-quantum cryptography (PQC) system, appears as a ray of hope. In the quantum era, ROUND5 is a compelling choice for safeguarding blockchain applications. With respect to some of its contemporaries based on lattices, ROUND5 has 44 observably reduced public and private key sizes. For blockchain applications, where node storage constraints and communication overhead can be bottlenecks, this translates to a big benefit. Envision a blockchain in which transactions move quickly around the network without being hampered by large, unwieldy keys. This idea is made possible by ROUND5, which streamlines key management throughout the blockchain ecosystem. ROUND5 is remarkable for its ability to perform key cryptographic operations—such as key generation, encapsulation, and decapsulation—at impressive speeds. These processes are crucial for secure blockchain transactions, and ROUND5's efficiency significantly improves transaction processing times. In the fast-paced blockchain ecosystem, even the smallest time savings can lead to a smoother and more seamless user experience.ROUND5 boasts a security level comparable to other cryptographic primitives, allowing developers to evaluate the trade-off between speed and security to achieve the optimal balance. Therefore, based on the features of each blockchain network, the adjustments for security render digital ledgers to be secured in the places where it's needed most. For instance, a private blockchain with known participants may wish to sacrifice speed to the maximum, while a public blockchain may be able to offer more security for its heterogeneous users. ROUND5 does not merely provide a solution for the quantum computing era. It ensures that blockchain networks can exist in a quantum computing world while not having to compromise their security for gains in speed or processing power. ROUND5 cultivates an increasing confidence in an emerging decentralized world with the capability of both efficiency and security operations. Therefore, ROUND5 is an option that transcends what is needed in the quantum computing era. It stands to champion subsequent innovations to allow any subsequent innovations a safe and secure port in the quantum computing storm.

Discussion

This study contributes to the literature by applying the lattice-based ROUND5 cryptosystem for the blockchain key encryption scheme and its successful performance relative to quantum vulnerability. The use of this post-quantum cryptography approach allows for a scheme that champions quantum safety, something required by the ever-evolving field of cryptography. The results of the testing indicate that ROUND5 is reliable and effective relative to encryption time, time complexity, and extra memory overhead.

Whereas comparing it to current blockchain implementations shows that this solution is vulnerable to attacks from classical competitors. Ultimately, however, current implementations will be vulnerable to malicious quantum computing attacks down the line, but this quantum-resistant solution supports the possibility of blockchain development to remain safe down the line. Furthermore, because ROUND5 is lattice-based, this solution is also efficient and scalable with no adverse performance costs, making it ideal for real world use in blockchain implementations. But the considerations discussed seemed like they could have been eased by some practical deployment concerns and improved usability of functionality. Yet all in all, this article, regardless, presents a strong theoretical foundation for complementing post-quantum cryptography with the current digital era in addition to what's being done for security via blockchain.

Limitations

One of the main drawbacks is the comprehensive assessment of ROUND5's security in relation to blockchain. Whereas the algorithmic lattice-based approach is an opportunity, it requires a cryptanalysis of lattice-based encryption to ensure that ROUND5 is not subject to unexpected exploitation or detectable attacks from quantum computers. Moreover, the performance review of ROUND5 in comparison to existing blockchain networks would require a lot of changes and practical considerations like potential performance overhead or integration issues. Thus, a full performance review is required to assess transaction throughput, latency, and resource utilization in a blockchain setting to see how this would impact ROUND5 and similarly, additional assessments to determine feasibility for like frameworks due to regulations and ancillary protocols and a potential for integration within a current framework.

Conclusion

This research looks into the viability of using ROUND5, a lattice-based encryption technique, as a quantum-resistant approach for improving blockchain security. It shows how ROUND5 can be used to create a key encryption method for a blockchain that is effective, efficient, and secure. These results not only expand the applied theoretical perspective required to apply ROUND5 to a rapidly evolving technology, blockchain but also empirically justify applying ROUND5 to reinforce crucial parts of blockchain technology that are susceptible to new attacks that may be posed by quantum computing. Thus, this contributes to advancements for post-quantum blockchain solutions.

REFERENCES

1. D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," *arXiv preprint arXiv:1906.11078*, 2019.
2. A. B. Haque, A. N. Islam, S. Hyrynsalmi, B. Naqvi, and K. Smolander, "Gdpr compliant blockchains–a systematic literature review," *Ieee Access*, vol. 9, pp. 50593–50606, 2021.
3. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Satoshi Nakamoto*, 2008.
4. O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM (JACM)*, vol. 56, no. 6, pp. 1–40, 2009.
5. H. Nejatollahi, N. Dutt, S. Ray, F. Regazzoni, I. Banerjee, and R. Cammarota, "Post-quantum lattice-based cryptography implementations: A survey," *ACM Computing Surveys (CSUR)*, vol. 51, no. 6, pp. 1–41, 2019.
6. H. Baan, S. Bhattacharya, S. Fluhrer, O. Garcia-Morchon, T. Laarhoven, R. Rietman, M.-J. O. Saarinen, L. Tolhuizen, and Z. Zhang, "Round5: Compact and fast post-quantum public-key encryption," in *Post-Quantum Cryptography: 10th International Conference, PQCrypto 2019, Chongqing, China, May 8–10, 2019 Revised Selected Papers 10*, pp. 83–102, Springer, 2019.
7. S. Bhattacharya, O. Garcia-Morchon, T. Laarhoven, R. Rietman, M.-J. O. Saarinen, L. Tolhuizen, and Z. Zhang, "Round5: Kem and pke based on glwr," *Cryptology ePrint Archive*, 2018.
8. S. J. Alsunaidi and F. A. Alhaidari, "A survey of consensus algorithms for blockchain technology," in *2019 International Conference on Computer and Information Sciences (ICCIS)*, pp. 1–6, IEEE, 2019.
9. T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, "Blockchain technology innovations," in *2017 IEEE Technol. Eng. Manag. Soc. Conf. TEMSCON 2017*, no. 2016, pp. 137–141, 2017.
10. J. Clarke and F. K. Wilhelm, "Superconducting quantum bits," *Nature*, vol. 453, no. 7198, pp. 1031–1042, 2008.
11. A. Glassner, "An introduction to quantum computing," in *ACM SIGGRAPH 2024 Courses*, pp. 1–65, 2024.
12. P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*, pp. 124–134, Ieee, 1994.
13. S. Chandel, W. Cao, Z. Sun, J. Yang, B. Zhang, and T.-Y. Ni, "A multi-dimensional adversary analysis of rsa and ecc in blockchain encryption," in *Advances in Information and Communication: Proceedings of the 2019 Future of Information and Communication Conference (FICC), Volume 2*, pp. 988–1003, Springer, 2020.
14. C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, "Elliptic curve lightweight cryptography: A survey," *IEEE Access*, vol. 6, pp. 72514–72550, 2018.
15. J. Hoffstein, "Integer factorization and rsa," in *An Introduction to Mathematical Cryptography*, pp. 1–75, Springer, 2008.
16. S. Singh and E. Sakk, "Implementation and analysis of shor's algorithm to break rsa cryptosystem security," *Authorea Preprints*, 2024.
17. Y. Du, H. Duan, A. Zhou, C. Wang, M. H. Au, and Q. Wang, "Enabling secure and efficient decentralized storage auditing with blockchain," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 5, pp. 3038–3054, 2021.
18. B. Rodenburg and S. P. Pappas, "Blockchain and quantum computing," *Retrieved from*, 2017.
19. T. M. Fernandez-Carames 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.

First A. Md. Saiful Islam is a researcher in the field of digital identity security and post-quantum cryptographic security. His work has been accepted at the 4th International Conference on Electrical, Computer, and Communication Engineering (ECCE). His research interests include Quantum Computing, Blockchain and its security, Data privacy and protection, Cryptosystems, Machine Learning, the Internet of Things (IoT) and cybersecurity. He completed his graduation from the Department of Computer Science and Engineering at Mymensingh Engineering College, University of Dhaka. Contact him at sanjid.saiful.1@gmail.com

Second B. Puja Rani Saha is a researcher at the Alpha Science Lab, Mymensingh Engineering College. Her works have been accepted in international conferences, including IEEE Xplore. Her research interests include Quantum Computing, Blockchain and its security, Information Security, Post-Quantum Cryptography, Machine Learning.She completed her graduation from the Department of Computer Science and Engineering at Mymensingh Engineering College, University of Dhaka. Contact her at pujas192335@gmail.com

Third C. Muhammed Muminul Hoque is a researcher in the field of digital identity security and post-quantum cryptographic security. He earned his Bachelor's degree in Computer Science and Engineering from Mymensingh Engineering College, University of Dhaka. His research has been accepted at international conferences, including IEEE Xplore. His interests include data privacy, blockchain, lattice-based cryptography, and post-quantum cryptography. Contact him at muminul951@gmail.com.

Fourth D. AKM Bahalul Haque is a Researcher at the Department of Software Engineering at LUT University. Earlier, he was a lecturer at the Department of Electrical and Computer Engineering, North South University. His works have been accepted and published in international conferences and peer-reviewed journals including Technological Forecasting and Social Change, Electronic Markets, PeerJ Computer Science, IEEE Access, Expert Systems, Cybernetics and Systems, various International conference proceedings such as European Conference in Information Systems, IEEE TENCON, ICSOB and Tylor and Francis Books, and Springer Book. His research interests include Explainable AI, blockchain, data privacy and protection, and Social Computing. Contact him at bahalul.haque@northsouth.edu

Fifth E. Tushar Kanti Saha was born in Rajbari on 28 November 1981 in Bangladesh. He received his PhD degree from Saitama University, Japan in 2018 and B.Sc. and M.Sc. in Computer Science and Engineering from Islamic University, Bangladesh. He is currently working as a Professor at the Department of Computer Science and Engineering at Jatiya Kabi Kazi Nazrul Islam University, Trishal, Mymensingh, Bangladesh. His research interests include Information Security, Homomorphic Encryption, Post-Quantum Cryptography, Machine Learning, and Medical Informatics. He has published several papers in different international journals. He has also published several conference papers which were presented in national and international venues. Contact him at tushar@jkkniu.edu.bd

Sixth F. Ekram Hossain is a researcher in the field of digital identity security and assistive technologies. His current research interests include secure national identity verification, AES-256 encryption, and privacy-preserving authentication systems, as well as the application of deep learning to assistive device development. Hossain has published work on topics such as the "Privacy Preserving and Secure Digital Identity Verification Mechanism," which presents an AES-encrypted smart NID with OTP-based two-factor authentication, and "i-Glove: An Intelligent Glove System Based on Deep Learning to Support Deaf-Blind Individuals in Recognizing Banknotes." He received his Bachelor of Science degree in Computer Science & Engineering from Mymensingh Engineering College.Contact him at ekramhossain117@gmail.com.