Grenze International Journal of Engineering and Technology, June Issue

Quantum-Safe Cryptography for Security Enhancement using Lattice-based LWE with Enhanced Approach

Parshvi Shah[1] and Sujata Deshmukh[2]
[1-2]Fr. Conceicao Rodrigues College of Engineering, Computer Engineering Department, Mumbai, India
Email: pshah@fragnel.edu.in, sujata.deshmukh@fragnel.edu.in

***Abstract*— The fast evolution of Internet of Things (IoT) systems has presented a variety of security issues caused by the heterogeneity of devices, a lack of calculational resources, and the growing vulnerability to cyberattacks. Conventional cryptography is no longer sufficient and especially with the development of quantum computing that can break into popular encryption algorithms. This paper presents a quantum-resistant cryptography system based on an improved lattice-based Learning with Errors (LWE) algorithm to achieve secure and efficient communication in IoT networks. The suggested architecture combines optimized poly-computation with Residue Number System (RNS) and Karatsuba multiplication to minimize computation costs and still provide high security assurances. It includes secure key creation, effective data processing and robust encryption-decryption processes optimized to resource-constrained devices. More security measures, such as authentication and integrity checking, are used to increase resilience to both classical and quantum attacks. Experimental evidence shows that the proposed methodology has better performance about shorter encryption time, lower latency and optimization of using memory than traditional and available methods based on lattices. Besides, advanced threats like brute-force, replay and quantum-based attacks are resisted highly using the framework. Overall, this study provides a scalable, efficient and quantum-resistant solution to secure next-generation IoT systems. It is important to note that the results demonstrate the feasibility of improved LWE-based cryptography in practice and can fill significant gaps of the existing IoT security architecture, as well as precondition the development of the post-quantum security in the future.**

***Keywords*— Quantum-Safe Cryptography, Internet of Things (IoT), Learning with Errors (LWE), Lattice-Based Cryptography, Post-Quantum Security, RNS–Karatsuba Optimization, Secure Communication, Lightweight Encryption.**

I. INTRODUCTION

A. Background of IoT Security Challenges

The Internet of Things (IoT) has experienced a great deal of development, which has greatly altered the healthcare field, transportation, and smart cities, yet it has also brought about important security issues. IoT-based systems are heterogeneous and resource-constrained devices that tend to have weak security controls, which render them highly susceptible to cyberattacks. Poor encryption, insecure communication protocols, and weak authentication present a risk to the IoT networks in the form of Distributed Denial of Service (DDoS), spoofing, and data breaches [1]. Also, the growing interconnectedness of AI-based attacks and massive botnets has further complicated the threat environment and is a compelling target to cyber criminals of IoT systems [2].

Grenze ID: 01.GIJET.12.2.328_26

The other significant issue is that most IoT devices are designed to be vulnerable, meaning most of their functionality takes precedence over security, which leads to default credentials, unpatched software, and poor monitoring systems [3]. The large-scale deployment of heterogeneous devices also poses a challenge in ensuring a similar level of security among networks. With the ongoing development of the IoT, the need to overcome such vulnerabilities has become a key issue in the pursuit of a secure and reliable communication system.

B. Problem statement

The use of IoT technologies has been embraced more; the problem of providing secure communication is a significant challenge because of limitations inherent in currently existing cryptographic methods. Conventional encryption schemes like RSA and ECC are more susceptible to new threats of quantum computing that can successfully crack these encryption schemes. In addition, IoT devices are also prone to having limited computer, memory, and energy resources, which prevents the application of advanced security measures. Existing IoT security programs do not offer holistic security of all layers, which expose systems to threats like unauthorized access, data interception, and malware injection [4]. Also, poor authentication measures and inconsistency in security measures contribute to the probability of exploitation further [5]. The absence of scalable, lightweight, and quantum-resistant cryptographic systems poses a major vulnerability in the security of IoT ecosystems. Hence, the need is for an efficient quantum-safe encryption method that guarantees the safety of data transmission and low computational overhead that would be appropriate in the context of real-world applications in IoT.

C. Research objectives

Aim

To develop a quantum-safe cryptographic framework for IoT systems using an enhanced lattice-based Learning with Errors (LWE) approach for secure and efficient communication.

Objectives

- To design an improved LWE-based encryption model incorporating efficient polynomial computation techniques (RNS–Karatsuba).
- To enhance key generation and management mechanisms for stronger resistance against quantum attacks.
- To evaluate the performance and security of the proposed framework in comparison with existing cryptographic approaches.

D. Key contributions

The paper suggests a quantum-resistant cryptographic system of the IoT based on lattice-based LWE. It combines RNS- Karatsuba optimization of polynomials to provide better computational efficiency, builds on key generation and management, and offers resistance against quantum attacks. The framework is proven by simulations, which show better security, less latency and an increase in performance than the current approaches.

II. Related Work

The current studies of IoT security have been done with the aim of eliminating the vulnerabilities that appear due to the heterogeneity of devices, their scalability, and limited resources. Elliptic Curve Cryptography (ECC), Attribute-Based Encryption (ABE) and hybrid encryption models are lightweight cryptographic algorithms that have been extensively considered as means of securing IoT communications. The lower computation costs of ECC is believed to make it effective, yet the issue of scalability and key management remains a problem in large scale IoT networks [1]. Symmetrical and asymmetrical cryptography are employed in hybrid schemes, which have proven more flexible, but have also proven to be challenged in balancing security and computational expenses. Even the well-known cryptography algorithms are now considered to be insecure due to the introduction of quantum computing. It has sparked the interest in post-quantum cryptography (PQC), algorithms for lattice including Learning with Errors (LWE) and Ring-LWE. The approaches are regarded as good candidates for quantum resistant security, and have been instantiated on schemes like CRYSTALS-Kyber [6]. Moreover, the recent studies have proposed hybrid quantum-resistant schemes based on LWE and classical encryption that can offer enhanced protection to IoT even while keeping the flexibility of a wide range of devices [7].

However, in spite of these developments, there are still a number of limitations. Lattice-based cryptographic schemes are secure, but in general, they are computationally complex and demand significant memory, which is difficult to execute on IoT devices with limited resources [8]. Moreover, it has been found that very few lattice-

based models can provide strong adaptive security guarantees, which means that there are loopholes in resistance to sophisticated attacks [9]. The introduction of new technologies like blockchain, artificial intelligence, and machine learning is another area of study that will be incorporated into enhancing the security of IoT. Although such methods enhance threat detection and decentralized security, they also provide extra complexity and implementation difficulties [10]. Altogether, current literature identifies a dire need to create lightweight, scalable, and quantum-resistant cryptographic systems.

III. Proposed Framework

A. System Overview

The desirable system will be comprised of IoT devices, a secure communication channel and a receiving server. IoT sensors generate data, which is preprocessed and encrypted with an enhanced LWE-based model and sent over. The model includes effective operations of polynomials and safe key exchanges. Encrypted data is decrypted and authenticated at the receiver end to make sure that it is authentic and intact.

B. Key Generation and Management

The lattice structure is the basis of key generation, in which the generation of the public and private keys is made using random polynomial vectors and noise parameters. The system ensures secure key distribution using lightweight protocols suitable for IoT devices. The main management entails regular updates and secure storage to avert key leakage and replay attacks. With the improved method, the size of the key is lessened while maintaining the security guarantees.

C. Data Processing

Raw IoT data is normally passed through pre-processing (normalization, formatting, structuring packets) prior to encryption. This is to ensure that this is consistent with the encryption operations based on polynomials. The data is broken down into small blocks which are easily computed to reduce computational overhead and increases transmission efficiency. Also, mechanisms of error tolerance are incorporated to handle noisy environments, typical of the IoT systems.

D. Polynomial Computation (RNS–Karatsuba)

Polynomial computation is a key component of lattice-based cryptography. The given framework is a combination of the Residue Number System (RNS) and Karatsuba multiplication, which are used to speed up the work of polynomials. RNS can do parallel computation by coding large numbers with small residues and Karatsuba can reduce the complexity of multiplication. This combination approach significantly decreases computation time and memory usage, and LWE could be applied in real-time IoT applications.

$$\mathrm{T(n)} = \mathrm{O}(\mathrm{n}^{1.58})(\text{Karatsuba multiplication})$$

$$\mathrm{T(n)} = \mathrm{O}(\mathrm{n}^{2})(\text{Traditional multiplication})$$

The Karatsuba multiplication algorithm reduces the computational complexity of polynomial operations from $\mathrm{O}(\mathrm{n}^2)$to approximately $\mathrm{O}(\mathrm{n}^{1.58})$. When combined with the Residue Number System (RNS), this significantly accelerates large integer and polynomial computations.

E. LWE-based Encryption Model

$$\mathrm{c} = \mathrm{A} \cdot \mathrm{s} + \mathrm{e} + \mathrm{m}(\mathrm{mod q})$$

where Arepresents a randomly generated matrix acting as a public parameter, sdenotes the secret key vector, eis a small error (noise) vector introduced to ensure security, mis the plaintext message, and cis the resulting ciphertext

$$\mathrm{m} = \mathrm{c} - \mathrm{A} \cdot \mathrm{s}(\mathrm{mod q})$$

During decryption, the receiver uses the secret key sto remove the linear component $\mathrm{A} \cdot \mathrm{s}$from the ciphertext. The remaining noise term is sufficiently small, allowing accurate recovery of the original message m.
The encryption model is founded on the infeasibility of the Learning with Errors problem, and it guarantees quantum resistance. Plaintext messages are converted to a form of polynomials and is joined with noise and public key elements, randomly generated, to create a ciphertext.

F. Security Enhancements

The framework has additional security measures that are incorporated to enhance security. These are message authentication codes (MACs) to verify integrity, a secure hash to verify data and adaptive noise tuning to resist advanced attacks. This framework also includes defense against side-channel attacks and replay attacks and provides complete coverage.

G. Encryption and Decryption Workflow

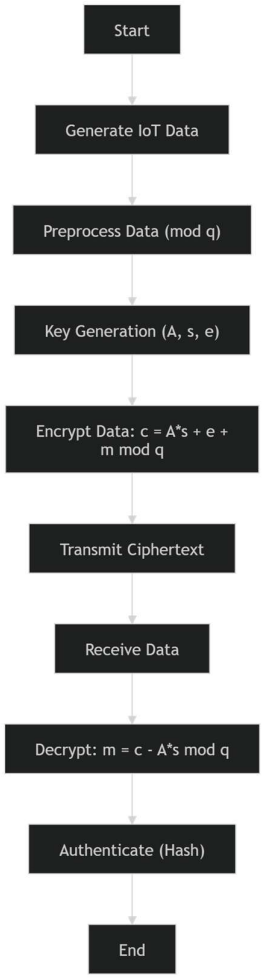

Figure 1. Decryption Workflow

The process starts with the generation of data in the IoT devices and preprocessing and encryption by the LWE-based model. The encrypted information is conveyed via a safe channel. At the receiver, the system will be able to decrypt the message with the private key and remove the noise element to get the original message.

Algorithm 1: LWE-Based Secure IoT Communication Framework
Input: IoT sensor data (m), modulus parameter (q), lattice dimension (n)
Output: Decrypted and authenticated message (m')
1: Acquire IoT sensor data (m).
2: Preprocess the collected data through normalization and formatting:
$m \rightarrow mp$
3: Generate random public matrix: $A \in Zqn \times n$
4: Generate secret key vector
$s \in Zqn$

5: Generate small error vector
e∈ {−1,0,1} n
6: Encode plaintext message (m_p) into ciphertext space.
7: Compute ciphertext:
c← (A·s+e+⌊q/2⌋·mp) modq
8: Transmit ciphertext (c) through the secure communication channel.
9: Compute intermediate decrypted vector:
v← (c−A·s) modq
10: Recover plaintext message:
m′←Round (⌊q/2⌋v)
11: Generate cryptographic hash value:
h←Hash(m′)
12: Verify integrity and authenticity of the received message using (h).
13: Return decrypted and authenticated message (m').
14: End.

where (A) denotes the random public matrix, (s) represents the secret key vector, (e) is the small error (noise) vector introduced to ensure LWE hardness, and (q) is the modulus parameter. The ciphertext (c) is generated by embedding the plaintext message into the lattice structure with an added noise component to achieve quantum resistance. During decryption, the receiver removes the lattice component using the secret key and applies a rounding function to recover the original plaintext message accurately despite the presence of noise.

IV. Experimental Setup

A. Simulation Environment

The proposed LWE-based model achieves the lowest encryption time due to optimized polynomial computation using RNS–Karatsuba.

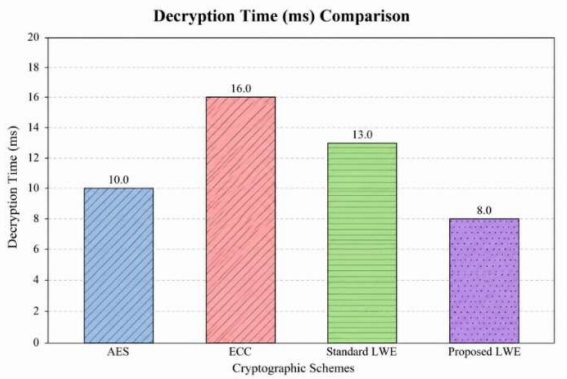

Figure 2. Decryption Time

The suggested framework is modeled by a simulated IoT environment that is created to have virtual devices, channels, and vectors of attack. Network simulators and emulators are tools that are employed to model real-world IoT situations, including the limited capacity of the constrained devices and heterogeneous architectures [11]. Encryption schemes, communication latency, and resilience to cyberattacks can be tested using simulation platforms without being physically deployed. These tools are vital in verifying the scalability, interoperability, and security characteristics of IoT systems.

B. Parameter Configuration

The experimental design comprises the setting of cryptographic and network parameters like the key size, noise distribution (in LWE), the degree of polynomials and the bandwidth of the communication. Other parameters include the processing power of a device, memory restrictions, and packet size, which represent realistic IoT conditions. Parameters that are used to evaluate security, such as the level of confidentiality, integrity, and authentication strength are also specified by [12]. Standard metrics for IoT security, such as accuracy, reliability, and error rates, are used to measure system performance and effectiveness.

C. Evaluation Scenarios

A variety of scenarios are used to test the strength of the proposed framework in different situations. These conditions include normal communications, heavy network conditions, and simulated attack conditions, such as DDoS, data interception, and unauthorized access.Recent challenges in the IoT, such as attacks through botnets and AI-inspired intrusions, are also seen to be indicative of prevailing security challenges [13]. The performance of the framework is measured in terms of encryption time, computational efficiency, memory, and resistance to attacks, making sure that a broad overview of its applicability in real-life IoT settings is considered.

V. Results and Discussion

A. Performance Metrics

The efficiency of the proposed framework is measured based on the encryption time, decryption time, computational overhead, memory consumption, and throughput. Findings show that the improved LWE model saves execution time and consumption of resources as compared to traditional cryptographic methods. Reference [14] emphasizes that lightweight cryptography research indicates that computation optimization and minimizing the complexity of algorithms are crucial in IoT spaces with low processor power. Also, RNSKaratsuba is much faster to operate with polynomials, and helps reduce latency as well as increase efficiency [15]. The framework is also more scalable and energy efficient, which makes it applicable in real-time IoT applications.

B. Comparative Analysis

The effectiveness of the proposed method is compared to the currently used methods, including ECC, AES-based models, and standard lattice-based schemes. Findings indicate that although ECC provides a trade-off between security and efficiency, it has scalability and future quantum vulnerabilities [16]. In the same vein, the conventional encryption methods demand more computational capabilities, which makes them inapplicable in limited settings. Lattice-based methods, in contrast, have quantum resistance but can cause overhead.

Table I. Performance Comparison of Cryptographic Techniques for IoT Security

Criteria	AES	ECC	Standard LWE	Proposed LWE (RNS–Karatsuba)
Quantum Resistance	No	No	Yes	Yes
Encryption Time	Medium	High	Medium	Low (Optimized)
Decryption Time	Medium	High	Medium	Low (Optimized)
Computational Overhead	Low	High	High	Reduced
Memory Consumption	Medium	Medium	High	Low (Optimized)
Key Size	Small	Small	Large	Reduced Size
Scalability (IoT)	Moderate	Low	Moderate	High
Security Strength	High	High	Very High	Very High (Enhanced)
Resistance to Attacks	Moderate	High	Very High	Very High
Latency	Medium	High	Medium	Low
Throughput	Medium	Low	Medium	High
Suitability for IoT	Moderate	Limited	Limited	Highly Suitable

The suggested improved LWE framework solves this problem, making computations more optimal, which leads to higher performance and less consumption of resources [17]. Another advantage of using the model is better throughput and reduced latency that can be identified through comparative analysis than hybrid and lightweight encryption models.

Table II. Numerical Performance Evaluation

Algorithm	Encryption Time (ms)	Memory (KB)	Throughput (kbps)
AES	12	220	180
ECC	18	300	150
Standard LWE	14	350	170
Proposed LWE	9	180	240

C. Security Analysis

This security analysis shows that the suggested framework has a high resistance area against both classical and quantum attacks. Lattice-based cryptography, especially LWE, is known to be robust because the math problems underpin them are hard [18]. Noise added to the encryption process guarantees security against brute-force and cryptanalytic attacks. Moreover, other mechanisms like authentication and secure hashing are useful in

improving data integrity and avoiding replay and spoofing attacks. Recently, research on post-quantum cryptography affirms that lattice-based schemes are some of the most promising to secure IoT systems during the quantum era [19]. In general, the presented framework demonstrates a good balance between security, efficiency, and scalability; thus, it is extremely applicable in the next-generation IoT environments.

VI. Conclusion and Future Work

This paper introduces a quantum-resistant cryptography system of IoT based on a lattice-based LWE system with RNS-Karatsuba optimization. The findings show that it is more computationally efficient, latency is lower, and resistant to quantum and classical attacks. The framework is helpful in dealing with constraints of the classical cryptography techniques in resource-constrained settings. Future efforts on practical applications, hardware optimisation, and the incorporation of emerging technologies like blockchain and AI can enhance the scalability, adaptability, and autonomous threat detection capabilities of next-generation IoT systems.

References

[1] Z. Arabi, R.R. Oskouei, and M. Hosseinzadeh, "Enhancing security in IoT networks: A multifaceted approach to vulnerability analysis and protection," Array, vol. 29, p. 100626, 2025.

[2] A. Mahboubi, K. Luong, H. Aboutorab, H.T. Bui, S. Camtepe, K. Ansari, and B. Barry, "The evolving threat landscape of botnets: Comprehensive analysis of detection techniques in the age of artificial intelligence," Internet Things, vol. 33, p. 101728, 2025.

[3] W. Alsabbagh, C. Kim, and P. Langendörfer, "Investigating the security of OpenPLC: Vulnerabilities, attacks, and mitigation solutions," IEEE Access, vol. 12, pp. 11561–11583, 2024.

[4] A. Sharma and K. Bhushan, "A comprehensive survey on IoT security: Challenges, security issues, and countermeasures," Comput. Sci. Rev., vol. 59, p. 100839, 2026.

[5] M. Kokila and S. Reddy K, "Authentication, access control and scalability models in Internet of Things security: A review," Cyber Security Appl., vol. 3, p. 100057, 2024.

[6] R. O'Connor, A. Khalid, M. O'Neill, and W. Liu, "Better security estimates for approximate, IoT-friendly R-LWE cryptosystems," in Proc. IEEE Asia Pacific Conf. Circuits Syst. (APCCAS), 2022, pp. 611–615.

[7] J. Xiong, L. Shen, Y. Liu, and X. Fang, "Enhancing IoT security in smart grids with quantum-resistant hybrid encryption," Sci. Rep., vol. 15, no. 1, p. 3, 2025.

[8] M. El-Hajj and P. Beune, "Lightweight public key infrastructure for the Internet of Things: A systematic literature review," J. Ind. Inf. Integr., vol. 41, p. 100670, 2024.

[9] S. Hasib, A. Rasool, M. Gyanchandani, R. Haripriya, and L. Kumar, "A structured review of lattice based attribute based encryption methods for post quantum security," Discover Comput., vol. 29, no. 1, 2026.

[10] I.A. Reshi and S. Sholla, "Challenges for security in IoT, emerging solutions, and research directions," Int. J. Comput. Digit. Syst., vol. 12, no. 4, pp. 1231–1241, 2022.

[11] D.A. Patil and S. G, "A comprehensive survey on securing the social Internet of Things: Protocols, threat mitigation, technological integrations, tools, and performance metrics," Sci. Rep., vol. 15, no. 1, p. 40190, 2025.

[12] H. Taherdoost, N. Mohamed, and Y. Farhaoui, "Evaluating IoT data security metrics and emerging trends," Int. J. Service Sci. Manage. Eng. Technol., vol. 16, no. 1, pp. 1–23, 2025.

[13] M. Lefoane, I. Ghafir, S. Kabir, and I.-U. Awan, "Internet of Things botnets: A survey on artificial intelligence based detection techniques," J. Netw. Comput. Appl., vol. 236, p. 104110, 2025.

[14] S.U. Brahmeshwar, N.K. Upadhyay, N. Sharma, and K. Jaswal, "Lightweight cryptography for securing IoT networks: Balancing performance, scalability, and security in resource-constrained environments," Int. J. Res. Appl. Sci. Eng. Technol., vol. 12, no. 12, pp. 2154–2160, 2024.

[15] E. Alkim, D.Y.L. Cheng, C.M.M. Chung, H. Evkan, L.W.L. Huang, V. Hwang, C.L.T. Li, R. Niederhagen, C.J. Shih, J. Wälde, and B.Y. Yang, "Polynomial multiplication in NTRU Prime: Comparison of optimization strategies on Cortex-M4," Cryptology ePrint Archive, 2020.

[16] B. Hanafi and M. Ali, "Analyzing the research impact in post quantum cryptography through scientometric evaluation," Discover Comput., vol. 28, no. 1, p. 32, 2025.

[17] L.H. Mahdi and A.A. Abdullah, "Fortifying future IoT security: A comprehensive review on lightweight post-quantum cryptography," Eng. Technol. Appl. Sci. Res., vol. 15, no. 2, pp. 21812–21821, 2025.

[18] D.S. Amirkhanova, M. Iavich, and O. Mamyrbayev, "Lattice-based post-quantum public key encryption scheme using ElGamal's principles," Cryptography, vol. 8, no. 3, p. 31, 2024.

[19] C.L. Chen, K.W. Zeng, W.Y. Li, C.F. Lee, L.C. Liu, and Y.Y. Deng, "Lightweight post-quantum cryptography: Applications and countermeasures in Internet of Things, blockchain, and e-learning," Eng. Proc., vol. 103, no. 1, p. 14, 2025.