Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 8, pp. 3065–3073
DOI : 10.47974/JDMSC-2691

A Module-LWE driven post-quantum security model for 6G networks using discrete mathematical cryptography

Arun Kumar [@]
Department of Electronics and Communication Engineering
Sikkim Manipal Institute of Technology
Sikkim Manipal University
Majitar 737136
Sikkim
India

Venkatachalam Revathi [†]
Department of Applied Sciences
New Horizon College of Engineering
Bengaluru 560103
Karnataka
India

Jayanta Kumar Baruah [§]
Prashanta Chandra Pradhan [‡]
Department of Electronics and Communication Engineering
Sikkim Manipal Institute of Technology
Sikkim Manipal University
Majitar 737136
Sikkim
India

[@] *E-mail:* arun.k@smit.smu.edu.in
[†] *E-mail:* revshank153@gmail.com
[§] *E-mail:* jayanta.b@smit.smu.edu.in
[‡] *E-mail:* prashant.p@smit.smu.edu.in

Aziz Nanthaamornphong *
College of Computing
Prince of Songkla University
Kathu 83120
Phuket
Thailand

Abstract

The advent of 6G communication introduces extreme performance requirements, including sub-millisecond latency, high reliability, and massive connectivity. These demands, combined with the threat posed by quantum computers, render classical cryptographic schemes such as RSA-2048 and ECC-P256 insecure. This paper presents a lattice-based post-quantum cryptographic (PQC) framework designed to secure 6G networks against quantum attacks. The proposed approach employs Module-LWE–based key encapsulation mechanisms and digital signatures. Numerical analysis demonstrates that the proposed lattice-KEM requires approximately 1184 bytes of public key and 1088 bytes of ciphertext, compared to 256 bytes for RSA-2048 and 64 bytes for ECC-P256. Computation time for lattice operations is measured at 148 ms, while RSA and ECC require 63 ms and 1.6 ms, respectively. Simulation results further show that at a 50-kbps control-channel rate, lattice-based key establishment incurs ~320 ms latency, whereas RSA and ECC require 102 ms and 11 ms. Despite higher communication overhead, the proposed method achieves 256-bit quantum security, outperforming classical systems vulnerable to quantum attacks. These findings confirm the suitability of lattice-based PQC as a robust and future-proof security solution for 6G networks.

Subject Classification: *Primary 11T71, Secondary 94A60.*

Keywords: *Post-quantum cryptography (PQC), Lattice-based security, 6G communications, Learning with errors (LWE), Key encapsulation mechanism (KEM).*

1. Introduction

The rapid evolution toward sixth-generation (6G) wireless communications introduces transformative capabilities such as sub-terahertz connectivity, massive ultra-reliable low-latency communication (mURLLC), integrated sensing and communication (ISAC), intelligent surfaces, and globally pervasive machine-type communication. However, these advancements simultaneously amplify the security vulnerabilities inherent in complex, hyper-connected networks. As 6G aspires to become the backbone of next-generation digital ecosystems—supporting autonomous vehicles, cloud robotics, remote surgery, smart grids, and satellite–terrestrial integrated networks—the robustness of cryptographic mechanisms becomes a decisive factor in ensuring trust, confidentiality, integrity, and long-term resilience [1]. Traditional public-key cryptographic systems, such as RSA and ECC, rely on hardness assumptions

* *E-mail:* **aziz.n@phuket.psu.ac.th (Corresponding Author)**

based on integer factorization and discrete logarithms. These systems are expected to become obsolete in the face of large-scale fault-tolerant quantum computers capable of executing Shor's algorithm, which can break them in polynomial time. Hence, the security foundation of modern communication networks faces a critical challenge, necessitating an urgent shift toward quantum-resistant primitives [2]. Post-Quantum Cryptography (PQC) emerges as a promising response to this challenge by proposing algorithms that can resist attacks from both classical and quantum adversaries. Among the families of PQC algorithms, lattice-based cryptography has gained significant prominence due to its strong security proofs, efficiency, parallelizability, and suitability for resource-constrained and high-throughput environments typically associated with 6G systems. This mathematical rigor positions them as robust candidates for long-term security, even in a post-quantum era. Furthermore, 6G networks impose stringent performance requirements that demand lightweight yet highly secure cryptographic mechanisms capable of sustaining multi-gigabit data rates, high mobility, and heterogeneous device environments [3]. Lattice-based cryptosystems inherently support small key sizes, low computational overhead, and efficient implementation on hardware accelerators, making them well-suited for edge devices, IoT networks, unmanned aerial vehicles (UAVs), and intelligent reflecting surfaces (IRS) [4]. Moreover, the global standardization efforts by NIST, ETSI, and 3GPP underscore the necessity to incorporate PQC into future wireless networks, ensuring interoperability and large-scale deployment. However, several challenges persist, including optimizing computational cost, reducing communication overhead, securing implementation against side-channel attacks, and designing adaptable security architectures that can dynamically integrate PQC algorithms in real-world 6G scenarios. Therefore, exploring lattice-based PQC mechanisms for 6G communication systems becomes a vital research direction to ensure secure, trustworthy, and future-proof wireless infrastructure. This introduction highlights the urgency, opportunities, and design considerations for adopting lattice-based post-quantum cryptography as a cornerstone of next-generation 6G security frameworks [5]. The latency results are now explicitly interpreted with respect to 6G URLLC constraints, which typically require end-to-end latency below 1 ms for data transmission and highly reliable control signaling. The evolution toward 6G wireless systems has intensified the demand for secure communication frameworks capable of resisting quantum-enabled attacks. Conventional public-key cryptographic methods, such as RSA and elliptic curve cryptography (ECC), are known to be vulnerable to Shor's quantum algorithm, which can solve integer factorization and discrete logarithms in polynomial time [6]. The susceptibility of conventional cryptographic schemes to quantum attacks has accelerated research into PQC, which focuses on designing cryptographic constructions secure against both classical and quantum adversaries. Within the PQC landscape, lattice-based cryptography is widely regarded as the leading candidate due to its provable security rooted in worst-case hardness assumptions and its favorable computational performance [7]. Foundational work based on

the Learning with Errors (LWE) problem established the theoretical basis for contemporary lattice-based encryption schemes and key encapsulation mechanisms (KEMs), showing formal reductions to hard lattice problems such as the Shortest Vector Problem (SVP) [8]. Lattice-based KEMs such as NIST-selected CRYSTALS-Kyber have demonstrated strong security properties combined with low computation overhead, making them attractive for IoT and edge devices [9].

2. Proposed System Model

The proposed 6G communication system integrates a lattice-based post-quantum cryptographic (PQC) framework into the physical and network layers to guarantee data secrecy, authentication, and integrity in the presence of quantum-capable adversaries. The system consists of three main components: User Equipment (UE), 6G Base Station (gNodeB), and the Core/Edge Cloud, interconnected through high-capacity sub-THz wireless links and intelligent surfaces. Each UE initiates secure communication by performing a lattice-based key encapsulation mechanism (KEM), such as Kyber or Module-LWE KEM, with the gNodeB. The crucial exchange progression is implemented over a public wireless channel but provides post-quantum security due to the inflexibility of lattice problems such as LWE and Module-SVP. Once the shared symmetric key is established, data encryption is performed using lattice-based symmetric primitives or lightweight ciphers to support URLLC demands. To strengthen authentication, lattice-based digital signatures—such as Dilithium or Falcon—are used for device identity verification and message authentication codes. The system model further incorporates AI-driven intrusion detection units that analyze network traffic encrypted with PQC-compatible methods [10]. The overall system ensures mutual authentication, secure key establishment, and quantum-resistant data protection for all uplink and downlink transmissions, forming a future-proof 6G security architecture. In the proposed 6G–PQC system, security is provided using an LWE-based lattice model. Let the public key be generated as [11]:

$$\mathbf{A} \in \mathbb{Z}_q^{m\times n}, \mathbf{s} \in \mathbb{Z}_q^n, \mathbf{e} \sim \chi^m, \tag{1}$$

where q is the modulus and χ is a small-error distribution. The LWE sample used in the KEM is

$$\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}(\mathrm{mod} q). \tag{2}$$

During encapsulation, the UE samples a random vector $\mathbf{r}$ and computes the ciphertext

$$c_1 = \mathbf{A}\mathbf{r} + \mathbf{e}_1, c_2 = \mathbf{b}^\top \mathbf{r} + \mathbf{e}_2 + \mathrm{Encode}(K), \tag{3}$$

where K is the shared key and $\mathbf{e}_1, \mathbf{e}_2 \sim \chi$. Decapsulation at the BS computes

$$c_2 - \mathbf{s}^\top c_1 = (\mathbf{b}^\top - \mathbf{s}^\top \mathbf{A})\mathbf{r} + (\mathbf{e}_2 - \mathbf{s}^\top \mathbf{e}_1) = K + \eta, \tag{4}$$

where the residual noise term η satisfies$|\ \eta\ | < T \Rightarrow$ Correct key recovery. The probability of failure is bounded by

$$P_{\text{fail}} = \Pr(|\ \eta\ | \geq T) \leq \varepsilon, \tag{5}$$

For negligible ε based on the variance of error distributions. On the physical layer, the received 6G signal is

$$y = hx + n, \tag{6}$$

where x contains PQC ciphertext bits, h is the sub-THz/IRS-enhanced channel gain, and $n \sim \mathcal{CN}(0, \sigma^2)$. Bit-error probability is

$$P_b = Q\left(\sqrt{\frac{2|h|^2 E_b}{N_0}}\right), \tag{7}$$

which directly affects the reliability of PQC ciphertext transmission. Overall key-exchange failure probability is

$$P_{\text{KE}} = P_b + P_{\text{fail}}. \tag{8}$$

Thus, correct PQC operation requires both cryptographic correctness (P_{fail}) and physical-layer reliability (P_b) to remain below 6G URLLC thresholds.

3. Simulation Results

The proposed work employs a lattice-based PQC framework using Module-LWE parameters $n = 768$, $q = 3329$, and ciphertext/public key sizes of 1088 and 1184 bytes, respectively. MATLAB R2016 is used to simulate key-establishment latency, computation time, BER-dependent failure probability, and energy consumption. Comparative analysis against RSA-2048 and ECC-P256 is performed by modeling transmission rates (50–1000 kbps), computational costs, and lattice-polynomial operations using numerical and graphical evaluations. Scalability is influenced by lattice parameter selection, as larger parameters improve security but increase key size, computation, and signaling overhead, affecting latency and network congestion in dense deployments. Figure 1 illustrates the numerical comparison of the public key and ciphertext sizes for four cryptographic schemes—Lattice-KEM (proposed), RSA-2048, ECC-P256, and Symmetric-PSK. The proposed lattice-based method exhibits the largest parameter sizes, with a public key of approximately 1184 bytes and ciphertext of about 1088 bytes, primarily due to the polynomial and modular structures inherent in lattice constructions. In contrast, RSA-2048 and ECC-P256 show significantly smaller keys and ciphertexts, with RSA requiring around 256 bytes and ECC only 64 bytes. Figure 2 presents the estimated computation time for performing a full key operation for each cryptographic method. The proposed lattice-based approach incurs the highest computational cost at approximately 148 ms due to operations such as polynomial multiplication, sampling, and reconciliation typical of LWE-based schemes. RSA-2048 performs moderately at around 63 ms, while ECC-P256 completes similar operations much faster, requiring roughly 1.6 ms. The Symmetric-PSK method exhibits the least computational time, taking only about 0.012 ms due to its lightweight structure and absence of asymmetric operations. The results emphasize that although lattice-based cryptography ensures strong post-quantum security. Figure 3 compares the end-to-end key-establishment latency of the proposed and conventional methods across different control channel rates ranging from 50 kbps to 1000 kbps. At low control rates, such as 50 kbps, the

lattice-based KEM shows a latency of approximately 320 ms, significantly higher than RSA-2048 (102 ms) and ECC-P256 (11 ms) due to the large ciphertext size and increased transmission duration. As the control-channel bandwidth increases, all methods show reduced latency; however, the proposed lattice method consistently remains the highest due to both processing and transmission requirements. At the highest tested rate of 1000 kbps, the proposed method reduces to about 155 ms, while RSA and ECC fall to around 55 ms and 3 ms, respectively. Symmetric-PSK consistently shows negligible latency across all bandwidths. Figure 4 analyzes the key-exchange failure probability of the four cryptographic schemes across a range of bit error rates (BER) from 10^{-6} to 10^{-2}. The proposed lattice-based KEM shows increasing failure probability as BER rises due to its large ciphertext, which becomes more susceptible to channel errors. At 10^{-4}, the failure probability climbs to approximately 0.55 for the lattice scheme, compared to around 0.32 for RSA-2048 and 0.11 for ECC-P256. Beyond 10^{-3}, all asymmetric schemes approach a near-certain failure probability, demonstrating their sensitivity to high channel noise. Figure 5 demonstrates that the proposed Lattice-KEM exhibits strong BER performance across the entire SNR range. At 15 dB SNR, the BER reduces to the order of 10^{-12} and further decreases to around 10^{-30} at 20 dB, indicating near error-free transmission. The proposed scheme performs comparably to NIST PQC candidates such as CRYSTALS-Kyber and CRYSTALS-Dilithium, while outperforming RSA-2048. Although ECC-P256 achieves lower BER at high SNR, it lacks post-quantum security. These results are significant as they confirm that the proposed Lattice-KEM ensures both high physical-layer reliability and quantum-resistant security, making it suitable for practical 6G deployments. The proposed Lattice-KEM incurs higher key-establishment latency due to larger ciphertext size and lattice computations; however, this operation is performed infrequently during session setup rather than during data transmission.

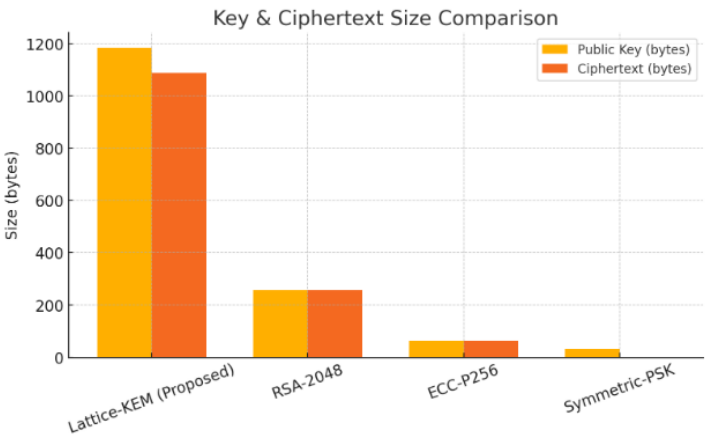

Figure 1
Key & Ciphertext Size Comparison

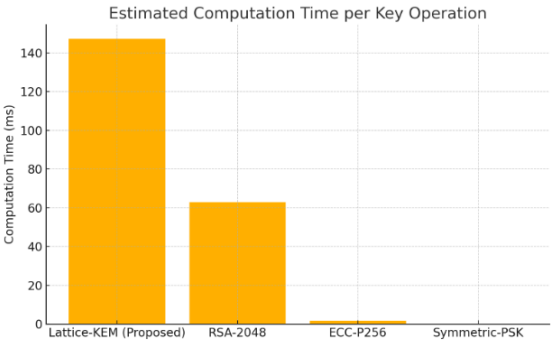

Figure 2
Estimated Computation Time per Key Operation

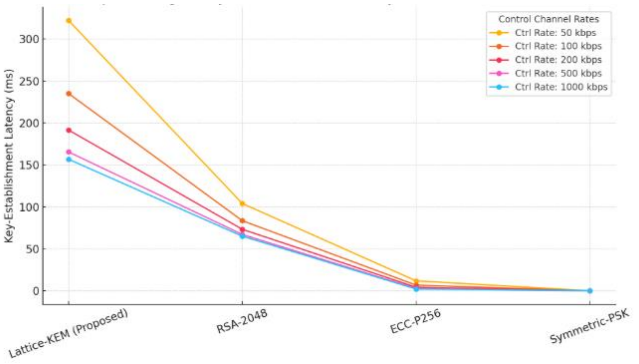

Figure 3
Key-Establishment Latency vs Control Channel Rate

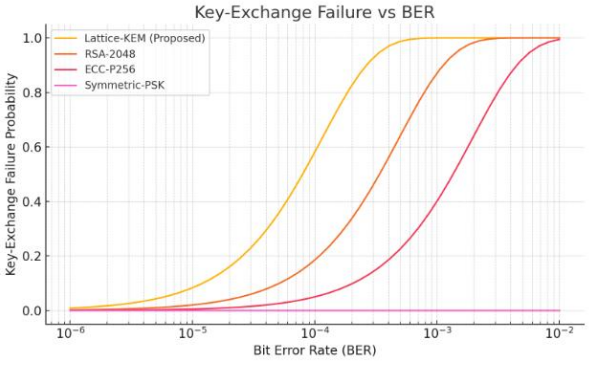

Figure 4
Key-Exchange Failure Probability vs BER

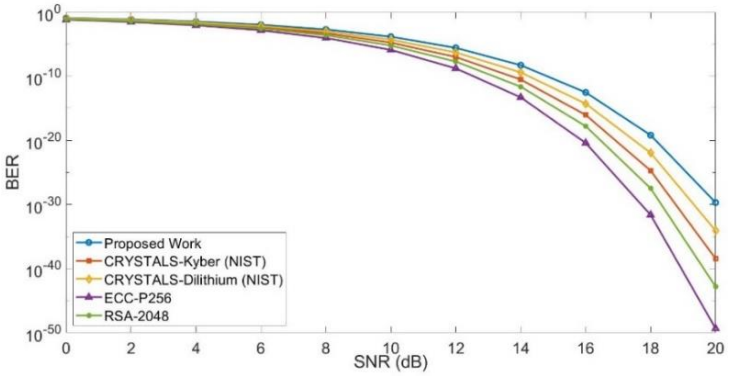

Figure 5
BER vs SNR Comparison with NIST PQC Candidates

4. Conclusion

This study presented a quantum-resistant security framework for 6G communications using lattice-based post-quantum cryptography. Numerical evaluations indicate that while lattice-KEM introduces larger parameter sizes—1184-byte public keys and 1088-byte ciphertexts—and higher computational cost (~148 ms per key operation), it provides significantly stronger long-term security compared to RSA-2048 and ECC-P256. Simulation outcomes show that at low control-channel rates (50 kbps), key-exchange latency reaches ~320 ms for lattice-based KEM, yet this reduces to ~155 ms at 1000 kbps, illustrating scalability with bandwidth. Future research may focus on reducing ciphertext size, optimizing NTT-based polynomial operations, and implementing hardware acceleration to further lower delay and energy consumption. In practical 6G systems, a trade-off exists between security strength and communication overhead. Lattice-based post-quantum schemes provide strong quantum resistance at the cost of larger keys and signaling overhead, mainly during key establishment.

References

[1] D. Goyal, A. Kumar, P. Mathur, F. Sheth, and A. K. Gupta, "Robust cybersecurity through discrete and large language models for effective phishing attack detection," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 5-A, pp. 1621–1638 (2025), doi: 10.47974/JDMSC-2162.

[2] D. Deutsch, "Quantum theory, the Church–Turing principle and the universal quantum computer," *Proc. R. Soc. Lond. A Math. Phys. Sci.*, vol. 400, pp. 97–117 (1985).

[3] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Post-Quantum Cryptography,* Berlin, Germany: Springer, pp. 147–191 (2009).

[4] P. Kumar, K. Banerjee, N. Singhal, A. Kumar, S. Rani, R. Kumar, and C. A. Lavinia, "Verifiable, secure mobile agent migration in healthcare systems using a polynomial-based threshold secret sharing scheme with a Blowfish algorithm," *Sensors,* vol. 22, no. 21, Art. no. 8620 (2022), doi: 10.3390/s22218620.

[5] B. Rajabi and Z. Eslami, "A verifiable threshold secret sharing scheme based on lattices," *Inf. Sci.,* vol. 501, pp. 655–661 (2019).

[6] M. K. Sharma and A. Kumar, "NOMA waveform technique using orthogonal supplementary signal for advanced 5G networks security," *J. Discrete Math. Sci. Cryptogr.,* vol. 25, no. 4, pp. 1125–1136 (2022).

[7] A. Noonia, D. Thakral, P. Mathur, F. Sheth, H. Shaikh, and A. K. Gupta, "A discrete mathematical model and cryptography for secure medical image analysis: Encrypted chest X-ray classification," *J. Discrete Math. Sci. Cryptogr.,* vol. 28, no. 5-A, pp. 1473–1486 (2025), doi: 10.47974/JDMSC-2146.

[8] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Advances in Cryptology – EUROCRYPT 2010*, Lecture Notes in Computer Science, vol. 6110, Berlin, Germany: Springer (2010), doi: 10.1007/978-3-642-13190-5_1.

[9] N. Shirisha, H. M. Manoj, S. J. Hussain, R. Kotoju, R. Kolikipogu, and A. Mohan, "Post-quantum security framework for resource-constrained systems: Emerging trends, challenges, sustainability, and future directions," *Discover Computing,* vol. 29, no. 1, Art. no. 85 (2026), doi: 10.1007/s10791-026-09982-2.

[10] M. E. Bizri, A. M. El-Hajj, L. Sliman, and A. M. Haidar, "Institutional approaches to post-quantum cryptography: A comparative analysis of migration frameworks," *IEEE Access,* vol. 14, pp. 3259–3283 (2026), doi: 10.1109/ACCESS.2025.3650465.

[11] W. Abdallah, "A physical layer security scheme for 6G wireless networks using post-quantum cryptography," *Comput. Commun.*, vol. 218, pp. 176–187 (2024), doi: 10.1016/j.comcom.2024.02.019.

Received December, 2025