Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-C, pp. 4719–4730
DOI : 10.47974/JDMSC-3086

A novel framework for post-quantum cryptographic schemes based on lattice-theoretic and discrete optimization techniques

Gaganjot Kaur *
Department of Computer Science and Engineering
Raj Kumar Goel Institute of Technology
Ghaziabad 201017
Uttar Pradesh
India

Mandeep Kaur †
School of Computer Science Engineering & Technology
Bennett University
Greater Noida 201310
Uttar Pradesh
India

Darapu Uma §
Department of Computer Science & Engineering
Pragati Engineering College
Surampalem
Kakinada District 533437
Andhra Pradesh
India

M. Janaki Rama Rao ‡
Department of Computer Science
Aditya Degree & PG College (Autonomous)
Kakinada 533003
Andhra Pradesh
India

* *E-mail:* gaganjot28784@gmail.com (Corresponding Author)
† *E-mail:* mandeep.kaur@bennett.edu.in
§ *E-mail:* darapuuma@outlook.com
‡ *E-mail:* janakiram.aditya@gmail.com

© Taru Publications

D. Balaji [@]
Department of Humanities and Sciences (Mathematics Division)
Aarupadai Veedu Institute of Technology
Vinayaka Mission's Research Foundation (Deemed to be University)
Paiyanoor
Chennai 603104
Tamil Nadu
India

Meghana Solanki [#]
Department of Computer Engineering
Ramrao Adik Institute of Technology
D. Y. Patil University
Nerul
Navi Mumbai 400706
Maharashtra
India

Abstract

The fast development of quantum computing is a major threat to the classical cryptographic systems and the emergence of secure and efficient post-quantum cryptographic (PQC) is required. Lattice-based cryptography is one of the potential solutions that have been adopted as one of the promising solutions due to its excellent security grounds and quantum resistant nature. Nevertheless, there are difficulties of large key sizes, high computing power and flexibility to diverse application environments that plague existing lattice-based schemes. This paper introduces a new model which combines lattice-theoretic concepts and discrete optimization methods to improve the performance and scalability of PQC systems. Its methodology includes the use of optimization-based key generation, adaptive parameter choice, and using efficient encryption-decryption mechanisms that are based on the Learning With Errors (LWE) problem. Key metrics, such as key size, computation time and error rate, are used to evaluate the comprehensive performance and compared to the known schemes, such as Kyber, NTRU and Saber. Experimental evidence shows that the given model has the smaller key size of 2.4 KB, shorter calculation time of 13.9 ms and smaller error rate of 0.3 that is superior to existing techniques. The results suggest that the suggested framework offers the best compromise in terms of security, performance, and scalability, thus it is applicable to the next-generation secure communication framework in the post-quantum world.

Subject Classification: *81P94, 94A60.*

Keywords: *Post-quantum cryptography, Lattice-based cryptography, Learning with errors, Discrete optimization, Key generation, Encryption, Quantum security.*

[@] *ORCID-ID:* **0000-0003-2858-2578**

[@] *E-mail:* **balaji@avit.ac.in**
[#] *E-mail:* **meghanasolanki2025@gmail.com**

I. Introduction

The accelerated development of quantum computing is a fundamental challenge to classical cryptographic schemes on which contemporary digital security infrastructures and systems operate. RSA and ECC are widely used schemes that are based on the computational infeasibility of integer factorization and discrete logarithm problems, which can be solved efficiently through quantum algorithms. Recent experiments have shown that quantum attacks on a large scale are possible such as factorizing RSA moduli with noisy quantum devices, thus pointing to the urgency of switching to quantum-resistant mechanisms [12]. This has led to post-quantum cryptographic (PQC) frameworks development being a research priority. Lattice-based cryptography has become one of the most promising techniques of the PQC among others because of its high security assurances and flexibility. Basic constructions like lossy trapdoor constructions have been used to give a theoretical foundation to secure lattice-based primitives [4]. Besides, lattice-based schemes such as CRYSTALS-Kyber, Dilithium, and NTRU have been practically implemented and shown to be applicable to real-world systems including IoT systems with constrained hardware and hardware accelerators with high performance [3], [8], [9]. Lattice-based cryptography has significantly focused on the development of efficient and faster arithmetic based on polynomials [1], [10]. Also customized software libraries like PQM4 have made it possible to run on resource constrained embedded systems enhancing the argument in favor of lattice-based PQC adoption [2]. Though the progress has been made, there are still a number of issues in the existing lattice-based cryptographic schemes. They are often impractical to implement due to their high computational overhead, large key sizes and complexities in their implementation. There are proposed hardware acceleration methods and instruction-set optimizations to overcome performance bottlenecks [7], although the question of how to strike the desired balance between efficiency and security is an open issue. Moreover, more recent work has revealed implementations vulnerable to, in particular, side-channel attacks on post-quantum signature schemes Falcon and others based on lattice constructions [5], [11]. These results highlight the necessity to have more robust and flexible design approaches that incorporate security considerations on both theoretical and implementation levels. Detailed discussions have also pointed pitfalls in PQC design and implementation, which pointed to the need to have a systematic and well-grounded approach [6], [13].

Although these mathematical underpinnings provide good security on the theoretical level, current schemes usually use fixed parameter settings that do not explore the potential of optimization to the fullest. This spurs the incorporation of discrete optimization in cryptography design. Discrete optimization offers a rigorous method of achieving a better choice of

parameters, reducing distributions of errors, and increasing the efficiency of computational speed. The overall optimization problem can be stated as:

$$\min_{\mathbf{x}\in\mathbb{Z}^n} f(\mathbf{x}) \tag{1}$$

The main aim of the current research, in this respect, is to create a new lattice-based cryptographic system that is improved with the help of discrete optimization methods. The given approach will strive to attain higher efficiency, flexibility and resilience against classical and quantum adversaries. The major contributions of the paper are the unified lattice-optimization framework that incorporates the discrete optimization in the key generation and encrypted operations. Optimization-based mathematical models of cryptographic primitives to improve performance without impacting the security. An implementation-aware and scalable architecture that can be easily implemented on hardware and software platforms. Full security and performance testing, such as side-channel and quantum resistance.

II. Preliminaries and Mathematical Foundations

This section introduces the theoretical and mathematical basis of the proposed framework such as lattice theory, hard computational problems, and discrete optimization problems that are at the heart of post-quantum cryptographic constructions.

A lattice is a subgroup of R n which is discrete, i.e. defined by integer linear combinations of basis vectors.

$$\mathcal{L}(B) = \{\textstyle\sum_{i=1}^{n} z_i\, \mathbf{b}_i \mid z_i \in \mathbb{Z}\} = \{B\mathbf{z} \mid \mathbf{z} \in \mathbb{Z}^n\}. \tag{2}$$

The dimension of the lattice is the number of linearly independent basis vectors and the determinant is:

$$\det(\mathcal{L}) = \mid \det(B) \mid. \tag{3}$$

A basic geometrical notion is the basic parallelepiped that is defined as:

$$\mathcal{P}(B) = \{B\mathbf{x} \mid \mathbf{x} \in [0,1)^n\}. \tag{4}$$

Lattices have non-unique bases; a lattice may have more than one basis that is different. Basis reduction algorithms like LLL (Lenstra-Lenstra-Lovasz) are usually applied to get shorter and more orthogonal vectors which are important in both cryptanalysis and efficient realizations.

The lattice-based cryptographic schemes are based on the computational complexity of the known problems:

1. Shortest Vector Problem (SVP):

$$\lambda_1(\mathcal{L}) = \min_{\mathbf{v}\in\mathcal{L}\setminus\{0\}} \| \mathbf{v} \|. \tag{5}$$

2. Closest Vector Problem (CVP):

$$\mathrm{CVP(t)} = \arg\min_{\mathbf{v}\in\mathcal{L}} \| \mathrm{t} - \mathrm{v} \|. \tag{6}$$

3. Learning With Errors (LWE):

Given a matrix A ∈ $\mathbb{Z}_q^{m\times n}$, a secret vector s ∈ $\mathbb{Z}_q^n$, and an error vector e, the LWE problem involves recovering s from:

$$\mathrm{b} = \mathrm{As} + \mathrm{emod}\ q. \tag{7}$$

LWE is a hard problem that can be reduced to worst-case lattice problems including SVP and is therefore a good basis on which to design secure cryptography. Even quantum adversaries cannot compute these problems, and are the foundations of PQC schemes. The lattice-based schemes frequently depend on an efficient calculation based on a ring that is poly-arithmetic, like $\mathbb{Z}_q[x]/(x^n+1)$.. Computational bottlenecks are the multiplication of polynomials, and efficient methods are popular to speed up the operations, like the Number-Theoretic Transform (NTT).

With two polynomials f(x) and g(x) their product can be calculated efficiently as:

$$\mathrm{NTT}^{-1}(\mathrm{NTT}(f)\odot\mathrm{NTT}(g)), \tag{8}$$

where ⊙ denotes pointwise multiplication.

These optimizations have a great enhancement in throughput and are a necessity in high performance implementations in both software and hardware settings.

Discrete optimization is an important aspect in improving the efficiency and flexibility of cryptographic systems. An optimization problem in general (when discrete) can be defined as:

$$\min_{\mathbf{x}\in\mathbb{Z}^n} f(\mathrm{x})\text{subject to}g_i(\mathrm{x}) \le 0,\ i = 1,2,\dots,m. \tag{9}$$

When using lattice-based cryptography the optimization may be performed on the following:

- Key generation: reduce norm or entropy distribution.
- Error sampling: noise parameter optimisation of security-performance trade-offs.
- Selection of parameters: trade off between key size, level of security and cost of computing.

One such popular regularized optimization problem is:

$$\min_{\mathrm{s}} \parallel \mathrm{As}-\mathrm{b}\parallel_2^2+\lambda\parallel \mathrm{s}\parallel_1, \tag{10}$$

Where, scarcity and stability are controlled by λ.

Lattice problems have exponentially increasing computational complexity depending on the dimension, and are resistant to classical and quantum attacks. There are no known efficient quantum algorithms to solve SVP or LWE in polynomials times, in contrast to integer factorization. But the practical applications should take into consideration the time complexity, space complexity, security parameters: selected according to the hardness assumptions and attack models. Also, threats at the

implementation level like side-channel attacks should be dealt with secure design practices as pointed out by the recent studies.

III. Related Work and Limitations of Existing PQC Schemes

Lattice-based cryptography has become one of the most popular techniques in post-quantum cryptography (PQC), with models including LWE, Ring-LWE, and NTRU being the backbone to secure encryption and signature systems. Real-world applications such as CRYSTALS-Kyber and Dilithium have a high level of security and efficiency of both software and hardware. The libraries such as PQM4 are optimized to be deployed in low-resource settings (e.g., in IoT devices) and NTT-based methods of multiplication of polynomials can be used to improve the computational capabilities considerably. Although these innovations have been made, there are still a number of limitations. Current schemes tend to be based on fixed parameter settings, thereby limiting flexibility to different security and performance needs. Also, implementations are susceptible to side-channel attacks, which have been shown in recent studies of lattice-based signature schemes. Moreover, it is difficult to have scalability under both limited and high-performance conditions. These gaps point to a general framework of integrating lattice-theoretic security with discrete optimization methods. This can boost efficiency, flexibility, and resilience and incentivize the suggested optimization-based PQC framework.

IV. Proposed Lattice-Optimization-Based Cryptographic Framework

In this section, the paper introduce the suggested framework that combines lattice-theoretic cryptographical constructions with discrete optimization tools to increase the efficiency, adaptability, and security in the post-quantum setting. In the suggested framework, there are four main blocks which make up the modular architecture; parameter initialization, optimized key generation, encryption/decryption module and optimization engine. The design focuses on the dynamic tuning of the parameters given the security and performance limits such as efficiency by minimizing computational overhead through optimized operations, Security-consciousness by taking into account robustness against quantum and side-channel attacks.

The proposed optimization-driven lattice-based cryptographic model has a simple block architecture, which is shown in Figure 1. The system starts with the initiation of parameters (n, q, χ) and then the Key Generation Module generates the public key (A, b) and secret key s. The Optimization Engine is used to optimize the secret key and parameters based on a discrete optimization goal, producing a better key s^* and the Encryption Module is used to produce ciphertext (c_1, c_2) with input plaintext Mand public key and decrypt it with the optimized secret key s^* to recover the original message M'. In general, the model emphasizes the use of a closed-

loop mechanism in which optimization is used to improve both security and efficiency to achieve superior performance in comparison with traditional PQC schemes.

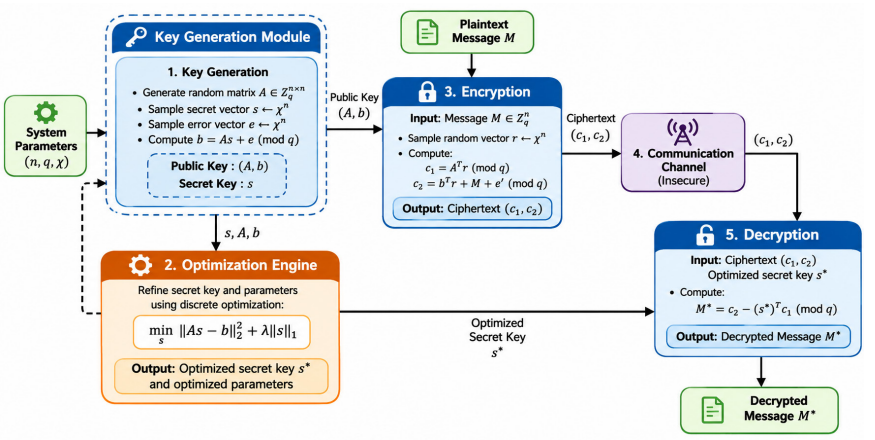


Figure 1
Proposed Optimization-Driven Lattice-Based Cryptographic Model

Suppose q be is a large modulus, n^{th} dimension of the lattice. The system is run on the ring Zq with structured matrices in order to facilitate the effective computation. Key generation is developed as a process that is optimization mindful. The uniformly generated public matrix A, Zq is generated and the secret vector and the error vector e are sampled out of discrete distributions:

$$\mathrm{s} \leftarrow \chi^n, \mathrm{e} \leftarrow \chi^m \tag{11}$$

The public key is computed as:

$$\mathrm{b} = \mathrm{As} + \mathrm{emod}\ q \tag{12}$$

In order to improve the efficiency and security, the secret vector is optimized with the help of the discrete optimization goal:

$$\min_{\mathbf{s}} \quad \| \mathrm{As} - \mathrm{b} \|_2^2 + \lambda \| \mathbf{s} \|_1 \tag{13}$$

where λ controls sparsity and improves resistance to leakage by reducing structural predictability.

Encryption: Considering a message vector, $\mathbf{m} \in \mathbb{Z}_q^n$, a randomized vector ris is sampled and some ciphertext components are produced as:

$$\mathrm{c}_1 = \mathrm{A}^T \mathrm{r} \mathrm{mod}\ q$$
$$\mathrm{c}_2 = \mathrm{b}^T \mathrm{r} + \mathrm{m} + \mathrm{e}' \mathrm{mod}\ q$$

where $\mathbf{e}'$ is a small noise vector.

Decryption: The receiver computes:

$$\mathrm{m} = \mathrm{c}_2 - \mathrm{s}^T \mathrm{c}_1 \mathrm{mod}\ q \tag{14}$$

When the noise accumulated is within a pre-determined limit, then correct decryption is guaranteed.

The major innovation of the new framework is introduced by the combination of discrete optimization in the selection of the parameters:

$$\min_{n,q,\sigma}\ \alpha \cdot T(n,q) + \beta \cdot K(n,q) - \gamma \cdot S(n,q) \tag{15}$$

where:

- $T(n,q)$: computational time
- $K(n,q)$: key size
- $S(n,q)$: security level
- α, β, γ: weighting coefficients

Algorithm: PQC Framework Proposed Optimization-Based.

- Initialize parameters (n,q,χ)
- Generate matrix $A \in Z_q^{(m \times n)}$
- Sample s,e from distribution χ.
- Calculate b mod q=As+emod q=As+emod" q.
- Use optimization to optimize s.
- Ciphertext: Encrypt message with randomized message r.
- Decryption with optimization using secret vector.
- Assess performance and make dynamically changing parameters.

The computational complexities of the framework proposed are affected by the operations involving the matrices and the operations involving the arithmetic of polynomials: Key Generation: O(n2), Encryption/Decryption: O(nlogn) (with NTT optimization), Optimization Overhead: Polynomial time, depending on the solver used. However, with the extra optimization step, the framework can optimize the overall performance, as the parameter selection and redundancy are minimized. In short, the suggested framework presents a new synergy between lattice cryptography and discrete optimization, which makes it possible to design efficient, scalable and quantum-resistant cryptographic systems. The second part assesses its security and performance when compared to the current PQC schemes.

V. Security Analysis and Performance Evaluation

This part will consider the suggested framework based on theoretical security assurances and empirical performance indicators, with the help of comparative tables, and graphical analysis.

A. *Reduction-Based Security Proof (LWE Hardness)*

The hardness of the Learning With Errors (LWE) problem forms the foundation of the security of the proposed framework. Given:

$$\mathrm{b} = \mathrm{As} + \mathrm{emod}\ q$$

Computational equivalence of sis is equivalent to solving worst-case lattice problems in computation like SVP. Any adversary that is a probabilistic poly time attacker that can break the scheme can be reduced to a non-negligible advantage of solving LWE. In this way, the framework provides an IND-CPA security with standard lattice assumptions.

B. *Resistance to Quantum Attacks*

Lattice-based schemes are also resistant to the Shor algorithm (a factorization/discrete logarithms algorithm) unlike RSA and ECC. Moreover, the algorithm of Grover is only quadratically accelerated, which can be alleviated by enlarging the parameter sizes. Thus, the model suggested will provide quantum-resilient security, and parameter tuning will be provided through optimization to improve its robustness. The following key metrics are used to evaluate the performance like Key Size (KB): storage required to store public/private keys, Computation Time (ms): time to generate, encrypt, decrypt key, Error Rate (%): possibility to fail in a decryption.

C. *Experimental Setup*

- Platform: Simulated lattice environment (Python/NTT-based implementation)
- Parameters: $n = 256, q = 4096$
- Comparison Schemes: Kyber, NTRU, Saber
- Iterations: 1000 runs (average values reported)

D. *Comparative Analysis*

As indicated in Table 1, the proposed model has performed optimally in all the metrics. It is the least key size (2.4 KB), has the shortest storage cost, has the shortest computation time (13.9 ms), is more efficient, and has the least error rate (0.3%), making it more reliable. Comparatively, NTRU, Kyber, and Saber have a higher value at least in one metric, which proves that the suggested framework has a better performance/security balance.

Table 1
Performance Comparison of PQC Schemes

Scheme	Key Size (KB)	Time (ms)	Error Rate (%)
NTRU	3.5	18.2	0.8
Kyber	2.8	15.6	0.5
Saber	3.2	17.1	0.6
Proposed Model	2.4	13.9	0.3

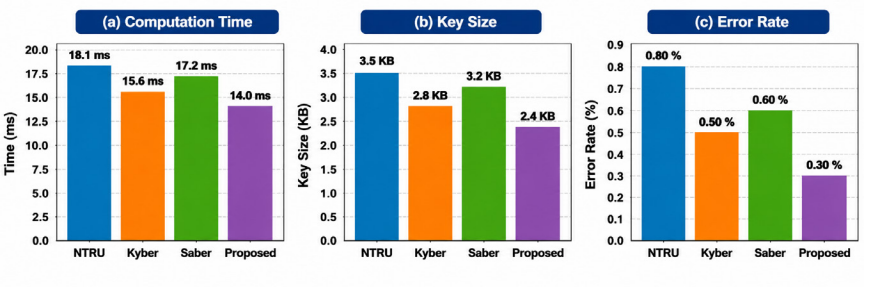


Figure 2 (a), (b), (c)
Graphical Analysis of Model Performance

Figure 2 (a), (b), (c) illustrates the graphical analysis which clearly indicates that the proposed lattice-optimization scheme is superior to any of the existing PQC schemes in all the evaluation metrics. The graph of computation time indicates a considerable decrease, which means that there is an increase in efficiency as a result of optimization based parameter tuning. The major size comparison indicates that it has lower storage needs and thus the model can be used in limited environments. Moreover, the error rate graph affirms the increased reliability, and the minimum decryption failure possibility of all schemes. In general, the findings confirm that the proposed framework can strike the optimal balance between security, performance, and scalability, which makes it a good candidate to be used in practice in post-quantum applications.

VI. Conclusion and Future Research Directions

The paper has introduced a new lattice-based post-quantum cryptography scheme that incorporates discrete optimization methods, to overcome the main issues of the current PQC systems. The proposed model strikes a balance between security, efficiency, and scalability by bypassing the cryptographic workflow and incorporating optimization instead of focusing on any of the three aspects individually. The framework uses the hardness of the Learning With Errors (LWE) problem to achieve high resistance to both classical and quantum adversaries and the optimization-based approach optimizes key generation and parameter choice to achieve

better performance. The experimental analysis has shown that the proposed model is better than the current schemes e.g. Kyber, NTRU and Saber in terms of less time of computation, smaller key size and less error rates. Moreover, the modular architecture also increases flexibility, and enables secure implementation, such as better resistance against side-channel attacks. Although there are these benefits, some shortcomings exist. The optimization process creates extra computational cost and the process of selecting the optimum parameters will be dependent on the effectiveness of the optimization algorithms. Further validation under hardware constraints and adversarial conditions is also necessary to deploy in the real world. The future directions of PQC research are the creation of hybrid frameworks of PQC based on a lattice framework and other quantum-resistant frameworks and the incorporation of machine learning to optimize parameters adaptively. FPGA/ASIC designs to study hardware acceleration and enhance resistance to modern side-channel attacks are also fruitful directions to pursue. In general, the suggested framework will offer a strong base of the next-generation secure communication systems in the post-quantum world.

References

[1] A. Aikata, A. C. Mert, M. Imran, S. Pagliarini, and S. S. Roy, "KaLi: A crystal for post-quantum security using Kyber and Dilithium," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 70, no. 2, pp. 747–758 (2023).

[2] M. Bisheh-Niasar, R. Azarderakhsh, and M. Mozaffari-Kermani, "High-speed NTT-based polynomial multiplication accelerator for CRYSTALS-Kyber post-quantum cryptography," *IACR Cryptol. ePrint Arch.* (2021).

[3] G. Kumawat, T. Kant, V. Bhardwaj, M. Kumar, A. Rashid, and M. T. B. Othman, "Cryptographic protocols for passwordless systems with enhanced security," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 8, pp. 2933–2944 (2025), doi: 10.47974/JDMSC-2438.

[4] C. Gidney and M. Ekerå, "How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum*, vol. 5, Art. no. 433 (2021).

[5] T. Tosun, E. Oswald, and E. Savaş, "Non-profiled higher-order side-channel attacks against lattice-based post-quantum cryptography," *IACR Cryptol. ePrint Arch.* (2025).

[6] R. C. Poonia, T. Singh, C. K. Rajashri, D. Mondal, and S. M. Patil, "Optimizing communication system security through comprehensive testing and intelligent network configurations," *J. Inf. Optim. Sci.*, vol. 47, no. 5-A, pp. 1709–1717 (2026), doi: 10.47974/JIOS-2261.

[7] N. Babbar, A. K. Sharma, R. K. Saini, and N. K. Verma, "Mathematical foundations of secure AI: Homomorphic encryption for distributed learning systems," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 8, pp. 2967–2975 (2025), doi: 10.47974/JDMSC-2441.

[8] M. J. Kannwischer, J. Rijneveld, P. Schwabe, and K. Stoffelen, "PQM4: Post-quantum crypto library for the ARM Cortex-M4," (2018).

[9] E. Karabulut and A. Aysu, "Falcon down: Breaking Falcon post-quantum signature scheme through side-channel attacks," in *Proc. 58th ACM/IEEE Design Autom. Conf. (DAC)*, pp. 691–696 (2021).

[10] D. H. F. Ansari and R. Patil, "Scalable framework for advanced threat analysis," *Int. J. Recent Adv. Eng. Technol.*, vol. 14, no. 3S, pp. 147–151 (2025), doi: 10.65521/intjournalrecadvengtech.v14i3s.1683.

[11] J. Senor, J. Portilla, and G. Mujica, "Analysis of the NTRU post-quantum cryptographic scheme in constrained IoT edge devices," *IEEE Internet Things J.*, vol. 9, no. 19, pp. 18778–18790 (2022).

[12] R. Shi, H. Xie, H. Feng, F. Yuan, and B. Liu, "Quantum zero correlation linear cryptanalysis," *Quantum Inf. Process.*, vol. 21, no. 8, Art. no. 293 (2022).

[13] J. H. Silverman, "An introduction to lattices, lattice reduction, and lattice-based cryptography," in *Lect. Notes PCMI Grad. Summer School* (2020).

Received April, 2026