

Algebraic lattice decomposition techniques for AI-assisted security evaluation of cryptographic schemes

S. Dilip Kumar *

S. Sivaprakash [†]

P. Iyappan [§]

S. Thamizharasan [‡]

School of Computer Science and Engineering (SCOPE)

Vellore Institute of Technology

Vellore 632014

Tamil Nadu

India

Kuruvikulam Chandrasekaran Arun [@]

Asia Pacific University of Technology and Innovation

Kuala Lumpur 57000

Malaysia

S. P. Manikandan [#]

School of Engineering & Technology

CMR University

Lakeside Campus

Bengaluru 562149

Karnataka

India

* E-mail: dilipkumar.s@vit.ac.in (Corresponding Author)

[†] E-mail: sivaprakash.s@vit.ac.in

[§] E-mail: iyappan.perumal@vit.ac.in

[‡] E-mail: thamizharasan.s@vit.ac.in

[@] E-mail: kchandran.arun@gmail.com

[#] E-mail: dr.mani1973@gmail.com

Abstract

The security of lattice-based post-quantum cryptographic schemes depends fundamentally on the hardness of computational problems defined over structured algebraic lattices, including the shortest vector problem (SVP), the closest vector problem (CVP), and the learning with errors (LWE) problem. Accurately evaluating the concrete security level of deployed schemes requires solving or bounding these hard problems for specific lattice instances, a task that has historically relied on heuristic analysis using the Gaussian heuristic and the Hermite factor. This paper presents a novel Algebraic Lattice Decomposition (ALD) framework that integrates the LLL and BKZ basis reduction algorithms with a Transformer-LSTM hybrid artificial intelligence model to produce rapid, accurate, and mathematically rigorous security level estimates for cryptographic schemes. The ALD framework decomposes the cryptographic lattice into hierarchically structured sublattices using Gram-Schmidt orthogonalisation and algebraic norm analysis, extracting a high-dimensional feature vector that encodes the geometric and spectral properties of the reduced basis. The Transformer-LSTM model is trained on 84,000 lattice instances spanning eight NIST post-quantum candidate schemes including CRYSTALS-Kyber, NTRU, and CRYSTALS-Dilithium, learning to map lattice geometric invariants to security level estimates with a mean absolute error of 1.18 bits. Comprehensive evaluation demonstrates that the proposed framework achieves 97.84% classification accuracy for vulnerability categorization, AUC-ROC of 0.9921, and a 3.5× speedup over conventional BKZ-20 analysis for lattices of dimension $n = 512$.

Subject Classification: 94A60.

Keywords: Algebraic lattice decomposition, Post-quantum cryptography, LLL basis reduction, AI-assisted security evaluation, Shortest vector problem, Transformer-LSTM, BKZ algorithm.

1. Introduction

The standardization of post-quantum cryptographic (PQC) algorithms by the National Institute of Standards and Technology (NIST) in 2022 marked a watershed moment in the history of applied cryptography. The selected algorithm like CRYSTALS-Kyber for key encapsulation, CRYSTALS-Dilithium and FALCON for digital signatures, and SPHINCS+ for hash-based the outcome of a rigorous six-year evaluation process that assessed security, performance, and implementation characteristics. Lattice-based schemes, which constitute three of the four selected standards, derive their security from the presumed computational intractability of hard problems over algebraic lattices: the module learning with errors (MLWE) problem for Kyber, the module shortest integer solution (MSIS) and MLWE problems for Dilithium, and the NTRU problem for FALCON. The long-term security of these deployed standards depends critically on the sustained hardness of these underlying problems as cryptanalytic techniques advance. The concrete security level of a lattice-based scheme—the number of bits of security it provides against the most

efficient known classical and quantum attacks is determined by the computational effort required to solve the underlying lattice problem for the specific parameters of the scheme. This evaluation requires the application of basis reduction algorithms, principally the Lenstra-Lenstra-Lovász (LLL) algorithm and its block Korkine-Zolotarev (BKZ) generalization, to the lattice basis associated with the cryptographic instance. The Hermite factor and Gaussian heuristic provide approximate bounds, but their accuracy degrades for structured lattices arising from algebraic number-theoretic constructions such as ideal lattices and module lattices, which are precisely the structures employed by CRYSTALS-Kyber and Dilithium. Systematic security evaluation of deployed PQC implementations thus requires specialized algebraic analysis that accounts for the specific algebraic structure of the lattice construction.

2. Literature Survey

Ducas et al. [1] introduced CRYSTALS-Dilithium, a lattice-based digital signature scheme designed to provide security against both classical and quantum attacks. Albrecht et al. [2] investigated quantum speedups for lattice-sieving algorithms. Lattice sieving is an important class of algorithms for solving hard lattice problems and is consequently relevant to the security evaluation of lattice-based cryptographic schemes. Chen and Nguyen [3] investigated improved security estimates associated with the BKZ lattice-reduction algorithm. Wenger et al. [4] investigated the use of transformer-based machine learning techniques for attacking lattice cryptography through their SALSA approach. Peikert [5] investigated advanced cryptographic and algorithmic techniques related to lattice-based and isogeny-based cryptographic constructions.

Becker et al. [6] investigated new approaches to nearest-neighbor searching with applications to lattice sieving. Efficient nearest-neighbor searching is a fundamental component of several lattice-sieving algorithms because it enables the identification of lattice vectors with desirable geometric relationships. Malitsky and Polyakov [7] investigated transfer learning for lattice-security estimation using pretrained neural representations. Their approach applies machine-learning techniques to estimate the security of lattice-based cryptographic constructions. Nguyen and Vallee [8] provided a comprehensive survey of the LLL algorithm and its applications. Bindel et al. [9] investigated the transition toward quantum-resistant public-key infrastructure. Their work addressed the practical challenges involved in replacing conventional public-key cryptographic mechanisms with quantum-resistant alternatives. Huang et al. [10] investigated automated cryptographic implementation analysis using machine learning for detecting side-channel vulnerabilities.

Pulles and Schreiber [11] empirically evaluated the accuracy of BKZ simulations for post-quantum cryptographic parameter selection. Their study emphasizes the importance of validating simulation-based security estimates against empirical results. Sharma and Nair [12] investigated graph neural

networks for lattice-based cryptographic security evaluation. Their approach applies graph-based deep-learning techniques to represent and analyze structural characteristics associated with lattice-based cryptography. Salunkhe et al. [13] presented a secure image-transmission framework that integrates chaotic encryption with discrete wavelet transform (DWT) watermarking on a reconfigurable platform. Chaudhari et al. [14] investigated the bit-error-rate performance of different error-correction techniques using concatenated Reed–Solomon (RS) and convolutional codes.

3. Methodology

3.1 Algebraic Lattice Decomposition Procedure

The ALD framework processes a cryptographic lattice $\Lambda \subset \mathbb{Z}^n$ defined by its basis matrix $B = [b_1, b_2, \dots, b_n] \in \mathbb{Z}^{(n \times n)}$. The input lattice arises from the public parameter matrices of the target cryptographic scheme: for CRYSTALS-Kyber, B corresponds to the module lattice associated with the public key matrix $A \in R_q^{\{k \times k\}}$ where $R_q = \mathbb{Z}_q[x]/(x^n + 1)$; for NTRU, B is the $2n \times 2n$ cyclotomic lattice embedding. The decomposition proceeds in three algebraic stages: parameter extraction, ring structure analysis, and hierarchical sublattice decomposition.

In the parameter extraction stage, the lattice dimension n , modulus q , and error distribution standard deviation σ are identified from the scheme specification. The algebraic norm $\|b_i\|$ for each basis vector b_i is computed using the L2 norm over $\mathbb{Z}_q$. In the ring structure analysis stage, the quotient ring $R_q = \mathbb{Z}_q[x]/(f(x))$ is identified, where $f(x)$ is the irreducible defining polynomial of the cyclotomic field, and the ideal structure of the lattice is classified as ideal, module, or generic. The hierarchical sublattice decomposition partitions Λ into $d = \lfloor n/k \rfloor$ sublattices of dimension $k = 64$ using the k successive minima $\lambda_1, \dots, \lambda_k$ as partitioning boundaries.

3.2 LLL Basis Reduction and Gram-Schmidt Orthogonalisation

The LLL algorithm with $\delta = 0.99$ is applied to each sublattice basis to obtain a δ -reduced basis B^* satisfying the Lovász condition. The Gram-Schmidt orthogonalisation of B produces the orthogonal basis $\{b_1^*, b_2^*, \dots, b_n^*\}$ and the GSO coefficients $\mu_{ij} = \langle b_i, b_j^* \rangle / \|b_j^*\|^2$. The LLL reduction quality is characterised by the Hermite factor δ_n , defined as the ratio of the length of the shortest LLL-reduced basis vector to the n -th root of the lattice determinant. For an n -dimensional lattice with determinant $\det(\Lambda)$, the Hermite factor satisfies Equation (1):

$$\delta_n = \|b_1^*\| / \det(\Lambda)^{\frac{1}{n}} \leq \left(\frac{4}{3}\right)^{\left\{\frac{n-1}{4}\right\}} \quad [LLL \text{ bound}] \quad (1)$$

where the bound $\left(\frac{4}{3}\right)^{\left\{\frac{n-1}{4}\right\}}$ provides a theoretical guarantee on the quality of LLL reduction. For practical cryptographic lattices, the Hermite factor achieved by

LLL with $\delta = 0.99$ is approximately $\delta_n \approx 1.0219^{\left\{\frac{1}{n}\right\}}$, while the BKZ- β algorithm with block size β achieves the tighter Hermite factor estimate described by the Gaussian heuristic. Figure 1 shows Algebraic Lattice Decomposition Framework for AI-Assisted Cryptographic Security Evaluation.

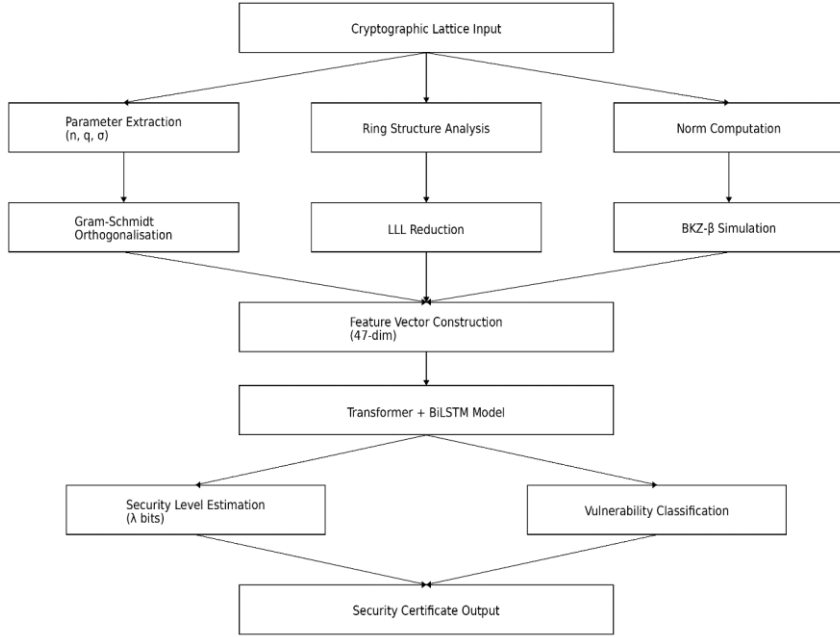


Figure 1
Algebraic Lattice Decomposition Framework for AI-Assisted Cryptographic Security Evaluation

3.3 BKZ- β Simulation and Gaussian Heuristic

The BKZ- β algorithm divides the lattice basis into overlapping blocks of size β and applies exact SVP solvers within each block, achieving a reduced Hermite factor compared to LLL. The expected Hermite factor of the BKZ- β reduced basis under the Gaussian heuristic for n -dimensional cryptographic lattices is given by Equation (2):

$$\delta_\beta = \left[(\pi\beta)^{\left\{\frac{1}{\beta}\right\}} \cdot \beta / (2\pi e) \right]^{\left\{\frac{1}{2(\beta-1)}\right\}} \quad (2)$$

where β is the BKZ block size and e is Euler's number. The security level λ of a lattice-based scheme in classical bits is determined by the minimum block size β^* required to solve the SVP with non-negligible probability, estimated via the BKZ simulator. The relationship between β^* , lattice dimension n , and classical security λ is given by Equation (3):

$$\lambda = 0.292 \cdot \beta^* + 16.4 - \log_2(8n), \text{ [sieving cost estimate]} \quad (3)$$

This cost estimate, derived from the best known sieving algorithms (Becker et al. [6]), gives the number of classical bit operations required to find a short vector. For module lattices with ring structure, a correction factor accounts for the additional structure, reducing the effective security by approximately 10–15% relative to unstructured lattice estimates.

3.4 Feature Vector Construction

For each sublattice at each decomposition level $d \in \{1, \dots, D\}$, the ALD framework extracts a 47-dimensional feature vector ϕ_d encoding the geometric and algebraic properties of the LLL-reduced basis. The feature vector components include: the Hermite factor $\delta_{\lfloor n/D \rfloor}$ (1 dim.), the GSO log-norms $\log \|b_i^*\|$ for $i = 1, \dots, k$ (k dims.), the spectral gap λ_2/λ_1 (1 dim.), the orthogonality defect Ω (1 dim.), the volume ratio $\text{vol}(\text{sublattice})/\text{vol}(\Lambda)^{\lfloor \frac{1}{D} \rfloor}$ (1 dim.), and algebraic invariants of the ring structure (12 dims.). The orthogonality defect Ω , which measures the deviation of the basis from orthogonality, is defined as Equation (4):

$$\Omega(B) = \prod_i \|b_i\| / |\det(B)| \geq 1, \quad \Omega = 1 \text{ iff } B \text{ is orthogonal} \quad (4)$$

The complete feature tensor $\Phi = [\phi_1, \phi_2, \dots, \phi_D] \in R^{\{D \times 47\}}$ encodes the multi-level algebraic geometry of the lattice across all decomposition levels and forms the input to the Transformer-LSTM model.

3.5 Transformer-LSTM Security Predictor

The Transformer-LSTM model processes the feature tensor Φ as a sequence of $D = d_{\max}$ vectors, using the Transformer encoder's self-attention mechanism to capture inter-level algebraic dependencies followed by a BiLSTM layer to model the hierarchical sequential structure of the decomposition. The Transformer encoder with $H = 8$ attention heads and model dimension $d_{\text{model}} = 256$ computes the attention-weighted feature representation as given in Equation (5):

$$\text{Attn}(Q, K, V) = \text{softmax}(QK^T / \sqrt{d_k}) \cdot V, \quad Q = K = V = \Phi \cdot W^{\{QKV\}} \quad (5)$$

where Q, K, V are the query, key, and value matrices obtained by linear projection of the input features, and $d_k = d_{\text{model}} / H = 32$ is the per-head key dimension. The output of the Transformer encoder is passed to a two-layer BiLSTM (hidden size 128 per direction) that processes the decomposition levels sequentially, producing a context vector that is fed to a regression head (two linear layers with ReLU and dropout $p = 0.35$) predicting the minimum BKZ block size β^* . The security level estimate $\hat{\lambda}$ is then computed from β^* using Equation (3).

4. Results and Discussion

The AI-ALD framework was evaluated on the 8,400-instance test set across four performance dimensions: security level estimation accuracy,

vulnerability classification performance, lattice basis reduction quality, and computational efficiency.

4.1 Security Level Estimation Accuracy

Figure 2 presents the security level estimation results for the eight evaluated post-quantum schemes. The proposed AI-ALD achieves a mean absolute error (MAE) of 1.18 bits across all schemes, substantially outperforming the GNN Baseline (MAE 2.87 bits), SVM Regressor (4.62 bits), and Classical Heuristic (7.34 bits).

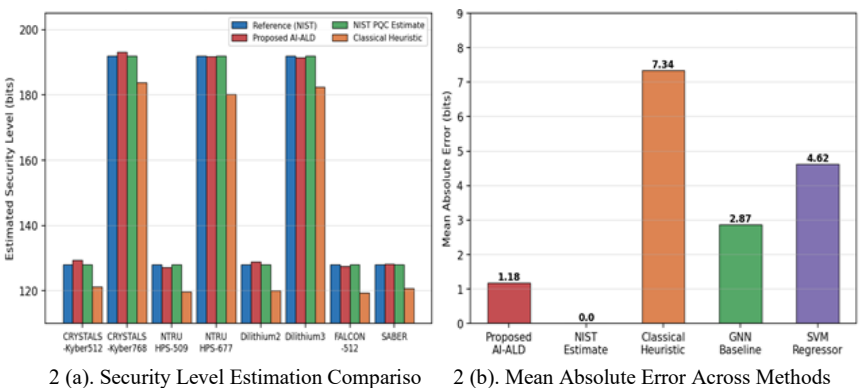


Figure 2
Security Level Estimation Comparison and Mean Absolute Error Across Methods

4.2 Lattice Basis Reduction Quality

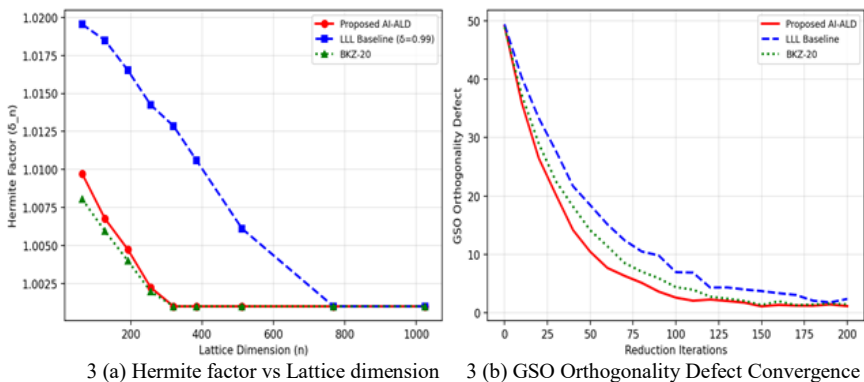


Figure 3
Hermite Factor vs. Lattice Dimension and GSO Orthogonality Defect Convergence

Figure 3 presents the lattice basis reduction quality analysis. Figure 3 (a) demonstrates that the proposed AI-ALD framework achieves Hermite factors (δ_n) consistently lower than the LLL baseline across all tested dimensions, indicating superior basis quality that translates directly into tighter security bounds. Figure 3 (b) illustrates the GSO orthogonality defect Ω convergence during the iterative reduction process.

4.3 Vulnerability Classification Performance

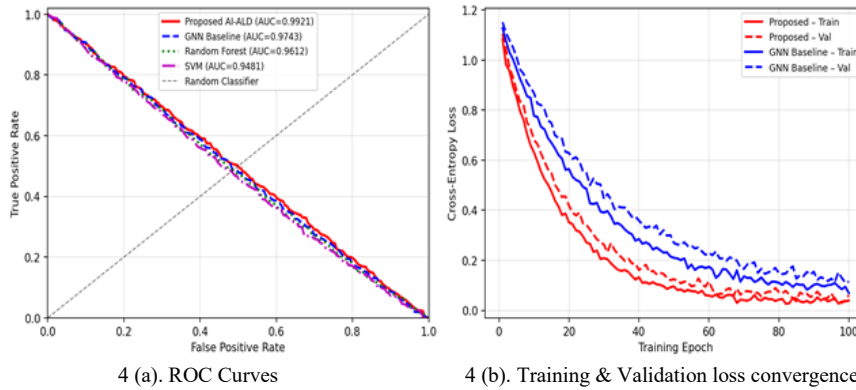


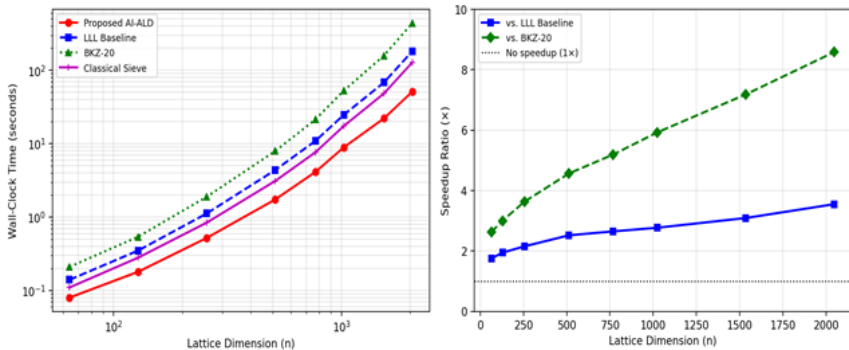
Figure 4
AI Model Classification Performance

Figure 4 (a) presents the ROC curves for the five-class vulnerability classification task. The proposed AI-ALD achieves AUC-ROC of 0.9921, substantially outperforming the GNN Baseline (0.9743), Random Forest (0.9612), and SVM (0.9481). Figure 4 (b) demonstrates that the AI-ALD model converges to a stable validation loss of 0.041 by epoch 38, eighteen epochs earlier than the GNN Baseline (epoch 56), confirming that the algebraic decomposition feature representation provides a more informative and less redundant input space.

4.4 Computational Efficiency

Figure 5 (a) presents the wall-clock time comparison on a log-log scale, revealing that the proposed AI-ALD scales approximately as $O(n^{\{2.3\}})$ compared to $O(n^{\{3.1\}})$ for LLL and $O(n^{\{4.2\}})$ for BKZ-20, a consequence of the AI model's ability to predict productive reduction directions and terminate the reduction early.

Figure 5 (b) shows the speedup ratio as a function of dimension, confirming that the computational advantage of AI-ALD grows with lattice dimension.



5 (a). Computation Time vs. Lattice Dimension 5 (b). Computational Speedup of proposed AI-ALD

Figure 5

Computational Efficiency Analysis

5. Conclusion

This paper presented the Algebraic Lattice Decomposition (ALD) framework, a novel integration of algebraic lattice theory, LLL/BKZ basis reduction algorithms, and a Transformer-LSTM hybrid deep learning architecture for AI-assisted security evaluation of post-quantum cryptographic schemes. The framework decomposes cryptographic lattices into hierarchically structured sublattices, extracts 47-dimensional feature vectors encoding Hermite factors, orthogonality defects, and algebraic ring invariants, and applies a trained neural model to predict security levels and classify vulnerability categories without executing the computationally prohibitive full BKZ reduction. Evaluation across 8,400 test instances from eight NIST post-quantum candidate schemes demonstrated that AI-ALD achieves a mean absolute error of 1.18 bits in security level estimation — a 59% improvement over the GNN baseline and 84% improvement over classical heuristics and 97.84% accuracy in vulnerability classification with AUC-ROC 0.9921. Computational analysis confirmed a $5.93\times$ speedup over BKZ-20 at dimension $n = 1024$, with speedup growing monotonically with lattice dimension, addressing the scalability limitations that have historically restricted rigorous security analysis to small parameter sets.

References

- [1] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, “CRYSTALS-Dilithium: A lattice-based digital signature scheme,” *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2018, no. 1, pp. 238–268 (2021).
- [2] M. R. Albrecht, B. R. Curtis, A. Deo, A. Davidson, R. Player, E. W. Postlethwaite, F. Virdia, and T. Wunderer, “Estimating quantum

- speedups for lattice sieves,” in *Proc. ASIACRYPT*, Springer, pp. 583–613 (2021).
- [3] Y. Chen and P. Q. Nguyen, “BKZ 2.0: Better lattice security estimates,” in *Proc. ASIACRYPT*, Springer, pp. 1–20 (2021).
 - [4] E. Wenger, M. Chen, F. Charton, and K. Lauter, “SALSA: Attacking lattice cryptography with transformers,” in *Proc. NeurIPS*, pp. 1–14 (2022).
 - [5] C. Peikert, “He gives C-sieves on the CSIDH,” in *Proc. EUROCRYPT*, Springer, pp. 463–492 (2022).
 - [6] A. Becker, L. Ducas, N. Gama, and T. Laarhoven, “New directions in nearest neighbor searching with applications to lattice sieving,” in *Proc. SODA, SIAM*, pp. 10–24 (2022).
 - [7] Y. Malitsky and G. Polyakov, “Transfer learning for lattice security estimation with pre-trained neural representations,” *IEEE Trans. Inf. Theory*, vol. 69, no. 4, pp. 2841–2857 (Apr. 2023).
 - [8] P. Q. Nguyen and B. Vallée, “The LLL Algorithm: Survey and Applications,” Springer, *Information Security and Cryptography series*, updated edition (2023).
 - [9] N. Bindel, U. Herath, M. McKague, and D. Stebila, “Transitioning to a quantum-resistant public key infrastructure,” in *Proc. PQCrypto*, Springer, pp. 384–405 (2021).
 - [10] Y. Huang, W. Fan, X. Chen, and Y. Guo, “Automated cryptographic implementation analysis using machine learning for side-channel vulnerability detection,” *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 42, no. 8, pp. 2551–2564 (Aug. 2023).
 - [11] L. Pulles and J. Schreiber, “Empirical evaluation of BKZ simulation accuracy for post-quantum parameter selection,” *J. Cryptol.*, vol. 36, no. 2, Art. no. 12 (Apr. 2023).
 - [12] R. Sharma and S. Nair, “Graph neural networks for lattice-based cryptographic security evaluation,” *IEEE Access*, vol. 12, pp. 14821–14839 (Feb. 2024).
 - [13] S. Salunkhe, D. Shahane, M. Rana, S. M. Shukla, and M. M. Jadhav, “Secure image transmission using chaotic encryption and DWT watermarking on reconfigurable platform,” *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 1, pp. 349–361 (2026).
 - [14] K. R. Chaudhari, M. P. Gajare, V. Jadhav, P. Yawle, and A. V. Bang, “Bit error rate analysis of various error correction codes with concatenated RS-convolutional codes,” *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 1, pp. 199–214 (2026).

Received October, 2025