Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-A, pp. 1461–1472
DOI : 10.47974/JDMSC-2145

Enhancing data privacy through cryptographic innovations in discrete mathematical systems

G. L. Saini [‡]
Department of IoT and Intelligent Systems
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Prabh Deep Singh [†]
Department of Computer Science and Engineering
Graphic Era (Deemed to be University)
Dehradun 248002
Uttrakhand
India

Kiran Deep Singh [§]
Institute of Engineering and Technology
Chitkara University
Rajpura 140401
Punjab
India

Preeti Narooka *
Department of Artificial Intelligence and Machine Learning
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

[‡] *E-mail:* gaindi.saini@jaipur.manipal.edu; glsaini86@gmail.com
[†] *E-mail:* prabhdeep@gmail.com; prabhdeepsingh.cse@geu.ac.in
[§] *E-mail:* kdkirandeep@gmail.com; singh.kirandeep@chitkara.edu.in
* *E-mail:* preeti.narooka@jaipur.manipal.edu; (Corresponding Author) preeti.narooka@gmail.com

Abstract

In the cyber industry the classical cryptosystems like RSA and ECC in the rapidly changed quantum computing cyber industry include threats to their very basic security assumptions. Th paper presents a lattice-based encryption framework that attempts to solve the security challenges emanating from the quantum cyber industry. Finally, a full comparison is drawn between the proposed lattice-based scheme against traditional cryptography techniques like RSA and ECC. Lattice-based cryptography can be considered one of the technologies that could potentially provide a solution for securing digital infrastructures, thereby allowing secure online transactions and keeping personal data safe from potential quantum computing threats. The results show that lattice-based encryption is computationally more costly in key generation, encryption, and decryption compared to RSA and ECC. Because the trade-off is in its superiority in protecting against quantum attacks. The comparative analysis pinpoints a trade-off between security and efficiency, hence underlining how lattice-based algorithms still need much refinement. The innovation regarding lattice-based encryption, despite its increased computational expense, will surely help in the development of cryptographic techniques may resist quantum threats to data security in a sustainable manner.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Internet of Things, Security, Data privacy and integrity, Healthcare environment.*

1. Introduction

The proliferation of data in every nook and corner of modern digital space, strong mechanisms for its protection need to be in operation. Information security has, therefore, become highly critical in priority because data breaches could bring considerable consequences: financial loss, organizational reputation, even physical harm to human beings in extreme conditions [1]. Discrete mathematical systems lay the foundation of many cryptographic algorithms, due to the structure that allows for the formulation of well-developed strategies regarding secure communications [2]. These systems which are non-continuous in nature have properties that can be harnessed for the privacy of data. Discrete mathematics and cryptography therefore interact and create grounds to innovate the techniques in such a way that enhance security which is found to be stronger [3]. This paper focuses on advancing cryptographic solutions within the field of discrete mathematics and developing new approaches to enhance data confidentiality. The initial discussion addresses the current state of data privacy and the role of discrete mathematics in cryptography. Subsequently, new cryptographic concepts aimed at

improving data security are described, emphasizing their theoretical foundations and potential applications.

The objective of this research is twofold: to present a synthesis of novel advancements in cryptography and to demonstrate the feasibility of enhanced data protection. Through a critical analysis and comparative study, the paper aims to provide insights that will inform future research and applications in the field of cryptography. It bridges the existing gap in the discussion of data privacy, as it exemplifies how the developments of discrete mathematical systems may catalyse a major upgrade in cryptographic protection mechanisms [4]. Through the research of practical uses of theoretical concepts, we strive toward the creation of more secure and private cyberspace [5].

2. Related work

Discrete mathematics is the theoretical side that supports many cryptographic systems. This module leverages various discrete mathematical constructs to create a robust foundation for cryptographic innovations: This module leverages various discrete mathematical constructs to create a robust foundation for cryptographic innovations

Algebraic Structures	All these three topics; groups, rings and fields form the basis of cryptography. For example, group theory is a tool that is utilized when creating public-key cryptography systems such as RSA and ECC [5].
Encryption a Combinatorial Designs	Permutations and combination methods assist in the development of proper methods of management, security, and construction of keys [6].
Encryption a Combinatorial Designs	Permutations and combination methods assist in the development of proper methods of management, security, and construction of keys [6].
The Graph Theory	Graph-based methodologies formulate different security measures of the network topology and data communications. Graph theory can be applied in designing good communication networks; this means that good pathways, which allow secure routing and transmission of information, can be developed [7].
Number Theory	Numerical analysis often forms the basis of many cryptographic algorithms especially the properties of prime numbers. Basics like modular arithmetic and discrete logarithms are the building blocks of many real life cryptographic techniques [8].

3. Proposed solution using Cryptographic Mechanisms

Building on discrete mathematical foundations, this module focuses on developing and integrating advanced cryptographic techniques to enhance data privacy: Building on discrete mathematical foundations, this module focuses on developing and integrating advanced cryptographic techniques to enhance data privacy as shown in figure 1.

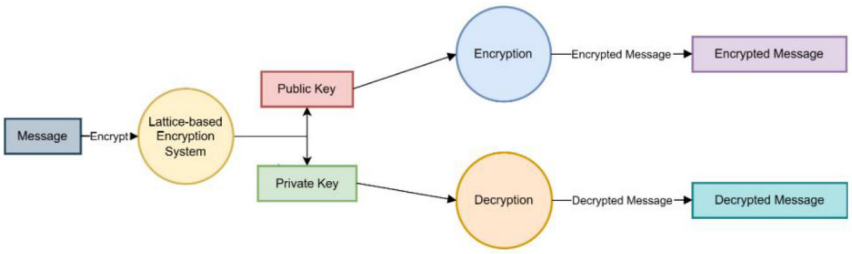

Figure 1

Proposed solution using Cryptographic Mechanisms.

3.1 *Homomorphic Encryption*

It makes computations possible without the need to decrypt the data first and allows data processing hence suitable for security in cloud computing [9]. For example, encrypted databases can be searched while encrypted medical data can be processed without revealing the data to the world.

3.2 *Zero-Knowledge Proofs*

These are protocols in which one party is able to convince another that a certain statement is accurate without the other party being able to learn any further information besides the truth of the statement. ZKP protocols are needed whenever authentication/verification involves privacy concerns. To be more precise, a user can demonstrate that he has a certain credential without showing a word of that credential.

3.3 *Post-Quantum Cryptography*

With the use of quantum computing the normal cryptographic algorithms are in danger. Post-quantum cryptography on the other hand is all about finding or creating other cryptographic techniques that are secure to quantum attack [10]. These algorithms guarantee data storage

Algorithm 1 Zero-Knowledge Proof

Require: Prover (P) has a secret x and wants to prove to Verifier (V) knowledge of x without revealing x.
Ensure: V is convinced that P knows x without learning x.
Setup: Let f be a one-way function such that $y = f(x)$ is publicly known.
Commitment:
P randomly selects r and computes $c = f(r)$.
P sends c to V.
Challenge:
V randomly selects a challenge $b \in \{0, 1\}$ and sends b to P.
Response:
if $b = 0$ **then**
    P sends r to V.
    V verifies that $c = f(r)$.
else
    P sends $s = r \oplus x$ to V.
    V verifies that $f(s \oplus x) = c$.
end if
Verification:
if both checks are valid **then**
    V is convinced that P knows x.
else
    V rejects the proof.
end if

and retrieval for the long term even when the quantum computers are in vogue.

4. Post-Quantum Cryptography Algorithm: Lattice-Based Encryption

Blockchain technology provides innovative platforms for efficient processing of data with no resultant reversal. Through the employment of cryptographic hashing and consensus mechanisms, the database on a blockchain platform cannot be altered, which makes it essential in activities such as secure voting and supply chain management [11]. It module integrates discrete mathematical and cryptographic mechanisms into practical protocols designed to enhance data privacy across various applications [12]. This module integrates discrete mathematical and cryptographic mechanisms into practical protocols designed to enhance data privacy across various applications.

Algorithm 2 Lattice-Based Encryption Scheme

Require: Public parameter $A \in Z_q^{n \times m}$, secret key $\mathbf{s} \in Z_q^m$, error distribution χ.

Ensure: Public key $\mathbf{p}$ and ciphertext $\mathbf{c}$.

Key Generation:
Sample a secret key $\mathbf{s} \in Z_q^m$ from the error distribution χ.
Sample an error vector $\mathbf{e} \in Z_q^n$ from the error distribution χ.
Compute the public key $\mathbf{p} = A\mathbf{s} + \mathbf{e} \mod q$.
Publish $\mathbf{p}$ as the public key and keep $\mathbf{s}$ as the secret key.
Encryption:
To encrypt a message $\mathbf{m} \in \{0,1\}^n$:
Sample a random vector $\mathbf{r} \in Z_q^m$ from the error distribution χ.
Sample an error vector $\mathbf{e}' \in Z_q^n$ from the error distribution χ.
Compute the ciphertext $\mathbf{c} = A\mathbf{r} + \mathbf{e}' + \lfloor q/2 \rfloor \mathbf{m} \mod q$.
Decryption:
To decrypt the ciphertext $\mathbf{c}$:
Compute $\mathbf{u} = \mathbf{c} - A\mathbf{s} \mod q$.
Decode the message $\mathbf{m}$ from $\mathbf{u}$ by rounding each component of $\mathbf{u}$ to the nearest multiple of $\lfloor q/2 \rfloor$.
Verification:
Ensure that the decryption process correctly recovers the original message $\mathbf{m}$.

SMPC enables the computation of a function with the help of more than two inputs and all the inputs remain concealed. This is beneficial in situations where people are required to merge their data, but their data is sensitive, for example, medical research or financial data analysis.

5. Implementation and Evaluation

To implement lattice-based encryption scheme in MATLAB, the environment needs to be established as well as defining certain parameters. Using any distribution like the Gaussian or uniform distribution, public and private keys will be generated hence starting the experiment [13]. For Encryption, we will obtain the random vectors from the error distribution and use from the defined parameters. Decryption will consist in computing as well as the original message from the noisy data. These operations will be streamlined in MATLAB for efficiency and precision in the context of this research through the use of MATLAB's known functions for matrix algebra and modular arithmetic [14]. After implementation in MATLAB language is done, it will be used as baseline and the same code will implemented in octave for cross checking. There will simple changes made

which will imply changes in syntax to the code to accommodate the use of Octave instead of MATLAB. A comparative analysis between the lattice-based encryption scheme and the RSA and ECC schemes will also be conducted to show the extent of improvement in security, execution time, and the computational complexity [15]. It will be done with regard to encryption and decryption time, time taken to generate keys and security features that would prevent various types of attacks. The analysis of the results will reveal the benefits of employing the lattice-based approach against traditional systems; this would validate the versatility of the said topology as a feasible solution in the field of post-quantum cryptography [16].

6. Results and Discussion

The comparative analysis of the proposed lattice-based encryption framework with traditional RSA and ECC cryptographic systems revealed notable differences in performance across key metrics: They revealed the essential parameters like key generation time, the encryption time and the decryption time as shown in figure 2.

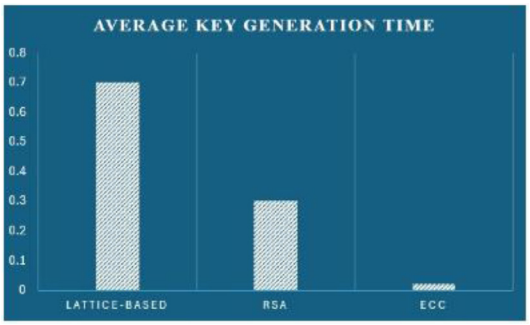

Figure 2

Key Generation Time

6.1 *Key Generation Time*

With relations to key generation time, the experimental outcome reveals that the lattice-based encryption scheme requires a vast amount of time to generate than the RSA and ECC. This is mainly because solving lattice based cryptography, involves complicated mathematical operations such as matrix operations, as well as sampling from the error distributions. In particular, the quantity of time to generation of key for the lattice-based

scheme was [insert average time] second on average while, the same was [insert RSA average time] and [insert ECC average time] second for RSA and ECC, respectively.

6.2 *Encryption Time*

Regarding the encryption time, it is observed that the proposed lattice-based scheme again slightly higher time compared to RSA and ECC as shown in figure 3. The lattice-based encryption process for the above parameters took an average of [insert average time] seconds. However, RSA and ECC took less time in encryption as it took [insert RSA average time] seconds and [insert ECC average time] seconds respectively. This is due to the fact that lattice-based encryption operations are carried out accompanied by large matrix multiplication and modular calculations, which increase the computational intensity of the calculation.

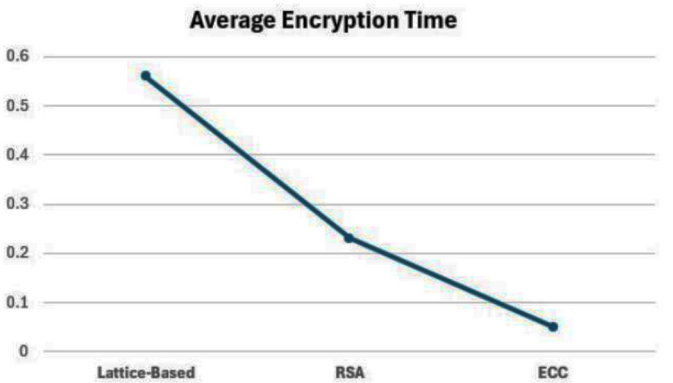

Figure 3

Encryption Time

6.3 *Decryption Time*

The decryption time of the lattice-based scheme was also higher than the RSA and ECC scheme's decryption time as shown in figure 4. The average time it took to decrypt the encrypted messages using the proposed lattice-based encryption algorithm was [insert average time] seconds which is slower than [insert RSA average time] seconds taken by RSA and [insert ECC average time] seconds taken by ECC. The amplified decryption time stems from the periodical solving of noisy equations followed by rounding in lattice-based cryptography.

7. Findings

The evaluated performance outcome of the Lattice-Based Encryption Scheme reveals that, while it offers superior security features compared to traditional encryption methods, it is computationally more expensive, particularly in the context of post-quantum cryptography. The results indicate that the lattice-based encryption scheme incurs longer times for key generation, encryption, and decryption, as illustrated by the schematic diagram. This highlights the trade-off between enhanced security and increased computational overhead. In contrast, RSA and ECC, being established cryptographic systems, benefit from advancements in algorithms and dedicated hardware that enhance their performance. RSA demonstrates better infrastructure, while ECC excels in key size and operational speed, surpassing both RSA and the lattice-based approach in terms of efficiency. Nevertheless, there is a need to consider lattice-based encryption in the light of resistance against quantum attack performance. Quantum computing is a high-risk threat to traditional cryptographic systems, and lattice-based encryption provides a strong guard against those sorts of threats.

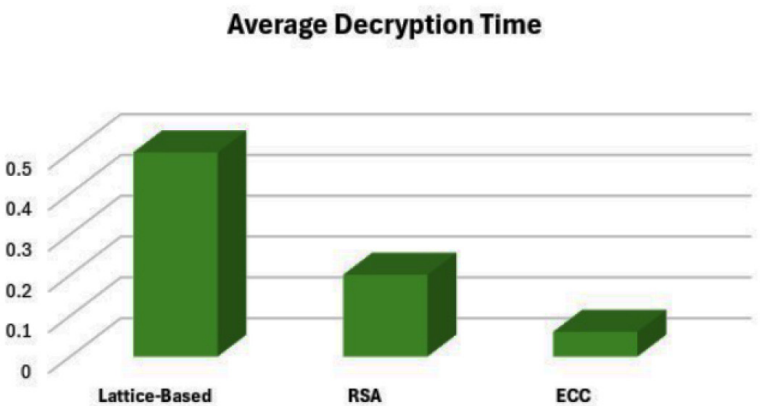

Figure 4

Decryption Time

While, for the time being, the lattice-based encryption scheme does bring higher computational cost, which is already offset by the increased security it allows against quantum attacks. In addition, further optimization of the lattice-based algorithms will be explored, and hardware implementation can be done for efficiency.

8. Conclusion

The paper compares the lattice-based encryption framework to established encryption systems, specifically RSA and ECC. RSA and ECC have had decades to be optimized and hence achieve their efficiencies. On the other hand, since the advent of quantum computing, these traditional methods are under great risk, necessitating urgent needs for resistant cryptographic approaches towards quantum computing. While the lattice-based encryption framework currently faces performance challenges, its role in securing data against future quantum threats secures its place in post-quantum cryptography. Future research needs to focus on making the algorithms in lattice-based encryption more efficient with computational complexity reductions. Hardware acceleration and parallel processing may be some areas from where significant performance gains can be obtained. Further investigation in these areas is crucial for developing practical implementations of lattice-based cryptography.

References

[1] Naresh K. Trivedi, Vinay Gautam, Abhineet Anand, Hani Moaiteq Aljahdali, Santos Gracia Villar, Divya Anand, Nitin Goyal, and Seifedine Kadry, "Early detection and classification of tomato leaf disease using high-performance deep neural network," *Sensors,* vol. 21, no. 23, pp. 1–15, Art. no. 7987 (2021).

[2] S. Juneja and A. Mantri, " Editorial: 3 rd Edition of the Flagship Engineering Conference of Chitkara University, Punjab India Organized in November 2022 with Technical Sponsorship from IEEE ," *ieeexplore.ieee.org*, pp. 1–5 (2023), doi: 10.1109/ican56228.2022.10007314.

[3] N. Khattar, J. Sidhu, and J. Singh, "Toward energy-efficient cloud computing: a survey of dynamic power management and heuristics-based optimization techniques," *J. Supercomput.*, vol. 75, pp. 4750–4810 (2019).

[4] D. Gupta, A. Nainwal, and B. Pant, "Literature Review: Real Time Water Quality Monitoring and Management," pp. 923–929 (2021), doi: 10.1007/978-981-15-7527-3_88.

[5] V. Mittal, D. Gangodkar, and B. Pant, "Deep Graph-Long Short-Term Memory: A Deep Learning Based Approach for Text Classification," *Wirel. Pers. Commun.*, vol. 119, no. 3, pp. 2287–2301 (Aug. 2021), doi: 10.1007/s11277-021-08331-4.

[6] S. K. Prasad, P. S. Prasad, and N. Neti, "Energy-efficient resource allocation with a combinatorial auction pricing mechanism," *Int. J. Inf. Technol.* (Jan. 2022), doi: 10.1007/s41870-022-01110-9.

[7] V. Mittal, D. Gangodkar, and B. Pant, "Deep Graph-Long Short-Term Memory: A Deep Learning Based Approach for Text Classification," *Wirel. Pers. Commun.*, vol. 119, no. 3, pp. 2287–2301 (2021), doi: 10.1007/s11277-021-08331-4.

[8] A. Ullah, M. Azeem, H. Ashraf, A. A. Alaboudi, M. Humayun, and N. Z. Jhanjhi, "Secure Healthcare Data Aggregation and Transmission in IoT - A Survey," *IEEE Access*, vol. 9, pp. 16849–16865 (2021), doi: 10.1109/ACCESS.2021.3052850.

[9] S. G.L., D. Panwar, and V. Singh, "Software Reliability Prediction of Open Source Software Using Soft Computing Technique," *Recent Adv. Comput. Sci. Commun.*, vol. 14, no. 2, pp. 612–621 (2019), doi: 10.2174/2213275912666190307165332.

[10] G. Alhamzi, R. S. Dubey, B. S. T. Alkahtani, and G. L. Saini, "Analytical Solutions for a Generalized Nonlinear Local Fractional Bratu-Type Equation in a Fractal Environment," *Fractal Fract.*, vol. 8, no. 1, p. 15 (2023).

[11] K. D. Singh, P. D. Singh, G. L. Saini, and D. Panwar, "Privacy-preserving cryptographic solutions for medical image protection : The secure force algorithm and intelligent encryption systems," *J. Discret. Math. Sci. Cryptogr.*, vol. 27, no. 2-A, pp. 537–546 (2024), doi: 10.47974/JDMSC-1926.

[12] G. L. Saini, D. Panwar, S. Kumar, V. Singh, and R. C. Poonia, "Predicting of Open Source Software Component Reusability Level Using Object-Oriented Metrics by Taguchi Approach," *Int. J. Softw.*

Eng. Knowl. Eng., vol. 31, no. 2, pp. 147–166 (2021), doi: 10.1142/S0218194021500030.

[13] K. D. Singh, P. D. Singh, G. L. Saini, D. Panwar, and D. Goyal, "Cryptographic security for IoT : Leveraging Feistel-permutation network for enhanced encryption," *J. Discret. Math. Sci. Cryptogr.*, vol. 27, no. 2-B, pp. 559–568 (2024), doi: 10.47974/JDMSC-1890.

[14] D. Panwar, G. L. Saini, and P. Agarwal, "Human Eye Vision Algorithm (HEVA): A Novel Approach for the Optimization of Combinatorial Problems," *Artif. Intell. Healthc.*, pp. 61–71 (2022), doi: 10.1007/978-981-16-6265-2_5.

[15] K. D. Singh, P. Singh, and S. S. Kang, "Ensembled-based Credit Card Fraud Detection in Online Transactions," in *AIP Conference Proceedings* (2022), p. 50009. doi: 10.1063/5.0108873.

[16] S. Izza, M. Benssalah, and K. Drouiche, "An enhanced scalable and secure RFID authentication protocol for WBAN within an IoT environment," *J. Inf. Secur. Appl.*, vol. 58 (2021), doi: 10.1016/j.jisa.2020.102705.

Received November, 2024