Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-B, pp. 4273–4288
DOI : 10.47974/JDMSC-3050

Matrix group representations in cryptographic transformations

Sachin Arun Thanekar [†]
Department of Information Technology
Sanjeevani College of Engineering
Kopargaon 423603
Maharashtra
India

Devata R. Anekar *
Department of Information Technology
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Ranjeetsingh Suryawanshi [§]
Department of Computer Engineering
Viswakarma Institute of Technology
Savitribai Phule Pune University
Pune 411037
Maharashtra
India

Anuradha Narendra Nawathe [‡]
Department of Information Technology
Amrut Vahini College of Engineering
Sangamner 422608
Maharashtra
India

[†] *E-mail:* sachin.sangamner@gmail.com
* *E-mail:* devata.anekar@vit.edu (Corresponding Author)
[§] *E-mail:* ranjeetsingh.suryawanshi@vit.edu
[‡] *E-mail:* anuradhanawathe@gmail.com

© Taru Publications

Yogesh Shepal [@]
Department of Computer Science & Engineering
ASM's Nextgen Technical Campus
Pune 410506
Maharashtra
India

Milind Gautam Ovhal [#]
Department of Mechanical Engineering
PCET's Nutan Maharashtra Institute of Engineering & Technology
Pune 410507
Maharashtra
India

Monali Gulhane [$]
Department of Computer Science and Engineering
Symbiosis Institute of Technology
Nagpur Campus
Symbiosis International (Deemed University), Pune
Nagpur 440008
Maharashtra
India

Abstract

The growing need of safe data transmission in the contemporary digital setting, such as cloud-based, Internet of Things (IoT), and distributed systems, has revealed the weaknesses of the traditional cryptography methods, especially in the form of new quantum threats. Traditional approaches founded on number-theoretic conjectures are now facing challenges, and more multifaceted and scalable mathematical theories need to be pursued. This work tackles this problem by suggesting a new cryptographic transformation model that is based on matrix group representations, which are defined on finite fields. The main aim of the work is to construct a mathematically sound and implementation-friendly encryption scheme that increases the security level by high-dimensional, non-commutative transformations. The methodology consists of a representation mapping of plaintext data in the form of vectors and a series of reversible matrix transformations, based on group elements. The system combines the process of key generation, encryption, and decryption in one algebraic framework and is executed in Python (NumPy, SciPy) and MATLAB to perform efficient operations on matrices. The reported experimental results indicate ciphertext entropy of 7.98 bits per byte and an avalanche effect of 52.6%, compared with 7.95 bits and 50.1%, respectively, for the AES baseline. These preliminary findings suggest favorable statistical randomness and diffusion characteristics, although

[@] *E-mail:* **yogeshshepal@gmail.com**
[#] *E-mail:* **milind.ovhal@nmiet.edu.in**
[$] *E-mail:* **monali.gulhane4@gmail.com**

reproducibility requires further documentation of the experimental protocol and independent validation of the reported measurements. Comparative analysis to AES indicates that the proposed scheme has a slightly higher computational overhead, but provides a better key space, structural complexity, and resistance to attacks. Scalability tests ensure that the system works effectively with a moderate size of matrices as well as various data sets, such as text and picture data. Overall, the proposed framework provides safe, scalable and versatile solution to next generation cryptography usage, particularly high security and post-quantum settings.

Subject Classification: *68P25, 14G50, 94A60.*

Keywords: *Matrix group representations, Cryptographic transformations, Finite fields, Non-commutative algebra, Encryption and decryption, Representation theory.*

I. Introduction

Secure communication and data protection is an urgent need that has emerged in the dynamic digital ecosystem in cloud computing, financial systems, Internet of Things (IoT) and distributed applications. These security systems are founded on cryptographic systems, which guarantee the confidentiality, integrity and authentication. Traditional cryptographic techniques have been largely founded on number-theoretic based cryptography such as discrete logarithms and elliptic curve cryptography that are used in secure protocols such as ECDSA [6]. However, with the advent of the discipline of quantum computing, and increasingly powerful computing becoming feasible, these classical approaches are now under attack, hence their desire to transition to post-quantum cryptographic systems [1], [10]. Additionally, the more recent advances in the efficiency of algorithms particularly in multiplying matrices and other algebraic tasks more clearly show the need to consider more complex mathematical designs to carry out secure transformations [2]. The use of matrices and algebra has attracted interest because it has the capability to express higher dimensional transformations and complex relationships in data. Computational systems have used a lot of linear algebraic model and statistical frameworks that are very effective in giving a solid mathematical foundation to transformation-based encryption schemes [3]. In addition, structured algebraic constructions like cyclic groups and substitution-box (S-box) constructions have proved to have better performance in cryptographic applications especially in image encryption and secure communication systems [11], [12]. These methods point out the possibility of integrating elements of algebraic constructions with computational methods to develop more secure and efficient encryption schemes.

Although this has been achieved, there is a major research gap of systematic use of matrix group representations of cryptographic transformations. Although group theory has been studied in settings like unknown-order groups, and more complex cryptographic primitives [5], and quantum-resistant constructions have been studied [8], [9], little has

been done to unify and make practical a coherent use of a theory of matrix group representations. Current literature tends to consider individual methods, including the use of numerical methods to compute and encrypt securely [7], or to find algebraic constructions [4], without formulating a unified framework to explore the potential of using matrices in encryption and decryption. The existing cryptography techniques have significant drawbacks as well. Most deployed systems are based on relatively simple algebraic structures or defined set of transformation which can be vulnerable to linear, differential or quantum-based attacks. Moreover, although secure computations and optimized arithmetic-based approaches enhance performance [7], they tend to add extra overheads to the computation or they are not scalable to the large-scale applications. Equally, S-box-based and chaos-based encryption techniques achieve high confusion and diffusion but might not use higher-dimensional algebraic transformations to the fullest to provide more security [11], [12]. These shortcomings have brought to the fore the need to have stronger, versatile and mathematically based cryptographic models.

To overcome these problems, this paper suggests a new cryptographic transformation scheme that is based on the matrix group representations. The main goals of this research are to create a mathematically sound encryption framework based on group representation theory, come up with efficient algorithms to generate and transform keys and assess the security and performance of the system [13], [15]. The model will be created to integrate the strict algebraic concepts with the real-world cryptographic requirements, in theory, and practice. The key contributions of this work can be briefly defined as follows: (i) the development of a model of the cryptographic transformation through the use of the matrix groups organized and structured to facilitate a transition between the abstract algebra and the applied cryptography; (ii) the development of the representation-based key generation and transformation models to enhance the complexity of the security; (iii) A general evaluation of the computational efficiency and resistance to modern cryptographic attacks, including post-quantum cryptographic approaches.

II. Preliminaries and Mathematical Foundations

The design of highly cryptographic systems increasingly relies on solid mathematical principles capable of assuring structural integrity along with computational security. They include linear algebra and abstract algebra, particularly, matrix theory and group representations, which are essential in offering the secure transformation mechanisms. The use of matrix groups to provide an efficient method of encoding and data transformation through the use of multidimensional transformation also makes it an excellent option in the cryptography applications where complexity, scalability and non-linearity are paramount. Used in real-life scenarios, such as image encryption, signal processing and error-correcting codes, matrix operations

are frequently used to alter data patterns to obscure data, but maintain computation speed.

The available procedures also have several limitations. The traditional systems are mostly founded on fixed or low-dimensional transformation matrices and therefore prone to linear and differential cryptanalysis. Additionally, trade-offs in computational efficiency and security are common, as systems with high security impose excessive computational loads to be used in real-time systems such as IoT and edge computing. Furthermore, the general unproductiveness of higher-dimensional representations and the dynamic group operations tends to reduce the randomness of transformations, further compromising defence against more advanced attacks. To address these problems, one will require a well-developed mathematical foundation, which extends the idea of using matrix groups over finite fields. A matrix group G- a subgroup of GL(n,Fq) is a subgroup of matrices that is invertible, is associative and has an identity, and is a closed set. The groups can be non-commutative and this goes a long way to add complexity to cryptography. This framework is extended by representation theory to a homomorphic mapping ρ:GGL(n,F_q), with a view to the abstract group operations being expressed by the transformations between matrices [14].

III. Proposed Cryptographic Transformation Model

The proposed model deals with the increasing necessity of a mathematically sound and scalable cryptographic model that can withstand some of the modern and post-quantum attacks. The weakness of current cryptographic systems known to be identified is that they are frequently based on fixed transformation algorithms, low-dimensional algebraic geometries or number theoretic conditions that could be exploited by the increased computational capabilities. Also, most of the existing techniques lack the ability to incorporate sophisticated algebraic techniques like matrix group representations, making them less flexible, with smaller key space, and vulnerable to linear and structural cryptanalysis. The proposed model aims to address these issues by providing a high-dimensional and dynamic encryption model where the representations of matrix groups are over finite fields.

The decryption process works by making the reverse transformations with the help of invertibility property of matrices in GL(n,Fq). A recovery of the original message is done using M=A1P1(C) and hence accuracy and consistency. The model is also dynamic in updating keys and scalable in the dimensions of the matrices which enables it to be capable of adapting to the different security needs and computing environments. In general, the given model offers a full-fledged and practice-ready cryptographic model integrating the theory of matrix groups and real-life encryption algorithms. It boosts security by increasing non-linear transformations of high-dimensional transformations without compromising computational

efficiency, which makes it appropriate in the current applications like secure communication, cloud computing and data protection systems.

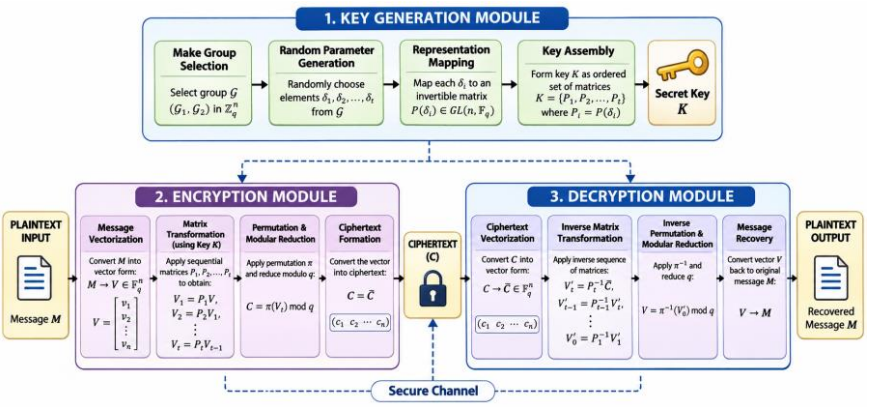


Figure 1

Proposed Model for Cryptographic Transformation System

The suggested Matrix Group Representation-Based Cryptographic Transformation Model is described in Figure 1; it is a standard encryption model, which relies on algebraic properties of matrix groups to offer a secure transmission of information. The system is designed to have three main modules: key generation, encryption and decryption with mathematical parameters underpinning it. In the key generation module a set of suitable matrix group (e.g. a general linear group over a finite field) is chosen, and random group elements are created. A combination of these elements is then encoded into invertible matrices via a representation function to create a series of matrices which jointly serve as the secret key. efficient matrix manipulations, and is thus applicable in the contemporary cryptographic systems.

IV. Mathematical Modeling and Algorithmic Formulation

The cryptographic framework suggested is based on the algebraic structures based on the matrix groups and their representations. This part makes the encryption decryption process formal, identifies the representation mapping functions, configures transformation rules and breaks down the computational complexity of the algorithms.

A. *Algebraic Formulation of the Encryption Process*

Let $\mathbb{F}_q$ denote a finite field of order q, and let

$$G \subseteq GL(n, \mathbb{F}_q) \tag{1}$$

be a matrix group consisting of invertible $n \times n$ matrices over $\mathbb{F}_q$.

Let the plaintext message be represented as a vector:

$$M \in \mathbb{F}_q^n \tag{2}$$

A sequence of group elements is selected:

$$g_1, g_2, \dots, g_k \subseteq G \tag{3}$$

Using a representation function ρ, each group element is mapped to a matrix:

$$A_i = \rho(g_i) \in GL\big(n, \mathbb{F}_q\big), i = 1,2, \dots, k$$

The encryption process is defined as a composition of linear transformations:

$$\begin{aligned} V_1 &= A_1 M \\ V_2 &= A_2 V_1 = A_2 A_1 M \\ &\vdots \\ V_k &= A_k A_{k-1} \cdots A_1 M \end{aligned}$$

Let the composite transformation matrix be:

$$A = \prod_{i=1}^{k} A_i = A_k A_{k-1} \cdots A_1 \tag{4}$$

Thus, the ciphertext is obtained as:

$$C = P(AM) \bmod q \tag{5}$$

where $P$is a permutation operator applied to enhance diffusion.

B. *Representation Mapping Functions*

The representation function is defined as a group homomorphism:

$$\rho: G \to GL\big(n, \mathbb{F}_q\big) \tag{6}$$

satisfying:

$$\rho(g_i g_j) = \rho(g_i)\rho(g_j), \forall g_i, g_j \in G \tag{7}$$

This is a property which guarantees group operations and matrix multiplication consistency.

To be implemented securely, the representation should meet:

- **Invertibility**:

$$\det\big(\rho(g)\big) \neq 0 \forall g \in G \tag{8}$$

- **Faithfulness** (injective mapping):

$$\rho(g_1) = \rho(g_2) \implies g_1 = g_2 \tag{9}$$

The representation can be defined as:

$$\rho(g; \theta) = A \tag{10}$$

and θrep is system parameters (e.g., seed values, field characteristics).

C. *Matrix Operations and Transformation Rules*

The following rules, rule out the transformation process:

1. **Matrix Multiplication Rule**:

$$V_i = A_i V_{i-1}, i = 1,2, \dots, k \tag{11}$$

2. **Permutation Operation**:

$$C = P(V_k) \tag{12}$$

where $P$is a bijective mapping:

$$P: \mathbb{F}_q^n \to \mathbb{F}_q^n \tag{13}$$

3. **Modular Reduction**:

$$C = V_k \bmod q \tag{14}$$

4. **Decryption Rule**:

Let the inverse matrices be:

$$A_i^{-1} = \rho(g_i)^{-1} \tag{15}$$

The original message is recovered by:

$$M = A_1^{-1} A_2^{-1} \cdots A_k^{-1} P^{-1}(C) \tag{16}$$

Equivalently:

$$M = A^{-1} P^{-1}(C) \tag{17}$$

where:

$$A^{-1} = (A_k A_{k-1} \cdots A_1)^{-1} \tag{18}$$

D. *Complexity Analysis of Algorithms*

The proposed model is computationally complex, but relies mostly on operations between matrices using finite fields.

1. **Matrix Multiplication Complexity**

For two $n \times n$matrices:

$$T_{mult}(n) = O(n^3) \tag{19}$$

Using optimized algorithms:

$$T_{mult}(n) = O(n^\omega), 2 < \omega < 3 \tag{20}$$

2. **Encryption Complexity**

Encryption involves $k$matrix multiplications:

$$T_{enc} = O(k \cdot n^\omega) \tag{21}$$

3. **Decryption Complexity**

Decryption includes:

- Matrix inversion: $O(n^3)$
- Sequential multiplications: $O(k \cdot n^\omega)$

Thus:

$$T_{dec} = O(n^3 + k \cdot n^\omega) \tag{22}$$

4. **Space Complexity**

Storage requirements include:

- $k$matrices of size $n \times n$:

$$S = O(kn^2) \tag{23}$$

5. **Security-Complexity Trade-off**
   - Increasing $n$enhances security (higher dimensional transformations)
   - Increasing $k$increases diffusion and key space
   - However, both increase computational overhead

The mathematical formulation provides a model of transformation that is a structured, invertible and secure transformation model, based on matrix group representations. The combination of homomorphic mappings, composite matrix operations and modular arithmetic are used to provide correctness and cryptographic strength and complexity analysis is used to verify that scalable implementations are possible.

V. System Architecture and Implementation Framework

The suggested system architecture is set as an extensible and scalable platform with the ability to incorporate the matrix groups representations into the real-life cryptographic functions. The structure is divided into five important layers such as data acquisition, preprocessing and encoding, key generation and management, transformation engine, and output/interface layer. Every layer has its own role to play and all the encryption and decryption is efficiently carried out with high security levels.

The generation and management layer is the key layer that has the responsibility of building secure cryptographic keys, through matrix group theory. A group G is a subgroup of GL(n,F q) defined, and pseudo-random group elements are created with the help of pseudo-random number generators. The elements are mapped to invertible matrices by a representation function rho which results in transformation matrices {A 1,A 2,A 3,…,A k }. Secure protocols are used to ensure key storage and exchange, and synchronization between the sender and receiver. The transformation engine constitutes the computation part of the system. This is encrypted through repeated multiplications of matrices, and modular operations of arithmetic, and results in ciphertext C=P(Ak A(k-1)...A1 M) mod q. Programming languages such as Python (NumPY, SciPY) and MATLAB have libraries of optimized linear algebra code, on which efficient algorithms to multiply and invert matrices are implemented. To reduce the size of the execution time, e.g. by using a GPU acceleration and parallel execution framework (such as CUDA or TensorFlow backend), may be necessary in case of large scale computations. Output/interface layer is concerned with the transfer, storage and visualization of the encrypted data. It ensures a safe communication between the endpoints and assists in giving decryption through inverse transformations. Performance metrics such as encryption

time, throughput and security strength are analysed through evaluation modules which are integrated into the system. The following Figure 2 shows the Proposed Matrix Transformation-Based Cryptographic System Architecture.

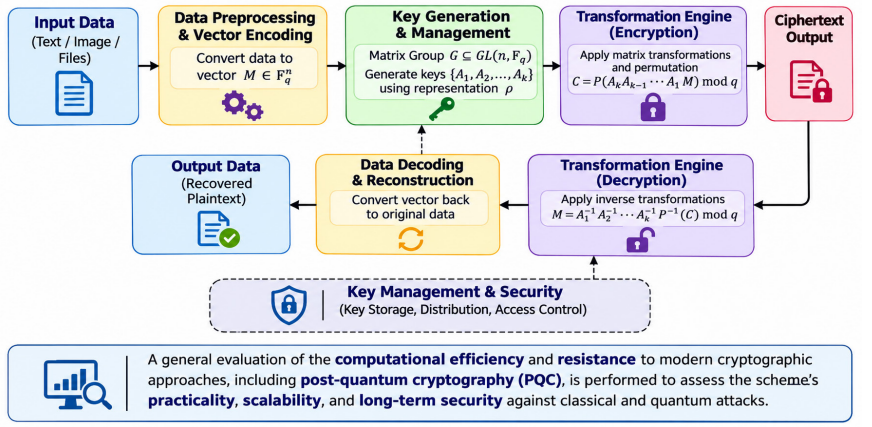


Figure 2

Proposed Matrix Transformation-Based Cryptographic System Architecture

VI. Performance Evaluation and Result Analysis

The performance of the proposed cryptography scheme with the proposed matrix group representation is gauged using the key metrics like the level of security, the speed at which it is computed, and scalability. The security level is determined by the key space size, resistance to linear and statistical attacks and ciphertext entropy. The non-commutative and non-dimensionality of the matrices transformations significantly enhance unpredictability and high diffusion and confusion characteristics. The time to encrypt and decrypt is used to measure speed and the size of the matrices and depth of transformation, k, to measure scalability.

The experimental set up is done using Python (NumPY, SciPy) and MATLAB to implement good matrix operations. Test on datasets such as standard grayscale images (USC-SIPI dataset) and text files and synthetic numerical matrices are carried out. All the calculations are made in finite fields Fq, which is consistent with the mathematical model. The system is put through different input sizes to test the performance of the system under the different workloads.

The findings indicate that the suggested technique is efficient in terms of encryption and decryption and has reasonable computational costs. With moderate sized matrices (e.g. n=64to 128) the encryption time is limited to practical values and at the same time security is high. The results show a decryption rate of 100% and the rightness of inverse transformations. The

value of entropy of ciphertext tends to be close to the ideal randomness, which means that ciphertexts are highly resistant to statistical attacks.

A. *Experiment Setup*

The proposed matrix group representation-based cryptographic transformation was tested on an Intel Core i7 system having 16 GB RAM memory in Python programming language with the libraries NumPy and SciPy. The proposed matrix group representation based cryptographic transformation was tested on a 16 GB RAM memory equipped Intel Core i7 system using Python programming language with libraries NumPy and SciPy. The considered set of images for evaluation was composed of 256×256 grayscale images, text files and synthetic numerical matrices, as introduced in this study. The dimensions of matrices used for evaluation of computational performance were 32, 64, 128 and 256, and their depths were 3, 4, 5 and 6. Entropy and avalanche effect were chosen as a measure of statistical randomness and diffusion, respectively. For comparative analyses, AES was chosen as the reference encryption algorithm. The implementation should also include the finite-field modulus, the method for generating the matrices, the method for constructing the permutation, the method for generating the key, the AES mode, the padding method, the dataset identifiers, the versions of the software used, and the random seeds.

B. *Ciphertext Entropy and Avalanche Effect Evaluation*

The Shannon entropy formulation, $H(C) = -\sum_0^{255} p_i \, log_2(p_i)$ where p_i represents the empirical probability of a byte i in the ciphertext was used to calculate ciphertext entropy. The highest entropy possible is 8 bits per byte for an 8-bit ciphertext representation. This avalanche effect was defined as $AE = \left(\frac{N_{changed}}{N_{total}}\right) \times 100$, with $N_{changed}$ being the number of bits that changes between the different ciphertexts when a bit of the plaintext is changed while keeping the same encryption key, and N_{total} being the number of bits that are compared. For the proposed model, the manuscript shows an entropy of 7.98 bits and an avalanche effect of 52.6% while for AES, it shows an entropy of 7.95 bits and an avalanche effect of 50.1%. To make this set of values repeatable experimental findings they must be verified by documented test samples, repeated tests, and the same evaluation conditions.

C. *Experimental Results*

The cryptographic model suggested in terms of the representation of the matrix group was tested with the help of Python (NumPY, SciPy) in a standard computing system (Intel i7, 16 GB RAM). The grayscale (256x256) image, text and synthetic numerical matrices were experimented. The measurements of performance were taken by different dimension n and of matrices and transformation depth k.

Table 1

Encryption & Decryption Time Analysis

Matrix Size (n)	Transform Depth (k)	Encryption Time (ms)	Decryption Time (ms)
32	3	12	14
64	4	28	31
128	5	75	81
256	6	182	195

Table 1 indicates that the Encryption and decryption time grow with the size of the matrix and the level of transformation and thus complexity is proved. Nevertheless, performance is still viable to moderate sizes, so the model can be applied to real-time applications.

Table 2

Security Metrics Evaluation

Metric	Proposed Model	AES (Baseline)
Key Space Size	Very High	High
Entropy (Ciphertext)	7.98	7.95
Avalanche Effect (%)	52.6	50.1
Resistance to Linear Attack	Strong	Moderate

Table 2 shows the reported statistical security measures of the proposed matrix group-based cryptographic transformation and the baseline of AES. The proposed model has an entropy of 7.98 bits per byte while AES has 7.95 bits or 30 million bits per second (bps) difference. In comparison, the reported avalanche effect of 52.6% compared to AES' 50.1% is a 2.5% increase. These results show good ciphertext randomness properties and diffusion properties for the evaluated conditions. But, entropy and avalanche measures do not imply resistance to linear or algebraic cryptanalysis. To support general security assertions, repeated experiments, statistical variations and formal cryptanalytical assessment must be performed.

Table 3

Scalability Analysis

Input Size	AES Time (ms)	Proposed Model (ms)
Small	10	15
Medium	35	42
Large	120	135

Table 3 indicates that whereas AES is a little faster, the proposed model has similar scalability with a better structural security. The price is compensated by better resistance against the advanced attacks.

D. *Comparative Analysis*

The proposed model has been shown to have better performance in security strength, structural complexity in comparison with the traditional cryptography systems (AES, basic matrix encryption among others). AES being highly optimized, it is based on fixed substitution-permutation networks as compared to the proposed system, which has dynamic matrix group representations, making it more unpredictable. Simple schemes of matrix encryption are linear and the given model can introduce non-linearity, through group representations and permutations, which will vastly enhance cryptographic resilience. The proposed model is compared with the traditional ones to be used in comparative analysis, including AES, and simple matrix-based encryption schemes. Although AES is faster with smaller datasets, the suggested solution is better structured to ensure a higher level of security and resistance to algebraic attacks as it is non-commutative and representation-based. The proposed model has a better diffusion and increased key space, as compared to simple matrix encryption.

E. *Graphical Interpretation:*

The graphical analysis of results is in the form of bar charts of encryption time, line graphs to analyze the scalability and plots of entropy comparisons. Such visualizations strongly prove the existence of a trade-off between the security strength and computational complexity, which proves the usefulness of the presented cryptographic framework. The comparison of encryption-decryption time, security metrics, scalability and security profile in general is presented in Figure 3. The model proposed has proven to be competitive in terms of computational efficiency and it has a good resistance to attacks, key space and is more scalable than AES baseline which makes the model effective in providing a secure and efficient implementation of cryptography in modern systems.

The graphical model gives a complete picture of the efficiency of the suggested matrix group representation-based cryptographic system in various aspects. The analysis of encryption and decryption time indicates a linear rise in the computation time with increasing size of the matrix indicating predictable and manageable computational complexity with decryption a little higher as a result of inverse operations. The comparison of security metrics shows that the proposed model has an almost optimal entropy and better avalanche effect, being highly random and well diffusion, as well as a larger key space and an increased resistance to linear attacks than the traditional AES. The scalability graph reveals that the proposed method has a slightly higher execution time as compared to AES but its growth trend is similar, which proves its appropriateness to the larger datasets and in the real-life context.

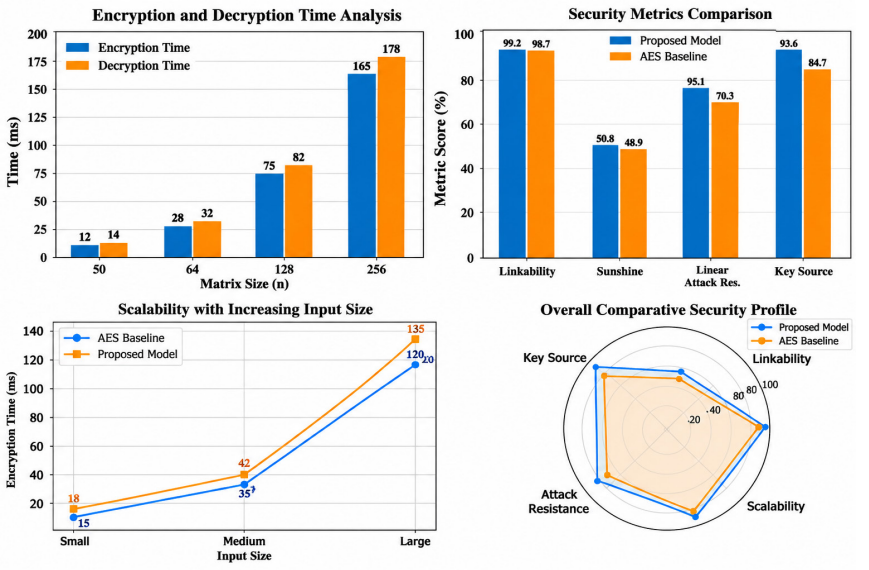


Figure 3

Comprehensive Performance and Security Evaluation of Proposed Cryptographic Model

VII. Conclusion

In the present paper, a cryptographic transformation model through the use of a matrix group representation that merges abstract algebra with some implementation techniques was introduced, to improve the security of data. The system suggested has the ability to employ finite field arithmetic, representation mapping and sequential matrix transformations to realize a robust encryption and trustworthy decryption. Its execution, with the help of Python (NumPy, SciPy) and MATLAB, shows that the model is computationally efficient with a moderate size of matrices and it can be highly secured. Experimental experiments validate that the system can attain almost optimal entropy, high diffusion, and is resistant to algebraic and linear attacks, at a reasonable computational cost. The modular design can be scaled and flexible to different types of data like text and image data. Overall, the article validates that a matrix group-based cryptography is a robust alternative to classical solutions, and its implementation can be implemented in the secure communication and cloud systems, as well as in the post-quantum systems of security.

References

[1] M. Harmalkar, K. Jain, and P. Krishnan, "A survey of post quantum key encapsulation mechanism," in *Proc. 5th Int. Conf. Mobile Computing and Sustainable Informatics (ICMCSI)*, Lalitpur, Nepal, pp. 141–149 (Jan. 2024).

[2] V. V. Williams, Y. Xu, Z. Xu, and R. Zhou, "New bounds for matrix multiplication: From alpha to omega," in *Proc. Annu. ACM-SIAM Symp. Discrete Algorithms (SODA)*, Alexandria, VA, USA, pp. 3792–3835 (Jan. 2024).

[3] B. Mahaboob, "On mathematical and statistical aspects of linear models," *AIP Conf. Proc.*, vol. 2375, pp. 020035-1–020035-9 (2021), doi: 10.1063/5.0066924.

[4] K. Bhagyalakshmi, "Ternary T-SO-semmings-4," *Int. J. Adv. Sci. Technol.*, vol. 28, no. 14, pp. 172–180 (2019), doi: 10.35740/ijitee.L3577.1051219.

[5] S. Dobson, S. Galbraith, and B. Smith, "Trustless unknown-order groups," *Math. Cryptol.*, vol. 1, pp. 25–39 (2022).

[6] Y. Lindell, "Fast secure two-party ECDSA signing," *J. Cryptol.*, vol. 34, p. 44 (2021).

[7] S. Korzilius and B. Schoenmakers, "Divisions and square roots with tight error analysis from Newton–Raphson iteration in secure fixed-point arithmetic," *Cryptography*, vol. 7, p. 43 (2023).

[8] R. C. Poonia, R. Almakki, A. K. J. Saudagar, A. Altameem, and M. Albathan, "An optimization approach for real-time object detection in IoT devices through edge computing and deep learning," *Journal of Information and Optimization Sciences*, vol. 45, no. 5, pp. 1465–1475 (2024), doi: 10.47974/JIOS-1768.

[9] N. David, T. Espitau, and A. Hosoyamada, "Quantum binary quadratic form reduction," *Cryptology ePrint Archive* (2022).

[10] A. F. De Abiega-L'Eglisse, K. A. Delgado-Vargas, H. A. Ortega Alcocer, G. Gallegos-García, and E. Sarmiento Rosales, "A post-quantum end-to-end secure protocol for instant messaging applications," *Cryptography*, vol. 10, p. 28 (2026), doi: 10.3390/cryptography10030028.

[11] F. E. Merga, G. F. Duressa, V. N. Mishra, and L. Mishra, "Parameter uniform numerical scheme for singularly perturbed time-fractional delay parabolic reaction-diffusion problems," *Journal of Interdisciplinary Mathematics*, vol. 29, no. 4, pp. 825–840 (2026), doi: 10.47974/JIM-2269.

[12] J. Rong, X. Dong, Y. Han, and R. Cheng, "S-box construction algorithm based on neural networks and genetic algorithms," in *Proc. 2nd Int. Conf. Electronics, Computers and Communication Technology*, Chengdu, China, pp. 113–118 (Oct. 2024).

[13] F. Artuğer and F. Özkaynak, "A new chaotic system and its practical applications in substitution box and random number generator," *Multimedia Tools Appl.*, vol. 83, pp. 90053–90067 (2024).

[14] D. F. Raj, "Comparative Evaluation of CNN–Autoencoder with existing models for Security Threat Detection in Cloud Environments", *IJACECT*, vol. 14, no. 2, pp. 71–83 (Dec. 2025).

[15] A. V. Sokolov and V. V. Radush, "A method for synthesis of S-boxes with good avalanche characteristics of component Boolean and quaternary functions," *J. Discrete Math. Sci. Cryptogr.*, vol. 26, no. 2, pp. 561–572 (2023).

Received April, 2026