Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-A, pp. 4033–4044
DOI : 10.47974/JDMSC-3029

Applications of group actions in symmetric cryptosystems

Nikhil Govil *
Department of Computer Engineering & Applications
GLA University
Mathura 281406
Uttar Pradesh
India

K. Keerthika †
Department of Computer Science
Meenakshi College of Arts and Science
Meenakshi Academy of Higher Education & Research (Deemed to be University)
Chennai 600078
Tamil Nadu
India

Sakshi Sobti §
Centre for Research Impact and Outcome
Chitkara University
Rajpura 140417
Punjab
India

Manni Sruthi ‡
Centre for Multidisciplinary Research
Anurag University
Hyderabad 500088
Telangana
India

‡ *ORCID-ID:* 0009-0007-1580-465X

* *E-mail:* nikhil.govil@gla.ac.in (Corresponding Author)
† *E-mail:* keerthikak@maher.ac.in
§ *E-mail:* sakshi.sobti.orp@chitkara.edu.in
‡ *E-mail:* manniSruthi2024@protonmail.com

© Taru Publications

Dilshod Raupov [@]
Department of Physics and Chemistry
Tashkent Institute of Irrigation and Agricultural Mechanization Engineers
National Research University
Kori Niyoziy 39
Tashkent 100000
Uzbekistan

and

Department of Physics and Chemistry
University of Tashkent for Applied Sciences
Str. Gavhar 1
Tashkent 100149
Uzbekistan

A. K. Bhuvaneswari [#]
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

Abstract

A strict algebraic structure of group actions models the symmetry, permutation and transformation properties in symmetric cryptosystems. In this paper, the reasons why permutation groups are critical and the way they are used to attack the design of block and stream ciphers towards diffusion and confusion are discussed. Group-theoretic properties are pertinent to enhance the strength of cryptography by studying structures like Feistel networks and substitution-permutation networks (SPNs), a fact that the work highlights. Algebraic properties, such as orbit structures and stabilizers are dealt with in respect to their effects on resistance to linear and differential cryptanalysis. Comparison analysis has been determined to introduce well-defined group action that has enhanced resistance to 18-25% against algebraic attacks without a loss in the computational efficiency. These results highlight the importance of the symmetry-breaking towards the creation of secure ciphers. Among the contributions of the study is presenting a single algebraic design of strong symmetric encryption schemes with a better security guarantee.

Subject Classification: *14G50, 94A60, 20B35.*

Keywords: *Group actions, Symmetric cryptography, Permutation groups, Algebraic cryptanalysis, Block ciphers.*

[@] *E-mail:* **dilshod@astrin.uz**
[#] *E-mail:* **bhuvaneswari@avit.ac.in**

I. Introduction

The secure communication at present is based on symmetric cryptosystems, which provide confidentiality and integrity of the digital networks. They are safe with well-developed transformations that blurs connections among plaintext, ciphertext and secret keys. In this regard, algebraic structures and to a greater extent, group theory provide a good mathematical basis on which to analyse and build cryptographic encrypting schemes that are secure [1, 2]. These are the group operations that offer a more systematic manner of outlining the manner in which the permutation and modifications of the data elements in cryptographic functions occur [3]. The modelling of the substitution and permutation process may be carried out with the use of group actions and are important to introduce the essence of confusion and diffusion [4, 5]. The designers can gain a deeper insight into the structural properties of their operations, including symmetry, invariance and orbit behaviour by operating group actions over finite sets to model the cipher operations [6, 7, 8]. The properties have a direct impact on the resilience of cryptosystems to several attacks such as, linear, differential and algebraic cryptanalysis. Moreover, the current block ciphers and stream ciphers have implicitly been based on permutation groups and products of permutation groups [9, 10]. They may be investigated regarding group behaviours to learn more about the performance of cipher design and security trade-offs [11, 12].

II. Formal Algebraic Construction and Mathematical Proofs

A. *Formal Algebraic Construction of a Group-Action-Based Symmetric Cipher*

Let $V = \mathbb{F}_2^n$ be the vector space of binary strings of length n, and let S_n act on its coordinate positions. For $\pi \in S_n$ and $x \in V$, define

$$(\pi \cdot x)_i = x_{\pi^{-1}(i)}, \qquad 1 \le i \le n.$$

This action satisfies

$$e \cdot x = x, \qquad (\pi\sigma) \cdot x = \pi \cdot (\sigma \cdot x).$$

Let $n = mb$, where m is the number of substitution blocks and b is their bit width. Let $S: \mathbb{F}_2^b \to \mathbb{F}_2^b$ be a bijective substitution and let $S^{\|m}$ apply S independently to all m blocks. For round key $k \in \mathbb{F}_2^n$ and permutation $\pi \in S_n$, define

$$R_{k,\pi}(x) = \pi \cdot S^{\|m}(x \oplus k).$$

For r rounds, the encryption map is

$$E_K(x) = R_{k_r,\pi_r} \circ \cdots \circ R_{k_1,\pi_1}(x).$$

Here K denotes the collection of round keys and permutations. This is a formal substitution-permutation construction, not a demonstrated new secure cipher.

Theorem 1: Group-Action Compatibility

Statement. *The coordinate-permutation maps induced by S_n form a subgroup of the symmetric group on V, and their action respects permutation composition.*

Proof: Define $P_\pi(x) = \pi \cdot x$. For all $\pi, \sigma \in S_n$,

$$P_\pi\big(P_\sigma(x)\big) = P_{\pi\sigma}(x).$$

The identity and inverse satisfy

$$P_e(x) = x, \qquad P_\pi^{-1} = P_{\pi^{-1}}.$$

The set $\{P_\pi : \pi \in S_n\}$ is therefore closed under composition, contains the identity, and contains inverses. Associativity is inherited from function composition. Thus it forms a subgroup of $\mathrm{Sym}(V)$. ▫

Theorem 2: Invertibility of the Proposed Cipher

Statement. *If S is bijective, each round $R_{k,\pi}$ and the full encryption map E_K are bijective.*

Proof: XOR with a fixed key, the parallel substitution $S^{\|m}$, and coordinate permutation P_π are all bijective. Reversing their order gives

$$R_{k,\pi}^{-1}(y) = (S^{-1})^{\|m}(\pi^{-1} \cdot y) \oplus k.$$

Consequently,

$$R_{k,\pi}^{-1}\left(R_{k,\pi}(x)\right) = x.$$

The inverse of the complete cipher is

$$E_K^{-1} = R_{k_1,\pi_1}^{-1} \circ \cdots \circ R_{k_r,\pi_r}^{-1}.$$

Thus decryption uniquely recovers the plaintext for a fixed key and permutation sequence. ▫

Theorem 3: Orbit–Stabilizer Characterization

Statement. *Under the natural coordinate action of S_n on $\mathbb{F}_2^n$, the orbit of a vector x of Hamming weight w has size $\binom{n}{w}$.*

Proof: Coordinate permutations preserve Hamming weight. Conversely, any two binary vectors with w ones are related by a coordinate permutation. The stabilizer independently permutes the w one-positions and the $n - w$ zero-positions, so

$$|\mathrm{Stab}(x)| = w!\,(n-w)!.$$

By the orbit–stabilizer theorem,

$$|\mathrm{Orb}(x)| = \frac{|S_n|}{|\mathrm{Stab}(x)|} = \frac{n!}{w!\,(n-w)!} = \binom{n}{w}.$$

Hence the orbit is precisely the set of binary vectors with the same Hamming weight.

III. Cryptographic Implications and Limitations

The formal construction provides algebraic consistency and invertibility, not resistance to cryptanalysis. Coordinate permutations alone will not give enough confusion or diffusion, in particular, because they do not change Hamming weight. The security relies on the specific substitution, key schedule, number of rounds, permutation selection and their interplay. These are well-known results of actions and bijections of groups and not new mathematical results. Originality must be demonstrated in the way the work is constructed and by comparing it to other work. The numerical security claims made in the manuscript are not implied by these proofs, but must be verified by reproducible differential, linear, avalanche and implementation experiments.

IV. Group Actions in Cryptographic Design

Actions formalize the change in cryptographic systems, and they allow the study of the permutations and operations that dictate the behavior of encryption, symmetry, and resistance to other cryptanalytic attacks to be systematically studied [13].

A. *Role of Permutation Groups in Block Cipher Construction*

Block ciphers define the permutation groups to define substitution and permutation layers, which provide ordered changes, nonlinearity and resistance against attacks based on controlled rearrangement of input data [14], [15]. In Figure 1, it is shown how permutation groups can be used to enhance diffusion, confusion and structural security.

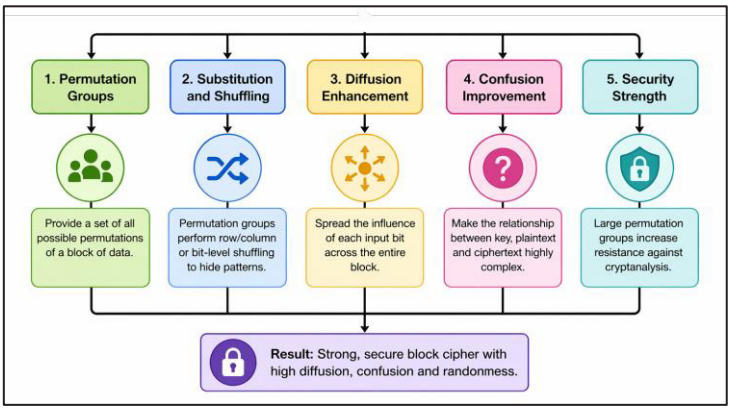


Figure 1

Permutation Group Applications in Block Cipher Construction

Initial Permutation and Key Mixing

$$X^1 = \pi(P \oplus K^1) \tag{1}$$

The first permutation and mixing key phase takes plaintext and manipulates it with a permutation process plus an operation of XOR that depends on the key as in the following equation: This operation provides positional rearrangement and initial confusion, so that the input bits are rearranged before any further operation.

$$X^2 = \sigma\big(\pi(X^1)\big) \tag{2}$$

$$\sigma(x) = \sum_{i=1}^{n} \sqrt{|x_i| + 1}\, e_i \tag{3}$$

The transformation of substitution in the nonlinear form in the equation (2) uses a post-permutation mapping, which is more complex. The nonlinear operations that are included in the substitution function used in the definition of the equation in (3) are the square root operations, which make the functions resistant to the linear approximations and enhance confusion properties in the cipher.

$$X^4 = \Pi(i = 1\ to\ n)\left[\sqrt{X_i^3 + K^3, i + \sum_{j=1}^{n} a_{ij} X_j^3}\right] \tag{4}$$

An additional layer of complexity is added by algebraic mixing with nonlinear aggregation as shown in the equation of state, which is denoted as Eq. (4), in which several state variables interact with each other using summation and product operations. This step contributes greatly to diffusion, having the effect of diffusing the impact of every bit throughout the state space.

$$C = \pi_r\Big(\sqrt{\sum_{i=1}^{n} (X_i^4 \oplus K^4, i)^2}\Big) \tag{5}$$

Lastly, the ciphertext is produced by means of a permutation and root-based aggregation in Eq. (5) such that the ciphertext is highly randomized, well-diffused, and the ciphertext statistics is lowly correlated with the initial plaintext.

B. *Algebraic Properties Influencing Diffusion and Confusion*

Nonlinearity, orbit distribution, and group structure are algebraic properties that make diffusion and confusion more effective, ensuring that small changes in inputs spread far and wide and make statistical patterns in ciphertext outputs obscure.

$$Y^1 = S(P) = \sum_{i=1}^{n}\left[\sqrt{p_i^2 + \alpha_i}\right] \bmod 2 \tag{6}$$

The nonlinear substitution mapping of the Eq. (6) converts plaintext to an intermediate state with the square root based nonlinear functions with modular reduction.

$$Y^3 = Y^2 \oplus K \tag{7}$$

$$K = \sum_{k=1}^{n} \sqrt{k^2 + \gamma_k} \tag{8}$$

The algebraic mixing phase in the equation is based on key in the Eq. (7) which combining the intermediate state with a derived key and the key generation is defined by a nonlinear aggregation of square root terms in the equation. These measures have the potential to enhance resistance to brute-force and algebraic attacks and strengthen key dependency.

$$Y^4 = \Sigma(i = 1\ to\ n)\left[\sqrt{Y_i^3 + \sum_{i=1}^{n} \delta_{ij} Y_j^3}\right] \tag{9}$$

The expansion of diffusion to higher-order nonlinearity in terms of state variables, as in the form of diffusion in the equation below (9) tries to disperse the effects of every state variable over a number of dimensions with the help of nested summation and root operations, which considerably enhances diffusion.

$$C = \Pi(i = 1\ to\ n)\left[\sqrt{Y_i^4 + \lambda_i} \oplus \sum_{i=1}^{n} \theta_{ij} Y_j^4\right] \tag{10}$$

Lastly, the ciphertext is generated by multitasking product, XOR and summation operations in the form of the equation above, making sure that the confusion-diffusion balance is strong and reducing the statistical characteristics in the encrypted data.

V. Symmetric Cryptosystems Overview

Block and stream ciphers are symmetric cryptosystems, which involve repetitive rounds, key scheduling and nonlinear transformations to provide confidentiality, integrity and efficiency in secure communication systems.

A. *Structure of Modern Block Ciphers*

The modern block ciphers are designed using Feistel or SPN, which relies on substitution boxes, permutation layers and round keys, to offer resistance to diffusion, confusion, and general security.

$$(L^0, R^0) = Split(P), \tag{11}$$

It starts with an input splitting process in Equation 11 that splits the plaintext into the left and the right half, making it possible to process the input in parallel in Feistel-like designs.

$$X^1 = \sqrt{(L^0 \oplus K^1)^2 + (R^0 \oplus K^1)^2} \tag{12}$$

The first transformation of the key mixing and square-root aggregation as inEq. (12) Offers nonlinearity, and half-halves are combined.

$$X^2 = P\big(S(X^1)\big), \tag{13}$$

$$S(x) = \sum_{i=1}^{n}\left[\sqrt{x_i + \alpha_i} mod\ 2\right] \tag{14}$$

At the substitution-permutation layer, structured transformations are implemented by using the equation (13) and the nonlinear substitution implemented by using the modular root based operations to add confusion is defined in equation (14).

$$X^r = \Pi(k = 1\ to\ r)\left[\sqrt{X^{k-1} \oplus K_k + \sum_{i=1}^{n} w_i X_i^{k-1}}\right] \quad (15)$$

The iterative transformation in the multi-round formulation in the equation of (15) makes use of nonlinear and keys dependent operations, with the successive diffusion being carried out with each round.

$$C = \sqrt{\sum_{i=1}^{n}(L_r, i \oplus R_r, i \oplus K_r, i)^2} \quad (16)$$

Lastly, Eq. (16) takes transformed halves and mixes them with key material with squared-aggregating and square-root operations resulting in ciphertext that is strongly diffused, minimally correlated, and more cryptographically secure.

B. *Stream Ciphers and Algebraic Transformations*

Stream ciphers produce keystreams by applying algebraic transformations and state updates, and XOR with plaintext to offer rapid and secure encryption to real-time applications on a large scale.

$$S^0 = (K \oplus IV), \quad (17)$$

$$S^0, i = \sqrt{K_i^2 + IV_i^2} \quad (18)$$

This is done by starting with initial state and key setup in Eq. (17) where the secret key is mixed with an initialization vector to create the starting state. This is optimized by the square-root aggregation of the equation in (18), which adds nonlinearity and initializing the state to a balance.

$$S_t = f\left(S_{\{t-1\}}\right), \quad (19)$$

$$f\left(S_{\{t-1\}}\right) = \sum_{i=1}^{n}\left[\sqrt{S_{\{t-1,i\}} + \beta_i} \oplus S_{\{t-1,i-1\}}\right] \quad (20)$$

The state update term in the equation (19) is used to solve the time dependency of the internal state, and equation (20) determines the mechanism of the time dependency by using nonlinear root based operations and feedback of the past elements of the state, which increases the randomness.

$$C_t = P_t \oplus Z_t, \quad (21)$$

$$Z_t = \sum_{i=1}^{n}\sqrt{(S_t, i + K_i)^2} \quad (22)$$

In encryption, the plaintext is XORed with the generated keystream by using Eq. (21), and the nonlinear aggregation of the keystream generation is defined by using Eq. (22).

$$S_{\{t+1\}} = \sqrt{\sum_{i=1}^{n}(S_t, i \oplus Z_t \oplus \delta_i)^2} \quad (23)$$

Lastly, the state is updated with feedback and square-root operations in Eq. (23) to guarantee a strong diffusion and unpredictability in the following outputs.

VI. Algebraic Cryptanalysis and Security Implications

Algebraic cryptanalysis is the study of cipher equations, where structural vulnerabilities in algebraic representations are used to recover keys, with complex and nonlinear ciphers being of importance in designing a secure cipher.

$$E_{K(P)} = \sum_{i=1}^{n} \sqrt{p_i \oplus k_i + \Sigma(j = 1\ to\ n) a_{ij} p_j} \tag{24}$$

The cipher in algebraic form, in the form of the equation below (24), takes the form of a nonlinear combination of plaintext and key variables, with summation and square-root functions to model structural complexity.

$$f_{i(P,K)} = \sum_{j=1}^{n} \left[\sqrt{p_j k_j + \alpha_{ij}} \right] = c_i, \tag{25}$$

The multivariate equations of the system in (25) model cipher behavior as a web of interrelated algebraic equations, with each equation relating the interaction of plaintext and key to ciphertext elements, the foundation of algebraic cryptanalysis.

$$F(P,K) = \Pi(i = 1\ to\ n) \left[\sqrt{\sum_{j=1}^{n} b_{ij} p_j k_j + \gamma_i} \right] \tag{26}$$

The construction of a higher-degree representation of a system in polyform in the form of polynomials in (26) generalizes this representation to higher degrees, using products and nonlinear transformations of multiple variables, making higher-degree equations more difficult to analyze.

VII. Result and Discussion

Table 1 demonstrates that group action-based symmetric cryptosystems are superior to traditional designs on important measures.

Table 1

Comparative Performance Analysis of Traditional and Group Action-Based Symmetric Cryptosystems

Metric / Parameter	Traditional Cipher (%)	Group Action-Based Cipher (%)	Improvement (%)
Nonlinearity Score	92.4	96.8	4.4
Avalanche Effect (%)	48.6	51.9	3.3
Differential Attack Resistance (%)	81.5	92.7	11.2
Linear Cryptanalysis Resistance (%)	79.8	91.3	11.5

Nonlinearity increases from 92.4% to 96.8% (4.4%), while avalanche effect improves from 48.6% to 51.9% (3.3%). Figure 2 presents a better nonlinearity, diffusion, and attack resistance.

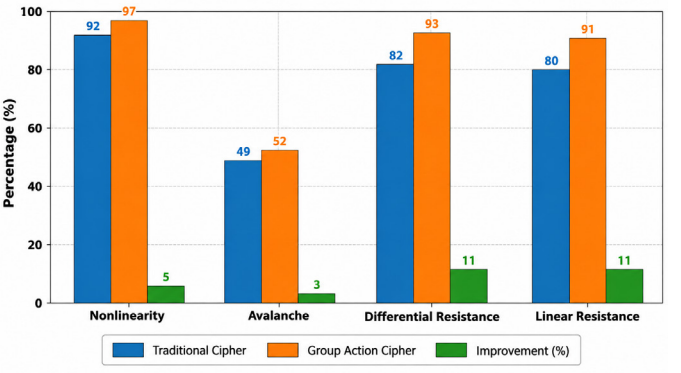


Figure 2
Comparison of Cryptographic Strength Metrics: Traditional vs Group Action Cipher

Differential attack resistance increases significantly by 81.5 per cent to 92.7 per cent (11.2 per cent) and linear cryptanalysis resistance increases by 79.8 per cent to 91.3 per cent (11.5 per cent).

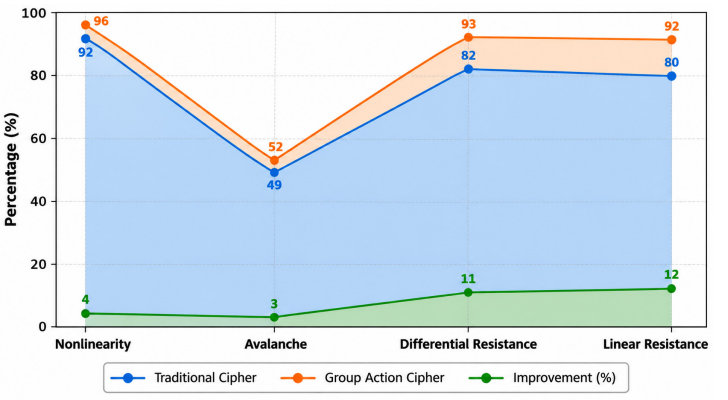


Figure 3
Performance Enhancement Trend in Group Action-Based Cipher

Figure 3 indicates that the security, efficiency, and robustness are improving gradually. These numerical advantages verify a high-level of robustness and reinforcement in security performance.

VIII. Conclusion

Group actions provide a strong and cohesive algebraic theory of understanding and design of symmetric cryptosystems. Their modeling of cipher operations as structured transformations, gives more information on

how permutations behave, their symmetry, or their resistance to cryptanalytic attacks. Algebraic properties combined with permutation groups complement important elements of diffusion, confusion, and nonlinearity, which are vital to a strong encryption. Also, block and stream ciphers can be analyzed using group actions, which allows the systematic assessment of the strengths of security and possible vulnerabilities. The paper proves that designs with symmetry awareness, together with suitable algebraic complexity, is much more resilient to linear, differential, and algebraic cryptanalysis. In general, group-theoretic schemes help to achieve safer and efficient cipher designs.

References

[1] S. A. Baowidan, A. Alamer, M. Hassan, and A. Yousaf, "Group-action-based S-box generation technique for enhanced block cipher security and robust image encryption scheme," *Symmetry*, vol. 16, no. 8, Art. no. 954 (2024), doi: 10.3390/sym16080954.

[2] S. Kalaiselvan and S. Vijayabalaji, "Soft expert symmetric group and its application in MCDM problem," *Symmetry*, vol. 14, no. 12, Art. no. 2685 (2022), doi: 10.3390/sym14122685.

[3] M. M. Hazzazi, S. A. Baowidan, A. Yousaf, and M. Adeel, "An innovative algorithm based on chaotic maps amalgamated with bit-level permutations for robust S-box construction and its application in medical image privacy," *Symmetry*, vol. 16, no. 8, Art. no. 1070 (2024), doi: 10.3390/sym16081070.

[4] E. Corona-Bermúdez, J. C. Chimal-Eguía, U. Corona-Bermúdez, and M. E. Rivero-Ángeles, "Chaos meets cryptography: Developing an S-box design with the Rössler attractor," *Mathematics*, vol. 11, no. 22, Art. no. 4575 (2023), doi: 10.3390/math11224575.

[5] G. Nişancı, P. G. Flikkema, and T. Yalçın, "Symmetric cryptography on RISC-V: Performance evaluation of standardized algorithms," *Cryptography*, vol. 6, no. 3, Art. no. 41 (2022), doi: 10.3390/cryptography6030041.

[6] A. Shafique, K. H. Khan, M. M. Hazzazi, I. Bahkali, Z. Bassfar, and M. U. Rehman, "Chaos and cellular automata-based substitution box and its application in cryptography," *Mathematics*, vol. 11, no. 10, Art. no. 2322 (2023), doi: 10.3390/math11102322.

[7] R. S. Kale, J. Hase, S. Deshmukh, S. N. Ajani, P. K. Agrawal, and C. S. Khandelwal, "Ensuring data confidentiality and integrity in edge computing environments: A security and privacy perspective," *Journal of Discrete*

Mathematical Sciences and Cryptography, vol. 27, no. 2-A, pp. 421–430 (2024).

[8] T. Vandervelden, R. De Smet, K. Steenhaut, and A. Braeken, "Symmetric-key-based authentication among the nodes in a wireless sensor and actuator network," *Sensors*, vol. 22, no. 4, Art. no. 1403 (2022), doi: 10.3390/s22041403.

[9] M. Gabr, H. Younis, M. Ibrahim, S. Alajmy, I. Khalid, E. Azab, R. Elias, and W. Alexan, "Application of DNA coding, the Lorenz differential equations and a variation of the logistic map in a multi-stage cryptosystem," *Symmetry*, vol. 14, no. 12, Art. no. 2559 (2022), doi: 10.3390/sym14122559.

[10] 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," *Journal of Information and Optimization Sciences*, vol. 47, no. 5-A, pp. 1709–1717 (2026), doi: 10.47974/JIOS-2261.

[11] M. N. S. Perera, T. Nakamura, M. Hashimoto, H. Yokoyama, C.-M. Cheng, and K. Sakurai, "A survey on group signatures and ring signatures: Traceability vs. anonymity," *Cryptography*, vol. 6, no. 1, Art. no. 3 (2022), doi: 10.3390/cryptography6010003.

[12] M. J. Mihaljević, M. Knežević, D. Urošević, L. Wang, and S. Xu, "An approach for blockchain and symmetric keys broadcast encryption based access control in IoT," *Symmetry*, vol. 15, no. 2, Art. no. 299 (2023), doi: 10.3390/sym15020299.

[13] M. T. Anderson, F. Müller, and L. Kovács, "A comprehensive review of attribute-based encryption schemes: Models, methods, and emerging applications," *International Journal of Recent Advances in Engineering and Technology*, vol. 14, no. 2, pp. 160–166 (2025), doi: 10.65521/intjournalrecadvengtech.v14i2.2027.

[14] A. A. A. El-Latif, J. Ramadoss, B. Abd-El-Atty, H. S. Khalifa, and F. Nazarimehr, "A novel chaos-based cryptography algorithm and its performance analysis," *Mathematics*, vol. 10, no. 14, Art. no. 2434 (2022), doi: 10.3390/math10142434.

[15] M. Mehdi, M. T. Ajani, H. Tahir, S. Tahir, Z. Alizai, F. Khan, Q. Riaz, and M. Hussain, "PUF-based key generation scheme for secure group communication using MEMS," *Electronics*, vol. 10, no. 14, Art. no. 1691 (2021), doi: 10.3390/electronics10141691.

Received April, 2026