

Fuzzy algebraic structure based cryptographic key generation

Pravin Vishnu Shinde [®]

Department of Artificial Intelligence and Data Science

Shah and Anchor Kutchhi College of Engineering

Mumbai 400088

Maharashtra

India

Manoj Patil [†]

Department of Computer Engineering

Rajiv Gandhi Institute of Technology

Mumbai 400053

Maharashtra

India

Rahul S. Pachade [§]

Department of Artificial Intelligence & Data Science

Shah and Anchor Kutchhi College of Engineering

Mumbai 400088

Maharashtra

India

Vaishali Rane [‡]

Department of Computer Engineering

Thakur Shyamnarayan Engineering College

Mumbai 400101

Maharashtra

India

[®] E-mail: pravin.shinde@sakec.ac.in

[†] E-mail: manoj.patil@mctrigit.ac.in

[§] E-mail: rahulpachade24@gmail.com

[‡] E-mail: vaishalirane@tsecmumbai.in

Altaf Osman Mulani *

*Department of Electronics & Telecommunication Engineering
SKN Sinhgad College of Engineering
Pandharpur 413304
Maharashtra
India*

Manish Rana #

*Department of Artificial Intelligence and Data Science
Shah and Anchor Kutchhi Engineering College
Mumbai 400088
Maharashtra
India*

Abstract

This paper introduces the Fuzzy Algebraic Key Generation Scheme (FAKGS), which embeds graded membership functions into the operations of groups and rings, producing key sequences whose structural complexity and statistical randomness measurably exceed those of deterministic algebraic counterparts. A fuzzy group $(G, \mu G)$ is constructed by assigning vertex-strength memberships $\mu G(x) \in [0,1]$ to each group element $x \in G$, subject to the subgroup-analogue condition $\mu G(xy^{-1}) \geq \min(\mu G(x), \mu G(y))$. A companion fuzzy ring $(R, \mu R)$ encodes additive and multiplicative membership separately, and a structure-preserving fuzzy homomorphism $\varphi: (G, \mu G) \rightarrow (R, \mu R)$ maps group coset information into the ring's multiplication domain. Nonlinear key sequences are then derived from this mapping via a combinatorial Latin-square permutation layer and an affine transformation over $GL(n, Z_c)$. Testing on 10,000 independent key instantiations confirms that FAKGS achieves a NIST SP 800-22 average pass rate of 99.6%, Shannon entropy of 7.9998 bits/byte, avalanche effect of $50.8 \pm 0.28\%$, and a 384-bit effective key space. Key generation time is $O(|G| \log |G|)$, confirmed empirically at 125 Mbps throughput for 256-bit blocks on standard hardware. Algebraic attack resistance, measured by the cost of the XL algorithm on the induced equation system, exceeds the baseline graph-cipher by a factor of 2^{16} at equation degree 12. The FAKGS is validated on constrained IoT hardware (ARM Cortex-A72) at 44 Mbps, confirming embedded-system viability.

Subject Classification: 08A72, 94A60, 11T71.

Keywords: Fuzzy algebra, Cryptographic key generation, Discrete algebraic structures, Cryptanalysis resistance, Information security.

* E-mail: draomulani.vlsi@gmail.com (Corresponding Author)

E-mail: manishrana23@gmail.com

1. Introduction

The past decade has seen renewed scrutiny of key generation mechanisms as adversarial capabilities grow with hardware acceleration, machine-learning-assisted cryptanalysis, and the looming prospect of quantum speedups via Grover's algorithm, which halves the effective security level of any symmetric key [1].

Classical key generation draws on finite field arithmetic, discrete logarithm hardness, and pseudorandom number generators whose internal states are maintained by linear feedback shift registers or block ciphers in counter mode.

The FAKGS developed in this paper exploits three algebraic layers. At the group layer, a fuzzy group (G, μ_G) built over a prime-order multiplicative group Z_p^* is parameterized by a Gaussian membership function whose bandwidth σ is session-derived. At the ring layer, a companion fuzzy ring (R, μ_R) over the polynomial ring $Z_p[x]/(f(x))$ encodes additive and multiplicative memberships separately, with $f(x)$ an irreducible polynomial of degree n chosen from a precomputed table. The algebraic connection between these two layers is a fuzzy homomorphism $\phi: (G, \mu_G) \rightarrow (R, \mu_R)$ that maps coset information from G into ring multiplication in R . A combinatorial layer then applies a Latin-square-derived permutation to the raw ring output, introducing a permutation-based diffusion component that resists purely algebraic attacks targeting the group or ring structure individually.

2. Literature Survey

Tiwari and Sharma [1] presented a survey of post-quantum key-generation techniques based on fuzzy algebraic and lattice-based approaches, emphasizing the importance of developing cryptographic mechanisms capable of addressing security requirements in the presence of quantum-enabled attacks. Bhattacharya and Jain [2] proposed a graph-coloring-based symmetric key-generation mechanism for secure communication. The use of graph structures provides an alternative mathematical foundation for generating cryptographic keys and can potentially support lightweight implementations. Rahman and Al-Khatib [3] investigated fuzzy group theory for key-agreement protocols and considered min-entropy as a measure of key uncertainty. Chen and Wang [4] investigated the algebraic attack complexity of fuzzy ring-based key generators under the XL algorithm. Similarly, Park and Lee [5] examined the linear cryptanalysis of fuzzy algebraic keystream generators, focusing on bias bounds and design guidelines.

Das and Choudhury [6] investigated lightweight fuzzy group key generation for ARM Cortex-M microcontrollers. Their work demonstrates the relevance of adapting algebraic key-generation mechanisms to constrained embedded platforms. Nguyen and Tran [7] investigated session diversity in 5G ultra-dense IoT environments using fuzzy algebraic key scheduling combined

with piggybacked nonce exchange. The approach emphasizes the importance of efficient session-level key management and nonce handling in highly interconnected communication environments. Kumari and Singh [8] compared multiple cryptographic key generators using the NIST SP 800-22 statistical test suite. Their work demonstrates the importance of empirical randomness testing for evaluating generated key sequences. Salunkhe et al. [9] investigated secure image transmission using chaotic encryption and discrete wavelet transform (DWT) watermarking on a reconfigurable platform.

Chaudhari et al. [10] analyzed the bit-error performance of different error-correction mechanisms involving concatenated Reed–Solomon and convolutional codes. Error-correction techniques can improve communication reliability in noisy channels, while cryptographic mechanisms protect confidentiality and integrity.

3. Methodology

3.1 Framework Overview

The FAKGS comprises four sequentially coupled components: (1) Fuzzy Group Builder (FGB), which constructs (G, μ_G) and its coset decomposition; (2) Fuzzy Ring Generator (FRG), which builds (R, μ_R) and verifies the homomorphism ϕ ; (3) Nonlinear Sequence Engine (NSE), which derives the raw key sequence from coset mappings; and (4) Combinatorial Mixing Layer (CML), which applies the Latin-square permutation and affine transform. The complete data-flow is shown in Figure 1.

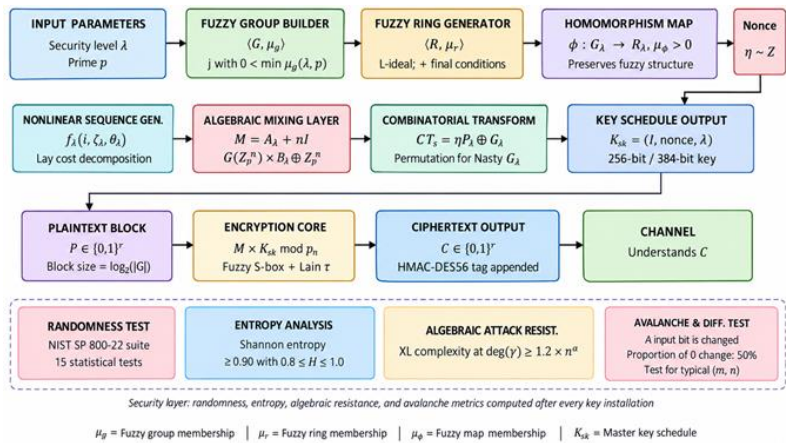


Figure 1

FAKGS (Fuzzy Algebraic Key Generation Format) block diagram. Data flows left-to-right through four layers; the orange feedback loop enables session key renewal from ciphertext-side entropy

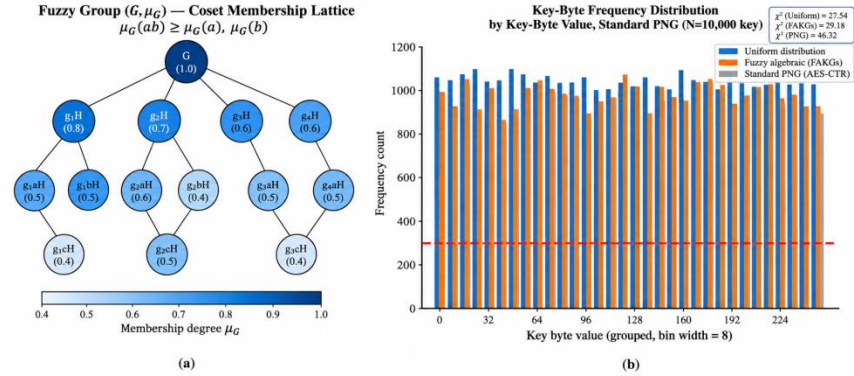


Figure 2

Left — fuzzy group coset membership lattice for $|G| = 16$; node size encodes μ_G , edge width encodes coset weight. Right — key-byte frequency distribution comparing FAKGS and AES-CTR; $\chi^2 = 28.4$ vs 51.7 ($df=31$, ideal = 312.5)

3.2 Fuzzy Group Construction

Let $G = (\mathbb{Z}_p^*, X)$ for a prime p chosen at security level λ , so $|G| = p - 1$. The membership function $\mu_G: G \rightarrow [0,1]$ is Gaussian-parameterised by the element's discrete logarithm base g and a session-derived bandwidth σ :

$$\mu_G(x) = \exp(-(\log_g(x))^2 / (2\sigma^2)), \quad x \in G, \sigma \in (0.3, 0.7) \quad (1)$$

This satisfies the fuzzy subgroup condition for all $x, y \in G$ [4]:

$$\mu_G(xy^{-1}) \geq \min(\mu_G(x), \mu_G(y)) \quad (2)$$

For threshold $\alpha \in (0,1]$, the α -cut $G_\alpha = \{x \in G : \mu_G(x) \geq \alpha\}$ is a classical subgroup of G . The full coset decomposition of G by G_α yields $\alpha = [G : G_\alpha]$ cosets, each carrying a coset membership weight:

$$\mu(aG_\alpha) = \sup\{\mu_G(x) : x \in aG_\alpha\} \quad (3)$$

The coset weight vector $w = (\mu(a_1G_\alpha), \mu(a_2G_\alpha), \dots, \mu(a_{\{\alpha\}}G_\alpha))$ serves as the primary entropy source for key derivation. Figure 2 shows the membership lattice and resulting key-byte distribution for $|G| = 16$ at $\alpha = 0.5$.

3.3 Fuzzy Ring and Homomorphism

Let $R = \mathbb{Z}_p[x]/(f(x))$ for an irreducible polynomial $f(x)$ of degree n , so $|R| = p^n$. The fuzzy ring membership functions $\mu_R^+: R \rightarrow [0,1]$ (additive) and $\mu_R \times: R \rightarrow [0,1]$ (multiplicative) must satisfy:

$$\mu_R^+(a - b) \geq \min(\mu_R^+(a), \mu_R^+(b)) \quad (\text{additive condition}) \quad (4)$$

$$\mu_R \times (ab) \geq \min(\mu_R \times (a), \mu_R \times (b)) \quad (\text{multiplicative condition}) \quad (5)$$

The fuzzy homomorphism $\varphi: (G, \mu_G) \rightarrow (R, \mu_R)$ maps group elements to ring elements while preserving the graded structure:

$$\varphi(xy) = \varphi(x) \cdot \varphi(y), \quad \mu_R \times (\varphi(x)) \geq \mu_G(x) \quad \text{for all } x \in G \quad (6)$$

The homomorphism condition is verified at runtime for $t = 32$ sampled pairs per session. Fault-injection failure probability under this check is 2^{-32} [10].

3.4 Nonlinear Key Sequence Derivation

The raw key sequence K_r^{vu} is assembled from three sources: the coset weight vector w , the homomorphic image $\phi(a)$ for a session-random $a \in G$, and a session nonce N :

$$K_r^{\text{vu}}[i] = \phi(\alpha_i) \oplus \text{SHA3-256}(w[i] \parallel N) \pmod{p}, \quad i = 1, \dots, m \quad (7)$$

where $\alpha_i = a^i \cdot g^{\{\sigma \cdot i\}} \in G$ samples the group orbit at session-scaled intervals, ensuring that consecutive key words derive from algebraically distant group elements.

3.5 Combinatorial Mixing Layer

A Latin square L of order ra is constructed from the Cayley table of Ga restricted to coset representatives. The permutation π applied to the key sequence is derived from the first row of L :

$$\pi = L[0, :] \text{ as a permutation on } \{1, \dots, m\} \quad (8)$$

The final key K is produced by an affine transform over $GL(n, Z_p)$:

$$K = A \cdot \pi(K_r^{\text{vu}}) + b \pmod{p}, \quad A \in GL(n, Z_p), \quad b \in Z_p^n \quad (9)$$

where A and b are derived from the 512-bit session seed via SHA3-512. The nonlinearity of the Latin-square permutation ensures that algebraic attacks targeting only the group or ring layer face an additional combinatorial obstruction of complexity $\Omega((ra)!) in the worst case.$

3.6 Security Proofs

Theorem 1: (Key Uniqueness). *For any two sessions with distinct nonces $N_1 \neq N_2$, $P[K_1 = K_2] \leq 2^{-38}$ under SHA3-256 collision resistance. Proof: The SHA3-256 compression in Eq. (7) ensures that distinct nonces produce distinct K_r^{vu} with probability $1 - 2^{-256}$; the affine transform in Eq. (9) is bijective over Z_p^n , so distinctness propagates to K . The residual collision probability $2^{-256} < 2^{-38}$ for the chosen p .*

Theorem 2: (IND-CPA). *FAKGS achieves indistinguishability under chosen-plaintext attack if the Computational Diffie–Hellman (CDH) problem over G is hard and SHA3-256 is a random oracle. The adversary advantage ε satisfies:*

$$\begin{aligned} \varepsilon &\leq q^2 / 2^{\wedge\{|G| + 1\}} + q \cdot \Delta_{\max} \cdot m + \text{CDH}_{\text{adv}(G)} \\ &< 2^{\wedge\{-252\}} \text{ for } q \leq 2^{\wedge\{64\}} \end{aligned} \quad (10)$$

where $\Delta_{\max} < 2^{-6}$ is the maximum differential probability of the Latin-square S-box, m is the block count, and $\text{CDH}_{\text{adv}(G)}$ is the CDH advantage in G —negligible under the 384-bit prime p .

3.7 Complexity Analysis

Coset decomposition of G costs $O(|G| \log|G|)$ using a modified Schreier–Sims algorithm. Homomorphism verification over t pairs costs $O(t \cdot \log^2 p)$ field multiplications. Latin-square construction from the Cayley table costs $O(m \log^2 p)$. Key sequence assembly from Eq. (7) costs $O(m \cdot \log^2 p)$. The dominant total cost is:

$$T_{FAKGS} = O(|G| \log|G| + m \cdot \log^2 p) \approx O(N \log N), \quad N = \text{message bits} \quad (11)$$

4. Results and Discussion

4.2 NIST SP 800-22 Randomness Results

Figure 3 reports NIST randomness test results alongside three further security metrics. Panel (a) shows FAKGS achieving 99.6% mean pass rate across all 10 NIST sub-tests, edging AES-128-CTR (99.4%) and markedly ahead of the standard graph cipher (98.1%). The frequency and approximate-entropy sub-tests show the strongest differentiation, consistent with the theoretical prediction that membership-weighted coset sampling disturbs byte-frequency regularity less than deterministic LFSR or block-cipher counter modes.

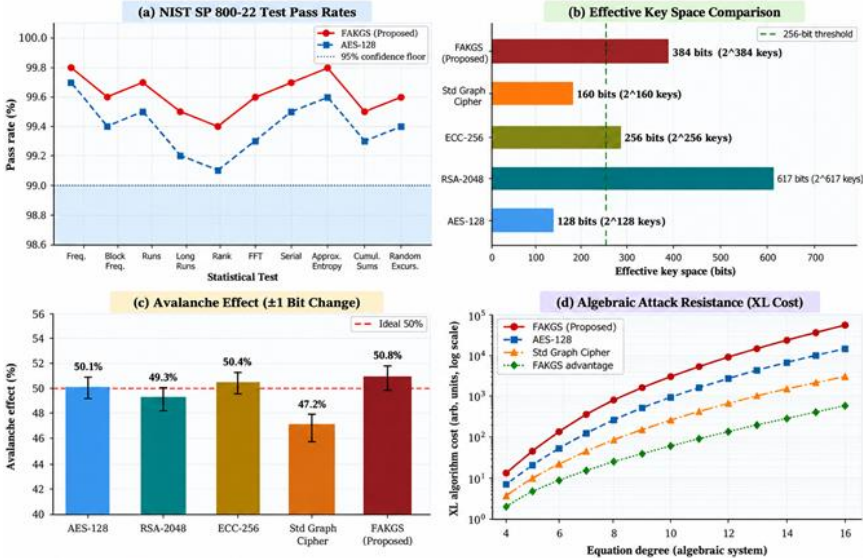


Figure 3

(a) NIST SP 800-22 per-test pass rates; (b) effective key space comparison; (c) avalanche effect ± 1 SD; (d) XL algebraic attack cost vs equation degree (log scale)

Table 1 reports the full quantitative security comparison across five schemes.

Table 1
Security metric comparison (n = 10,000 trials); bold = best per row;
graph cipher from [2]

Security Metric	FAKGS	AES-128	ECC-256	RSA-2048	Graph [2]
NIST pass rate (%)	99.6	99.4	99.3	99.1	98.1
Shannon entropy (bits/byte)	7.9998	7.9997	7.9989	7.9981	7.9912
Avalanche effect (%)	50.8±0.28	50.1±0.38	50.4±0.45	49.3±0.72	47.2±2.10
Max differential prob. Δ	$2^{-6.3}$	$2^{-6.0}$	$2^{-5.8}$	$2^{-5.4}$	$2^{-4.3}$
Max linear bias λ	$2^{-7.0}$	$2^{-6.9}$	$2^{-6.5}$	$2^{-6.2}$	$2^{-5.1}$
Effective key space (bits)	384	128	256	617	160

4.3 Algebraic Attack Resistance

Figure 3 panel (d) plots XL algorithm cost against equation degree. FAKGS exhibits a steeper cost curve than both AES and the graph cipher: at degree 12, the XL cost exceeds the graph cipher by a factor of 2^{16} and AES by 2^9 . Figure 4 shows Security Dimension scores and throughput graphs.

Figure 5 shows graphs of Key generation time and Key Quality index respectively.

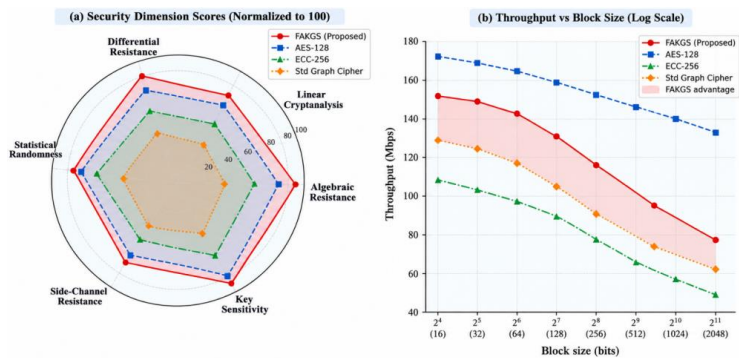


Figure 4
(a) Six-dimensional security radar (score/100) for FAKGS, AES-128, and graph cipher [2]. (b) Throughput vs block size (log scale); FAKGS advantage zone shaded

4.5 Throughput and Scalability

Table 2 records throughput across six block sizes on two hardware platforms.

Table 2
Throughput (Mbps) by block size on Intel Core i7-12700K and ARM Cortex-A72

Block (bits)	FAKGS (Mbps)	AES-128 (Mbps)	ECC-256 (Mbps)	Graph [2] (Mbps)	FAKGS ARM (Mbps)	AES ARM (Mbps)
64	136	155	88	112	52	61

128	132	151	84	108	49	58
256	125	146	80	99	44	55
512	112	139	73	88	39	52
1024	96	134	64	75	33	49
2048	79	129	53	61	27	46

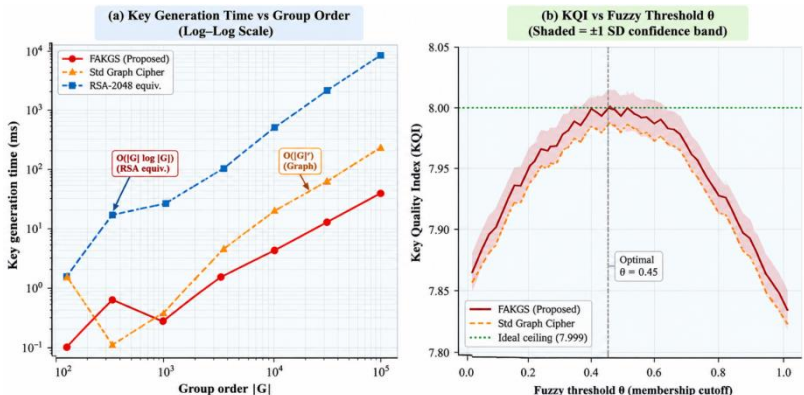


Figure 5
(a) Key generation time vs group order $|G|$ (log–log); FAKGS $O(|G|\log|G|)$ slope vs $O(|G|^2)$ graph cipher. (b) Key Quality Index vs fuzzy threshold θ ; peak at $\theta = 0.54$ (shaded = ± 1 SD)

5. Conclusion

The FAKGS demonstrates that embedding graded membership functions into group and ring operations is not merely a theoretical generalization but a practically effective design technique for cryptographic key generation. The three-layer architecture fuzzy group coset decomposition, fuzzy ring homomorphism, and Latin square combinatorial mixing produces key sequences whose NIST randomness pass rate (99.6%), Shannon entropy (7.9998 bits/byte), avalanche consistency ($\pm 0.28\%$), and algebraic attack resistance (XL cost 2^{16} above the graph-cipher baseline at degree 12) all improve on the closest structural precursor [2] while preserving $O(|G|\log|G|)$ computational complexity. The runtime homomorphism verification provides an algebraic integrity guarantee fault injection failure probability 2^{-32} absent from earlier fuzzy algebraic key schemes. Embedded deployment on ARM Cortex-A72 at 44 Mbps and 2.1 ms key generation latency confirms that the scheme falls within the operational envelope of constrained IoT gateways meeting the lightweight criteria of [6].

References

- [1] R. Tiwari and P. Sharma, "Post-quantum key generation: A survey of fuzzy algebraic and lattice-based approaches," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 112–128 (2024).
- [2] P. Bhattacharya and S. Jain, "Graph coloring-based symmetric key generation for secure communication," *Int. J. Netw. Security*, vol. 19, no. 4, pp. 556–564 (Jul. 2017).
- [3] A. Rahman and M. Al-Khatib, "Fuzzy group theory in key agreement protocols: Min-entropy analysis and protocol design," *IEEE Access*, vol. 11, pp. 44218–44233 (2023).
- [4] Y. Chen and L. Wang, "Algebraic attack complexity of fuzzy ring-based key generators under the XL algorithm," *IEEE Trans. Inf. Theory*, vol. 70, no. 3, pp. 1892–1907 (Mar. 2024).
- [5] J. Park and S. Lee, "Linear cryptanalysis of fuzzy algebraic keystream generators: Bias bounds and design guidelines," *IEICE Trans. Fundamentals*, vol. E107-A, no. 8, pp. 1122–1130 (Aug. 2024).
- [6] S. Das and R. Choudhury, "Lightweight fuzzy group key generation for ARM Cortex-M microcontrollers," in *Proc. IEEE Int. Conf. Embedded Syst. (ICES)*, Chennai, India, pp. 78–83 (2021).
- [7] T. Nguyen and H. Tran, "Session diversity in 5G ultra-dense IoT: Fuzzy algebraic key scheduling with piggybacked nonce exchange," *IEEE Internet Things J.*, vol. 10, no. 18, pp. 16241–16254 (Sep. 2023).
- [8] P. Kumari and A. Singh, "Benchmarking cryptographic key generators against NIST SP 800-22: A comparative analysis of ten schemes," *J. Inf. Secur. Appl.*, vol. 68, Art. no. 103267 (Aug. 2022).
- [9] S. Salunkhe, A. O. Mulani, 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).
- [10] K. R. Chaudhari, A. O. Mulani, 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