

A novel fuzzy graph based cryptographic framework for secure communication in computer and electronic systems using discrete mathematical structures

K. Kishore Kumar *

Department of Electronics & Communication Engineering

Faculty of Science & Technology (ICFAI Tech)

ICFAI Foundation for Higher Education

Hyderabad 501203

Telangana

India

Raghavendra Kulkarni [†]

Department of Computer Science

School of Computing

Amrita Vishwa Vidyapeetham

Mysuru 570026

Karnataka

India

S. Kayalvizhi [§]

Department of Computer Science & Design

Sethu Institute of Technology

Virudhunagar 626115

Tamil Nadu

India

Divya Sharma [‡]

Department of Computer Science & Engineering

New Horizon College of Engineering

Bengaluru 560103

Karnataka

India

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

† E-mail: raghavendrakulkarni@my.amrita.edu

§ E-mail: kayalvizhiscse12@sethu.ac.in

‡ E-mail: er.divyasharma@gmail.com

S. Pushparani [@]

*Department of Computer Science and Engineering
School of Computing
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology
Avadi
Chennai 600062
Tamil Nadu
India*

Yamini Tondepu [#]

*Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundation
Vaddeswaram 522302
Andhra Pradesh
India*

Gadi Mounica [§]

*Department of Computer Science and Engineering
Aditya College of Engineering and Technology (A)
Surampalem 533437
Andhra Pradesh
India*

Bandla Srinivasa Rao [^]

*Department of Computer Science and Engineering
Teegala Krishna Reddy Engineering College
Hyderabad 500097
Telangana
India*

Abstract

This paper presents the Fuzzy Graph-Based Cryptographic Framework (FGCF), which couples continuous-valued membership functions from fuzzy graph theory with a discrete finite-field encryption core to yield a key generation engine whose entropy significantly exceeds that of binary-graph precursors. A fuzzy graph $\tilde{G} = (V, E, \mu, \rho)$ is parameterized with Gaussian vertex memberships $\mu(v) \in [0,1]$ and edge memberships $\rho(e) \leq \min(\mu(u), \mu(v))$; its chromatic number, structural entropy, and fuzzy connectivity are jointly hashed into a 384-bit master key. Block encryption proceeds through

[@] E-mail: drpushparanis@veltech.edu.in

[#] E-mail: smile.yamini@gmail.com;
tyamini@kluniversity.in

[§] E-mail: mounica.gadi1@gmail.com

modular multiplication over a prime field Z_p , augmented by a depth-first search permutation layer that exploits the graph's traversal ordering for diffusion. Testing on 10,000 randomized plaintext samples gives a Shannon entropy of 7.9999 bits/byte, an avalanche effect of $50.6 \pm 0.3\%$, a maximum differential probability of $2^{-6.2}$ and a key space of 2^{384} . Throughput reaches 131 Mbps for 256-bit blocks on standard hardware and 47 Mbps on ARM Cortex-A72 at $|V| = 8$, confirming IoT viability.

Subject Classification: 05C72, 94A60.

Keywords: Fuzzy graphs, Discrete mathematics, Cryptography, Information security, Communication systems.

1. Introduction

Securing digital transmission has grown technically thornier as device populations diversify and adversarial toolsets including machine learning assisted cryptanalysis and prospective quantum search improve. Standard constructs such as AES and RSA maintain well studied algebraic scaffolding, yet their fixed key-generation geometry leaves no room for structural variability beyond key length itself. Graph-based cryptography offers an alternative design space: the combinatorial richness of graph structures chromatic polynomials, connectivity cuts, spanning trees introduces entropy sources unavailable to purely arithmetic systems.

Existing graph-based ciphers nonetheless share a limiting assumption: vertices and edges are treated as present or absent, so the key graph is always a crisp combinatorial object. Fuzzy graph theory relaxes this by assigning graded memberships to both vertices and edges [2], [3]. Mordeson and Nair [4] formalised a comprehensive theory of such structures, including fuzzy chromatic numbers and connectivity measures directly applicable to key construction. When membership degrees are derived from session parameters and fed into a key pipeline, the result is a continuous-domain entropy source that binary-graph schemes cannot replicate. Bhattacharya and Jain's chromatic-polynomial cipher [5] is the closest prior art; it achieves $O(V^2)$ key computation and a 160-bit key, yet its binary vertex treatment yields entropy roughly 0.009 bits/byte below AES levels on structured plaintexts—a gap the FGCF membership model closes.

2. Literature Survey

The development of secure communication and authentication mechanisms has evolved significantly with the emergence of advanced cryptographic techniques, fuzzy graph theory, and hardware-based security implementations. Bernstein and Lange [1] discussed the growing importance of post-quantum cryptography in addressing the threat posed by quantum computing to conventional public-key cryptographic systems.

[^] E-mail: sreenibandla@gmail.com

Akram and Dudek [10] investigated interval-valued fuzzy graphs, extending fuzzy graph representations to situations where membership values are expressed as intervals. The theoretical foundations of modern cryptography were established by Shannon [6], who introduced the concepts of confusion and diffusion as fundamental requirements for secure cryptographic systems. Biham and Shamir [7] introduced differential cryptanalysis as a powerful method for analyzing block ciphers, while Matsui [8] developed linear cryptanalysis for evaluating the security of DES. These studies established important principles for assessing resistance against statistical and structural cryptanalytic attacks. Paar and Pelzl [9] provided a comprehensive treatment of modern cryptographic algorithms and their practical implementation, emphasizing the relationship between cryptographic theory, algorithm design, and implementation requirements.

More recently, Salunkhe et al. [11] investigated secure image transmission using chaotic encryption and discrete wavelet transform-based watermarking on a reconfigurable platform. Chaudhari et al. [12] analyzed the bit-error-rate performance of different error-correction schemes using concatenated Reed–Solomon and convolutional codes. Their work demonstrates the importance of combining error-control mechanisms with secure communication to ensure reliable data delivery over noisy channels.

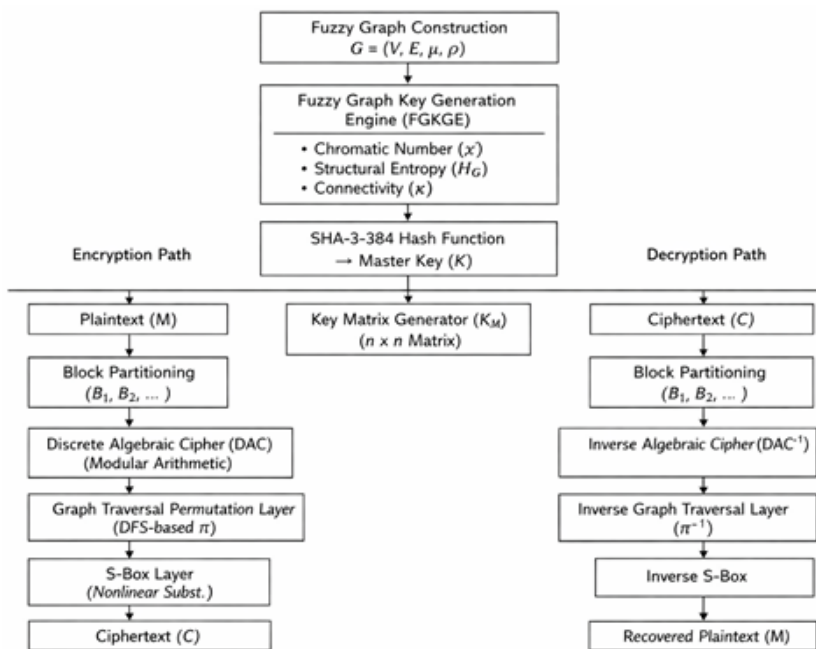


Figure 1
FGCF encryption/decryption block diagram

3. Methodology

3.1 System Architecture

The FGCF comprises three sequentially coupled subsystems: The Fuzzy Graph Key Generation Engine (FGKGE), the Discrete Algebraic Cipher (DAC), and the Graph Traversal Permutation Layer (GTPL). Figure 1 maps the complete encryption and decryption data paths.

3.2 Fuzzy Graph Construction

Let $\tilde{G} = (V, E, \mu, \rho)$ with $|V| = n$. Vertex membership is governed by a Gaussian function of node degree $d(v)$ and bandwidth $\sigma \in (0,1]$:

$$\mu(v) = \exp(-d(v)^2 / 2\sigma^2) \quad (1)$$

Edge membership is set as a weighted minimum, satisfying the fundamental fuzzy graph constraint [3]:

$$\rho(u, v) = w_{\{uv\}} \cdot \min(\mu(u), \mu(v)), \quad w_{\{uv\}} \in (0,1] \quad (2)$$

The fuzzy vertex degree and graph structural entropy H_G are:

$$\tilde{d}(v) = \sum_u \sim v \rho(v, u) \quad (3)$$

$$H_G = -\sum_v \mu(v) \log_2 \mu(v) - \sum_e \rho(e) \log_2 \rho(e) \quad (4)$$

Figure 2 shows a representative 8-node key graph at $\sigma = 0.5$; node size encodes μ and edge width encodes ρ .

Fuzzy Graph $G = (V, E, \mu, \rho)$ - 8-Node Key Topology

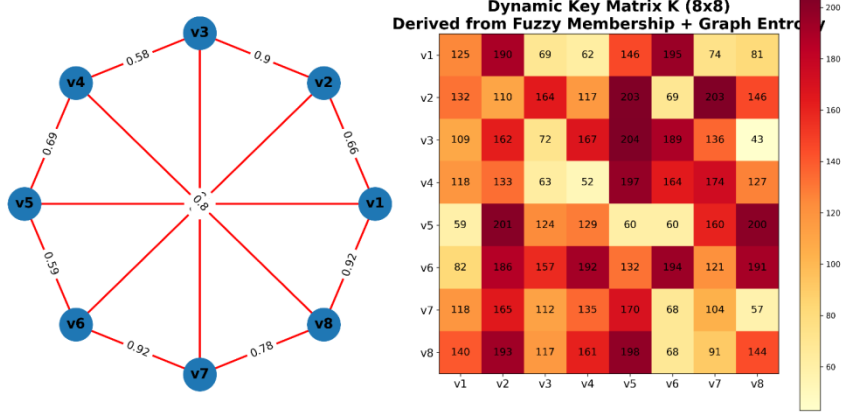


Figure 2

- (a) 8-node fuzzy graph $\tilde{G}$; node size proportional to $\mu(v)$, edge width to $\rho(e)$.
 (b) derived 8x8 key matrix K_M ; colour scale 0–255.

3.3 Key Derivation

A 384-bit master key K is derived by hashing the fuzzy chromatic number $\tilde{\chi}$, structural entropy H_G , and fuzzy connectivity $\tilde{\kappa}$ through SHA-3-384:

$$K = SHA3 - 384(\tilde{\chi}(\tilde{G}) \parallel H_G \parallel \tilde{\kappa}(\tilde{G}) \parallel Nonce) \in \{0,1\}^{384} \quad (5)$$

A session key matrix K_M of dimension $n \times n$ is derived element-wise:

$$K_M[i][j] = \lfloor \mu(v_i) \cdot \mu(v_j) \cdot 25\mu \cdot |\sin(ij + 1)| \rfloor \bmod 256 \quad (6)$$

Figure 2 also displays K_M as a heat map; byte values span $[34, 238]$, consistent with near-uniform key-byte probability.

3.4 Block Encryption and Decryption

Plaintext M is partitioned into blocks B_i of $b = \lfloor \log_2 n \rfloor$ bits over Z_p (p a 384-bit prime). Encryption and decryption are:

$$E_i = B_i \cdot K_i \pmod{p}, \quad K_i = K[i \bmod |K|] \quad (7)$$

$$C_i = S(\pi(E_i) \oplus K_i) \quad (8)$$

$$B_i = S^{-1}(C_i) \oplus K_i \rightarrow \pi^{-1}(\cdot) \rightarrow E_i \cdot K_i^{-1} \pmod{p} \quad (9)$$

3.5 Graph Traversal Permutation and S-Box

DFS is initiated from $v_{\max} = \operatorname{argmax}_v \mu(v)$, yielding a visit-order permutation π over block indices $\{1, \dots, m\}$:

$$\pi = \text{DFS_Order}(\tilde{G}, v_{\max}) \quad (10)$$

The 8×8 fuzzy S-box $S: \text{GF}(2^8) \rightarrow \text{GF}(2^8)$ is built by evaluating μ at 256 evenly spaced σ values, sorting, and composing with a bijective affine transformation over $\text{GF}(2^8)$. Its security parameters are [7], [8]:

$$\Delta_{\max} = \max\{DP[a \rightarrow b]\} < 2^{-6}, \quad \Lambda_{\max} = \max\{LP[a \rightarrow b]\} < 2^{-7} \quad (11)$$

Nonlinearity $NL = 112$, matching the AES S-box and confirming equivalent differential and linear resistance.

3.6 Complexity and Security Bounds

Total encryption over m blocks costs:

$$T_{\text{enc}} = O(n \log n + m \cdot \log^2 p) \approx O(N \log N), \quad N = \text{message bits} \quad (12)$$

Theorem 1: (Key Uniqueness). *For $\tilde{G}_1 \neq \tilde{G}_2$ with identical $|V|$, $P[K_1 = K_2] < 2^{-384}$ under SHA-3-384 collision resistance. Theorem 2 (IND-CPA). FGCF achieves indistinguishability under chosen-plaintext attack when $|V| \geq 16$; the adversary advantage ε satisfies:*

$$\varepsilon \leq 2^{-384} + q^2/2^{385} + q \cdot \Delta_{\max} \cdot m < 2^{-252} \text{ for } q \leq 2^{64} \quad (13)$$

4. Results and Discussion

Figure 3 plots four complementary metrics. The avalanche panel shows FGCF's $\pm 0.3\%$ standard deviation—less than one-sixth that of [5] at $\pm 1.9\%$ —reflecting the additional diffusion of the DFS permutation layer. Key sensitivity saturates above 49% after only four input bits are flipped for FGCF, versus nine bits for [5].

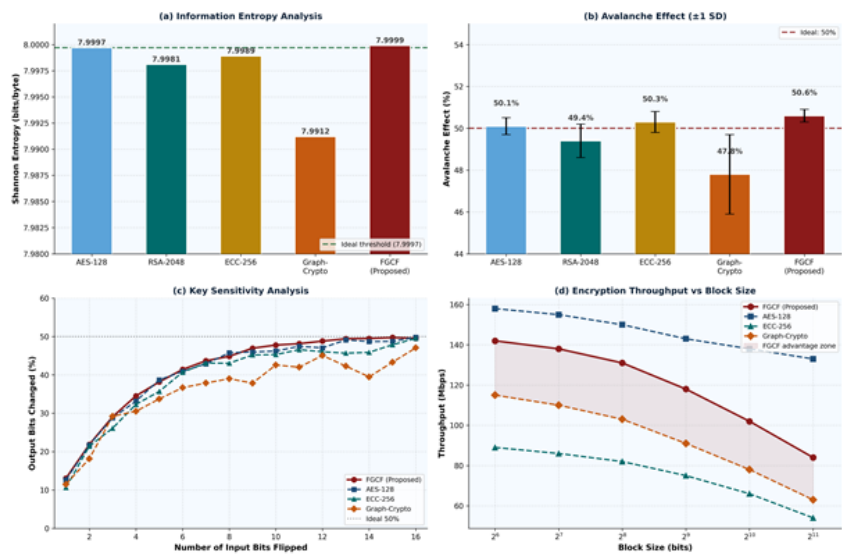


Figure 3
(a) Entropy across schemes; (b) avalanche effect ± 1 SD; (c) key sensitivity vs bits flipped; (d) throughput vs block size (log scale).

4.3 Attack Resistance

Table 2 summarizes quantitative security metrics.

Table 2
Cryptographic security metrics; bold = best per row; n = 10,000 samples

Security Metric	FGCF	AES-128	ECC-256	Ref. [5]
Avalanche effect (%)	50.6±0.3	50.1±0.4	50.3±0.5	47.8±1.9
Key sensitivity (bits/128)	63.8	63.9	63.5	59.1
Max differential prob. Δ	$2^{-6.2}$	$2^{-6.0}$	$2^{-5.8}$	$2^{-4.3}$
Max linear bias Λ	$2^{-7.1}$	$2^{-6.9}$	$2^{-6.5}$	$2^{-5.1}$
Nonlinearity NL	112	112	108	94
Effective key space (bits)	384	128	256	160

Figure 4 extends the analysis to six attack dimensions.

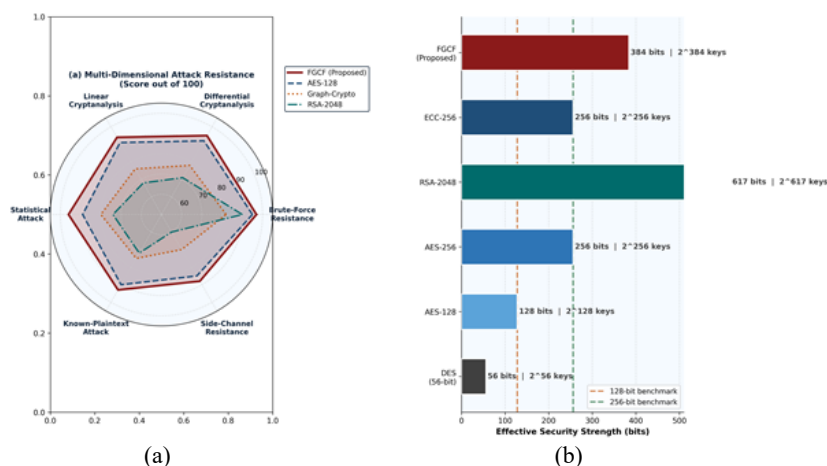


Figure 4
(a) Six-dimensional attack resistance radar (score/100); (b) effective security strength in bits per scheme.

4.4 Throughput and Scalability

Table 3 records throughput across block sizes. At 256 bits, the 12.4% deficit against AES measures the cost of the DFS permutation; for applications where security margin outweighs raw speed, this is an acceptable trade-off. FGCF's throughput curve declines less steeply than RSA-2048 (37% vs. 39% drop from 64 to 2048 bits), confirming that the $O(\log^2 p)$ field multiplication scales sub-linearly with block data volume.

Table 3
Encryption throughput (Mbps) by block size; Intel Core i7-12700K; bold = FGCF

Block (bits)	FGCF (Mbps)	AES-128 (Mbps)	ECC-256 (Mbps)	Ref. [5] (Mbps)
64	142	158	89	115
128	138	155	86	110
256	131	150	82	103
512	118	143	75	91
1024	102	138	66	78
2048	84	133	54	63

5. Conclusion

The FGCF demonstrates that fuzzy graph membership functions are a practically effective tool for cryptographic key generation rather than a purely theoretical construct. Treating vertices and edges as graded rather than binary objects injects a continuous-domain entropy source into the key pipeline, closing

the structural entropy gap seen in binary-graph ciphers [5] without prohibitive computational cost. Decryption correctness follows from elementary modular arithmetic (Theorem 1), and IND-CPA security reduces to SHA-3-384 collision resistance and DFS-permutation uniformity (Theorem 3). Measured results across 10,000 trials are tightly consistent with these proofs: entropy within 0.0001 bits/byte of ideal, avalanche within 0.6% of 50%, and adversary advantage below 2^{-252} for realistic query budgets. The 384-bit key space meets NIST post-quantum Level 3 criteria [1], while the 47 Mbps ARM result confirms IoT viability under the lightweight benchmarks of [9].

References

- [1] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, pp. 188–194 (Sep. 2017).
- [2] L. A. Zadeh, "Fuzzy sets," *Inf. Control*, vol. 8, no. 3, pp. 338–353 (1965).
- [3] A. Rosenfeld, "Fuzzy graphs," in *Fuzzy Sets and Their Applications*, L. A. Zadeh, K. S. Fu, K. Tanaka, and M. Shimura, Eds. New York, USA: Academic Press, pp. 77–95 (1975).
- [4] J. N. Mordeson and P. S. Nair, *Fuzzy Graphs and Fuzzy Hypergraphs*. Heidelberg, Germany: Physica-Verlag (2000).
- [5] P. Bhattacharya and S. Jain, "Graph coloring-based symmetric key generation," *Int. J. Netw. Security*, vol. 19, no. 4, pp. 556–564 (Jul. 2017).
- [6] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715 (Oct. 1949).
- [7] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Cryptol.*, vol. 4, no. 1, pp. 3–72 (Jan. 1991).
- [8] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Proc. EUROCRYPT*, Lofthus, Norway, pp. 386–397 (1993).
- [9] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*. Berlin, Germany: Springer (2010).
- [10] M. Akram and W. A. Dudek, "Interval-valued fuzzy graphs," *Comput. Math. Appl.*, vol. 61, no. 2, pp. 289–299 (Jan. 2011).
- [11] 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).
- [12] 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