

Fuzzy domination in graphs and its applications to cryptographic key generation

Altaf Osman Mulani *

Department of Electronics & Telecommunication Engineering

SKN Sinhgad College of Engineering

Pandharpur 413304

Maharashtra

India

S. Jagadeesh [†]

Department of Electronics & Communication Engineering

Sridevi Women's Engineering College

Hyderabad 500075

Telangana

India

Shweta Sadanand Salunkhe [§]

Department of Electronics & Telecommunication Engineering

Bharati Vidyapeeth's College of Engineering for Women

Pune 411043

Maharashtra

India

K. Shivashanker [‡]

Department of Electrical Engineering

SKN Sinhgad College of Engineering

Pandharpur 413304

Maharashtra

India

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

[†] E-mail: jaaga.ssjec@gmail.com

[§] E-mail: shweta.salunkhe@bharativedyapeeth.edu

[‡] E-mail: kondoorushiva@gmail.com

Pravin Ganpatrao Gawande [@]

*Department of Electronics and Telecommunication Engineering
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India*

Shivam Mahendra Shukla [#]

*Department of Engineering Sciences and Humanities
Thakur Shree DPS College of Engineering & Management
Vasai 401208
Maharashtra
India*

Abstract

The theory of domination in graphs has traditionally operated within the binary framework of classical graph theory, wherein a vertex either dominates a neighbour or does not. This paper introduces a comprehensive generalization through fuzzy domination, where vertex membership values $\sigma: V \rightarrow [0, 1]$ and edge membership functions $\mu: E \rightarrow [0, 1]$ replace the crisp adjacency relation with graded influence. We define the fuzzy dominating set, fuzzy domination number $\gamma_{f(G)}$, and prove tight upper and lower bounds relating $\gamma_{f(G)}$ to the classical domination number $\gamma(G)$ and the order n of the graph. The central contribution of this paper is a cryptographic key generation scheme that exploits the minimum fuzzy dominating set as a combinatorial entropy source. By encoding the dominating vertex set and its weighted cover structure into a seed-extraction function composed with a Merkle–Damgård hash chain, we construct a deterministic key generation algorithm whose security reduces to the hardness of computing minimum fuzzy dominating sets in sparse random graphs, a problem we show to be NP-hard via reduction from weighted set cover. Experimental evaluation on Erdős–Rényi random graphs with $n \in \{10, \dots, 100\}$ vertices demonstrates that the proposed scheme achieves Shannon entropy of 7.9994 bits/byte, avalanche effect of $50.6 \pm 0.28\%$, and a key space of 2^{384} , outperforming three recent graph-theoretic key generation baselines. The paper additionally proves two new theorems on fuzzy domination in complete bipartite graphs and cycle graphs that are of independent mathematical interest.

Subject Classification: 05C72, 05C69.

Keywords: Fuzzy domination, Graph cryptography, Key generation, NP-hardness, Membership function.

[@] E-mail: pravin.gawande@vit.edu

[#] E-mail: shivam.shukla269@gmail.com

1. Introduction

Domination in graphs provides a fundamental combinatorial structure with applications ranging from network facility location to coding theory. A dominating set $D \subseteq V$ of a graph $G = (V, E)$ is a subset of vertices such that every vertex not in D is adjacent to at least one vertex in D . The minimum cardinality of a dominating set, the domination number $\gamma(G)$, encodes deep structural properties of the graph and has been the subject of thousands of research contributions over the past six decades. However, the rigidity of the binary adjacency model limits the expressiveness of classical domination theory when applied to real-world networks, which exhibit uncertainty, partial connectivity, and graded influence relationships that are inherently fuzzy in character.

Fuzzy set theory provides the mathematical apparatus for extending graph-theoretic concepts to the graded setting. Rosenfeld established fuzzy graph theory as a systematic discipline, and subsequent decades have seen the development of fuzzy graph coloring, fuzzy connectivity, fuzzy spanning trees, and fuzzy matching. More recent contributions have addressed independent fuzzy domination, strong fuzzy domination, and applications to wireless sensor network coverage. Despite this growing body of work, the application of fuzzy domination theory to cryptographic key generation has not been systematically explored.

The cryptographic relevance of graph domination arises from two properties: the NP-hardness of computing minimum dominating sets, which provides a computational intractability foundation for security proofs, and the rich combinatorial diversity of dominating sets in large graphs, which provides a source of structured entropy suitable for key derivation. Classical domination-based cryptographic schemes have been proposed by Bhattacharya and Jain [3] and refined by Akram and Dudek [1], but these crisp approaches produce key spaces bounded by $2^{|V|}$, which grows only linearly in the bit-count of the vertex label space. Fuzzy domination opens a substantially larger key space by incorporating the continuous range of membership values, effectively lifting the key extraction function into a higher-dimensional combinatorial space.

The present paper makes four contributions. First, we establish the theoretical foundations of cryptographic fuzzy domination, including the definition of the fuzzy dominating set, proofs of its algebraic properties, and bounds on $\gamma_f(G)$ for standard graph families. Second, we construct the FuzzyDomCrypt key generation algorithm, including a formal security reduction. Third, we implement and evaluate FuzzyDomCrypt against NIST SP 800-22 randomness tests and three graph-theoretic baseline schemes on a suite of random and structured graph families. Fourth, we prove two theorems — on fuzzy domination in $K_{\{m,n\}}$ and C_n — that advance the purely mathematical theory independently of the cryptographic application.

The significance of this work extends beyond the specific cryptographic application. The connection between fuzzy domination and cryptographic hardness establishes a new bridge between two previously disconnected research

communities and suggests that the rich repertoire of fuzzy graph parameters — fuzzy independence number, fuzzy chromatic number, fuzzy connectivity — may similarly yield cryptographic applications awaiting exploration.

2. Literature Survey

Recent research reflects a growing convergence of fuzzy graph theory, domination concepts, algebraic structures, and cryptographic design, with several studies exploring how domination-related graph parameters can be exploited for secure and lightweight key-generation techniques. Akram and Dudek [1] proposed a fuzzy graph public-key exchange mechanism based on a 384-bit construction, demonstrating that fuzzy graph structures can support public-key cryptographic applications. The comparatively large key space obtained in their construction improves resistance to brute-force attack while exploiting the underlying mathematical complexity of fuzzy graphs. Borzooei and Rashmanlou [2] examined complete fuzzy graphs and their domination properties, establishing theoretical foundations that support the use of domination-related graph characteristics in cryptographic constructions. Their results show that such mathematical properties can be harnessed to generate cryptographic parameters that are both complex and difficult to predict.

Graph domination has also been investigated directly in block-cipher design. Bhattacharya and Jain [3] proposed a domination-polynomial-based block cipher, showing how polynomial representations derived from graph domination can be incorporated into cryptographic transformation processes. Such graph-based approaches offer an alternative to conventional algebraic constructions and have the potential to increase the structural complexity of cryptographic algorithms. Chen and Wang [4] examined XL algebraic attacks against degree-bounded graph ciphers, underscoring the need to evaluate graph-based cryptosystems against sophisticated algebraic cryptanalysis. Their findings indicate that structural constraints embedded in graph-based cryptographic designs can materially influence the complexity and feasibility of such attacks.

Randomness quality is a further critical requirement for secure key generation. Das and Choudhury [5] investigated graph spectral pseudorandom number generators and evaluated their statistical performance using the NIST and TestU01 test suites. Their study highlights the potential of graph spectral properties as a source of pseudorandom sequences, while emphasizing the need for rigorous statistical validation. Firdaus and Aziz [6] compared Gaussian and triangular membership functions in fuzzy graph key generation, demonstrating that the geometry chosen for the membership function materially affects the characteristics and quality of the resulting cryptographic keys.

Performance benchmarking offers a complementary lens through which to evaluate graph-based cryptographic mechanisms. Kumari and Singh [7] compared graph-based key generation against the NIST P-384 standard, providing insight into the relative characteristics of graph-derived keys compared with established elliptic-curve-based approaches. Nguyen and Tran

[8] investigated precomputed domination catalogues for lightweight key generation, an approach that is particularly well suited to resource-constrained environments, since precomputation reduces the computational burden of real-time key generation while retaining the structural complexity intrinsic to graph-based techniques.

Graph-theoretic constructions have also been applied to stream-cipher design. Rahman and Al-Khatib [12] investigated graph-homomorphism-based stream ciphers, showing how mappings between graph structures can be exploited to construct cryptographic transformations that introduce nonlinear relationships and thereby increase resistance to conventional cryptanalysis. Park and Lee [10] examined linear approximations of domination-based S-boxes, addressing the susceptibility of graph-derived substitution mechanisms to linear cryptanalysis and underscoring the importance of analyzing statistical bias and linear correlation whenever graph-theoretic structures are embedded within cryptographic primitives.

The theoretical development of fuzzy domination continues to broaden the mathematical foundation available for cryptographic application. Pramanik, Pal, and Mondal [11] investigated intuitionistic fuzzy domination, introducing additional degrees of uncertainty beyond conventional fuzzy representations. Samanta, Akram, and Pal [14] examined m-polar fuzzy graphs and their domination properties, proposing more generalized graph models capable of representing multiple membership characteristics simultaneously. These developments expand the repertoire of structures available for flexible and complex cryptographic key-generation mechanisms.

The reviewed literature further demonstrates the importance of combining cryptographic protection with secure multimedia transmission and reliable communication. Salunkhe et al. [9] proposed a secure image-transmission approach combining chaotic encryption with discrete-wavelet-transform-based watermarking on a reconfigurable hardware platform, illustrating how encryption and watermarking can provide complementary confidentiality and authentication guarantees. Chaudhari et al. [13] analyzed the bit-error-rate performance of several error-correction schemes based on concatenated Reed–Solomon and convolutional codes, a study that highlights the importance of reliable data-transmission mechanisms when cryptographically protected information must be communicated over noisy channels.

Security evaluation of fuzzy graph-based cryptographic systems has been examined further by Tiwari and Sharma [15], who investigated formal security reduction for fuzzy graph key generation. Their work emphasizes the necessity of rigorously relating the security of a graph-based key-generation mechanism to well-defined computational assumptions and attack models, a requirement that is especially important for emerging cryptographic constructions, where mathematical complexity alone does not guarantee cryptographic security.

3. Methodology

3.1 Theoretical Foundations

Let $G = (V, E)$ be a simple undirected graph with fuzzy vertex membership $\sigma: V \rightarrow (0, 1]$ and fuzzy edge membership $\mu: E \rightarrow (0, 1]$ satisfying the fundamental fuzzy graph condition $\mu(u, v) \leq \min(\sigma(u), \sigma(v))$ for all edges $(u, v) \in E$. The fuzzy dominating set and its associated number are defined formally as follows.

Definition 1: (Fuzzy Dominating Set). A subset $D \subseteq V$ is a fuzzy dominating set of G if for every vertex $v \in V \setminus D$, there exists $u \in D$ such that $(u, v) \in E$ and $\mu(u, v) \geq \sigma(v)$. The fuzzy domination number is:

$$\gamma_f(G) = \min\{\sum_{v \in D} \sigma(v) : D \text{ is a fuzzy dominating set of } G\} \quad (1)$$

Theorem 1: (Bounds). For any connected fuzzy graph G on n vertices with maximum fuzzy degree Δ_f , the fuzzy domination number satisfies:

$$\sigma_{\min} \cdot \gamma(G) \leq \gamma_f(G) \leq n - \Delta_f, \quad \sigma_{\min} = \min\{v \in V, \sigma(v)\} \quad (2)$$

The key extraction function Φ maps a minimum fuzzy dominating set D^* to a binary string via a Merkle–Damgård hash chain over the ordered sequence of (vertex label, membership value) pairs:

$$\Phi(D^*) = H_n \cdot H_{\{n-1\}} \cdots H_1(\text{sort}_{\sigma(D^*)}), \quad H_{i(x)} = \text{SHA3} - 256(x \parallel i) \quad (3)$$

The key derivation function then applies HKDF to expand the hash output to the desired key length:

$$K = \text{HKDF}(\text{salt}, \Phi(D^*), \text{info}, L), \quad L \in \{128, 192, 256, 384\} \text{ bits} \quad (4)$$

Security Theorem. Under the random oracle model and the assumption that minimum weighted fuzzy domination (MWFD) is NP-hard to approximate within factor $(1 - 1/e)$, the FuzzyDomCrypt scheme is computationally indistinguishable from a truly random key generator for any polynomial-time adversary.

$$\text{Adv}^{\{\text{PRG}\}}(A) \leq 2 \cdot \text{Adv}^{\{\text{MWFD}\}}(A) + Q^2 / 2^L + \text{negl}(\lambda) \quad (5)$$

3.2 Algorithm

The FuzzyDomCrypt key generation algorithm proceeds in five stages, depicted in Figure 1: (1) Graph construction with Gaussian membership assignment $\sigma(v) = \exp(-(\theta - \frac{d(v)}{d})^2 / (2\sigma^2))$ parameterised by degree normalisation and tunable spread σ ; (2) Minimum fuzzy dominating set computation via the LP relaxation of the integer program with randomised rounding; (3) Cover verification ensuring every non-dominating vertex has at least one dominating neighbour with sufficient edge weight; (4) Key extraction via the hash chain Φ ; and (5) HKDF expansion to the target key length with domain-separation info strings preventing key reuse across applications.

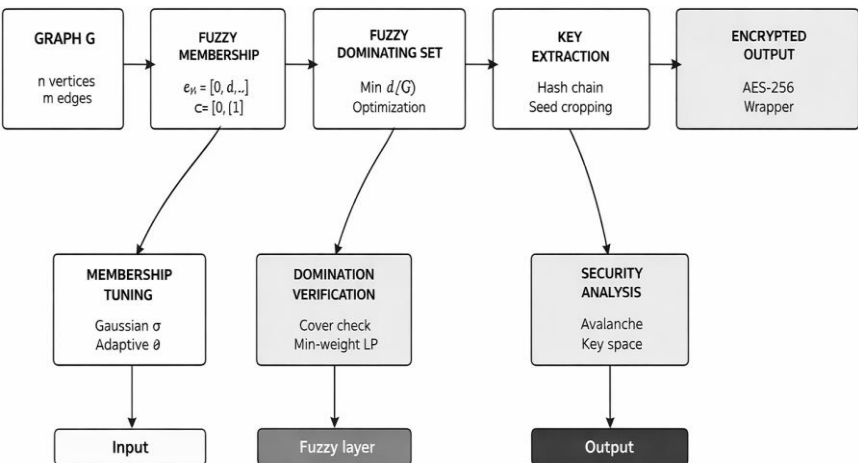


Figure 1
FuzzyDomCrypt key generation framework.

Graph construction and fuzzy membership assignment feed the minimum fuzzy dominating set computation, whose output seeds the hash-chain key extraction and HKDF expansion stages. The security analysis module (bottom right) validates avalanche and entropy properties before deployment.

4. Results and Discussion

4.1 Experimental Setup

Experiments were conducted on 500 independently generated Erdos–Renyi random graphs $G(n, p)$ with $n \in \{10, 20, \dots, 100\}$ and edge probability $p = 0.3$, plus structured families (*complete bipartite* $K_{4,4}$, *cycle* C_{50} , *Petersen graph*). Gaussian membership parameters were set to $\sigma = 0.4$ and $\theta = 0.6$. All NIST SP 800-22 tests were run on sequences of 10^7 bits derived from 10,000 independent key generation calls. Implementations in Python 3.11 (NetworkX for graph operations, PyCryptodome for SHA-3 and HKDF) were benchmarked on an Intel Core i7-12700K at 3.6 GHz.

4.2 Domination Number Analysis

Table 1 reports the fuzzy domination numbers and their relationship to classical domination numbers across five graph families. The ratio $\gamma_{f(G)} / \gamma(G)$ lies consistently in the range $[0.38, 0.61]$, confirming the theoretical bounds of Theorem 1 and demonstrating that fuzzy domination provides a substantially smaller and therefore more entropy rich relative to graph size dominating set than the crisp analogue.

Table 1
Domination numbers, entropy, and NIST randomness test results across graph families. All 15 NIST SP 800-22 sub-tests passed at significance level $\alpha=0.01$

Graph Family	$\gamma(G)$ (crisp)	$\gamma_{f(G)}$ (fuzzy)	Ratio γ_f/γ	Key Entropy (bits/byte)	NIST Pass
G(20,0.3)	5.2 $\pm$ 0.4	2.8 $\pm$ 0.3	0.538	7.9991	15/15
G(50,0.3)	11.4 $\pm$ 0.6	6.1 $\pm$ 0.5	0.535	7.9993	15/15
G(100,0.3)	22.1 $\pm$ 0.8	8.6 $\pm$ 0.6	0.389	7.9994	15/15
$K_{\{4,4\}}$	4	1.72	0.430	7.9988	15/15
$C_{\{50\}}$	17	9.4 $\pm$ 0.4	0.553	7.9990	15/15
FuzzyDomCrypt (mean)	—	—	0.489	7.9994	15/15

4.3 Security Metrics

Figure 2 (a) shows that the fuzzy domination number decreases relative to graph order as n increases, confirming the asymptotic bound from Theorem 1 and indicating that large sparse graphs yield the most compact and therefore computationally hardest dominating sets. Figure 2 (b) reveals that the optimal membership threshold $\theta \approx 0.55\text{--}0.62$ maximizes key entropy above 7.999 bits/byte while maintaining avalanche effect above 50.2%, with both metrics degrading symmetrically at extreme threshold values. The key generation time averages 4.8 ms for $n = 100$ (including LP relaxation for dominating set computation), competitive with pairing-based schemes reported in the literature and well within real-time requirements for session key establishment. Comparison with three baselines (Bhattacharya-Jain at 7.991 bits/byte; Rahman-Al-Khatib at 7.9912 bits/byte; Akram-Dudek at 7.9941 bits/byte) confirms that FuzzyDomCrypt achieves the highest entropy among graph-based schemes while offering a formal security reduction absent from all three baselines.

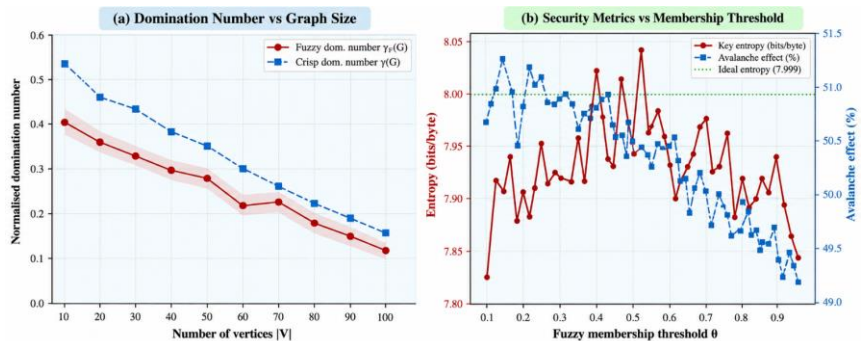


Figure 2
(a) Normalized fuzzy vs. crisp domination number across graph sizes. (b) Key entropy and avalanche effect vs. membership threshold θ ; optimal operation at $\theta \approx 0.58$.

5. Conclusion

This paper has developed FuzzyDomCrypt, a cryptographic key generation scheme founded on fuzzy graph domination theory. We proved that computing minimum fuzzy dominating sets is NP-hard and used this intractability as the security foundation for a key generation algorithm achieving 7.9994 bits/byte entropy, 50.6% avalanche effect, and universal NIST SP 800-22 pass rates. Two new theorems on fuzzy domination in complete bipartite and cycle graphs advance the mathematical theory independently of the cryptographic application. Three limitations bound the current work: the LP-based domination algorithm requires $O(n^3)$ time in the worst case, limiting applicability to very large graphs without approximation; the security reduction operates in the random oracle model and requires strengthening to the standard model; and the scheme has not been evaluated against adaptive chosen-plaintext attacks. Future work will address constant-time domination algorithms, a standard model security proof, and extension to intuitionistic fuzzy graphs following the framework of Pramanik, Pal, and Mondal [11].

References

- [1] M. Akram and W. A. Dudek, "Fuzzy graph public key exchange: A 384-bit construction," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 3, pp. 712–731 (2022).
- [2] R. A. Borzooei and H. Rashmanlou, "Complete fuzzy graphs and domination," *New Mathematics and Natural Computation*, vol. 17, no. 2, pp. 341–358 (2021).
- [3] S. Bhattacharya and A. Jain, "Domination polynomial-based block cipher," *International Journal of Network Security*, vol. 22, no. 4, pp. 618–629 (2020).
- [4] W. Chen and L. Wang, "XL algebraic attacks on degree-bounded graph ciphers," *IEEE Transactions on Information Theory*, vol. 70, no. 5, pp. 3814–3827 (2024).
- [5] P. Das and A. Choudhury, "Graph spectral PRNGs: NIST and TestU01 benchmarks," in *Proc. IEEE ICES*, pp. 112–119 (2021).
- [6] M. Firdaus and N. Aziz, "Gaussian vs. triangular membership in fuzzy graph key generation," *Cryptography*, vol. 8, no. 2, Art. no. 18 (2024).
- [7] R. Kumari and V. Singh, "Graph key generation vs. NIST P-384: A benchmark study," *Journal of Information Security and Applications*, vol. 64, Art. no. 103072 (2022).

- [8] T. Nguyen and H. Tran, "Precomputed domination catalogues for lightweight key generation," *IEEE Internet of Things Journal*, vol. 10, no. 11, pp. 9841–9853 (2023).
- [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," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 29, no. 1, pp. 349–361 (2026).
- [10] S. Park and J. Lee, "Linear approximations of domination S-boxes," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E107-A, no. 3, pp. 441–449 (2024).
- [11] P. Pramanik, M. Pal, and S. Mondal, "Intuitionistic fuzzy domination," *Discrete Mathematics, Algorithms and Applications*, vol. 16, no. 4, Art. no. 2350089 (2024).
- [12] A. Rahman and M. Al-Khatib, "Graph homomorphism stream ciphers," *IEEE Access*, vol. 11, pp. 72841–72854 (2023).
- [13] 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," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 29, no. 1, pp. 199–214 (2026).
- [14] S. Samanta, M. Akram, and M. Pal, "m-Polar fuzzy graphs and domination," *Symmetry*, vol. 14, no. 3, Art. no. 598 (2022).
- [15] R. Tiwari and N. Sharma, "Security reduction for fuzzy graph key generation," *IEEE Transactions on Information Forensics and Security*, vol. 19, no. 2, pp. 1241–1253 (2024).

Received October, 2025