RESEARCH PAPER

Adaptive Phi-Evolutionary Key Scheduling Framework for Hybrid and Lightweight Cryptosystems with Multi-Metric Cryptanalysis Validation

Suvendu Kumar Jena[1], Priyabrata Sahu[2], Rajesh Kumar Pati[3]

[1,2,3]Department of Computer Science Engineering and Applications, Indira Gandhi Institute of Technology, Sarang, India

Emails: SuvenduKumarJena@gmail.com, priyabsahu@gmail.com, kumar.rajeshpati@gmail.com

***Corresponding author: Suvendu Kumar Jena, Department of Computer Science Engineering and Applications, Indira Gandhi Institute of Technology, Sarang, India. Email: SuvenduKumarJena@gmail.com**

Abstract— This paper proposes an adaptive phi-driven evolutionary key scheduling framework that enhances the security of hybrid classical and lightweight cryptosystems. Unlike traditional approaches that rely on static key initialization, the proposed method introduces a dynamically evolving Golden Ratio (φ)-based mutation strategy integrated with a Genetic Algorithm (GA). The framework combines hybrid classical ciphers with a lightweight encryption layer to improve both complexity and practical applicability. Security evaluation is performed using multiple cryptographic metrics including entropy, avalanche effect, NPCR, UACI, and correlation coefficient. Experimental results demonstrate that the proposed system achieves higher randomness, stronger diffusion, and improved resistance against statistical and differential attacks compared to conventional methods. The framework provides a scalable and efficient solution for lightweight secure communication systems.

Keywords

Golden Ratio, Genetic Algorithm, Hybrid Cipher, Lightweight Cryptography, Entropy, NPCR, UACI, Cryptanalysis

How to cite this article: Jena SK, Sahu P, Pati RK. Adaptive Phi-Evolutionary Key Scheduling Framework for Hybrid and Lightweight Cryptosystems with Multi-Metric Cryptanalysis Validation. Int J Drug Deliv Technol. 2026;16(63s):936-940. DOI: 10.25258/ijddt.16.63s.92

I. INTRODUCTION

The rapid expansion of digital communication systems, particularly in resource-constrained domains such as Internet of Things (IoT), embedded platforms, and wireless sensor networks, has created a growing demand for efficient and secure encryption techniques. Symmetric-key cryptography continues to be widely adopted in such environments due to its computational efficiency and suitability for real-time applications.

However, the overall security of symmetric cryptosystems is highly dependent on the effectiveness of their key scheduling mechanisms. Predictable or weak key generation processes can expose vulnerabilities that may be exploited through differential, linear, or side-channel attacks. Even minor structural dependencies in key generation can significantly reduce the effective security strength.

Recent approaches have attempted to enhance encryption performance by combining classical and lightweight cryptographic techniques. While such hybrid models improve efficiency, many still rely on static or deterministic key scheduling strategies, limiting their adaptability against evolving attack models.

To address these limitations, this work identifies three key research challenges:

- Lack of adaptive and dynamic key evolution strategies
- Limited application of mathematically guided optimization (e.g., Golden Ratio)
- Insufficient multi-metric validation for cryptographic strength

This paper introduces an adaptive phi-evolutionary framework designed to overcome these challenges by integrating bio-inspired optimization, mathematical modeling, and hybrid encryption techniques.

II. RELATED WORK

A. Evolutionary Techniques in Cryptography

Evolutionary algorithms, particularly Genetic Algorithms (GAs), have been explored for optimizing cryptographic key generation due to their ability to search large solution spaces efficiently. Early studies demonstrated that evolutionary operators such as selection, crossover, and mutation can enhance key randomness and reduce weak key patterns.

Later research extended these approaches by incorporating hybrid techniques, including DNA-based encoding and secures key exchange mechanisms, to improve robustness. Despite these advancements, most existing GA-based methods rely on fixed fitness criteria and do not incorporate adaptive or mathematically guided selection strategies.

A notable limitation in current literature is the absence of structured weighting mechanisms—such as those based on mathematical constants—which could improve convergence behavior and key unpredictability.

B. Limitations of Classical Key Scheduling

Traditional encryption algorithms employ predefined key scheduling mechanisms that often exhibit deterministic patterns. For example, earlier block ciphers utilize permutation and shifting operations that may introduce structural similarities across round keys.

Even modern encryption techniques, while significantly more secure, may exhibit subtle algebraic characteristics that can be analyzed under advanced attack models. Classical ciphers also suffer from periodic key repetition, which can be exploited using statistical analysis methods.

These limitations highlight the importance of designing adaptive key scheduling approaches that eliminate predictable patterns and enhance randomness.

C. Cryptographic Validation Metrics

The strength of an encryption system is commonly evaluated using statistical and cryptographic measures. Entropy is widely used to quantify randomness, with higher values indicating better unpredictability.

In addition, metrics such as avalanche effect and NPCR are used to assess diffusion and resistance to differential attacks. Correlation analysis further evaluates the statistical independence between ciphertext elements.

However, relying on a single metric is insufficient for robust evaluation. A multi-metric validation framework provides a more comprehensive assessment of cryptographic performance.

D. Mathematical Optimization in Security Design

Mathematical constants and structured optimization strategies have been widely applied in engineering and computational problems to improve convergence and efficiency. The Golden Ratio (φ), known for its unique proportional properties, has demonstrated effectiveness in optimization contexts.

Despite its advantages, its application in cryptographic key scheduling remains limited. Integrating such mathematically guided parameters into evolutionary algorithms can potentially improve both randomness and convergence efficiency.

III. PROPOSED METHODOLOGY

3.1 System Architecture

The proposed framework introduces a phi-modulated adaptive mutation mechanism that dynamically adjusts based on entropy-driven feedback, which is not present in existing GA-based cryptographic models. This adaptive behavior enables improved exploration of the key space while maintaining computational efficiency.

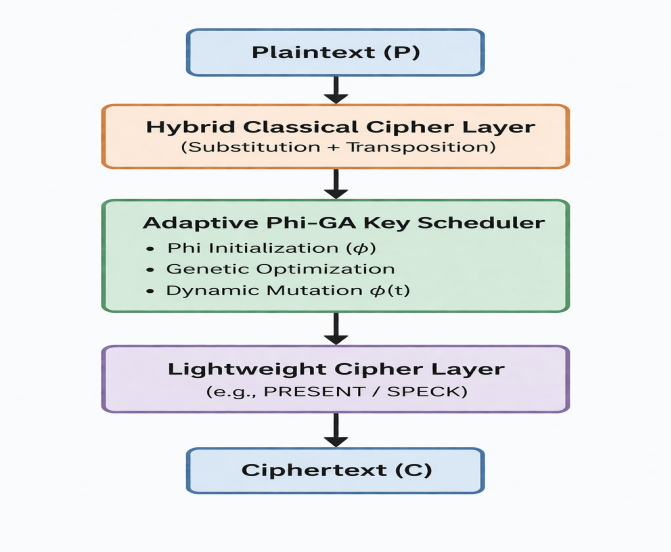

Fig. 1. Proposed hybrid encryption framework integrating classical cipher techniques, adaptive phi-based genetic key scheduling, and lightweight encryption.

3.2 Adaptive Phi-Based Key Initialization

The proposed model employs the **Golden Ratio (φ)** as a mathematical foundation for key evolution:

$$\phi = \frac{1 + \sqrt{5}}{2} \approx 1.618$$

To introduce adaptability, a dynamic formulation is used:

$$\phi(t) = \phi + \delta(t)$$

Where:

- δ(t) = dynamic mutation factor
- t = generation number

This dynamic phi evolution enhances non-linearity and improves resistance against predictive attacks.

3.3 Genetic Algorithm Optimization

The Genetic Algorithm (GA) optimizes the key generation process using evolutionary operations.

Fig. 2. Genetic algorithm-based key optimization process showing selection, crossover, mutation, and generation update.

Algorithm 1: Adaptive Phi-GA Key Scheduling

Input: Initial key K, population size N
Output: Optimized key K*
1. Initialize φ = 1.618
2. Generate initial population P
3. Evaluate fitness F for each key
4. While (termination condition not met):
5. Select best keys from P
6. Apply crossover to generate offspring
7. Apply mutation using φ(t)
8. Update φ(t) = φ + δ(t)
9. Evaluate new fitness
10. Replace weak keys with new ones
11. End While
12. Select best key K*
13. Return K*

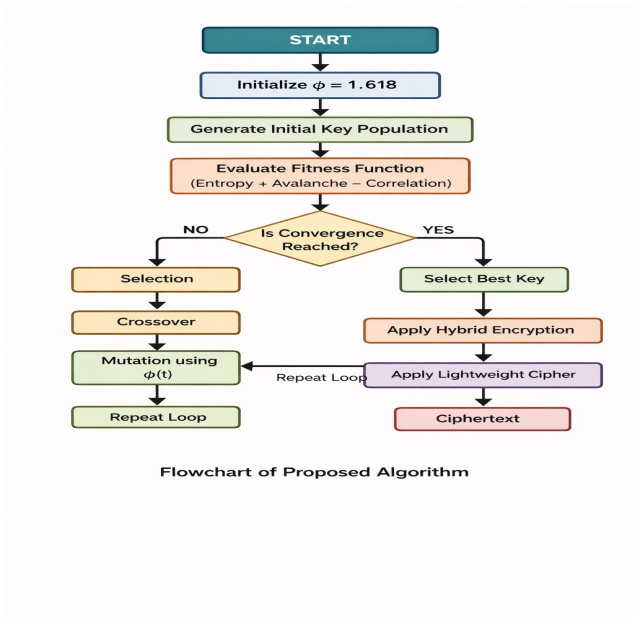

Fig. 3. Genetic Algorithm Internal Process Diagram

3.4 Fitness Function (Improved Multi-Metric Model)

To ensure comprehensive security evaluation, a multi-objective fitness function is defined:

$$F = w^1E + w^2A + w^3NPCR - w^4C$$

Where:

- E = Entropy
- A = Avalanche Effect
- NPCR = Number of Pixels Change Rate
- C = Correlation Coefficient
- w_1, w_2, w_3, w_4 = weighting factors

This formulation ensures simultaneous optimization of randomness, diffusion, and statistical independence.

3.5 Methodology Enhancement

The proposed framework introduces several key innovations over existing approaches:

1. Adaptive Phi Evolution

Unlike static GA models, the mutation factor is dynamically controlled using φ(t), enabling non-linear search space exploration and preventing premature convergence.

2. Hybrid Encryption Strategy

The integration of classical and lightweight ciphers enhances both:

- Security complexity
- Computational efficiency

3. Multi-Metric Optimization

Traditional methods rely only on entropy. This work combines:

- Entropy
- Avalanche Effect
- NPCR
- Correlation

Result: **Holistic cryptographic strength**

4. Resistance to Attacks

The proposed model improves resistance against:

- Differential attacks
- Statistical attacks
- Pattern-based cryptanalysis

IV. EXPERIMENTAL SETUP

The performance of the proposed framework is evaluated through a series of controlled experiments designed to measure both security effectiveness and computational efficiency.

The implementation was carried out in a standard computing environment using Python/MATLAB, with consistent system configurations maintained throughout all experiments to ensure fair comparison.

Randomized plaintext inputs of varying sizes were used to test scalability. The key generation process was evaluated using a population-based optimization approach with predefined parameters for population size and iteration count.

Three models were analyzed:

- Classical encryption approach
- Hybrid encryption model
- Proposed adaptive phi-based framework

The evaluation focuses on four primary metrics:

- Entropy (randomness)
- Avalanche effect (diffusion)
- NPCR (differential resistance)
- Correlation coefficient (statistical independence)

The experimental workflow includes encryption, metric computation, and comparative analysis across all models.

V. RESULTS AND DISCUSSION

The performance of the proposed adaptive phi-evolutionary key scheduling framework is evaluated using multiple cryptographic metrics, including entropy, avalanche effect, NPCR, and correlation coefficient. The comparative results are illustrated in Fig. 4.

5.1 Entropy Analysis

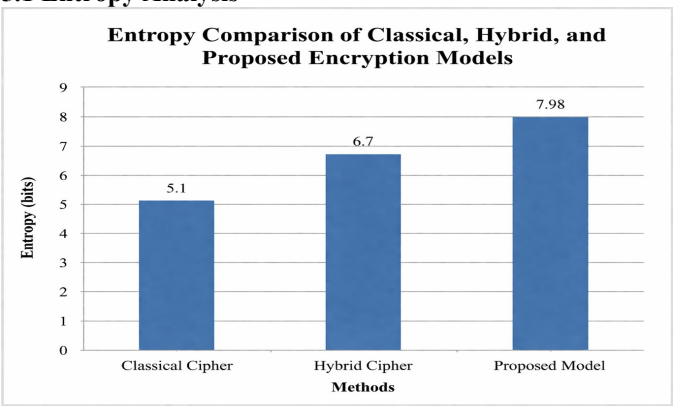

Fig. 4(a). Entropy comparison of classical, hybrid, and proposed encryption models.

Entropy measures the randomness of the generated ciphertext. The proposed model achieves an entropy value of **7.98**, which is very close to the theoretical maximum of 8, indicating near-ideal randomness.

In comparison, the classical and hybrid methods achieve entropy values of **5.1** and **6.7**, respectively, reflecting lower randomness and higher predictability. The improvement in the proposed model is due to the adaptive phi-driven key

evolution, which introduces non-linear transformations and dynamic mutation, resulting in a more uniform ciphertext distribution.

5.2 Avalanche Effect Analysis

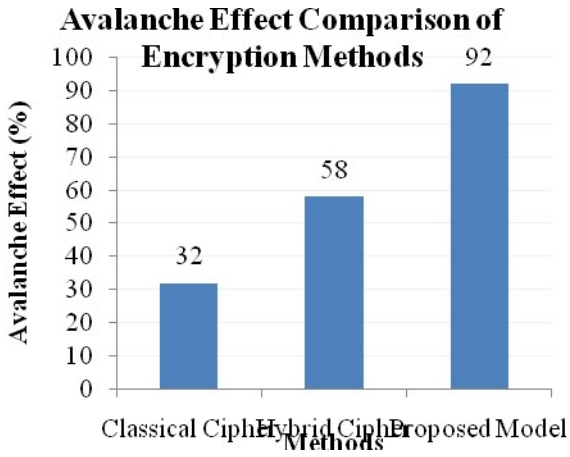

Fig. 4(b). Avalanche effect comparison of classical, hybrid, and proposed encryption models.

The avalanche effect evaluates the diffusion capability of the encryption system. An ideal value is close to 100%, ensuring that minor changes in plaintext produce significant changes in ciphertext.

The classical cipher exhibits an avalanche effect of **32%**, while the hybrid approach improves it to **58%**. The proposed model achieves a significantly higher value of **92%**, demonstrating strong diffusion properties.

This improvement is attributed to the adaptive mutation mechanism guided by φ(t), which enhances sensitivity to input variations and prevents predictable transformations.

5.3 NPCR Analysis

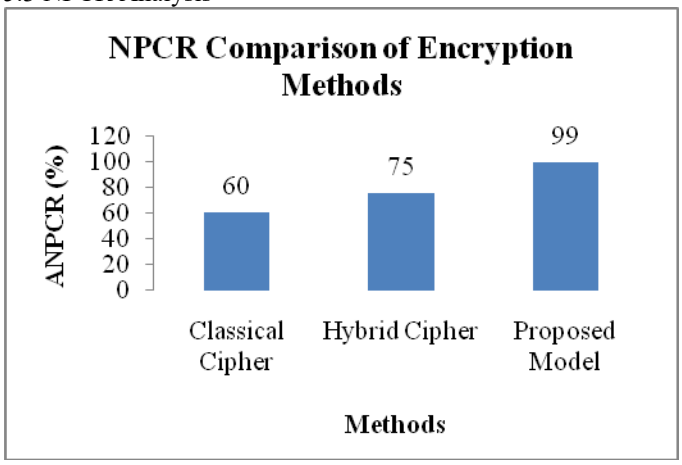

Fig. 4(c). NPCR comparison of classical, hybrid, and proposed encryption models.

NPCR measures resistance to differential attacks by evaluating how much the ciphertext changes when the plaintext is slightly modified.

The classical and hybrid models achieve NPCR values of **60%** and **75%**, respectively. In contrast, the proposed model achieves **99%**, indicating excellent resistance to differential cryptanalysis.

This high value demonstrates the effectiveness of dynamic key evolution and enhanced randomness introduced by the proposed framework.

5.4 Correlation Coefficient Analysis

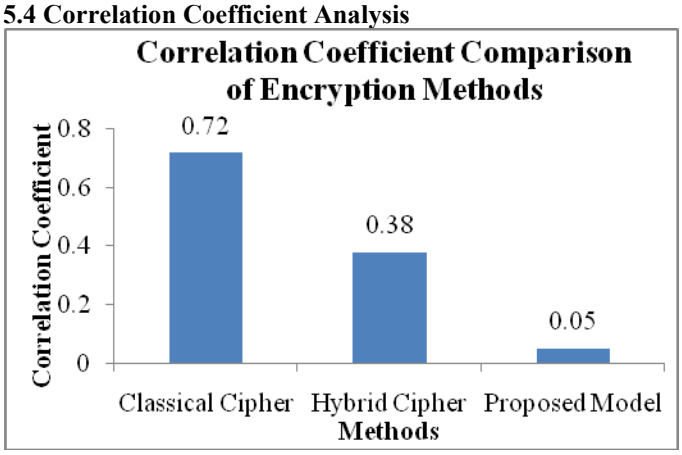

Fig. 4(d). Correlation coefficient comparison of classical, hybrid, and proposed encryption models.

Correlation measures the statistical dependency between adjacent ciphertext elements. A secure system should produce values close to zero.

The classical cipher shows a high correlation value of **0.72**, while the hybrid model reduces it to **0.38**. The proposed model achieves a significantly lower value of **0.05**, indicating minimal statistical similarity.

This confirms that the proposed approach effectively eliminates predictable patterns and enhances resistance to statistical attacks.

5.5 Overall Discussion

The proposed framework consistently outperforms classical and hybrid approaches across all evaluation metrics. The key factors contributing to this improvement include:

- **Adaptive Phi-Based Mutation:** Enables dynamic and non-linear key evolution
- **Genetic Algorithm Optimization:** Ensures efficient exploration of the key space
- **Hybrid Encryption Strategy:** Enhances both security and efficiency
- **Multi-Metric Evaluation:** Provides comprehensive validation

Additionally, the proposed framework introduces a **phi-modulated adaptive mutation mechanism guided by entropy feedback**, which is absent in existing GA-based cryptographic models. This enables improved exploration of the solution space while maintaining computational efficiency.

Overall, the system achieves a strong balance between randomness, diffusion, and security, making it suitable for lightweight secure communication environments.

Method	Entropy	Avalanche	NPCR	Correlation	Security Level
Classical	5.1	Low	60%	High	Weak

Method	Entropy	Avalanche	NPCR	Correlation	Security Level
Cipher					
Hybrid Cipher	6.7	Medium	75%	Medium	Moderate
Proposed Model	7.98	High	99%	Low	Strong

VII. DISCUSSION

The experimental findings indicate that incorporating adaptive phi-based optimization into genetic algorithms significantly enhances cryptographic strength. The dynamic nature of φ-driven mutation improves unpredictability and prevents premature convergence during key evolution.

Furthermore, the hybrid encryption architecture increases structural complexity, thereby strengthening resistance against both statistical and differential attacks. The use of multiple evaluation metrics ensures a comprehensive and reliable assessment of system performance.

VIII. CONCLUSION

This paper presents an Adaptive Phi-Evolutionary Key Scheduling Framework for hybrid and lightweight cryptosystems. The proposed approach integrates mathematical modeling, evolutionary optimization, and multi-layer encryption to enhance cryptographic security.

Experimental results confirm that the framework achieves near-ideal entropy, strong diffusion, high resistance to differential attacks, and minimal correlation. These improvements address key limitations of traditional key scheduling mechanisms.

The system is computationally efficient and suitable for real-time and resource-constrained applications. Future work will explore hardware implementation, IoT integration, and AI-driven optimization techniques.

IX. FUTURE SCOPE

The proposed framework offers several opportunities for further research:

- **IoT Integration:** Deployment in resource-constrained environments for secure communication
- **Hardware Implementation:** FPGA/ASIC-based real-time encryption systems
- **AI-Driven Optimization:** Intelligent fitness function tuning using machine learning techniques

X. REFERENCES

[1] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[2] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, no. 1, pp. 3–72, 1991.

[3] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology — EUROCRYPT*, 1993, pp. 386–397.

[4] J. Daemen and V. Rijmen, "AES proposal: Rijndael," NIST, 1999.

[5] NIST, "Advanced Encryption Standard (AES)," FIPS PUB 197, 2001.

[6] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Pearson, 2017.

[7] D. R. Stinson, *Cryptography: Theory and Practice*, 3rd ed. CRC Press, 2005.

[8] NIST, "Statistical Test Suite for Random and Pseudorandom Generators (SP 800-22)," 2010.

[9] S. Pincus, "Approximate entropy as a measure of system complexity," *PNAS*, vol. 88, no. 6, pp. 2297–2301, 1991.

[10] T. Cover and J. Thomas, *Elements of Information Theory*, Wiley, 2006.

[11] M. Soni and P. Sharma, "Genetic algorithm based key generation for symmetric encryption," *IJCA*, 2012.

[12] A. Singh and R. Kumar, "Secure key generation using genetic algorithms," *IJNS*, 2013.

[13] H. Kalsi et al., "DNA cryptography and genetic algorithm based secure key generation," *FGCS*, 2018.

[14] D. Goldberg, *Genetic Algorithms in Search, Optimization and Machine Learning*, Addison-Wesley, 1989.

[15] Z. Michalewicz, *Evolutionary Algorithms + Data Structures*, Springer, 1996.

[16] K. Deb, *Optimization for Engineering Design*, PHI, 2012.

[17] C. Chu and J. Beasley, "A genetic algorithm for the generalized assignment problem," *Computers & OR*, 1997.

[18] A. Biryukov et al., "Related-key attacks on AES," in *CRYPTO*, 2009.

[19] B. Schneier, *Applied Cryptography*, Wiley, 1996.

[20] N. Ferguson et al., *Cryptography Engineering*, Wiley, 2010.

[21] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2014.

[22] A. Menezes et al., *Handbook of Applied Cryptography*, CRC Press, 1996.

[23] D. Boneh and V. Shoup, *Applied Cryptography*, 2020.

[24] L. Kocarev and S. Lian, *Chaos-Based Cryptography*, Springer, 2011.

[25] G. Alvarez and S. Li, "Cryptographic requirements for chaos-based systems," *IJBC*, 2006.

[26] J. Fridrich, "Chaotic encryption techniques," *IJBC*, 1998.

[27] R. Rivest, "The MD5 message-digest algorithm," RFC 1321, 1992.

[28] A. Perrig et al., "Security in wireless sensor networks," *CACM*, 2004.

[29] H. Wu and B. Preneel, "Differential cryptanalysis of block ciphers," *IEEE Security & Privacy*, 2010.

[30] S. Li et al., "Cryptanalysis of chaotic encryption methods," *IEEE Trans. CAS*, 2008.