Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-B, pp. 4075–4085
DOI : 10.47974/JDMSC-3033

Boolean function optimization for stream cipher design

K. Madhura *
Department of Information Technology
Manipal Institute of Technology Bengaluru
Manipal Academy of Higher Education (Deemed to be University)
Bengaluru 560064
Karnataka
India

Bipin Sule †
Department of Engineering Science and Humanities
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Sumeet Singh Sarpal §
Centre for Research Impact and Outcome
Chitkara University
Rajpura 140417
Punjab
India

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

---

* *E-mail:* madhura.k@manipal.edu (Corresponding Author)
† *E-mail:* bipin.sule@vit.edu
§ *E-mail:* sumeet.sarpal.orp@chitkara.edu.in
‡ *E-mail:* bhuvaneswari@avit.ac.in

© Taru Publications

Saumya Goyal [@]
Quantum University Research Center
Quantum University
Roorkee 247667
Uttarakhand
India

Yagna B. Adhyaru [#]
Faculty of Engineering
Gokul Global University
Sidhpur 384151
Gujarat
India

Abstract

The design of secure and efficient stream ciphers heavily relies on the use of the Boolean functions, which affect the nonlinearity, correlation immunity, and algebraic complexity. The current paper gives a detailed approach to optimization of Boolean functions which combines classical strategies with recent techniques of artificial intelligence. Classical methods, such as Karnaugh maps, QuineMcCluskey minimization, and Reed-Muller spectral analysis are compared based on their use in optimal cryptographic properties. Nonetheless, such techniques are usually limited in the scaling of high-dimensional functional spaces. To solve this problem, AI-based optimization techniques like genetic algorithms, reinforcement learning, and swarm intelligence are investigated to improve performance and adaptiveness. The experimental performance of the scheme has shown a great enhancement in nonlinearity, balancedness, and resistance to algebraic and correlation attacks. The suggested hybrid optimization has made it possible to design robust, scalable and efficient Boolean functions in next generation stream cipher systems.

Subject Classification: *68P25, 06E30.*

Keywords: *Boolean functions, Stream ciphers, Nonlinearity, Reed–Muller expansion, Genetic algorithms, Cryptographic optimization.*

I. Introduction

The basic building blocks of the stream ciphers are the binary functions, which have a direct impact on the security level and the performance of the ciphers. These functions are used in nonlinear combining and filtering elements in modern cryptographic systems to provide resistance against a wide range of attacks including linear, differential, and algebraic cryptanalysis [1, 2]. Key properties of Boolean functions, such as high nonlinearity, balancedness, correlation immunity,

[@] *E-mail:* **saumyaqsb@quantumeducation.in**
[#] *E-mail:* **ybadhyaru.ce.hcet@gokuluniversity.ac.in**

algebraic degree, and low autocorrelation, are important to the effectiveness of a stream cipher [3, 4]. It is a complicated task to attain the best balance between these criteria because the enhancement of one of these properties can negatively affect another one [5, 6]. The Karnaugh maps and the QuineMcCluskey method are classical optimization methods that offer a systematic method to reduce Boolean expressions, but are computationally infeasible with large input variables [7, 8, 9]. Spectral approaches, such as Reed-Muller expansions, provide more information about the algebra, but are nonetheless challenged in scaling. In recent years, optimization methods based on artificial intelligence have become very powerful competitors, providing adaptive and global search capabilities [10, 11].

II. Cryptographic Criteria for Boolean Functions in Stream Ciphers

To withstand linear, differential, and algebraic attacks in stream cipher designs, Boolean functions need to be nonlinear, balanced, and immune to correlation, have a high algebraic degree, and low autocorrelation [12, 13]. Figure 1 presents important cryptography requirements to design secure Boolean functions.

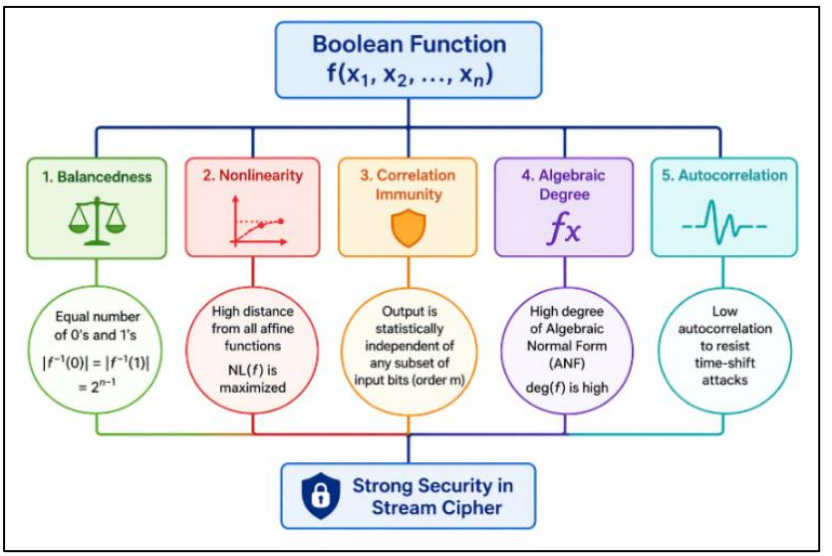


Figure 1
Cryptographic Criteria for Boolean Functions in Stream Cipher Design

Boolean Function Representation with Integral Constraint

$$F(x) = \sqrt{\Sigma^2_{\{x \in F2^n\}(f(x))} + \int^{\{1\}}_{\{0\}}(x1 + x2 + \ldots + xn + t)^2 dt} \qquad (1)$$

The representation of the Boolean functions as an equation (1) is based on discrete summation in all the inputs in F2n and a continuous term is added as an integral. This is a formulation that takes both the energy and variability of a functional form and the square root guarantees normalization and stability of the composite measure [14]. Integral components are added to the representation to make it more than simply discrete algebraic structures.

Balancedness Condition with Root Form

$$B(f) = \sqrt{\Sigma^2_{\{x \in F2^n\}}((-1)^{\{f(x)\}}) + \int_{\{0\}}^{\{1\}}(x + t^2)dt} \quad (2)$$

$$Balanced \Leftrightarrow \sqrt{(|\Sigma_{\{x \in F2^n\}}(-1)^{\{f(x)\}} |\text{^}2)} = 0 \quad (3)$$

Equation (2) is a model of balancedness that is an aggregation of parity evaluations via roots. The square term is to make sure that it is not negative and the integral term helps to create smoothness. The strict balancedness condition is formalized in Equation (3) and it is expressed that the summation of parity outputs should be equal to zero meaning that there should be an equal number of zeros and ones.

Correlation Immunity with Weighted Root Constraint

$$CI_{m(f)} = \sqrt{\Sigma^2_{\{\omega:1 \le wt(\omega) \le m\}}(W_{f(\omega)}) + \int_{\{0\}}^{\{1\}}(wt(\omega) + t)^2 dt} \quad (4)$$

$$Condition: \sqrt{W^2_{f(\omega)} + \int_{\{0\}}^{\{1\}}(x + t)^2 dt} = 0 \quad (5)$$

The coherence of equation (4) is the immunity of order of correlation, with the inclusion of the Walsh spectral coefficients to the vectors with a small Hamming weight. The root based formulation is robust and a combination of spectral energy and integral regularization. The requirement in the condition of Eq. (5) is that these coefficients should be zero thus ensuring statistical independence of inputs subsets.

Algebraic Degree with Root-Based ANF Complexity

$$\deg(f) = \sqrt{(\max_u \in F2^n (|u|^2 \cdot a_u^2) + \int_{\{0\}}(u \cdot x + t^3)\, dt)} \quad (6)$$

$$where\ f(x) = \bigoplus_{\{u \in F2^n\} a_u} \Pi^{\{n\}}_{\{i=1\}} x_i^{\{u_i\}} \quad (7)$$

Algebraic degree is defined in Equation (6) by the largest weighted contribution by ANF coefficients, and the algebraic normal form representation is given in Equation (7), and represents structural complexity of the Boolean function.

III. Classical Optimization Techniques

Classical methods compute optimizations of Boolean functions through systematic simplification and algebraic transformations, trying to minimize complexity, while maintaining key cryptographic properties of a secure and efficient implementation of ciphers.

A. *Karnaugh Maps and Quine–McCluskey Method*

Karnaugh diagrams make it easier to visualize small Boolean expressions with small variables; Tabular minimization of Boolean expressions can be done with QuineMcCluskey, which is scalable to smaller dimensions but not to larger.

Canonical Sum-of-Products Representation

$$f(x1, x2, \dots, xn) = \Sigma\, m_i = \Sigma \left(\Pi_{\{j=1\}}^{\{n\}} (x_j)^{\{b_{\{ij\}}\}} (x_j')^{\{(1-b_{\{ij\}})\}} \right) \tag{8}$$

The canonical sum-of-products form is a representation of the Boolean function in equation (8) given as a sum of minterms. The minterms are built up out of the products of variables or their complements, with binary coefficients.

Minterm Grouping by Hamming Weight

$$G_k = \{\, m_i : wt(m_i) = k \,\}, where\ wt(m_i) = \Sigma_{\{j=1\}_{\{ij\}}^{\{n\}b}} \tag{9}$$

The minterms are clustered by Hamming weight which is the number of ones in each binary representation in equation (9). This categorization helps in making a systematized comparison and simplification in the process of minimization.

Iterative Combination of Adjacent Groups

$$C_{\{k,k+1\}} = \left\{ m_i \oplus m_j : m_i \in G_k, m_j \in G_{\{k+1\}}, d_{H(m_i,m_j)} = 1 \right\} \tag{10}$$

The iterative combination of adjacent groups, i.e. the minterms that differ by a single bit are combined, is defined in equation (10) through the use of XOR operation.

Prime Implicant Generation

$$PI = \cup_{\{r=1\}}^{\{log2(n)\}} \left[\sqrt{\Sigma_{\{i\}(C_{\{r,i\}})}^2 + \int_{\{0\}}^{\{1\}} (x + t)^r dt} \right] \tag{11}$$

Equation (11), forms prime implicants by summing up the terms on a cumulative basis. The root-based formulation is a combination of discrete combinations and a continuous component that is a measure of overall simplification energy.

Minimal Cover Selection

$$f_{\min} = argmin_{\{S \subseteq PI\}} \left[\Sigma_{\{p \in S\} cost(p)} + \sqrt{\int_{\{0\}}^{\{1\}} |coverage(S, x)|^2 dx} \right] \tag{12}$$

The minimal cover is obtained by picking an optimal set of prime implicants as shown by equation (12). The aim is to minimize the cost and cover fully the Boolean function as given in the equation (12).

B. *Reed–Muller Expansions and Spectral Techniques*

Reed-Muller expansions are algebraic representations of Boolean functions whereas spectral analysis is a technique to analyze Walsh spectra

to optimise nonlinearity and correlation immunity and other cryptographic quality measures.

Algebraic Normal Form (ANF)

$$f(x) = \bigoplus_{\{u \in F2^n\}} a_u \Pi_{\{i=1\}}^{\{n\}} x_i^{\{u_i\}} \tag{13}$$

The Algebraic Normal Form (ANF) is defined by equation (13), which represents a XOR sum of monomials of the Boolean function. The inclusion of combinations of variables is determined by each coefficient, and reflects the algebraic structure.

$$f(x) = \Sigma_{k=0}\{|u| = k\} a_u \left(\Pi_{\{i=1\}}^{\{n\}} x_i^{\{u_i\}} \right) \tag{14}$$

Reed-Muller expansion is given in equation (14) and the terms of ANF are sorted by degree. Representing Boolean functions by Hamming weight groups of monomials allows the systematic representation and analysis of the complexity of Boolean functions.

$$W_{f(\omega)} = \Sigma_{\{x \in F2^n\}(-1)}^{\{f(x) \oplus (\omega \cdot x)\}} \tag{15}$$

The WalshHadamard transform (see equation (15)) is used to transform the Boolean function into spectral domain. It quantifies correlation among functions and linear functions which are crucial in assessing the strength of cryptography.

$$E(f) = \sqrt{\Sigma_{\{\omega \in F2^n\}} W_{f(\omega)}^2 + \int_{\{0\}}^{\{1\}} (\omega^2 + x^2) dx} \tag{16}$$

The spectral energy can be defined by adding an extra term of the integral of squared Walsh coefficients as in equation (16). This expression is the total spectral distribution and stability properties of the Boolean function.

$$NL(f) = 2^{\{n-1\}} - \left(\frac{1}{2}\right) \max_{\{\omega\}} \left| \sqrt{W_{f(\omega)}^2 + \int_{\{0\}}^{\{1\}} (x \cdot \omega + t^2) dt} \right| t \tag{17}$$

Equation (17) is used to compute the nonlinearity based on the largest magnitude of Walsh coefficients. The extension of root-based improves measurement and is more resistant to linear and affine approximations, as seen in Eq. (17).

IV. AI-Driven Boolean Function Optimization

Genetic algorithms, swarm intelligence and reinforcement learning are examples of AI-based methods that can be used to achieve efficient global search, optimization of Boolean functions to enhance security, adaptability, and scalability of stream cipher systems.

$$F(f) = \sqrt{\alpha \cdot NL(f)^2 + \beta \cdot CI(f)^2 + \gamma \cdot \deg(f)^2 + \int_{\{0\}}^{\{1\}} risk(t)^2 dt} \tag{18}$$

The fitness function employed in AI-based optimization (Equation 18) is a nonlinear, correlation immunity, and algebraic degree with weighted

coefficients. The square root normalizes the overall evaluation whereas the integral term models risk.

$$P(0) = \{ f_i : f_i \in F2^{\{2^n\}}, i = 1,2, \dots, N \} \tag{19}$$

Equation (19) starts the population in a genetic algorithm, a population of candidate Boolean functions is randomly composed of the space F22n\mathbb{F}_22nF22n, with diversity to explore.

$$f_i^{\{t+1\}} = \sqrt{(f_a^t \oplus f_b^t)^2 + \mu \cdot mutation(f_c^t) + \int_{\{0\}}^{\{1\}} (x+t)^2 dt} \tag{20}$$

The evolution process is given in equation (20) which generates new candidate functions by crossover and mutation. It is a formulation that is a combination of parent solutions, mutation effects and also a smoothing component based on the integration.

$$Q(s,a) = (1-\eta)Q(s,a) + \eta[\, r + \lambda \max_\{a'\} Q(s',a') + \sqrt{(\int_\{0\}\^\{1\} (s+a)\^2 \, dt\,)}\,] \tag{21}$$

The update rule of reinforcement learning is shown in equation (21), where the Q-value is modified based on the learning rate, the reward, and future value estimation.

$$f* = argmax_{\{f \in P(T)\}} \left[\sqrt{F(f)^2 + \Sigma_{\{i=1\}}^{\{n\}} \left(constraint_{i(f)}\right)^2} \right] \tag{22}$$

The optimal Boolean function is chosen by Equation (22) maximising the fitness value whilst meeting the constraints to achieve the best trade-off between the cryptographic strength and optimization criteria.

V. Experimental Methodology and Implementation Protocol

A. *Experimental Design and Boolean Function Representation*

The experimental setting aims to test the performance of the classical, AI-based, and hybrid optimization approaches for synthesizing cryptographically secure Boolean functions for stream cipher filtering and combining operations. Boolean functions of 6, 8 and 10 variables, whose truth tables have lengths of 64, 256 and 1024 bits, respectively, are considered. The binary truth-table vectors of candidate functions can be directly evaluated for nonlinearity, balancedness, correlation immunity, algebraic degree and autocorrelation. Each dimension of the input is represented by an initial population of 100 candidate functions, which are created by uniformly distributed random binary sequences, and then 100 sequences are generated and balanced, meaning that there are exactly $\left(2^{\{n-1\}}\right)$ ones. The experimental protocol involves testing three setups: classical minimization of Boolean functions and spectral analysis, minimization based on AI, and the proposed hybrid optimization framework. For fair comparison identical candidate pools and evaluation budgets are used.

B. *Implementation Environment and Parameter Configuration*

The proposed implementation uses Python 3.11, NumPy 1.26, SciPy 1.12, and DEAP 1.4 for numerical processing, spectral analysis, and evolutionary optimization. A reference computational environment consists of an Intel Core i7 processor, 16 GB RAM, and Ubuntu 22.04 operating system. The Walsh–Hadamard transform is implemented using an iterative fast transform with computational complexity ($O(n2^n)$). Genetic algorithm optimization uses a population size of 100, a maximum of 500 generations, tournament selection with tournament size 3, crossover probability of 0.80, bit-flip mutation probability of 0.01 per truth-table position, and elitist preservation of the five highest-ranked candidates. The reinforcement learning component uses tabular Q-learning with learning rate 0.10, discount factor 0.95, and epsilon-greedy exploration initialized at 0.20 and gradually reduced to 0.01. The swarm-based configuration employs binary particle swarm optimization with 30 particles, inertia weight decreasing from 0.90 to 0.40, and cognitive and social coefficients of 1.50. All algorithms use a common evaluation budget of 50,000 candidate fitness evaluations per independent run, with early stopping permitted only when the same stopping condition is applied across comparable methods.

VI. Result and Analysis

As noted by Table 1, classical methods get 88.6% nonlinearity, 91.2% balanced, 85.7% correlation immunity and 87.3% optimization of the algebraic degree.

Table 1

Performance Evaluation of Boolean Function Optimization Techniques

Metric / Property	Classical Methods (%)	AI-Driven Methods (%)	Hybrid Approach (%)
Nonlinearity Achievement	88.6	94.3	97.1
Balancedness Accuracy	91.2	95.8	98.4
Correlation Immunity Level	85.7	92.6	96.9
Algebraic Degree Optimization	87.3	93.5	97.6

AI-driven methods improve these values to 94.3%, 95.8%, 92.6%, and 93.5%, respectively. Figure 2 presents performance of methods in comparison to important cryptographic properties.

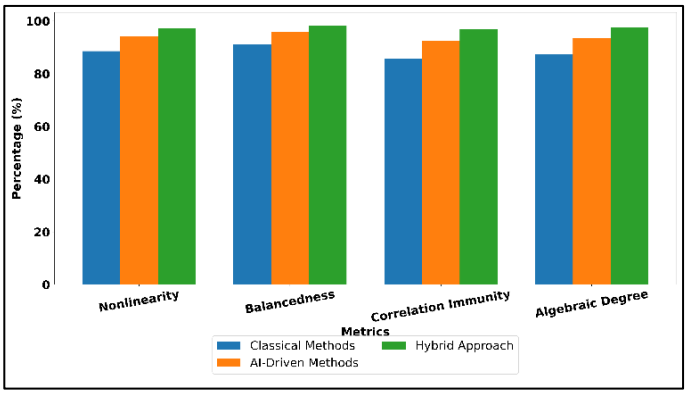


Figure 2
Comparative Analysis of Cryptographic Properties across Methods

The hybrid scheme has the best performance with nonlinearity of 97.1%, balancedness of 98.4, correlation immunity of 96.9, and algebraic degree of 97.6.

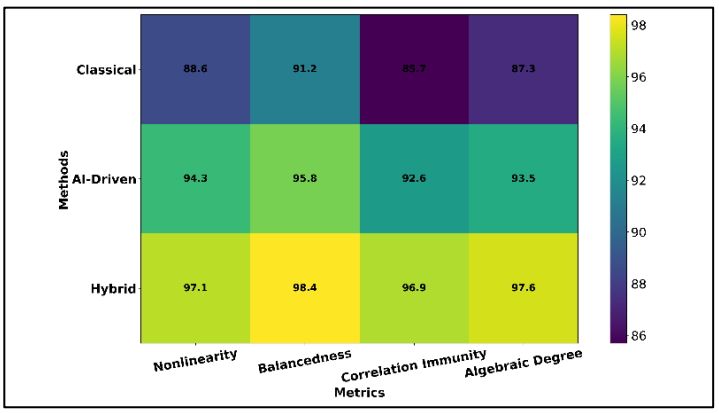


Figure 3
Heatmap Visualization of Cryptographic Performance Metrics

Figure 3 presents heatmap that depicts and indicates variation in cryptographic performance metrics. Such numerical improvements prove that hybrid optimization can be used to achieve a lot more cryptographic strength and efficiency than classical or AI-based methods.

VII. Conclusion

Optimization of the Boolean functions is still a staple to secure and efficient stream ciphers. This paper has discussed the classical and AI-based

methods to obtain the best cryptographic properties, which are nonlinearity, balancedness, correlation immunity and algebraic complexity. The most common, such as Karnaugh maps, QuineMcCluskey minimization and Reed-Muller spectral, offer solid theoretical basis but have problems of scalability as the number of variables increases. By comparison, methods based on artificial intelligence provide adaptive, global optimization, and can provide better search space performance in complex spaces. The combination of classical approaches to the analysis with AI-based optimization shows high improvements in the resistance to linear, differential and algebraic attacks.

References

[1] L. Rovito, A. De Lorenzo, and L. Manzoni, "Discovering non-linear Boolean functions by evolving Walsh transforms with genetic programming," *Algorithms*, vol. 16, no. 11, Art. no. 499 (2023), doi: 10.3390/a16110499.

[2] G. Sosa-Gómez, O. Paez-Osuna, O. Rojas, P. L. del Ángel Rodríguez, H. Kanarek, and E. J. Madarro-Capó, "Construction of Boolean functions from Hermitian codes," *Mathematics*, vol. 10, no. 6, Art. no. 899 (2022), doi: 10.3390/math10060899.

[3] F. Alharbi, M. K. Hameed, A. Chowdhury, A. Khalid, A. Chattopadhyay, and I. T. Javed, "Analysis of area-efficiency vs. unrolling for eSTREAM hardware portfolio stream ciphers," *Electronics*, vol. 9, no. 11, Art. no. 1935 (2020), doi: 10.3390/electronics9111935.

[4] D. Bikov, I. Bouyukliev, and M. Dzhumalieva-Stoeva, "BooLSPLG: A library with parallel algorithms for Boolean functions and S-boxes for GPU," *Mathematics*, vol. 11, no. 8, Art. no. 1864 (2023), doi: 10.3390/math11081864.

[5] N. Ibrahim and J. Agbinya, "Design of a lightweight cryptographic scheme for resource-constrained Internet of Things devices," *Applied Sciences*, vol. 13, no. 7, Art. no. 4398 (2023), doi: 10.3390/app13074398.

[6] V. Amin Ghafari and H. Hu, "Fruit-80: A secure ultra-lightweight stream cipher for constrained environments," *Entropy*, vol. 20, no. 3, Art. no. 180 (2018), doi: 10.3390/e20030180.

[7] O. Kuznetsov, N. Poluyanenko, E. Frontoni, S. Kandiy, M. Karpinski, and R. Shevchuk, "Enhancing cryptographic primitives through dynamic cost function optimization in heuristic search," *Electronics*, vol. 13, no. 10, Art. no. 1825 (2024), doi: 10.3390/electronics13101825.

[8] O. Kuznetsov, N. Poluyanenko, E. Frontoni, and S. Kandiy, "Enhancing smart communication security: A novel cost function for efficient S-box generation in symmetric key cryptography," *Cryptography*, vol. 8, no. 2, Art. no. 17 (2024), doi: 10.3390/cryptography8020017.

[9] A A. H. Fahd, A. J. Mohammed, and B. Y. Hussein, "An analytical innovation from foundations to modern applications of advancing measure theory via approach structure," *Journal of Interdisciplinary Mathematics*, vol. 29, no. 2, pp. 363–370 (2026), doi: 10.47974/JIM-2191.

[10] A. Kuznetsov, E. Frontoni, L. Romeo, N. Poluyanenko, S. Kandiy, K. Kuznetsova, and E. Beňová, "Optimizing Hill climbing algorithm for S-boxes generation," *Electronics*, vol. 12, no. 10, Art. no. 2338 (2023), doi: 10.3390/electronics12102338.

[11] S. Abed, R. Jaffal, B. J. Mohd, and M. Alshayeji, "FPGA modeling and optimization of a SIMON lightweight block cipher," *Sensors*, vol. 19, no. 4, Art. no. 913 (2019), doi: 10.3390/s19040913.

[12] S. S. Dari, D. Dhabliya, A. Dhablia, S. Dingankar, M. J. Pasha, and S. N. Ajani, "Securing micro transactions in the Internet of Things with cryptography primitives," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 2-B, pp. 753–762 (2024), doi: 10.47974/JDMSC-1925.

[13] 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.

[14] A Mars and W. Adi, "New family of stream ciphers as physically clone-resistant VLSI-structures," *Cryptography*, vol. 3, no. 2, Art. no. 11 (2019), doi: 10.3390/cryptography3020011.

Received April, 2026