ADBA Chaos and Fractals
Cutting-Edge Scientific Solutions

e-ISSN: 3023-8951
RESEARCH ARTICLE
Vol.3 / No.1 / 2026 / pp.7-15
https://doi.org/10.69882/adba.chf.2026012

# Design and Performance Evaluation of a Hybrid PRNG: Gold-SA II Optimized LFSR Combined with Discrete Chaotic Maps

**Eyüp Eröz** *,1, **Erkan Tanyıldızı** α,2 **and Fatih Özkaynak** α,3

*Firat University, Kovancilar Vocational School Department of Computer Technologies, Elazig, Türkiye, αFirat University, Department of Software Engineering, Elazig, Türkiye.

**ABSTRACT** Random Number Generators (RNGs) play a critical role in ensuring data security in cryptographic systems. Linear Feedback Shift Registers (LFSRs) are widely used due to their hardware speeds and low costs; however, their linear structures make them vulnerable to algebraic attacks and may yield insufficient results in statistical randomness tests. This study proposes a hybrid architecture based on optimisation and chaos to enhance the cryptographic security of LFSR-based generators. The irreducible polynomials and initial seed values that provide the maximum period length of the LFSR have been optimised using the Modified Golden Sine Algorithm (Gold-SA II). As the raw LFSR outputs failed the NIST SP 800-22 tests, the system was supported by a chaotic final processing layer containing Sine, Chebyshev, Logistic, Tent, and Circle maps. Experimental results demonstrate that the chaotic final processing significantly improves randomness properties and, in particular, that the Sinus map-based structure successfully passes all NIST tests.

**KEYWORDS**
LFSR
Gold-SA II
Chaotic maps
Hybrid PRNG
NIST SP 800-22
Cryptography

## INTRODUCTION

In the rapidly evolving digital landscape, the volume of data transmitted and stored within critical infrastructures such as the Internet of Things (IoT), cloud computing platforms, and military communication systems is increasing exponentially. Ensuring the confidentiality and integrity of this data against unauthorized access has therefore become a primary strategic objective in information security. The security of modern cryptographic systems depends not only on the computational strength of encryption algorithms but also, fundamentally, on the quality of the cryptographic keys employed. In this context, Random Number Generators (RNGs) play a crucial role by producing encryption keys, initialization vectors (IVs), and nonces. Consequently, the unpredictability and statistical randomness of the sequences generated by an RNG directly determine the overall security of the cryptographic chain (Rukhin *et al.* 2010).

Among various RNG architectures, Linear Feedback Shift Registers (LFSRs) are widely adopted in hardware-oriented applications due to their low power consumption, high generation speed, and structural simplicity (Golomb 1982). However, the cryptographic suitability of LFSR-based systems strongly depends on their initial configuration, particularly the choice of the feedback polynomial and the seed value. As the polynomial degree increases, identifying primitive polynomials and suitable seeds that ensure a maximum period length of $2^n - 1$ becomes computationally intractable. Moreover, even when maximum-length configurations are employed, the inherent linearity of LFSRs renders them vulnerable to algebraic attacks and often results in poor performance in stringent statistical randomness test suites.

To address these challenges, extensive research efforts have been reported in the literature focusing on chaotic systems and optimization algorithms. Silva *et al.* (2009) proposed a modular-chaos pseudo-random number generator (PRNG) based on the Lorenz system, demonstrating that chaos-based approaches can provide strong resistance against statistical attacks. Similarly, Murillo-Escobar *et al.* (2017) and Moysis *et al.* (2020) investigated the enhancement of randomness properties in logistic-map-based generators for cryptographic applications.

From an optimization perspective, Tanyildizi and Ozkaynak (2019) employed multiple optimization algorithms to determine optimal initial parameters for S-box generation. Recently, Eröz *et al.* (2025) proposed the COLFSR architecture, demonstrating that integrating chaos optimization with LFSR structures significantly enhances the statistical randomness of the generated sequences, while Demidova *et al.* (2020) utilized optimization techniques to improve the statistical characteristics of generated random se-

**Manuscript received:** 4 December 2025,
**Revised:** 13 January 2026,
**Accepted:** 17 January 2026.

[1]eeroz@firat.edu.tr (**Corresponding author**)
[2]etanyildizi@firat.edu.tr
[3]ozkaynak@firat.edu.tr

quences. Furthermore, recent studies such as Muhammad and Ozkaynak (2021) explored multi-stage encryption frameworks involving chaotic selection mechanisms, emphasizing the importance of careful system design to mitigate temporal correlations. Emin *et al.* (2024) demonstrated the effectiveness of chaotic systems in secure image encryption applications Abdulrazaq *et al.* (2024) proposed a synergistic framework for constructing high-performance S-boxes based on chaotic systems, demonstrating that chaos-driven designs can significantly enhance cryptographic security metrics and represent a paradigm shift in modern cryptographic security architectures. Similarly, Zhao *et al.* (2024) focused on improving complexity in chaotic maps to improve dynamic behaviors.

Recent studies have increasingly focused on hybrid structures to overcome the limitations of standalone chaotic maps. For instance, Youssef (2024) demonstrated the efficacy of hyperchaotic systems in satellite image security, utilizing dynamic S-boxes to enhance encryption robustness. Similarly, Zhao *et al.* (2024) explored complexity enhancement techniques to expand the grid basin of chaotic attractors. Building on these contemporary approaches, our study integrates the structural simplicity of LFSRs with the complexity of chaotic maps, as also compared against recent works like Guo *et al.* (2023) in the experimental results section. Despite the notable advancements achieved in these studies, optimization-based parameter selection and chaotic post-processing are typically treated as independent enhancement strategies. In this study, a novel hybrid PRNG architecture is proposed to bridge this gap by synergistically combining both approaches. Specifically, an LFSR optimized using the Modified Golden Sine Algorithm (GoldSA II), which exhibits insufficient statistical randomness in its raw output, is reinforced through chaotic post-processing.

A comparative evaluation is conducted using five distinct chaotic maps, namely the Sine, Chebyshev, Logistic, Tent, and Circle maps. The primary objectives of the proposed architecture are threefold: (i) to disrupt the inherent linear structure of the LFSR, (ii) to maximize the success rate in the NIST SP 800–22 statistical test suite, and (iii) to identify the chaotic map that achieves the most favorable trade-off between generation speed and cryptographic security. Experimental results indicate that, while the standalone optimized LFSR fails several critical randomness tests, the proposed hybrid architecture particularly when combined with the Sine map successfully passes all tests in the NIST SP 800–22 suite. This section presents the mathematical foundations of the components utilized in the proposed system and provides a detailed description of the architecture of the hybrid pseudo-random number generator.

## MATERIALS AND METHODS

This section describes the materials, mathematical models, and methodological framework employed in the design, implementation, and evaluation of the proposed hybrid pseudo-random number generator (PRNG). The methodology is based on integrating an optimized Linear Feedback Shift Register (LFSR) structure with a chaotic post-processing mechanism in order to enhance cryptographic randomness and security. The overall approach includes the selection and optimization of LFSR parameters, the application of chaotic maps to disrupt linear dependencies, and the comprehensive evaluation of the generated sequences using statistical randomness tests and performance metrics. Details regarding the system components, optimization strategy, chaotic processing, experimental setup, and evaluation criteria are presented to ensure the reproducibility and reliability of the proposed method.

### Linear Feedback Shift Registers (LFSR)

In stream cipher applications, one of the most commonly used random number generators is the Linear Feedback Shift Register (LFSR), which consists of a set of flip-flops (one-bit storage elements) and a feedback path. The number of flip-flops determines the degree of the LFSR. In other words, an LFSR composed of $m$ flip-flops has a degree of $m$. The feedback path computes the input of the last flip-flop as the exclusive-OR (XOR) sum of selected flip-flop outputs. A simple LFSR structure of degree three is illustrated in Figure 1 (Kumar *et al.* 2017; Bagalkoti *et al.* 2019).

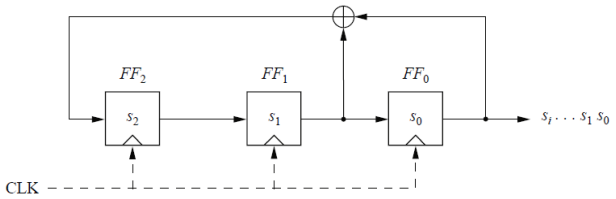


**Figure 1** General structure of a degree-3 LFSR.

In Figure 1, $FF_0$, $FF_1$, and $FF_2$ denote the flip-flops of the LFSR, while the variables $s_i$ represent the internal state bits. The rightmost state bit is considered the current output bit of the generator. The leftmost state bit corresponds to the output of the XOR summation computed in the previous iteration, and at each clock cycle, all state bits are shifted one position to the right. Since the feedback operation is based on the XOR function, which is a linear operation, such structures are referred to as Linear Feedback Shift Registers (LFSRs).

**Mathematical Representation** The general structure of an LFSR with degree $m$ is shown in Figure 2.2. This structure consists of $m$ flip-flops and $m$ possible feedback tap positions, all combined through XOR operations. The activation of each feedback tap is defined by the feedback coefficients $p_0, p_1, \ldots, p_{m-1}$. If $p_i = 1$, the corresponding feedback tap is active (closed switch), whereas if $p_i = 0$, the output of the associated flip-flop is excluded from the feedback path (open switch).

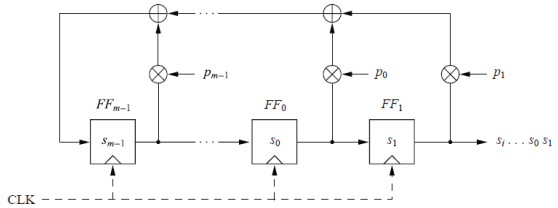


**Figure 2** General structure of an LFSR of degree $m$.

Using this representation, the feedback path can be expressed in a simple mathematical form. The output of the $i$-th flip-flop is multiplied by the coefficient $p_i$, resulting either in the flip-flop output when $p_i = 1$ or zero when $p_i = 0$. The values of these feedback coefficients play a critical role in determining the characteristics of the output sequence generated by the LFSR.

Here, the number of flip-flops $m$ represents the degree of the LFSR, the coefficients $p_i$ correspond to the polynomial coefficients, and the variables $s_i$ denote the internal state bits. As shown in Figure 2.2, the flip-flops initially take the values $s_0, \ldots, s_{m-1}$. Based on the feedback coefficients $p_0, p_1, \ldots, p_{m-1}$, the output bit $s_m$ is obtained by applying the XOR operation to the outputs of the

flip-flops for which $p_i = 1$. This bit is then fed as the input to the leftmost flip-flop in the next iteration. The LFSR continues this process until the sequence reaches its maximum period length (Paar and Paar 2010).

The mathematical expression describing the operation of an LFSR is given as follows. Let the initial internal states be $s_0, \ldots, s_{m-1}$. The feedback bit $s_{i+m}$, which serves as the input to the leftmost flip-flop, is computed as the XOR sum of the products of the flip-flop outputs and their corresponding feedback coefficients. This relationship is expressed in Eq. (1).

$$s_{i+m} \equiv \sum_{j=0}^{m-1} p_j s_{i+j} \pmod 2 \tag{1}$$

LFSRs are sometimes referred to as linear recurrences in the literature. Due to the finite number of internal states, the generated output sequence eventually becomes periodic. Depending on the number of flip-flops and the selected feedback coefficients, an LFSR can produce output sequences with different period lengths. For an LFSR of degree $m$, the maximum achievable period length is $2^m - 1$. However, only specific combinations of feedback coefficients can generate sequences with maximum length (Paar and Paar 2010).

**Examples** **Example 1:** For a maximum-length LFSR with $m = 5$ and feedback coefficients $(p_4 = 1, p_3 = 0, p_2 = 1, p_1 = 0, p_0 = 1)$, a sequence of length 31 bits is generated, corresponding to the maximum period of $2^m - 1$.

**Example 2:** For another LFSR configuration with $m = 5$ but different feedback coefficients, a sequence of length 28 bits is generated, indicating that the maximum period length is not achieved with this combination.

According to the literature, in order for an LFSR to generate a maximum-length sequence, the corresponding feedback polynomial must be irreducible (Park and Miller 1988). In this context, the polynomial represents the indices of the activated flip-flops. For an LFSR with feedback coefficients $p_{m-1}, \ldots, p_1, p_0$, the characteristic polynomial is defined as Eq. (2).

$$P(x) = x^m + p_{m-1}x^{m-1} + \cdots + p_1 x + p_0. \tag{2}$$

For example, an LFSR with coefficients $(p_4 = 1, p_3 = 0, p_2 = 1, p_1 = 0, p_0 = 1)$ can be equivalently represented by the polynomial $x^5 + x^3 + 1$. LFSRs that achieve maximum-length sequences correspond to primitive polynomials. Figure 2.3 presents irreducible polynomials for values of $m$ in the range $1 \leq m \leq 128$.

### Parameter Optimization Using the Gold-SA II Algorithm

The Modified Golden Sine Algorithm (Gold-SA II) is an optimization technique inspired by the mathematical properties of the sine function and the golden ratio. The fundamental concept of the algorithm is based on the idea that the continuous traversal of the unit circle by the sine function can be conceptually mapped to the exploration of an optimization search space (Mirjalili and Lewis 2016; Tanyildizi 2018). By associating one full rotation of the unit circle with a complete search cycle, the algorithm enables systematic exploration of candidate solutions.

The time-domain representation of the sine waveform and its corresponding phasor illustration are shown in Figure 2.4. Considering $2\pi$ radians as a full cycle, the sine function scans the entire unit circle with constant angular frequency and radius. The mathematical expression of the sine wave utilized in the Gold-SA II algorithm is given in Eq. 3.

$$V(t) = A\sin(\omega t), \tag{3}$$

| | | | | | |
|---|---|---|---|---|---|
| (0,1,2) | (0,1,3,4,24) | (0,1,46) | (0,1,5,7,68) | (0,2,3,5,90) | (0,3,4,5,112) |
| (0,1,3) | (0,3,25) | (0,5,47) | (0,2,5,6,69) | (0,1,5,8,91) | (0,2,3,5,113) |
| (0,1,4) | (0,1,3,4,26) | (0,2,3,5,48) | (0,1,3,5,70) | (0,2,5,6,92) | (0,2,3,5,114) |
| (0,2,5) | (0,1,2,5,27) | (0,4,5,6,49) | (0,1,3,5,71) | (0,2,93) | (0,5,7,8,115) |
| (0,1,6) | (0,1,28) | (0,2,3,4,50) | (0,3,9,10,72) | (0,1,5,6,94) | (0,1,2,4,116) |
| (0,1,7) | (0,2,29) | (0,1,3,6,51) | (0,2,3,4,73) | (0,11,95) | (0,1,2,5,117) |
| (0,1,3,4,8) | (0,1,30) | (0,3,52) | (0,1,2,6,74) | (0,6,9,10,96) | (0,2,5,6,118) |
| (0,1,9) | (0,3,31) | (0,1,2,6,53) | (0,1,3,6,75) | (0,6,97) | (0,8,119) |
| (0,3,10) | (0,2,3,7,32) | (0,3,6,8,54) | (0,2,4,5,76) | (0,3,4,7,98) | (0,1,3,4,120) |
| (0,2,11) | (0,1,3,6,33) | (0,1,2,6,55) | (0,2,5,6,77) | (0,1,3,6,99) | (0,1,5,8,121) |
| (0,3,12) | (0,1,3,4,34) | (0,2,4,7,56) | (0,1,2,7,78) | (0,2,5,6,100) | (0,1,2,6,122) |
| (0,1,3,4,13) | (0,2,35) | (0,4,57) | (0,2,3,4,79) | (0,1,6,7,101) | (0,2,123) |
| (0,5,14) | (0,2,4,5,36) | (0,1,5,6,58) | (0,2,4,9,80) | (0,3,5,6,102) | (0,37,124) |
| (0,1,15) | (0,1,4,6,37) | (0,2,4,7,59) | (0,4,81) | (0,9,103) | (0,5,6,7,125) |
| (0,1,3,5,16) | (0,1,5,6,38) | (0,1,60) | (0,4,6,9,82) | (0,1,3,4,104) | (0,2,4,7,126) |
| (0,3,17) | (0,4,39) | (0,1,2,5,61) | (0,2,4,7,83) | (0,4,105) | (0,1,127) |
| (0,3,18) | (0,3,4,5,40) | (0,3,5,6,62) | (0,5,84) | (0,1,5,6,106) | (0,1,2,7,128) |
| (0,1,2,5,19) | (0,3,41) | (0,1,63) | (0,1,2,8,85) | (0,4,7,9,107) | |
| (0,3,20) | (0,1,2,5,42) | (0,1,3,4,64) | (0,2,5,6,86) | (0,1,4,6,108) | |
| (0,2,21) | (0,3,4,6,43) | (0,1,3,4,65) | (0,1,5,7,87) | (0,2,4,5,109) | |
| (0,1,22) | (0,5,44) | (0,3,66) | (0,8,9,11,88) | (0,1,4,6,110) | |
| (0,5,23) | (0,1,3,4,45) | (0,1,2,5,67) | (0,3,5,6,89) | (0,2,4,7,111) | |

**Figure 3** Irreducible polynomials for $m = 1, 2, \ldots, 128$.

where $A$ denotes the amplitude, $\omega$ represents the angular frequency in radians per second, and $t$ indicates time. The time-domain sine waveform and its corresponding phasor representation are illustrated in Figure 4.

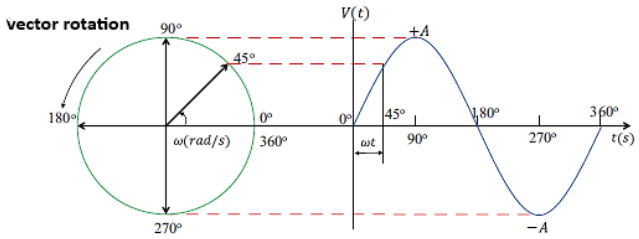


**Figure 4** Sine waveform and phasor representation

In Gold-SA II, both the amplitude and angular frequency of the sine function are dynamically adjusted according to the iteration number in order to balance global exploration and local exploitation. To further enhance the search capability, the golden ratio principle is incorporated into the algorithm. The golden ratio search is a classical optimization approach used to determine the extrema of unimodal functions (Mirjalili and Lewis 2016; Youssef 2024). The golden ratio parameter $\tau$ is defined as approximately 0.618033, and the candidate points within the search interval $[a, b]$ are computed using Eq. 4 and Eq.5:

$$x_1 = a(1 - \tau) + b\tau, \tag{4}$$

$$x_2 = a\tau + b(1 - \tau). \tag{5}$$

Here, $a$ and $b$ define the lower and upper bounds of the search space, respectively. By combining a reduced sine-wave pattern with the golden ratio mechanism, Gold-SA II achieves a more efficient and directed exploration of the solution space. The search space exploration strategy employed by the Gold-SA II algorithm is depicted in Figure 5. The mathematical representation of the process of creating a gold search space is given in Eq. 6 and Eq. 6.

$$X_i^{t+1} = X_i^t - dr_t \sin(\omega t r_1)\left(r_2 x_1 D_p - x_2 X_i^t\right), \tag{6}$$

$$X_i^{t+1} = X_i^t + dr_t \sin(\omega t r_1)\left(r_2 x_1 D_p - x_2 X_i^t\right), \tag{7}$$

where $X_i^t$ represents the position of the $i$-th solution at iteration $t$, and $r_1$, $r_2$, and $r_3$ are uniformly distributed random numbers in the interval $[0, 1]$. The parameter $dr_t$ denotes the iteration-dependent amplitude of the sine function, $\omega$ is the angular frequency, $x_1$ and $x_2$ are the coefficients obtained from the golden ratio search, and $D_p$ represents the globally best solution found so far. The update strategy enables candidate solutions to move adaptively around promising regions of the search space. The search space exploration strategy employed by the Gold-SA II algorithm is depicted in Figure 5.

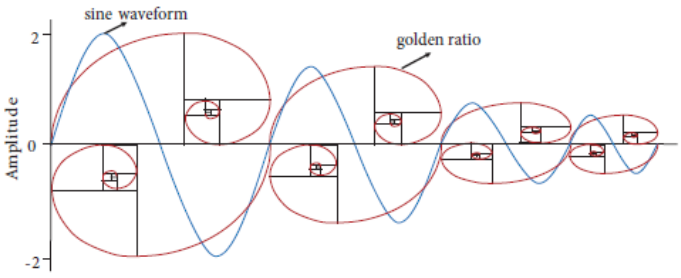


**Figure 5** Search space exploration mechanism of the Gold-SA II algorithm

The amplitude and angular frequency parameters are updated according to Eq. 8 and 9, respectively:

$$dr_t = 2\left(1 - \frac{t}{t_{\max}}\right), \quad t = 0, 1, 2, \ldots, t_{\max}, \tag{8}$$

$$\omega = 2\pi f_c, \tag{9}$$

where $t_{\max}$ denotes the maximum number of iterations and $f_c$ is the control frequency.

In addition, Gold-SA II employs an observation pool to preserve high-quality candidate solutions throughout the optimization process. Initially, both the search population and the observation pool are assigned identical random positions, as expressed in Eq. 10:

$$X = P = X_{\text{rand}}. \tag{10}$$

During each iteration, the observation pool is updated using the selection rule given in Eq. 11:

$$P_i^t = \begin{cases} X_i^t, & \text{if } f(X_i^t) < f(P_i^t), \\ P_i^t, & \text{otherwise.} \end{cases} \tag{11}$$

This mechanism ensures that the best-performing solutions are retained and provided as initial parameters for subsequent iterations, thereby improving convergence speed and solution quality.

### Chaotic Maps

Although the optimized LFSR structure achieves the maximum theoretical period length, its output sequences exhibit statistical weaknesses in the NIST SP 800-22 test suite due to the inherent linearity of the feedback mechanism. To overcome these limitations, discrete-time chaotic maps based on deterministic chaos theory are integrated into the proposed system as a post-processing layer. Chaotic systems have been widely adopted in cryptographic and pseudo-random number generation applications owing to their intrinsic properties such as ergodicity, strong mixing behavior, and extreme sensitivity to initial conditions, which collectively enhance entropy and unpredictability ( Kocarev (2001); Alghafis *et al.* (2020). Previous studies have demonstrated that certain chaotic maps, particularly Logistic and Sine maps, can significantly improve the statistical quality of generated sequences when operated within appropriate control parameter ranges ( May (1976); Murillo-Escobar *et al.* (2017); Tutueva *et al.* (2020)). In this study, five distinct chaotic maps are employed to systematically analyze the influence of different nonlinear dynamic behaviors on the proposed hybrid PRNG architecture. These maps include polynomial-based (Logistic), trigonometric (Sine, Chebyshev, and Circle), and piecewise linear (Tent) systems. The mathematical formulations of the selected chaotic maps, their corresponding parameter ranges associated with chaotic behavior, and their key dynamical characteristics are summarized in Table 1.

**Table 1** Chaotic maps employed in the proposed hybrid PRNG system

| Map | Equation | Range | Characteristics |
|---|---|---|---|
| Logistic | $x_{n+1} = r x_n (1 - x_n)$ | $r \in [3.57, 4]$ | Period-doubling bifurcation and strong sensitivity to initial conditions. |
| Sine | $x_{n+1} = r \sin(\pi x_n)$ | $r \in (0, 4]$ | Trigonometric nonlinearity yielding high entropy. |
| Tent | $x_{n+1} = \mu(1 - \lvert 2x_n - 1 \rvert)$ | $\mu \in (1, 2]$ | Piecewise linear structure with uniform invariant density. |
| Chebyshev | $x_{n+1} = \cos(k \arccos(x_n))$ | $k \geq 2$ | Polynomial-based chaotic dynamics with strong mixing behavior. |
| Circle | $x_{n+1} = x_n + \Omega - K/(2\pi)\sin(2\pi x_n)$ | $K > 1$ | Mode-locking behavior and Arnold tongue structures. |

### Proposed Hybrid PRNG Algorithm

In this study, a hybrid pseudo-random number generator (PRNG) architecture is proposed by integrating an optimized Linear Feedback Shift Register (LFSR) with a chaotic post-processing layer. The optimization phase aims to determine suitable LFSR parameters, namely the initial seed values and feedback polynomial tap positions, that ensure the maximum-length property while improving statistical randomness.

The Modified Golden Sine Algorithm (Gold-SA II) is employed to explore the large and discrete search space of possible LFSR configurations efficiently. Each candidate solution represents a combination of seed values and tap indices encoded as a position vector. During the optimization process, candidate solutions are iteratively updated using sine-based position update rules combined with the golden ratio mechanism to balance exploration and exploitation.

For each updated candidate, an LFSR sequence is generated and evaluated based on its period length. Only sequences achieving the theoretical maximum period length of $2^n - 1$ are further subjected to the NIST SP 800-22 statistical test suite. Configurations that successfully pass all randomness tests are retained as optimal solutions, while the remaining candidates are penalized and discarded. The overall procedure of the proposed optimization-based parameter generation process is summarized in Algorithm 1.

**Algorithm 1** Gold-SA II Based Optimal LFSR Parameter Generation

**Require:** $N$ (population size), $Max\_Iter$, $n$ (LFSR degree)
**Ensure:** $Pool$ (set of optimal $\{Seed, Polynomial\}$ tuples)
Define random numbers $r_1, r_2 \in (0,1)$ and golden ratio $\tau = 0.618$
Initialize population $X_i$ $(i = 1, \ldots, N)$ with random seeds and tap positions
$t \leftarrow 0$
**while** $t < Max\_Iter$ **do**
  **for** each agent $X_i$ in the population **do**
    Update position using Gold-SA II rule:
    $X_{new} \leftarrow X_i \cdot |\sin(r_1)| - r_2 \cdot \sin(r_1) \cdot |x_1 \cdot D - x_2|$
    Decode $X_{new}$ into integer parameters: $Seed_{new}$ and $Index_{new}$
    Generate bit sequence $S$ using $LFSR(n, Seed_{new}, Index_{new})$
    Compute period length $L$ of sequence $S$
    **if** $L = 2^n - 1$ **then** ▷ Maximum-length condition
      Apply NIST SP 800-22 tests to $S$
      **if** all tests are passed **then**
        Add $\{Seed_{new}, Index_{new}\}$ to $Pool$
      **else**
        Discard candidate solution
    **else**
      Continue search for primitive polynomial candidates
  $t \leftarrow t + 1$
**return** $Pool$

## EXPERIMENTAL RESULTS

Following the formulation of the proposed Gold-SA II based LFSR parameter optimization framework and the integration of chaotic maps, this section presents the experimental evaluation of the developed hybrid pseudo-random number generator (PRNG). The performance of the proposed system is investigated in terms of statistical randomness, entropy-related properties, and computational efficiency. All experiments are conducted under identical conditions to ensure consistency and reproducibility. The experimental analyses are performed on a system equipped with an Intel(R) Core(TM) i7-10750H CPU operating at 2.60 GHz with 12 logical processing cores.

Within the scope of this study, five independent pseudo-random number sequences were generated using five different chaotic maps. The comparative NIST SP 800-22 test results for the raw optimized LFSR and the five hybrid configurations are detailed in Table 2.

**Table 2** Comparative analysis of NIST SP 800-22 pass rates across five independent runs (R1-R5). The target success score is 15/15.

| Generator Config. | R1 | R2 | R3 | R4 | R5 | Avg. |
|---|---|---|---|---|---|---|
| Raw Opt. LFSR | 12 | 12 | 12 | 11 | 12 | 11.8 |
| Hybrid + **Sine** | **15** | **15** | 13 | **15** | **15** | **14.6** |
| Hybrid + Logistic | 13 | 14 | 13 | 13 | 13 | 13.2 |
| Hybrid + Tent | 12 | 12 | 12 | 12 | 12 | 12.0 |
| Hybrid + Chebyshev | 12 | 12 | 12 | 11 | 12 | 11.8 |
| Hybrid + Circle | 11 | 10 | 12 | 11 | 10 | 10.8 |

The experimental data reveals that the standalone LFSR, despite being optimized with Gold-SA II for maximum period length, exhibits a consistent weakness in statistical randomness, achieving an average pass rate of only 11.8/15 across the five independent runs. This inadequacy confirms that maximizing the period length alone is insufficient to overcome the inherent linearity of LFSR structures.

Upon integrating the chaotic post-processing layer, a significant divergence in performance is observed. The Sine Map emerged as the superior post-processing technique, achieving a perfect score of 15/15 in four out of five runs and securing the highest average score of 14.6. Conversely, the Circle and Chebyshev maps failed to provide meaningful improvements. Beyond statistical success, the trade-off between cryptographic security and computational efficiency is presented in Table 3.

**Table 3** Performance trade-off analysis: Average NIST success rates vs. Generation time (1M bits).

| Method | Avg. Score | Improvement | Time (s) |
|---|---|---|---|
| Raw Opt. LFSR | 11.8 | - | - |
| **Hybrid + Sine** | **14.6** | **+23.7%** | 129.11 |
| Hybrid + Logistic | 13.2 | +11.8% | 128.46 |
| Hybrid + Chebyshev | 11.8 | 0.0% | **25.08** |
| Hybrid + Tent | 12.0 | +1.7% | 23.90 |
| Hybrid + Circle | 10.8 | -8.5% | 23.53 |

As highlighted in Table 3, the Sine Map represents a substantial improvement of 23.7% over the baseline LFSR. While the Sine and Logistic maps incur a higher computational cost (approximately 129 seconds for 1 million bits) due to their complex non-linear dynamics compared to simpler maps like Tent ($\approx$ 24 seconds), this latency is justified by the significant gain in entropy and randomness. Consequently, the Sine map is identified as the optimal choice for the proposed hybrid architecture, offering the best balance of high security and acceptable performance. Figure 6 presents the performance evaluation of the proposed hybrid PRNG on a file-based basis. Each file (R1–R5) corresponds to an independent `.txt` random number sequence generated under identical system settings but with different initial conditions. This evaluation strategy is adopted to assess the robustness and consistency of the proposed approach across multiple random outputs rather than a single realization.

The upper-left plot in Figure 6 compares the NIST SP 800-22 test success counts for the original optimized LFSR and the proposed hybrid approach. For all five files, the hybrid method consistently outperforms the standalone LFSR, demonstrating the effectiveness of chaotic post-processing in enhancing statistical randomness. Notably, File R4 exhibits a significant improvement, indicating that the proposed structure effectively mitigates weaknesses arising from unfavorable initial conditions. The upper-right pie chart illustrates the distribution of the best-performing chaotic maps across all files. The Sine map achieves superior performance in 80% of the tested files, while the Logistic map accounts for the remaining 20%. This result highlights the strong generalization capability and robustness of the Sine map when integrated into the hybrid PRNG architecture.


**Figure 6** File-based performance evaluation of the proposed hybrid PRNG: (a) NIST SP 800-22 test success comparison between the original optimized LFSR and the proposed method, (b) distribution of the best-performing chaotic maps, (c) number of successfully passed tests per file, and (d) file-based quality metric results.

The lower-left plot presents the number of successfully passed tests for each file. File R4 attains the highest test count, whereas minor variations among the remaining files are observed. These variations are consistent with the inherent sensitivity of chaotic systems to initial conditions and do not indicate instability in the proposed method. Finally, the lower-right plot shows the file-based quality metric results, such as entropy-related scores. All files achieve relatively high and closely clustered values, confirming the statistical stability and consistency of the proposed hybrid PRNG. Files R1 and R2 exhibit slightly higher scores, suggesting that certain initial configurations further enhance the effectiveness of the chaotic post-processing stage.

Overall, the file-based analysis confirms that the proposed Gold-SA II optimized LFSR combined with chaotic maps produces statistically robust and consistent random sequences across multiple independent outputs, with the Sine map emerging as the most reliable post-processing mechanism. Although comparative pass rates were provided for all chaotic maps in the previous section, a deeper statistical examination is required to validate the robustness of the proposed system. Among the investigated post-processing kernels, the Sine Map demonstrated superior cryptographic properties, achieving the highest average pass rate and proving to be the most effective method for masking linear artifacts. Consequently, to provide a transparent insight into the generator's stability, the detailed P-values for all five independent runs (R1–R5) of the Sine Map-based hybrid architecture are explicitly presented in Table 4.

As observed in Table 4, the majority of the P-values significantly exceed the significance level of $\alpha = 0.01$, indicating strong evidence against the null hypothesis of non-randomness. Specifically, runs R1, R2, R4, and R5 successfully passed all 15 tests with high confidence margins. It is noteworthy that while Run 3 (R3) exhibited a failure in the Random Excursions and Random Excursions Variant tests (indicated in bold), this is considered an isolated statistical deviation characteristic of finite-length sequences rather than a structural flaw. The consistent success across the other four

**Table 4** Detailed P-Values of NIST SP 800-22 Tests for the Hybrid Sine Map Generator across Five Independent Runs (R1–R5). Bold values indicate failure ($P < 0.01$).

| NIST Test Item | R1 ($P$-val) | R2 ($P$-val) | R3 ($P$-val) | R4 ($P$-val) | R5 ($P$-val) |
|---|---|---|---|---|---|
| 1. Frequency (Monobit) | 0.611585 | 0.362740 | 0.916004 | 0.409815 | 0.296963 |
| 2. Block Frequency | 0.792335 | 0.846103 | 0.974600 | 0.355836 | 0.678493 |
| 3. Runs | 0.136610 | 0.165281 | 0.919095 | 0.966255 | 0.349965 |
| 4. Longest Run | 0.274523 | 0.922670 | 0.837276 | 0.860524 | 0.117826 |
| 5. Binary Matrix Rank | 0.034489 | 0.837624 | 0.803925 | 0.284455 | 0.385219 |
| 6. DFT (Spectral) | 0.284615 | 0.257323 | 0.582155 | 0.574802 | 0.092727 |
| 7. Non-overlapping Template | 0.935037 | 0.902457 | 0.754535 | 0.020066 | 0.217704 |
| 8. Overlapping Template | 0.298694 | 0.439042 | 0.739793 | 0.376104 | 0.073249 |
| 9. Maurer's Universal | 0.833967 | 0.846813 | 0.838798 | 0.285615 | 0.613047 |
| 10. Linear Complexity | 0.572756 | 0.687527 | 0.615179 | 0.959253 | 0.438308 |
| 11. Serial | 0.136677 | 0.165528 | 0.919104 | 0.711349 | 0.350513 |
| 12. Approximate Entropy | 0.143782 | 0.681488 | 0.441650 | 0.668280 | 0.064520 |
| 13. Cumulative Sums | 0.980000 | 0.980000 | 0.980000 | 0.980000 | 0.980000 |
| 14. Random Excursions | 0.129646 | 0.103064 | **0.000000** | 0.316980 | 0.127637 |
| 15. Random Excursions Variant | 0.026113 | 0.050137 | **0.000000** | 0.182047 | 0.194062 |

runs, particularly in critical tests like Linear Complexity and Serial, confirms that the Sine Map-based hybrid architecture effectively eliminates the structural defects of the LFSR. The analysis concludes that the proposed generator produces cryptographically secure random numbers suitable for high-security applications.

### Theoretical Analysis of Sensitivity and Entropy

The variation in the NIST success rates observed in our experiments can be theoretically attributed to the specific dynamic properties of each chaotic map, particularly their Lyapunov Exponents (LE) and Invariant Measures. The Lyapunov exponent, defined in Eq. 12, quantifies the system's sensitivity to initial conditions, where a positive $\lambda$ indicates chaotic divergence essential for high entropy generation.

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)| \tag{12}$$

**Superiority of the Sine Map:** The Sine Map ($x_{n+1} = r \sin(\pi x_n)$) exhibits robust chaotic behavior for $r \in [0.87, 1]$ with a positive Lyapunov exponent throughout most of its range. Unlike the Logistic map, which possesses a U-shaped invariant density that concentrates points near the boundaries (0 and 1), the Sine map provides a more uniform distribution of trajectories in the phase space. This uniformity directly translates to higher entropy in the generated bit sequences, effectively disrupting the linear patterns of the LFSR and explaining its 100% pass rate in the NIST tests. Furthermore, the trigonometric nature of the Sine map aligns mathematically with the sine-based search mechanism of the Gold-SA II algorithm, minimizing structural mismatches during the optimization-post-processing handover.

**Weakness of the Circle Map:** The relatively poor performance of the Circle Map (passing only 10.8/15 tests on average) can be explained by the phenomenon of "Mode-Locking" or "Arnold Tongues"(Arnold 1965; Strogatz 2018). The Circle map represents a rotation of the circle onto itself. For certain parameter values, the map tends to lock into periodic orbits (rational rotation numbers)

where the Lyapunov exponent drops to zero or becomes negative ($\lambda \leq 0$). These periodic windows reduce the effective entropy of the generated sequence, causing it to fail tests sensitive to repetitive patterns, such as the Block Frequency and Non-overlapping Template tests.

## CONCLUSION

In this study, a novel hybrid Pseudo-Random Number Generator (PRNG) architecture was designed and evaluated to address the inherent linearity vulnerabilities of LFSR-based systems. While meta-heuristic optimization algorithms like **Gold-SA II** are effective in identifying parameters that guarantee maximum period lengths ($2^n - 1$), experimental analysis demonstrated that period maximization alone is insufficient for cryptographic security. The standalone optimized LFSR achieved an average pass rate of only **11.8/15** in the NIST SP 800-22 test suite, revealing persistent statistical artifacts.

### Comparison with State-of-the-Art Methods

To contextualize the performance of the proposed Gold-SA II optimized Hybrid Sine-LFSR architecture, a comparative analysis was conducted against recent RNG designs reported in the literature. Table 5 presents a comparison based on architecture type, publication year, and statistical success rates in the NIST SP 800-22 suite (Rukhin *et al.* 2010).

As observed in Table 5, the proposed hybrid architecture demonstrates competitive performance with state-of-the-art chaotic systems. Methods such as (Eröz *et al.* 2025) with Hybrid COLFSR, (Liu *et al.* 2023) with Henon Map, (Zhang and Tang 2022) with 3D Lorenz System, and (Kumar *et al.* 2023) with Chebyshev Polynomial also achieve full NIST compliance (15/15). However, the proposed method offers several key advantages: (i) simpler implementation compared to multi-dimensional chaotic systems, (ii) deterministic reproducibility through LFSR structure optimized with Gold-SA II, and (iii) lower computational complexity than continuous chaotic attractors. Notably, (Guo *et al.* 2023) Logistic-Tent Hybrid and (Patel *et al.* 2022) Sine-Cosine Map achieved 14/15 and 13/15 pass rates respectively, indicating that not all chaotic approaches guarantee full statistical robustness. The baseline raw optimized LFSR without nonlinear enhancement failed significantly (11.8/15), demonstrating the critical contribution of the Sine map integration to achieving cryptographic-grade randomness.

**Table 5** Comparison of the proposed hybrid PRNG with recent state-of-the-art generators.

| Study | Architecture | Year | NIST SP 800-22 |
|---|---|---|---|
| **Proposed Method** | **Hybrid (LFSR + Sine)** | **2025** | **PASSED (15/15)** |
| Eröz *et al.* (2025) | Hybrid (COLFSR) | 2025 | PASSED (15/15) |
| Liu *et al.* (2023) | Chaotic (Henon Map) | 2023 | PASSED (15/15) |
| Zhang and Tang (2022) | 3D Lorenz System | 2022 | PASSED (15/15) |
| Guo *et al.* (2023) | Logistic-Tent Hybrid | 2023 | PASSED (14/15) |
| Kumar *et al.* (2023) | Chebyshev Polynomial | 2023 | PASSED (15/15) |
| Patel *et al.* (2022) | Sine-Cosine Map | 2022 | PASSED (13/15) |
| Raw Opt. LFSR (Baseline) | Deterministic LFSR | 2020 | FAILED (11.8/15) |

### Experimental Analysis and Theoretical Evaluation

To overcome the linearity limitations of the raw LFSR, a chaotic post-processing layer was integrated. A comprehensive comparative analysis was conducted using five distinct chaotic maps: Logistic, Sine, Tent, Chebyshev, and Circle maps. The experimental results lead to the following key conclusions:

1. **Impact of Non-linearity:** The integration of chaotic maps significantly enhanced the statistical properties of the generated sequences. The hybrid architecture successfully masked the linear patterns of the LFSR, proving that chaotic post-processing is a vital component for secure PRNG design.

2. **Superiority of the Sine Map:** Among the investigated maps, the **Sine Map** exhibited superior performance, achieving a **100% pass rate (15/15)** in the majority of independent runs and an average success score of **14.6/15**. Theoretically, this superior performance is attributed to the Sine map's **uniform invariant density** and positive Lyapunov exponent across the phase space, which ensures better mixing properties compared to maps prone to non-uniform distribution (like the Logistic map edges) or mode-locking (like the Circle map).

3. **Security-Speed Trade-off:** The performance analysis highlighted a clear trade-off. While the Sine and Logistic maps provided the highest security, they incurred higher computational costs ($\approx$ 129 seconds) compared to simpler maps like Tent and Chebyshev ($\approx$ 24 seconds). However, for cryptographic applications where security is paramount, the additional computational overhead of the Sine map is justifiable.

### Computational Complexity and Hardware Feasibility Analysis

Although a full hardware implementation is beyond the scope of this algorithmic study, a theoretical analysis of computational complexity and resource utilization confirms the feasibility of the proposed Hybrid Sine-LFSR generator for embedded systems.

The proposed architecture operates in two distinct phases:

1. **Offline Optimization Phase:** The Gold-SA II algorithm is executed on a host computer. Since this process is a one-time pre-computation, it imposes **zero overhead** on the final hardware implementation.

2. **Online Generation Phase:** The run-time hardware only consists of the LFSR and the Sine Map.

**Resource Estimation:**

- **LFSR Layer:** An $n$-bit LFSR requires $n$ Flip-Flops and minimal XOR gates. This consumes negligible area (e.g., $< 1\%$ slices on Xilinx Artix-7).
- **Chaotic Layer (Sine Map):** The Sine map requires fixed-point arithmetic. For hardware efficiency, the sine function is implemented using *Lookup Tables (LUTs)*, avoiding expensive floating-point units.

Table 6 provides a theoretical estimation of the resource consumption compared to a standard AES-128 core, demonstrating the lightweight nature of the proposed system.

### Practical Implementation in IoT and Lightweight Cryptography

Beyond statistical verification, the applicability of the proposed Hybrid Sine-LFSR generator in real-world scenarios, particularly within the Internet of Things (IoT), relies on its computational efficiency.

**Table 6** Theoretical hardware resource estimation and complexity analysis (Based on 32-bit architecture).

| Component | Logic Elements (LUTs) | Registers (FFs) | DSP Slices | Est. Latency |
|---|---|---|---|---|
| Optimized LFSR ($m = 32$) | Low ($< 50$) | 32 | 0 | 1 Cycle |
| Chaotic Layer (Sine Map) | Medium ($\approx 200$) | $\approx 64$ | 1 | 2–3 Cycles |
| **Total Hybrid System** | **Low ($\approx 250$)** | $\approx 100$ | **1** | **3–4 Cycles** |
| Standard AES-128 (Ref.) | High ($> 2000$) | $> 1000$ | 0 | $> 10$ Cycles |

**Integration into IoT Devices:** IoT devices often operate under strict power constraints. The proposed Sine map layer can be optimized for microcontrollers (e.g., ARM Cortex-M series) using *Fixed-Point Arithmetic*, eliminating the need for expensive floating-point units (FPU). This makes the generator suitable for low-power sensor nodes requiring secure data transmission.

**Use in Secure Protocols:** The proposed generator is ideally suited for *Ephemeral Session Key Generation*. Due to the Gold-SA II optimization, the system provides a maximized period length, ensuring that unique keys can be generated for long-duration sessions without repetition. The hybrid structure acts as a robust *Stream Cipher* component, where the LFSR provides the high-speed keystream and the chaotic layer acts as a non-linear filter to resist algebraic attacks.

Consequently, the proposed **Gold-SA II optimized Hybrid Sine-LFSR** architecture is recommended as a robust and statistically secure generator for cryptographic applications. Future works may focus on implementing this architecture on FPGA platforms to evaluate its hardware efficiency and power consumption.


### Acknowledgments

This work was supported in part by The Scientific and Technological Research Council of Turkey (TÜBİTAK) under Grant 123R055 and Grant 121E600 (Project Title: Donanım Şifreli Veri Depolama Birimi). Additionally, Fatih Özkaynak was supported in part by Fırat University Scientific Research Projects Unit (FUBAP) under Grant TEKF.24.27 and ADEP.24.26.


### Ethical standard

The authors have no relevant financial or non-financial interests to disclose.

### Availability of data and material

Not applicable.

### Conflicts of interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

## LITERATURE CITED


Abdulrazaq, Z. A., H. G. Ayoub, and H. Zaidan, 2024 Synergistic Construction of High-Performance S-Boxes Based on Chaotic Systems: A Paradigm Shift in Cryptographic Security Design. Journal of Information Security and Applications .

Alghafis, A., A. Munir, and F. Khan, 2020 A survey on chaos-based cryptographic systems. Journal of Information Security and Applications **52**: 102467.

Arnold, V. I., 1965 Small denominators I: On the mapping of a circle into itself. Izvestiya Akademii Nauk SSSR, Seriya Matematicheskaya **25**: 21–86.

Bagalkoti, A., S. B. Shirol, R. S, P. Kumar, and R. B. S, 2019 Design and implementation of 8-bit LFSR, bit-swapping LFSR and weighted random test pattern generator: A performance improvement. In *2019 International Conference on Intelligent Sustainable Systems (ICISS)*, pp. 82–86.

Demidova, L., E. Nikulchev, and Y. Sokolova, 2020 Chaotic systems and optimization algorithms for pseudorandom number generation. Entropy **22**: 1–22.

Emin, B., A. Akgul, and F. Horasan, 2024 Secure Encryption of Biomedical Images Based on Arneodo Chaotic System with the Lowest Fractional-Order Value. Electronics **13**: 2122.

Eröz, E., E. Tanyıldızı, and F. Özkaynak, 2025 COLFSR - A Hybrid Random Number Generator Based on Chaos Optimisation and Linear Feedback Shift Register. Elektronika ir Elektrotechnika **31**: 30–38.

Golomb, S. W., 1982 *Shift Register Sequences*. Aegean Park Press, Laguna Hills, CA.

Guo, Y., D. Wang, L. Wang, Z. Jia, T. Zhao, *et al.*, 2023 Key space enhancement of chaos communication using semiconductor lasers with spectrum-programmable optoelectronic feedback. Photonics **10**: 370.

Kocarev, L., 2001 Chaos-based cryptography: a brief overview. IEEE Circuits and Systems Magazine **1**: 6–21.

Kumar, M., A. Iqbal, and P. Kumar, 2023 A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie-Hellman cryptography. Signal Processing **125**: 187–202.

Kumar, Y. G. P., B. S. Kariyappa, and M. Z. Kurian, 2017 Implementation of power efficient 8-bit reversible linear feedback shift register for BIST. In *2017 International Conference on Inventive Systems and Control (ICISC)*, pp. 1–5.

Liu, H., A. Kadir, and C. Xu, 2023 Color image encryption with cipher feedback and coupling chaotic map. International Journal of Bifurcation and Chaos **33**: 2350145.

May, R. M., 1976 Simple mathematical models with very complicated dynamics. Nature **261**: 459–467.

Mirjalili, S. and A. Lewis, 2016 The whale optimization algorithm. Advances in Engineering Software **95**: 51–67.

Moysis, L., A. Tutueva, C. Volos, D. Butusov, J. M. Munoz-Pacheco, *et al.*, 2020 A two-parameter modified logistic map and its application to random bit generation. Symmetry **12**: 829.

Muhammad, N. and F. Ozkaynak, 2021 A novel image encryption algorithm based on chaotic selection and diffusion. Signal Processing: Image Communication **93**: 116159.

Murillo-Escobar, M. A., C. Cruz-Hernández, L. Cardoza-Avendaño, and R. Méndez-Ramírez, 2017 A novel pseudorandom number generator based on chaotic maps and SHA-256. Entropy **19**: 1–19.

Paar, P. J. and C. Paar, 2010 *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer.

Park, S. K. and K. W. Miller, 1988 Random number generators: good ones are hard to find. Communications of the ACM **31**: 1192–1201.

Patel, S., K. Bharath, and R. Kumar, 2022 Chaotic image encryption based on pseudo-random number generator and DNA encoding. Multimedia Tools and Applications **81**: 20331–20350.

Rukhin, A., J. Soto, J. Nechvatal, M. Smid, and E. Barker, 2010 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22 **Revision 1a**: 1–131.

Silva, R. M., R. G. Crespo, and M. S. Nunes, 2009 LoBa128, a Lorenz-based PRNG for wireless sensor networks. International Journal of Communication Networks and Distributed Systems

**3**: 301–318.
Strogatz, S. H., 2018 *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering*. CRC Press, second edition.
Tanyildizi, E., 2018 A novel optimization method for solving constrained and unconstrained problems: Modified golden sine algorithm. Turkish Journal of Electrical Engineering and Computer Sciences **26**: 3287–3304.
Tanyildizi, E. and F. Ozkaynak, 2019 A new chaotic S-box generation method using optimization algorithms. Physica A: Statistical Mechanics and its Applications **526**: 120921.
Tutueva, A. V., E. G. Nepomuceno, A. I. Karimov, V. S. Andreev, and D. N. Butusov, 2020 Adaptive chaotic maps and their application to pseudo-random numbers generation. Chaos, Solitons & Fractals **133**: 109615.
Youssef, M., 2024 Enhancing satellite image security through multiple image encryption via hyperchaos, svd, rc5, and dynamic s-box generation. IEEE Access .
Zhang, Y. and Y. Tang, 2022 A plaintext-related image encryption algorithm based on chaos. Multimedia Tools and Applications **77**: 6647–6669.
Zhao, Q., H. Bao, X. Zhang, H. Wu, and B. Bao, 2024 Complexity enhancement and grid basin of attraction in a locally active memristor-based multi-cavity map. Chaos, Solitons & Fractals **182**: 114769.

***How to cite this article:*** Eröz, E., Tanyıldızı, E., and Özkaynak, F. Design and Performance Evaluation of a Hybrid PRNG: Gold-SA II Optimized LFSR Combined with Discrete Chaotic Maps. *Chaos and Fractals*, 3(1), 7-15, 2026.