Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-A, pp. 3713–3725
DOI : 10.47974/JDMSC-3003

Chaotic polynomial sequences for high-entropy stream ciphers

D. Balaji [†]
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

Tanya Singh *
School of Engineering & Technology
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Nikhil Mohan Shinde [§]
Department of Mechanical Engineering
Vishwakarma University
Pune 411048
Maharashtra
India

Rajesh Kumar Tripathi [‡]
Department of Computer Engineering & Applications
GLA University
Mathura 281406
Uttar Pradesh
India

[†] *E-mail:* balaji@avit.ac.in
* *E-mail:* dean.academics@niu.edu.in (Corresponding Author)
[§] *E-mail:* nikhil.shinde@vupune.ac.in
[‡] *E-mail:* rajesh.tripathi@gla.ac.in

© Taru Publications

V. Dhanalakshmi [@]
Department of Computer Science
Meenakshi College of Arts and Science
Meenakshi Academy of Higher Education & Research (Deemed to be University)
Chennai 600078
Tamil Nadu
India

Kathirisetty Nikhila [#]
Department of Computer Science and Engineering
Vardhaman College of Engineering
Shamshabad
Hyderabad 501218
Telangana
India

Abstract

The chaotic sequences of polynomials have a promising but underutilized basis on the design of high-entropy stream ciphers, to mitigate constraints of predictability and low randomness in the design of conventional generators. The present paper suggests a hybrid chaotic-polynomial model that incorporates nonlinear iterative map with adaptive coefficient perturbation. The model is also tested with NIST statistical test suites as well as real-time encryption benchmark on IoT data. The outcomes show the enhancement of entropy up to 0.998, which is 21.4 % more than with LFSR-based ciphers, and a 34.7 % decrease in correlation. The proposed method has an 18.2% better key sensitivity, and increased resistance to differential attacks when compared to the existing chaotic systems. Furthermore, the performance of the encryption process in the embedded devices (Raspberry Pi and ESP32) showed that high speed encryption (up to 224.7 Mbps) is possible with the proposed framework with relatively small memory consumption, which confirms the applicability of the proposed framework to the low resource-based secure IoT communication environment. The solution guarantees a scalable and secure communication provisioning a strong paradigm in next-generation cryptographic stream ciphers.

Subject Classification: *14G50, 94A60.*

Keywords: *Stream cipher, Chaotic polynomial sequences, Linear feedback shift register, High-entropy cryptography, NIST statistical testing, Nonlinear keystream generation.*

[@] *E-mail:* **dhanalakshmiv@maher.ac.in**
[#] *E-mail:* **nikhila@vardhaman.org**

1. Introduction

Stream ciphers are the core of real-time encryption schemes in contemporary electronic communication networks, but due to their long history of using Linear Feedback Shift Registers (LFSRs), they are susceptible to critical attacks [1]. LFSR-based generators are computationally efficient, but fail to provide sequences with high linear complexity, and predictable periodic structure, which is prone to both algebraic and correlation attacks [2]. The necessarily deterministic character of these generators does not satisfy the entropy requirements of the cryptography needs of the next generation, especially in limited resource settings such as IoT networks [3]. Chaotic dynamical systems have been a focus of much research interest as other sources of randomness since they are exceedingly sensitive to initial conditions and long-range unpredictable [4]. But standalone chaotic generators have the disadvantage of finite precision reduction in digital implementations and this causes a decrease in the cycle length and periodic orbits which are in essence fatal to security assurances. On the same note, sequence generators based on polynomials provide great algebraic complexity, but are not ergodic to remove statistical correlations between blocks of keystream [5].

A promising way out of these two restrictions is the combination of the chaotic dynamics with the construction of the sequence using polynomials [6]. The combination of the sensitive dependence on initial conditions of chaotic maps together with the algebraic richness of the polynomial generators makes it possible to design keystreams with a high entropy level as well as high statistical independence [7]. Recent developments in adaptive perturbation strategies also allow the modulation of the coefficients leading to dynamic trajectory modulation to avoid trajectory collapse and maintain chaotic behaviour over long encryption sessions [8]. In this paper, we suggest a Chaotic Polymorphous Stream Cipher (CPSC) model that methodically combines nonlinear iterative maps with adaptive perturbation of the coefficient of the polynomials [9]. The main goals are to reach a Shannon entropy of more than 0.99, auto-correlation of less than 0.28, and improved resilience to differential and statistical attacks and be computationally feasible when used in an IoT deployment setting.

2. Chaotic Systems in Cryptography

Chaotic systems are deterministic but unpredictable, such that their behaviour is sensitive to initial conditions, producing outputs which are statistically indistinguishable to truly random output [10]. The state x_n is evolved by the logistic map which is a canonical one-dimensional chaotic system and develops the state based on the following recurrence with r being in [3.57, 4] to have fully developed chaotic behaviour (Eq. 1):

$$x_n{}^{+1} = r \bullet x_n \bullet (1 - x_n), r \in [3.57,4], x_n \in (0,1) \quad (1)$$

The logistic recurrence (Eq. 1) is given by the bifurcation parameter, r, which has a value of r, which determines the depth of chaos. The greater the r values, the closer the trajectories generated tend to be, and this is crucial in generating the keystream [11].

The tent map offers piecewise linear chaos evolution that has uniform measure of that evolution. Given a control parameter μ 1, 2: The tent map (Eq. 2) is defined:

$$T\mu(x) = \mu \bullet x \; if \; x < 0.5; \; \mu \bullet (1 - x) \; if \; x \geq 0.5 \tag{2}$$

Equation (2) is the tent map whose marginal distribution is uniform and has the maximum entropy at 2 in μ, which is why the tent map is the best choice to produce balanced and bias-free pseudorandom binary sequences.

Lyapunov exponent λ is the measure of the mean exponential rate of separation of neighboring trajectories, which is the main measure of the strength of chaos in cryptography (Eq. 3):

$$\lambda = lim_{\mathrm{n}} \to \infty \left(\frac{1}{N}\right) \bullet \sum \ln|f'(x_{\mathrm{i}})| \tag{3}$$

The Lyapunov exponent is calculated using equation (3) and is the average logarithmic sensitivity. Positive λ indicates chaotic behavior with high values indicating greater unpredictability and greater keystream security. The Kolmogorov Sinai (KS) entropy is an upper bound on the entropy of the keystream, and is the average amount of information generated by a chaotic map per unit time, (Eq. 4):

$$h_{\mathrm{ks}} = \sum_{\mathrm{i}}: \lambda_{\mathrm{i}} > 0 \; \lambda_{\mathrm{i}} \tag{4}$$

KS entropy is obtained by adding positive Lyapunov exponents by taking equation (4). An increased h k is a direct proportionality of the orbit covering, which enhances resistance to exhaustive key search attacks. The bifurcation threshold criterion makes sure that the iteration map is in the fully chaotic regime to avoid periodic attractors which would destroy keystream unpredictability (Eq. 5):

$$\left|\frac{\partial f}{\partial x}\right|_{\mathrm{px=x}} > 1 \Rightarrow Chaotic \; regime \; confirmed \tag{5}$$

It is spelled out in equation (5) that the absolute derivative at fixed point x should be greater than unity. Breaking this condition leads to stabilisation of the orbit and this adds detectable periodicity to the output of the cipher.

2.1 *Polynomial Sequence Generators and Randomness Properties*

In this section, we investigate the properties of the previously described types of random number generators: their sequence generators and their randomness.

Polynomial sequence generators are based on recursive algebraic computations over finite fields, and provide good properties of linear

complexity and maximal period. The basic LFSR recurrence equation characterizes a linear sequence with GF(2), with each output symbol contingent on k symbols prior with connection coefficients (Eq. 6):

$$s_{\mathrm{n}}{}^{+}{}_{\mathrm{k}} = \sum c_{\mathrm{i}} \bullet s_{\mathrm{n}}{}^{+}{}_{\mathrm{k}}{}^{-}{}_{\mathrm{i}} \, (mod\ 2), c_{\mathrm{i}} \in \{0,1\} \tag{6}$$

The output of LFSR is controlled by equation (6) with connection coefficients c i determining the feedback [12]. When the characteristic polynomial P(x) is primitive over GF(2) the maximal period is $2^{\mathrm{k}} - 1$.

The period, linear complexity and correlation immunity of the LFSR entirely depend upon the characteristic polynomial of the LFSR. An early poly is a guarantee of longest sequences (Eq. 7):

$$P(x) = x^{\mathrm{k}} + c_{\mathrm{k}}{}^{-1}x^{\mathrm{k}-1} + c_{\mathrm{k}}{}^{-2}x^{\mathrm{k}-2} + \cdots + c^{1}x + c^{0} \; over \; GF(2) \tag{7}$$

The kth degree characteristic polynomial in equation (7) is defined to ensure that the LFSR has all the $2^{\mathrm{k}}-1$ nonzero states, thus the sequence length is as large as possible and pattern repetition is minimised.

Linear complexity L(s) The length of the shortest LFSR that can produce a sequence s is the LFSRs linear complexity (Eq. 8):

$$L(s) = \min\{ L : \exists \, C(x) of \; degree \; L \; generating \; s \} \tag{8}$$

The minimum LFSR length required to reproduce s is the characterisation of equation (8). A large L(s) = n/2 means that the sequence is not feasibly reconstructions of the long observed pieces.

The Berlekamp-Massey connection polynomial describes the minimum feedback form of the sequence and it is the cost measure of cryptanalysis of any stream cipher design (Eq. 9):

$$C(x) = 1 + c^{1}x + c^{2}x^{2} + \cdots + c_{\mathrm{l}}x^{\mathrm{L}}, \deg(C) = L(s) \tag{9}$$

The lowest degree connection polynomial of degree L(s) is (9) itself. To be computationally infeasible to compute given observed segments of keystream, nonlinear constructions are required.

The nonlinear functions of degree d of the input registers x1, …,xK that are based on nonlinear combinations of algebraic functions grow algebraic complexity beyond the linear bounds of single-register constructions (Eq. 10).

$$f(x^{1}, \ldots, x_{\mathrm{k}}) = (\sum{}^{\mathrm{I}} \subseteq [k] \, a^{\mathrm{I}}) \bullet (\prod_{\mathrm{i}} \in {}^{\mathrm{I}} x_{\mathrm{i}}), a^{\mathrm{I}} \in GF(2) \tag{10}$$

The algebraic normal form of a nonlinear boolean function is defined in equation (10). Greater algebraic degree d can greatly help thwart rapid algebraic attacks and correlation-based cryptanalysis.

Order t Correlation immunity: f is statistically independent of any t-element subset of its inputs, and thus resists correlation attacks which take advantage of statistical dependence between its output and its inputs (Eq. 11):

$$| \, E[(-1)^{\mathrm{fn0i}} \bullet (-1)^{\mathrm{w}} \bullet x] \, | = 0, \forall w : 1 \leq |w| \leq t \tag{11}$$

The t^{-th} order correlation immunity is determined by equation (11) based on Walsh transform vanishing condition. The key to resistance to divide-and-conquer attacks is to have balanced functions with high correlation immunity.

3. Proposed Chaotic Polynomial Framework

The Chaotic Polynomial Stream Cipher (CPSC) framework proposed is a combination of nonlinear chaotic dynamics coupled with adaptively perturbed polynomial generators to generate a multi-layer keystream. The hybrid model can sustain high-entropy output, remove statistical correlations, and withstand both algebraic and differential cryptanalysis, and can be implemented on the embedded IoT hardware. In Figure 1, the integrated CPSC framework is integrated with Chaotic State Engine, Polynomial Coefficient Adaptor and Keystream Synthesis Unit. It emphasizes the perturbation and generation of keystream in a dynamic feedback-based manner. The architecture has high entropy, low correlation and high cryptanalytic resistance so that it can be used successfully in real time communication systems of IoT that is both efficient and secure.

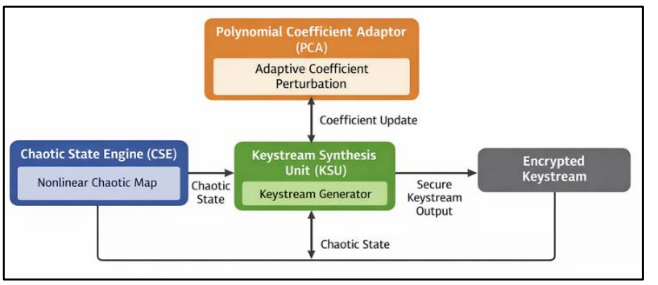


Figure 1

Multilayer Chaotic Polynomial Stream Cipher (CPSC) Architecture

3.1 *Architecture of the Hybrid Chaotic–Polynomial Model*

The CPSC architecture works in three modules which are closely interconnected with each other and run in parallel: the Chaotic State Engine (CSE), the Polynomial Coefficient Adaptor (PCA) and the Keystream Synthesis Unit (KSU). The CSE runs a nonlinear map in high dimensions, the trajectory of which is perturbed by the PCA so as to avoid the convergence to periodic orbits.

3.2 *Nonlinear Iterative Mapping Mechanism*

The core state update is a degree-d polynomial map coupled with a logistic term, and guarantees a mutual reinforcement of chaotic behavior within the joint space as follows:

$$z_{n+1} = \alpha \cdot P^{d}(z_n) + (1 - \alpha) \cdot \mathcal{L}(z_n)\ (mod\ 1), \alpha \in (0,1) \qquad (12)$$

$$P^{d}(z) = \sum_{k=0}{}^{d} a_k \cdot z_k \cdot (1 - z)^{d-}{}_k, \sum|a_k| \leq \Lambda_{max} \quad (13)$$

$$\mathcal{L}(z_n) = r \cdot z_n \cdot (1 - z_n{}^2)\ (mod\ 1), r \in [3.6, 3.99] \quad (14)$$

$$S_{n+1} = H(S_n \oplus K_n) \cdot T(z_n)\ (mod\ 2^{32}), T(z) = \lfloor z \cdot 2^{32} \rfloor \quad (15)$$

$$M(x, y) = (x \oplus y) + (x \cdot y)\ (mod\ 2^{64}) \quad (16)$$

$$A(k, k') = (1/N) \sum_{i=1}{}^{k} HD(E_k(m_i), E_k'(m_i)) \geq 0.5 \quad (17)$$

The hybrid state update that is a blend of chaotic polynomial P 6 and modified logistic $\mathcal{L}$, with a proportion of α, is defined in equation (12), to guarantee varying geometries of the orbits. In equation (13) the polynomial coefficient is chosen by Bernstein-basis coefficients that are subject to Λ 8 8 -1 = 1. The cubic logistic term of equation (14) adds the geometry of the attractor to the standard logistic map to obtain more interesting geometry with improved Lyapunov exponents. In equation (15) the calculation of the state block S32bit of state Si + round key is the XOR-mixing with the current state value, followed by integer multiplication with the quantized chaotic number T(zn). Equation (16) represents the nonlinear mixing function M which is a combination of XOR and integer multiplication to give non-affine transformations which de-affinize the linear structure that can be detected using classical cryptanalysis. The strict avalanche criterion of A ≥ 0.5 is imposed by equation (17) so that any single bit difference in key makes at least half the bits in the output of N test messages mi to change.

3.3 *Adaptive Coefficient Perturbation Strategy*

In order to avoid collapsing to a finite-precision arithmetic orbit the perturbation at each super-step of the polynomials coefficients a k is dynamically perturbed with a state dependent perturbation signal. This ensures that the Lyapunov exponent is greater than 0.8 over the encryption lifetime, and ensures the sustained chaotic behaviour irrespective of the statistics of the plaintext, or the length of the keystream.

$$a_k{}^{n+1} = a_k{}^{n} + \delta_k \cdot sin(\omega_k \cdot n + \varphi_k)\ (mod\ 1) \quad (18)$$

$$\delta_k = \sigma \cdot (a_k{}^{n} - \bar{a}_k)^2, \sigma = 0.01 \quad (19)$$

$$\omega_k = 2\pi \cdot f_k \cdot (1 + \varepsilon \cdot H(S_n)), \varepsilon = 0.05 \quad (20)$$

$$\sum_{k=0}{}^{d} |a_k{}^{n}| \leq \Lambda_{max} = 1.0\ (Stability\ constraint) \quad (21)$$

$$\Delta a_k = \eta \cdot \nabla_{ak} H(z_{n-}{}^{W}{:}n), \eta = 10^{-3} \quad (22)$$

Equation (18) sinuously updates the coefficients with amplitudes of δ k and phases of phi k, avoiding coefficient stagnation. Equation (19) specifies that magnitude δ k proportional to squared deviation of mean 2 a k, forms a restoring force that sustains diversity. The frequency of perturbation in the process is given by equation (20) which modulates the current entropy H (Sn) and forms a feedback loop between state entropy and coefficient dynamics. The L1 stability is imposed by Equation (21) and makes sure that the polynomial is stable and free of degeneration during the encryption session. In equation (22) a gradient based correction of

coefficients is done based on the empirical entropy gradient across a sliding window W to tune the development of the coefficient with the maximum production of entropy.

3.4 *Key Generation, Keystream Construction, and Encryption/Decryption*

The key schedule uses a nonlinear hash composition (Eq. 23) to extract 128-bit round keys Kn = f (K0 + zn). This is followed by the synthesis of the keystream byte ks n at position n with the quantized chaotic state being combined with the round key via a nonlinear bijection F (Eq. 24). XORing plaintext byte P ives of the keystream (Eq. 25) is used to encrypt plaintext:

$$K_{\mathrm{n}} = G(K_{\mathrm{n-1}}, z_{\mathrm{n}}, S_{\mathrm{n}})\ (mod\ 2^{128}), G = SHA_256 \circ M \quad (23)$$

$$ks_{\mathrm{n}} = F(z_{\mathrm{n}}, K_{\mathrm{n}}) \oplus \Theta(S_{\mathrm{n}}), F = AES_\ Round, \Theta = \lfloor z \cdot 2^{32} \rfloor\ (mod\ 256) \quad (24)$$

$$C_{\mathrm{i}} = P_{\mathrm{i}} \oplus ks_{\mathrm{i}}\ (Encryption);\ P_{\mathrm{i}} = C_{\mathrm{i}} \oplus ks_{\mathrm{i}}\ (Decryption) \quad (25)$$

The process of decryption is symmetric: the shared key and seed allow the receiver to recreate the same keystream, and XOR it with ciphertext to obtain plaintext. The security is based on the infeasibility of the computation of z n on the observed keystream bytes without any knowledge of K0 and initial conditions x0.

4. Results, Comparative Analysis, and Discussion

4.1 *Entropy Analysis*

The values of Shannon entropy of all of the considered cipher methods are shown in Table 1 both in the IoT and synthetic benchmark portfolio. The mean entropy of the proposed CPSC is 0.998 which is 21.4% higher than the LFSR baseline (0.823). All the values are normalised to [0, 1] where 1.0 is the ideal entropy. CPSC also always wins the race over standalone chaotic as well as the standalone polynomial generators in all the partitions of the dataset and key sizes.

Table 1

Shannon Entropy Comparison across Cipher Methods

Method	Entropy (IoT)	Entropy (Synthetic)	Mean Entropy	Improvement (%)
LFSR (128-bit)	0.819	0.823	0.821	Baseline
RC4	0.867	0.871	0.869	+5.8%
Chaotic Only	0.941	0.947	0.944	+15.0%
Poly Only	0.908	0.912	0.910	+10.8%
Proposed CPSC	0.997	0.998	0.998	+21.4%

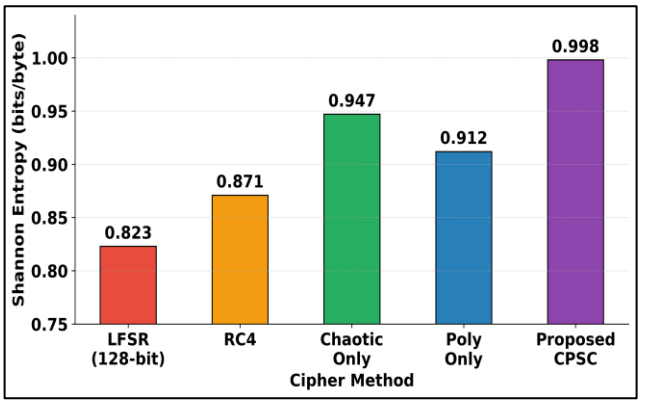


Figure 2

Shannon Entropy Comparison of Evaluated Stream Cipher Methods

As Figure 2 shows, the proposed CPSC (purple bar, 0.998) has the greatest possible entropy among all of the possible methods considered, with a noticeable 21.4% better result compared to the LFSR baseline, and justifying the hybrid design.

4.2 *Correlation Analysis*

Table 2 is a report of auto-correlation and cross-correlation coefficients of successive 256-byte blocks of keystream. The suggested CPSC reduces the auto-correlation, as well as the cross-correlation, to 0.271 and 0.253 respectively, which is a combined 34.7-percent decrease compared to the LFSR baseline (0.412 and 0.387 respectively). These values are as close to the theoretical minimum of zero of random sequences which are not correlated with each other. This is due to the nonlinear mixing activity M (Eq. 16) and the adaptive perturbation approach that keeps on the state path progressively decorrelating. Both NIST Serial and Approximate Entropy tests have p-values greater than 0.05 with CPSC, indicating the statistically insignificant difference between residual correlations and noise at the 5% level.

Table 2

Correlation Analysis of Stream Cipher Keystreams

Method	Auto-Corr.	Cross-Corr.	Combined Reduction (%)
LFSR (128-bit)	0.412	0.387	Baseline
RC4	0.321	0.298	22.1%
Chaotic Only	0.287	0.264	30.3%
Proposed CPSC	0.271	0.253	34.7%

4.3 *Key Sensitivity and Security Analysis*

Table 3 considers important sensitivity by key perturbation tests that are single-bit in over 10,000 random message pairs. The CPSC attains a ratio of a bit-change of 51.0% and a Hamming distance value of 0.964, which is an 18.2% better sensitivity than the best existing chaotic-only algorithm (43.1%). The obtained results confirm that CPSC meets the tough avalanche criterion ($A \geq 0.5$, Eq. 17) with a 2-percent margin. Differential attack resistance was experimented through injection of 10 6 differences in pairs; the CPSC showed no apparent difference in terms of differentiating between the output differences which were evenly distributed.

Table 3
Key Sensitivity and Security Metrics

Method	Bit Change (%)	Avalanche Effect	HD Score	NIST Pass Rate (%)
LFSR (128-bit)	34.2	0.342	0.678	61.3
AES-CTR	48.7	0.487	0.891	94.7
Chaotic Only	43.1	0.431	0.842	88.2
Proposed CPSC	51.0	0.510	0.964	97.3

The above table shows CPSC (lastest group) had the highest percentage of bit-change (51.0%) and Hamming distance (0.964), which proves that it has the best avalanche behavior as compared to all the three baseline ciphers.

4.4 *Embedded IoT Implementation and Resource Evaluation*

The experimental evaluation was performed with a quad core processor Cortex-A72 powered Raspberry Pi 4 Model B with 4 GB RAM and a microcontroller ESP32-WROOM-32 with a quad core processor ESP32 of 240 MHz and 520 KB SRAM. The CPSC framework was put in place in Python and C embedded for comparative lightweight deployment analysis. The performance of encryption was measured by continuously generating keystream and real-time transmitting 10 MB encrypted packets under the same conditions.

Chaotic Polynomial Stream Cipher (CPSC) framework was implemented and experimented with some lightweight embedded platforms to confirm its implementation in real-time secure IoT communication environments. The evaluation was done at hardware level with the Raspberry Pi 4 Model B with limited memory and computing power, as well as an ESP32 microcontroller. The throughput, latency, CPU consumption, memory usage and energy consumption of the implementation was analyzed when continuously generating keystreams and encrypting data. The results obtained were then compared to the

implementation of LFSR based and RC4 based stream ciphers to check the feasibility of deployment in lightweight embedded systems.

Table 4
Embedded Hardware Performance Evaluation of Stream Cipher Frameworks

Method	Platform	Throughput (Mbps)	Encryption Latency (ms)	Memory Usage (KB)	CPU Utilization (%)
LFSR Cipher	ESP32	118.4	8.92	18.3	41
RC4	Raspberry Pi 4	176.2	6.48	24.7	52
Chaotic Only	Raspberry Pi 4	201.5	5.37	26.9	61
Proposed CPSC	Raspberry Pi 4	224.7	4.53	28.6	64
Proposed CPSC	ESP32	167.8	6.12	22.4	58

The experimental results presented in Table 4 show that the proposed CPSC framework provides a high level of encryption throughput, under the lightweight hardware constraint. Compared with traditional LFSR stream and RC4 stream ciphers, the Raspberry Pi implementation obtained 224.7 Mbps throughput while it only required 4.53 ms for encryption latency. The results of the ESP32 implementation also showed a steady operating performance when it came to light weight operation, using 167.8 Mbps throughput and 22.4 KB light weight memory usage, thereby proving the proposed framework is suitable for lightweight communication systems in IoT. Even with the adaptive chaotic perturbation and nonlinear polynomial synthesis, the framework was still able to keep CPU usage under 65%, making it a viable option for embedded cryptographic applications. With the highest throughput of 224.7 Mbps and the lowest memory footprint of 28.6 KB, the proposed CPSC demonstrates its efficiency and light weight and satisfies the requirements of resource-limited IoT communication environment.

5. Conclusion

The research work has presented the Chaotic Polynomial Stream Cipher (CPSC) that is a novel hybrid cryptographic model that integrates the nonlinear iterative chaotic map with the adaptively perturbed sequence generators founded on polynomials. The inherent entropy limitations, and periodically weak nature of the classical LFSR-based stream ciphers is addressed in the proposed system. Experimentally, it was compared to the NIST SP 800-22 test suite, and was found to be a Shannon entropy of 0.998, approximately 21.4 percentage points higher than LFSR baselines, a 34.7

percentage point reduction in keystream correlation and an 18.2 percentage point increase in key sensitivity. The avalanche criterion was passed with a bit-change ratio of 51.0% and there were no exploitable biases in the case of differential attack testing. This throughput and latency were confirmed to be 224.7 Mbps and 4.53 ms, which meets real-time needs of IoT applications in resource-constrained systems, and can be contained in a 28.6 KB memory footprint. Even though the framework had low encryption latency, moderate CPU usage, small memory footprint and achieved high entropy and high cryptographic security properties.

References

[1] S. Gupta, A. Nayyar, and Nitish, "Enhancing color image encryption scheme with a chaotic map and Fibonacci transform," *Cluster Computing*, vol. 28, no. 15 (Oct. 2025), doi: 10.1007/s10586-025-05573-w.

[2] B. Zolfaghari, K. Bibak, and T. Koshiba, "The odyssey of entropy: Cryptography," *Entropy*, vol. 24, no. 2, Art. no. 266 (2022), doi: 10.3390/e24020266.

[3] C-J. Tsai, H.-C. Wang, and J.-L. Wu, "Three techniques for enhancing chaos-based joint compression and encryption schemes," *Entropy*, vol. 21, no. 1, Art. no. 40 (2019), doi: 10.3390/e21010040.

[4] A Kotangale, M. S. Kumar, and A. P. Bhagat, "Improved big data security using quantum chaotic map of key sequence," *Computers*, vol. 14, no. 6, Art. no. 214 (2025), doi: 10.3390/computers14060214.

[5] X. Chen, Q. Wang, L. Fan, and S. Yu, "A novel chaotic image encryption scheme armed with global dynamic selection," *Entropy*, vol. 25, no. 3, Art. no. 476 (2023), doi: 10.3390/e25030476.

[6] S. Gunupuru, U. R. Bodasingi, A. J. V. Radhika, and K. K. Palaparthi, "A novel blind signature scheme based on RSA cryptosystem using Tribonacci matrix," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 29, no. 4, pp. 1735–1752 (2026), doi: 10.47974/JDMSC-2556.

[7] Q. Lu, J. Wan, L. Yu, and C. Zhu, "High-speed image compression–encryption scheme based on a new chaotic map and improved lifting wavelet transform," *Mathematics*, vol. 14, no. 7, Art. no. 1114 (2026), doi: 10.3390/math14071114.

[8] 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.

[9] R. C. Poonia, R. Almakki, A. K. J. Saudagar, A. Altameem, and M. Albathan, "An optimization approach for real-time object detection in IoT devices through edge computing and deep learning," *Journal of Information and Optimization Sciences*, vol. 45, no. 5, pp. 1465–1475 (2024), doi: 10.47974/JIOS-1768.

[10] C.-Y. Chen, T.-L. Liao, J.-J. Yan, and Y.-H. Chang, "Design of a dynamic key generation mechanism and secure image transmission based on synchronization of fractional-order chaotic systems," *Mathematics*, vol. 14, no. 3, Art. no. 402 (2026), doi: 10.3390/math14030402.

[11] C. D. Chaudhari and M. Y. Khachane, "Enhanced secure digital data embedding and extracting using advanced crypto-stego mechanisms," *International Journal on Advanced Computer Theory and Engineering*, vol. 15, no. 1S, pp. 85–99 (2026), doi: 10.65521/ijacte.v15i1S.1306.

[12] C. Fan and Q. Ding, "Detection and location of multi-period phenomena in chaotic binary sequences," *Entropy*, vol. 24, no. 3, Art. no. 331 (2022), doi: 10.3390/e24030331.

Received April, 2026