Research Article

A New Pseudorandom Bit Generator Based on Mixing Three-Dimensional Chen Chaotic System with a Chaotic Tactics

Xuan Huang,¹ Lingfeng Liu ,² Xiangjun Li ,² Minrong Yu,² and Zijie Wu ²

¹School of Software & Communication Engineering, Jiangxi University of Finance and Economics, Nanchang, 330013, China

²School of Software, Nanchang University, Nanchang, 330029, China

Correspondence should be addressed to Lingfeng Liu; vatanoilcy@163.com and Xiangjun Li; lxjun_alex@163.com

Received 20 March 2019; Accepted 28 May 2019; Published 19 June 2019

Academic Editor: Christos Volos

Copyright © 2019 Xuan Huang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In this paper, a new chaotic system is proposed based on mixing three-dimensional Chen chaotic system with a chaotic tactics. This new system is proved to be chaotic under Wiggins' chaos definition and can generate chaotic sequences with high complexity. Furthermore, we propose a new pseudorandom bit generator (PRBG) based on this new system. A coding algorithm is used to make the sequences uniform. Both statistical and security tests are provided to show the generated sequences are with good randomness and high complexity to withstand attacks.

1. Introduction

Chaos is an interesting nonlinear physical phenomenon which exists in the natural world. The first mathematical definition of chaos was proposed by Li and York in [1], which is widely used for one-dimensional iterative map. After then, for different kinds of systems, some other chaos definitions have been proposed. Among them, the most widely used definitions are Devaney's chaos, Wiggins' chaos, and Smale's chaos. All these definitions focus on the different performances of chaos; e.g., Li-York's chaos focuses on the diffusion of chaotic trajectories, while Devaney's chaos focuses on the topological properties. Till now, there is still no accurate mathematical definition which can cover all the performances of chaos. However, the lack of general definition does not hinder the application of chaos. On the contrary, chaos has been widely used in almost all fields of science, engineering, and even humanities [2–6].

Pseudorandom bit sequence (PRBS) plays an important role in many fields, such as spread spectrum communication, numerical simulation, and cryptography [7, 8]. Recently, chaotic systems are regarded as effective nonlinear sources in generating PRBS for their wonderful properties, including sensitivity on initial conditions and parameters, ergodicity,

long-term unpredictability, and pseudorandomness [9–11]. Overall, the one-dimensional chaotic map is the most widely used chaotic system for designing PRBG. Addabbo proposed a random bit generator based on one-dimensional piecewise-linear chaotic map [12]. In [13], a new pseudorandom number generator on graphics processing units is presented, which is based on the chaotic iterations. Szczepanski presented a method of generating pseudorandom numbers by applying discrete chaotic dynamical systems which are ergodic or preferably mixing [14]. However, some studies show that the one-dimensional chaotic system is not secure enough, which may be attacked by the phase space reconstruction technology [15, 16].

Comparatively speaking, PRBG based on high-dimensional chaotic system is more secure in this sense and can offer a wider key space. In [17], the statistics and complexity of chaotic pseudorandom sequences generated by Lorenz system are analyzed. Shrestha presented an ultra-low-power, biologically inspired pseudo-random number generator based on the Hodgkin-Huxley silicon neuron circuit [18]. This kind of high-dimensional chaos-based PRBG is based on only one-dimensional chaotic orbit. In [19], Hu proposed a PRBG based on three-dimensional Chen chaotic system. This PRBG is based on a combination of three coordinates of chaotic orbit. However, due to the

combination strategy being quite simple, [20] points out that this PRBG is still not secure enough.

Motivated by the idea of [19], in this paper, we induce a chaotic tactics to select different dimensional coordinates of the three-dimensional Chen chaotic orbit. This chaotic tactics changes the three-dimensional chaotic orbit into one-dimensional orbit. This chaotic mixing tactics is obviously more secure than the fixed mixing tactics in [19]. We prove that the generated new system is still chaotic mathematically and show that the sequence generated by this new system is more complex than any dimensional variable of original Chen system numerically. Furthermore, we proposed a PRBG based on this new chaotic system. Both statistical and security analysis show that the generated PRBS is with good statistical characteristics and strong capacity to withstand attacks.

In the numerical tests, we use the fourth-order Runge-Kutta method for the numerical simulations of the Chen chaotic system to keep the numerical results as near as possible to the original system behavior. Our PRBG has several advantages. The generated sequence has a more complex behavior than any dimensional variables of original Chen system, which complicates the revealing of information from the orbits. Since we do not utilize any particular properties of Chen chaotic system, many other differential equation-based chaotic systems can also be used, which means that this method is not limited by the choice of system. Furthermore, our generated PRBG can pass the TestU01 statistical test suite, which is better than many other proposed chaotic PRBGs.

The rest of this paper is organized as follows. In Section 2, we present a new chaotic system based on Chen chaotic system with chaotic tactics. We prove that the proposed system is strict chaotic under Wiggins' chaos definition and analyze its complexity numerically in Section 3. In Section 4, we propose a PRBG based on this new system. The statistical and security tests are presented in Sections 5 and 6, respectively. Finally, Section 7 concludes the whole paper.

2. New System Based on Chen Chaotic System with Chaotic Tactics

The mathematical equation of Chen system can be described as follows [21]:

$$F := \begin{cases} \frac{dx}{dt} = a(y - x) \\ \frac{dy}{dt} = (c - a)x - xz + cy \\ \frac{dz}{dt} = xy - bz \end{cases} \quad (1)$$

where a , b , and c refer to the control parameters. Equation (1) will be chaotic with some suitable parameters. For example, letting $a = 35$, $b = 3$, and $c = 28$, the chaotic attractor of this system is shown in Figure 1.

The dynamical complexity of Chen chaotic system is rather high. The Lyapunov exponent of Chen system is about 2.168, which is larger than other most widely used chaotic systems. However, the complexity of each dimensional variable is rather low. Some numerical tests will be taken in the

FIGURE 1: Chen attractor with $a = 35$, $b = 3$, and $c = 28$.

next section. Therefore, in order to generate one-dimensional sequences with high complexity from Chen system, in this paper, we present a chaotic tactics. Actually, this chaotic tactics is used to mix the three-dimensional state variables of Chen chaotic system by using chaotic number sequences. The following zero-mean Logistic chaotic map is used here.

$$p_{i+1} = 1 - 2p_i^2 \quad (2)$$

where p_i is the state variable. By setting an initial value p_0 , we can generate a real-valued sequence: $p_0, p_1, \dots, p_m, \dots$. All these values locate in the interval $[-1, 1]$ if the initial value p_0 is selected in this domain as well.

Divide the interval $[-1, 1]$ into N subintervals τ_i , $i = 0, 1, \dots, N-1$. Denote $\tau_i = [t_i, t_{i+1})$, $i = 0, 1, \dots, N-2$, and $\tau_{N-1} = [t_{N-1}, t_N]$, where

$$t_i = -\cos\left(\frac{i}{N}\pi\right). \quad (3)$$

Let $\alpha = \{\tau_0, \tau_1, \dots, \tau_{N-1}\}$ be a finite measurable partition of $[-1, 1]$. If p_j is located in the subinterval τ_i , we change this real value into integer i . Then, the real-valued sequence: $p_0, p_1, \dots, p_m, \dots$ will be changed into an integer sequence $\{b_i\}$ as follows:

$$b_i = \begin{cases} 0, & p_i \in [t_0, t_1) \\ 1, & p_i \in [t_1, t_2) \\ \dots & \\ N-1, & p_i \in [t_{N-1}, t_N] \end{cases} \quad (4)$$

From [22] we know, the integer sequence is uniformly distributed. In this paper, we choose $N = 3$, and the interval $[-1, 1]$ is divided into three subintervals. The output signals of (1) can be mixed into one-dimensional sequence $\{s_i\}$ by the integer sequence $\{b_i\}$ as

$$s_i = H(x(iT), y(iT), z(iT)) = \begin{cases} x(iT), & b_i = 0 \\ y(iT), & b_i = 1 \\ z(iT), & b_i = 2 \end{cases} \quad (5)$$

FIGURE 2: The schematic of system G.

where T is the sampling interval of Chen chaotic system. We always set $T = 0.01$ through this paper. Denote $x(iT) := x_i$, $y(iT) := y_i$, $z(iT) := z_i$ in this paper. The sequence $\{s_i\}$ can be considered as the output signal of system G, whose schematic is briefly illustrated in Figure 2.

3. Chaos and Complexity Performances

In this section, we first prove that the system G is chaotic under Wiggins' chaos definition and then evaluate the complexity of this new system by using approximate entropy (ApEn) and permutation entropy (PE).

A system is chaotic under Wiggins' chaos definition if and only if this system has sensitive dependence on initial conditions and transitivity, which can be defined as follows.

Definition 1 (sensitive dependence on initial conditions, [23]). $F: S \rightarrow S$ is said to have sensitive dependence on initial conditions if there exists $\varepsilon > 0$, such that for any $x \in S$ and any neighborhood U of x , there exists $y \in U$ and an integer $n > 0$ such that

$$|F^n(x) - F^n(y)| > \varepsilon \quad (6)$$

where F^n refers to the trajectory of the system after n time iterations.

Definition 2 (transitivity, [23]). $F: S \rightarrow S$ is topological transitive; i.e., for any open subsets $U, V \in S$, there exists an integer $k > 0$ such that

$$F^k(U) \cap V \neq \emptyset \quad (7)$$

Theorems 4 and 5 will show that system G is mathematically chaotic. Before the proof, the following assumption is needed.

Assumption 3. The sequence $\{b_i\}$ is with good independence.

In order to prove this assumption, we numerically calculated the correlation function of sequence $\{b_i\}$, as shown in Figure 3. From Figure 3 we know that the sequence $\{b_i\}$ has a good independence and Assumption 3 holds.

Theorem 4. The new system G has sensitive dependence on initial conditions.

Proof. As the Chen system F is chaotic, then, for its initial condition (x_0, y_0, z_0) and its neighbor V , there exist $(x'_0, y'_0, z'_0) \in V$, $n_1, n_2, \dots, n_k \in \mathbb{Z}^+$ and $\varepsilon > 0$; we have

$$\|(x_{n_j}, y_{n_j}, z_{n_j}) - (x'_{n_j}, y'_{n_j}, z'_{n_j})\| > \varepsilon \quad (8)$$

Here, $\|\cdot\|$ denotes the Euclidean norm, $j = 1, 2, \dots, k$. Therefore, at least one equation holds in the following three equations for different j :

$$\|x_{n_j} - x'_{n_j}\| > \frac{\varepsilon}{\sqrt{3}} = \varepsilon_1 \quad (9)$$

$$\|y_{n_j} - y'_{n_j}\| > \frac{\varepsilon}{\sqrt{3}} = \varepsilon_1 \quad (10)$$

$$\|z_{n_j} - z'_{n_j}\| > \frac{\varepsilon}{\sqrt{3}} = \varepsilon_1 \quad (11)$$

Without loss of generality, we assume (9) holds for $j = j_1, j_2, \dots, j_l$, where $j_1, j_2, \dots, j_l$ are selected from 1 to k and are different from each other.

As we known, the integer sequence $\{b_i\}$ is uniformly distributed. Therefore, the probability of $b_i = 0$ equals $1/3$ approximately. As k and l approach infinity, according to the uniform distribution of $\{b_i\}$ and Assumption 3, we have

$$\text{Prob}\{b_{n_{j_p}} \neq 0 \mid 1 \leq p \leq l\} = \left(\frac{2}{3}\right)^l \rightarrow 0 \quad (12)$$

Then, there exists a value n_{j_p} , $1 \leq p \leq l$, which satisfies

$$b_{n_{j_p}} = 0 \quad (13)$$

Thus, we have

$$\begin{aligned} \|G^{n_{j_p}}(s_0) - G^{n_{j_p}}(s'_0)\| &= \|s_{n_{j_p}} - s'_{n_{j_p}}\| = \|x_{n_{j_p}} - x'_{n_{j_p}}\| \\ &> \varepsilon_1 \end{aligned} \quad (14)$$

which concludes our proof. $\square$

Theorem 5. The new system G has transitivity.

Proof. The above theorem is equivalent to the following: for any $s_0 \in U$ and an open subset V , there exists a natural number k such that $G^k(s_0) = s_k \in V$.

F is a chaotic system, so F is transitive. Then, for its initial condition $(x_0, y_0, z_0) \in U_F$ (U_F is the attractor of system F), there exist infinite number of natural numbers k_i , $i=1, 2, \dots, n$,

$$F^{k_i}(x_0, y_0, z_0) \in V_F \quad (15)$$

where V_F can be any subset of U_F . Then, for $i=1, 2, \dots, n$, we have

$$\begin{aligned} x_{k_i} &\in V_x, \\ y_{k_i} &\in V_y, \\ z_{k_i} &\in V_z \end{aligned} \quad (16)$$

FIGURE 3: Correlation tests of sequence $\{b_i\}$.

where $V_F = V_x \times V_y \times V_z$. Without loss of generality, set $b_0 = 0$. As n can approach to infinity, according to the uniform distribution of $\{b_i\}$ and Assumption 3, we have

$$\text{Prob} \{b_{k_i} \neq 0 \mid 1 \leq i \leq n\} = \left(\frac{2}{3}\right)^n \rightarrow 0 \quad (17)$$

Then, there exists a value k_j , $1 \leq j \leq n$, which satisfies

$$b_{k_j} = 0 \quad (18)$$

Thus, for any $s_0 \in U$, we have

$$G^{k_j}(s_0) = s_{k_j} = x_{k_j} \in V_x \quad (19)$$

For the arbitrariness of subset V_F , the subset V_x is arbitrary as well, which concludes our proof. $\square$

Next, we use ApEn and PE to analyze the complexity of $\{s_i\}$. The results show that our mixed sequence $\{s_i\}$ is more complex than the original x , y , z -dimensional state variables of Chen chaotic system.

ApEn is a complexity measure of time-series, which is introduced by Pincus in [24]. ApEn measures the probability of the new pattern generated in the sequences with the embedding dimension growing. The larger the probability is, the more complex the sequence is. Here, we calculate the ApEn of the sequence $\{s_i\}$ and then compare with the ApEn of x -dimensional, y -dimensional, and z -dimensional state variables of Chen chaotic system. The results are shown in Figure 4(a). From Figure 4(a) we can find that the ApEn of sequence $\{s_i\}$ is much larger than the ApEn of any dimensional variable of Chen system, which indicates that the sequence $\{s_i\}$ is much more complex in this sense.

PE is a complexity measure which is introduced in [25] by Bandt and Pompe. PE compared the size of some consecutive values in the sequence and summed up different order types and then used Shannon's entropy to measure the uncertainty of this ordering. As mentioned, PE is easily implemented and robust to noise, which has received wide attentions [26]. In this test, we select order $m = 6$ and embedding delay D

$= 2$ as suggested in [25]. The test results of sequence $\{s_i\}$ and its comparison to x -dimensional, y -dimensional, and z -dimensional state variables of Chen chaotic system are shown in Figure 4(b). The results also show that the sequence $\{s_i\}$ has greatly improved the complexity of each dimensional variable of Chen system.

4. The New PRBG

As shown in Section 3, the system G is chaotic and with high complexity. In this section, we propose a new PRBG based on system G .

The distribution of the Chen chaotic system is not uniform [19]. Therefore, we first make some effective changes to enhance the statistical properties of sequence $\{s_i\}$. Based on a large number of experiments, we propose the following coding algorithm:

$$t_i = \begin{cases} 7000 \cdot (s_i + 100) \bmod 256, & b_i = 0 \\ 7000 \cdot (s_i + 110) \bmod 256, & b_i = 1 \\ 7000 \cdot (s_i + 120) \bmod 256, & b_i = 2 \end{cases} \quad (20)$$

By using this algorithm, the output sequence $\{s_i\}$ is coded to be uniform integer sequence $\{t_i\}$. The sequence $\{t_i\}$ is in the finite field F_{256} , where $F_{256} = \{0, 1, 2, \dots, 255\}$. Finally, change t_i into 8-bit binary number, (e.g., 0 is encoded into 00000000 and 255 is encoded into 11111111), and then, we can get our PRBS.

The main frame of our PRBG is shown in Figure 5. This PRBG is based on mixing three-dimensional state variables of Chen chaotic system. The mixture method is based on the zero-mean Logistic chaotic map. Furthermore, (20) improves its statistical characteristics. We will show that our PRBG is with good randomness in Section 5. Furthermore, for a sample integer T , this PRBG will generate 8-bit data, which is much faster than the original method with $1 \text{ b}/T$.

FIGURE 4: The complexity of sequence $\{s_i\}$ and x-dimensional, y-dimensional, and z-dimensional variables of Chen system with $a = 35$, $b = 3$, and $c = 28$ (a) ApEn; (b) PE.

FIGURE 5: The main frame of new PRBG.

5. Statistical Tests

Statistical tests are essential for PRBG which is proposed in cryptographic applications. In this section, we will make some famous statistical tests to evaluate our PRBS. In these tests, the parameters of Chen system are selected as $a = 35$, $b = 3$, and $c = 28$, the initial value are selected as $p_0 = 0.4231$, $(x_0, y_0, z_0) = (1.3452, 4.2134, 6.7368)$.

5.1. Frequency Spectral Analysis. For an ideal pseudorandom sequence, there is no center frequency. While for a period sequence, a center frequency exists. The frequency spectral analysis of our PRBS is plotted in Figure 6. Obviously, there is no center frequency in the spectrum, which indicates that our PRBG is not periodic.

5.2. Beker and Piper's Statistical Tests. Beker and Piper's statistical tests include the frequency test, serial test, poker test, runs test, and correlation test [27]. These five tests are famous and can be found in many different works, e.g., [28]. The test results of the first four tests are shown in Table 1, where M refers to the threshold. The correlation tests are shown in Figure 7. Both results show that our PRBS are with good randomness.

FIGURE 6: Frequency spectrum analysis of the PRBS.

5.3. NIST Statistical Tests. Besides the Beker and Piper's statistical test suite, the NIST test suite may be the most widely used statistical tests [29]. The NIST test suite includes 16 tests which cover almost all the features of random sequences. In this test, the significance level of each test in NIST is set to 0.01, which means that 99% of test samples pass the tests if the random numbers are truly random. Here, we generate 1000 different binary sequences randomly with different initial values; the NIST test results are shown in Table 2. From Table 2 we can find that our PRBS have passed all the test suite and can be regarded with good randomness.

5.4. TestU01 Statistical Tests. In all the statistical test suites for random sequences, the TestU01 test is the most stringent testing. It is very difficult to pass all the tests successfully for PRBGs. In the TestU01 tests, three different crush type

TABLE 1: Results of Beker and Piper's statistical test.

	Frequency test	Serial Test	Poker test			Runs test
			$m=2$	$m=3$	$m=4$	
40000 b	0.079	2.964	2.896	6.544	14.284	1.692
60000 b	0.016	2.583	2.567	4.972	11.457	1.471
80000 b	0.009	2.049	1.479	4.579	9.130	1.336
100000 b	0.006	1.847	1.137	4.069	7.621	1.249
120000 b	0.004	1.397	1.018	3.217	5.987	1.014
T	3.84	5.99	7.81	14.07	26.00	1.96

FIGURE 7: Correlation tests of PRBS.

batteries are provided: there are Small-Crush, Crush, and Big-Crush, which evaluate sequences with 2^{29} bit, 2^{35} bit, and 2^{38} bit, respectively. Based on the storage space of our computer, we only use Small-Crush and Crush batteries to evaluate the randomness of our PRBG. The test results are shown in Table 3. From Table 3, we can find that all the test suites have been passed, which performs better than other proposed chaotic PRBGs in [30–33].

6. Security Analysis

Besides statistical tests, some other indexes are still required for a secure PRBG.

6.1. Key Space. In this PRBG, the initial values p_0 and (x_0, y_0, z_0) , as well as the control parameters of Chen system a , b , and c , can be commonly used as the secret keys. Let the greatest accuracy be 2^{-64} . The key space size is approximately equal to $2^{448} \gg 2^{128}$. Therefore, the key space of our PRBG is large enough to resist brute-force attack. Furthermore, when comparing to other studies, our method is still superior. Under the same accuracy, the key spaces of the PRBG proposed in [19, 34–36] are 2^{384} , 2^{400} , 2^{199} , and 2^{128} , respectively, which are all smaller than ours.

6.2. Key Sensitivity. Chaotic system is greatly sensitive to the initial values. In this test, we change the initial value slightly to generate new binary sequences and then compare

the difference between them. Denote H to be the number of differences between the new sequence and the primary one by each bit. The results are shown in Tables 4–7, where Table 4 shows the differences when p_0 changes; Tables 5, 6, and 7 show the differences when x_0 , y_0 , and z_0 change, respectively. All the results show that the variance ratio of each bit is near 50%, which means that the PRBG is extremely sensitive to the secret key.

6.3. Linear Complexity. For an ideal random sequence, its linear complexity should be $n/2$, where n is the sequence length. We test the linear complexity of our PRBS, and the result is shown in Figure 8. From Figure 8 we have that the linear complexity curve of our PRBS is approximately equal to the ideal line $n/2$, which indicates that our PRBG is with high linear complexity.

6.4. Resistance to Differential Attack. Differential attack, or chosen-plaintext attack, is to analyze the effects of a small difference in input keys on the difference of corresponding output sequences. A PRBG is said to resist differential attack if the output sequences are completely different for tiny difference on secret keys. As the results in Section 6.2, we can have that our PRBG is extremely sensitive to the secret keys and can effectively resist differential attacks.

6.5. Algorithm Speed Analysis. In this paper, the algorithms are simulated by Matlab R2014a on the 64-bit computer with

TABLE 2: The passing ratio and the uniformity of the P-values of each test from the NIST suite.

Test index	Passing ratio	P-value	Results
Approximate entropy	0.998	0.35974	SUCCESS
Block frequency	0.999	0.35479	SUCCESS
Cumulative sums	0.996	0.23154	SUCCESS
FFT	0.998	0.65942	SUCCESS
Frequency	0.999	0.54871	SUCCESS
Linear complexity	0.997	0.62321	SUCCESS
Random excursions	0.999	0.12654	SUCCESS
Random excursions variant	0.996	0.32648	SUCCESS
Longest runs of ones	0.999	0.15493	SUCCESS
Overlapping template of all ones	0.997	0.21489	SUCCESS
Rank	0.998	0.36541	SUCCESS
Runs	0.998	0.21582	SUCCESS
Serial	0.999	0.21648	SUCCESS
Universal statistical	0.996	0.11713	SUCCESS
Lempe-Ziv Compression Test	0.998	0.43546	SUCCESS

TABLE 3: TestU01 test results – Failure counts.

System	Parameters	Small-Crush(15)	Crush(144)
Our PRBG	Standard	0	0
Ref. [19]	Standard	1	6
Ref. [30]	Standard	14	122
Ref. [31]	Standard	2	12
Ref. [32]	Standard	3	19
Ref. [33]	Standard	3	15

TABLE 4: The difference between generated binary sequences with different p_0 .

	(0.4231, 0.4231 - 10^{-14})	(0.4231, 0.4231 + 10^{-14})
H	49.96%	50.04%

TABLE 5: The difference between generated binary sequences with different x_0 .

	(1.3452, 1.3452 - 10^{-14})	(1.3452, 1.3452 + 10^{-14})
H	49.90%	49.94%

TABLE 6: The difference between generated binary sequences with different y_0 .

	(4.2134, 4.2134 - 10^{-14})	(4.2134, 4.2134 + 10^{-14})
H	50.06%	50.08%

TABLE 7: The difference between generated binary sequences with different z_0 .

	(6.7368, 6.7368 - 10^{-14})	(6.7368, 6.7368 + 10^{-14})
H	50.04%	49.92%

3.3GHz CPU and 4GB memory. The computation precision is 2^{-64} . The mean speed of our PRBG algorithm is about 21.5054 MB/s, which is equivalent to the algorithm in [35]

TABLE 8: Algorithm Speed analysis.

Different algorithms	Speed (Mb/s)
Our algorithm	21.5054
Ref. [35]	20.5383
Ref. [36]	1.7
Ref. [37]	0.4844
Ref. [38]	0.2352

and is much faster than the algorithms in [37, 38], as seen in Table 8. These results indicate that our PRBG is competitive for practical use.

7. Conclusions

In this paper, firstly, we propose a new system based on mixing three-dimensional Chen chaotic system with a chaotic tactics and prove that this new system is chaotic under Wiggins' chaos definition. Complexity tests show that the output of this new system is more complex than any dimensional variable of Chen system. Then, we propose a new PRBG based on this new system. A coding algorithm is used to make the sequences uniform. Furthermore, we do several numerical simulations to prove that the generated PRBS is with good randomness characteristics and strong capacity to

FIGURE 8: Linear complexity of PRBS.

withstand different attacks, as well as high speed for practical use.

Data Availability

The [DATA TYPE] data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The contributions of this research are the following: National Natural Science Foundation of China (No. 61862042, 61601215, 61762062, 61862044); Science and Technology Innovation Platform Project of Jiangxi Province (No. 2018IBCD40005); Major Discipline Academic and Technical Leader Training Plan Project of Jiangxi Province (No. 20172BCB22030); Primary Research & Development Plan of Jiangxi Province (No. 20181ACE50033, No. 20171BBE50064, 2013ZBBE50018, 20111BBE50008); Jiangxi Province Natural Science Foundation of China (No. 20171BAB202027, No. 20142BAB207011); and Science & Technology Research Project of Education Department of Jiangxi Province (No. GJJ150104, GJJ161387).

References

- [1] T. Y. Li and J. A. Yorke, "Period three implies chaos," *The American Mathematical Monthly*, vol. 82, no. 10, pp. 985–992, 1975.
- [2] X.-F. Zhang, L. Wen, X.-B. Luo, and Z.-W. Xie, "Exact solutions of the generalized nonlinear schroinger equation with time- and space-modulated coefficients," *Physics Letters A*, vol. 376, no. 4, pp. 465–468, 2012.
- [3] Z. Jabeen and N. Gupte, "The dynamical origin of the universality classes of spatiotemporal intermittency," *Physics Letters A*, vol. 374, no. 44, pp. 4488–4495, 2010.
- [4] S. Banerjee, A. P. Misra, and L. Rondoni, "Spatiotemporal evolution in a $(2 + 1)$ -dimensional chemotaxis model," *Physica A: Statistical Mechanics and its Applications*, vol. 391, no. 1-2, pp. 107–112, 2012.
- [5] J. H. Park, "Synchronization of Genesio chaotic system via backstepping approach," *Chaos, Solitons & Fractals*, vol. 27, no. 5, pp. 1369–1375, 2006.
- [6] C.-S. Chen, "Quadratic optimal synchronization of uncertain chaotic systems," *Applied Mathematics and Computation*, vol. 217, no. 24, pp. 10377–10386, 2011.
- [7] N. Kalouptsidis, *Signal Processing Systems, in Telecommunications and Signal Processing Series*, Wiley, New York, NY, USA, 1996.
- [8] X. Wang, W. Zhang, W. Guo, and J. Zhang, "Secure chaotic system with application to chaotic ciphers," *Information Sciences*, vol. 221, pp. 555–570, 2013.
- [9] L. Liu, S. Miao, M. Cheng, and X. Gao, "A pseudorandom bit generator based on new multi-delayed Chebyshev map," *Information Processing Letters*, vol. 116, no. 11, pp. 674–681, 2016.
- [10] L. Liu and S. Miao, "Delay-introducing method to improve the dynamical degradation of a digital chaotic map," *Information Sciences*, vol. 396, pp. 1–13, 2017.
- [11] X. Huang, L. Liu, X. Li, M. Yu, and Z. Wu, "A new two-dimensional mutual coupled logistic map and its application for pseudorandom number generator," *Mathematical Problems in Engineering*, vol. 2019, Article ID 7685359, 10 pages, 2019.
- [12] T. Addabbo, M. Alioto, A. Fort, S. Rocchi, and V. Vignoli, "A feedback strategy to improve the entropy of a chaos-based random bit generator," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 53, no. 2, pp. 326–337, 2006.
- [13] C. Guyeux, R. Couturier, P.-C. Héam, and J. M. Bahi, "Efficient and cryptographically secure generation of chaotic pseudorandom numbers on GPU," *The Journal of Supercomputing*, vol. 71, no. 10, pp. 3877–3903, 2015.
- [14] J. Szczepański and Z. Kotulski, "Pseudorandom number generators based on chaotic dynamical systems," *Open Systems and Information Dynamics*, vol. 8, no. 2, pp. 137–146, 2001.
- [15] K. M. Short, "Steps toward unmasking secure communications," *International Journal of Bifurcation and Chaos*, vol. 04, no. 04, pp. 959–977, 1994.
- [16] F. Xiao and X.-P. Gao, "An approach for short-term prediction on time series from parameter-varying systems," *Journal of Software*, vol. 17, no. 5, pp. 1042–1050, 2006.
- [17] L. Nian-sheng, "Pseudo-randomness and complexity of binary sequences generated by the chaotic system," *Communications in Nonlinear Science and Numerical Simulation*, vol. 16, no. 2, pp. 761–768, 2011.
- [18] V. L. Shrestha, Q. Ma, M. R. Haider, and Y. Massoud, "An ultra-low-power pseudo-random number generator based on biologically inspired chaotic silicon neuron circuit," *IEICE Electronics Express*, vol. 9, no. 22, pp. 1756–1761, 2012.
- [19] H. Hu, L. Liu, and N. Ding, "Pseudorandom sequence generator based on the Chen chaotic system," *Computer Physics Communications*, vol. 184, no. 3, pp. 765–768, 2013.
- [20] F. Özkaynak and S. Yavuz, "Security problems for a pseudorandom sequence generator based on the Chen chaotic system," *Computer Physics Communications*, vol. 184, no. 9, pp. 2178–2181, 2013.

- [21] J. Lü and G. Chen, "A new chaotic attractor coined," *International Journal of Bifurcation and Chaos*, vol. 12, no. 3, pp. 659–661, 2002.
- [22] H. P. Hu, S. H. Liu, Z. X. Wang, and X. G. Wu, "A chaotic polyphase pseudorandom sequence," *Mathematica Physics*, vol. 24, no. 2, pp. 251–256, 2004 (Chinese).
- [23] S. Wiggins, *Chaotic Transport in Dynamical Systems*, Springer-Verlag, New York, NY, USA, 1992.
- [24] S. M. Pincus, "Approximate entropy as a measure of system complexity," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 88, no. 6, pp. 2297–2301, 1991.
- [25] C. Bandt and B. Pompe, "Permutation entropy: a natural complexity measure for time series," *Physical Review Letters*, vol. 88, no. 17, Article ID 174102, 2002.
- [26] J. P. Toomey and D. M. Kane, "Mapping the dynamic complexity of a semiconductor laser with optical feedback using permutation entropy," *Optics Express*, vol. 22, no. 2, pp. 1713–1725, 2014.
- [27] H. Beker and F. C. Piper, *Cipher Systems: The Protection of Communications*, Wiley, New York, NY, USA, 1982.
- [28] L. Liu, S. Miao, H. Hu, and Y. Deng, "Pseudorandom bit generator based on non-stationary logistic maps," *IET Information Security*, vol. 10, no. 2, pp. 87–94, 2016.
- [29] A. Rukhin, J. Soto, J. Nechvatal et al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Special Publication NIST 800-22, National Institute of Standards and Technology, 2010.
- [30] T. Addabbo, M. Alioto, A. Fort, and A. Pasini, "A class of maximum-period nonlinear congruential generators derived from the Renyi chaotic map," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 54, no. 4, pp. 816–828, 2007.
- [31] X. Wang, X. Qin, and L. Teng, "A novel true random number generator based on mouse movement and a one-dimensional chaotic map," *Mathematical Problems in Engineering*, vol. 2012, Article ID 931802, 9 pages, 2012.
- [32] X.-Y. Wang and X. Qin, "A new pseudo-random number generator based on CML and chaotic iteration," *Nonlinear Dynamics*, vol. 70, no. 2, pp. 1589–1592, 2012.
- [33] Y. Deng, H. Hu, W. Xiong, N. N. Xiong, and L. Liu, "Analysis and design of digital chaotic systems with desirable performance via feedback control," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, no. 8, pp. 1197–1200, 2015.
- [34] M. Francois, T. Grosge, D. Barchiesi, and R. Erra, "Pseudo-random number generator based on mixing of three chaotic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 4, pp. 887–895, 2014.
- [35] Y. Wang, Z. Liu, J. Ma, and H. He, "A pseudorandom number generator based on piecewise logistic map," *Nonlinear Dynamics*, vol. 83, no. 4, pp. 2373–2391, 2016.
- [36] M. A. Murillo-Escobar, C. Cruz-Hernandez, L. Cardoza-Avendano, and R. Mendez-Ramirez, "A novel pseudorandom number generator based on pseudorandomly enhanced logistic map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 407–425, 2017.
- [37] Y. Liu and X. J. Tong, "A new pseudorandom number generator based on complex number chaotic equation," *Chinese Physics B*, vol. 21, no. 9, Article ID 090506, 2012.
- [38] X. Tong and M. Cui, "Feedback image encryption algorithm with compound chaotic stream cipher based on perturbation," *Science China Information Sciences*, vol. 53, no. 1, pp. 191–202, 2010.