A new pseudorandom number generator based on complex number chaotic equation*

Liu Yang(刘 杨)† and Tong Xiao-Jun(佟晓筠)

School of Computer Science and Technology, Harbin Institute of Technology, Weihai 264209, China

(Received 21 December 2011; revised manuscript received 2 May 2012)

In recent years, various chaotic equation based pseudorandom number generators have been proposed, however, the chaotic equations are all defined in the real number field. In this paper, an equation is proposed and proved to be chaotic in the imaginary axis. And a pseudorandom number generator is constructed based on the chaotic equation. The alteration of the definitional domain of the chaotic equation from the real number field to the complex one provides a new approach to the construction of chaotic equations, and a new method to generate pseudorandom number sequences accordingly. Both theoretical analysis and experimental results show that the sequences generated by the proposed pseudorandom number generator possess many good properties.

Keywords: chaotic equation, pseudorandom number generator, complex number

PACS: 05.45.–a, 05.45.Gg **DOI:** 10.1088/1674-1056/21/9/090506

1. Introduction

Pseudorandom number generators (PRNGs)[1−15] play an important role in security schemes, such as generating cryptographic key streams and initializing variables in cryptographic algorithms. Though the sequences generated by PRNGs appear to be random, they are not truly so, because they can be reproduced by certain deterministic algorithms. When the period of the sequence is long enough, it has many good statistical characteristics.

Due to the random-like behaviors of chaos[16] and the sensitivity of chaotic trajectories to the initial conditions, many chaotic systems have been proposed and applied to information security fields. In recent years, researchers have exploited the single chaotic map[1−7] or more chaotic maps[7−14] to construct PRNGs. For example, in Ref. [1], an algorithm for a multiple pseudorandom-bit generator was presented based on a coupled map lattice. In Ref. [2], a PRNG was proposed to be constructed by using the piecewise linear map and the noninvertible nonlinearity transform, and the characteristic of the multi-value correspondence of the asymptotic deterministic randomness was studied. In Ref. [3], several one-dimensional chaotic maps together were used to generate pseudorandom numbers. In Ref. [4], the generation of a pseudorandom bit sequence using coupled congruential generators was proposed. Reference [5] proposed a multiple pseudorandom bit generator based on a spatiotemporal chaotic map. Reference [6] proposed an algorithm to generate pseudorandom numbers with the nearest-neighboring coupled-map lattices. Reference [7] proposed two algorithms to generate pseudorandom sequences, one was based on one logistic map, and the other was based on two logistic maps. Real number sequences obtained from the logistic maps were turned into binary sequences by a threshold function. Reference [8] proposed a chaotic digital encoder modular arithmetic. Reference [9] proposed a one-dimensional iterative chaotic map with infinite collapses within symmetrical region $[-1,0)\cup(0,1]$. Reference [10] presented a pseudorandom binary generator that adopted only binary operations, and the security relied on the large numbers of branches of the inverse of the function used in the algorithm. Reference [11] proposed the methods for constructing pseudorandom number generators based on an ensemble of hyperbolic automorphisms of the two-dimensional Sinai–Arnold cat map. Reference [12] generated pseudorandom num-

*Project supported by the National Natural Science Foundation of China (Grant No. 60973162), the Natural Science Foundation of Shandong Province, China (Grant No. ZR2009GM037), the Science and Technology of Shandong Province, China (Grant No. 2010GGX10132), and the Key Program of the Natural Science Foundation of Shandong Province, China (Grant No. Z2006G01).

†Corresponding author. E-mail: liuyang@hitwh.edu.cn

© 2012 Chinese Physical Society and IOP Publishing Ltd

bers by means of the sawtooth chaotic map and proposed a method of designing the security of sequences. Reference [13] exported the self-shrinking technique used in the classical cryptography into chaotic systems to develop keystreams with good statistical properties using a one-dimensional chaotic map. Reference [14] chose the chaotic equation based on the linear feedback shift register, and the chaotic sequence generated by the equation was transformed into a binary sequence by a binary system transformation.

At present, there are many chaos based PRNGs, but they are all performed within the real number field. In this paper, we generalize the definitional domain of the chaotic equation from the real number field to the complex one. We believe this generalization will give us a new way and a new method to generate pseudorandom sequences. We prove an equation chaotic in the imaginary axis, and demonstrate some characteristics of the equation. And we also construct the binary sequences based on this equation. Computer simulations confirm that the binary sequences are pseudorandom, which improves the security of chaos based PRNGs and increases the resistance against attacks.

The rest of this paper is organized as follows. In Section 2, we prove a complex number equation chaotic in the imaginary axis. In Section 3, we construct a pseudorandom number generator to obtian binary sequences from the complex number sequences. Section 4 presents the property analysis of the pseudorandom number sequences. Finally, a conclusion is drawn in Section 5.

2. New complex number chaotic equation

There are different definitions for chaos. The definition of Devaney[16] is as follows.

Definition 1 Let J be a set, f: $J \to J$ is chaotic in J, if

1) f is sensitive to the initial values. Namely, there exists $\delta > 0$, for every $x \in J$ and every adjacent area N of x, there exist $y \in N$ and $n \geq 0$ to make $|f^n(x) - f^n(y)| > \delta$.

2) f is topological transitive. Namely, for every coupled open sets U, $V \subseteq J$, there exists $k > 0$ to make $f^k(U) \cap V \neq \phi$.

3) The periodic points are dense in J. Namely, if O is the set of all the periodic points, then for the closure $\bar{O}$ of O, there is $\bar{O} = J$.

To prove the proposed equation, we will prove a lemma first.

Lemma 1 In the unit circle S, if θ is an angle in S, then equation $f(\theta) = 2\theta$ is chaotic.

Proof We will prove the equation chaotic according to Definition 1.

Let $\delta = 1$, for an arbitrary $\theta \in S$ and an arbitrary adjacent area N of θ, we take a point $\theta' \in N$. If we set $n_0 = \lceil \log_2 1/|\theta - \theta'| + 1 \rceil$, then we have

$$\begin{aligned} |f^{n_0}(\theta) - f^{n_0}(\theta')| &= |2^{n_0}\theta - 2^{n_0}\theta'| \\ &= 2^{n_0}|\theta - \theta'| \geq 2 > \delta. \end{aligned} \quad (1)$$

So, the equation is sensitive to the initial value.

2) For arbitrary open arcs U, $V \subseteq S$, let the arc length of U be I, then the arc length of $f^k(U)$ is $2^k I$. When $k \to \infty$, there is $2^k I \to \infty$, then there exists k_0 to make $2^{k_0} I > 2\pi$, so $f^{k_0}(U) \cap V \neq \phi$ holds. So, the equation is topological transitive.

3) We now prove the periodic points of the equation are dense. The idea is for every $\theta \in S$ (without loss of generality, we assume $\theta \in [0, 2\pi]$), we will find a periodic point sequence $\theta_1, \theta_2, \ldots$ to make $\lim\limits_{i\to\infty} \theta_i = \theta$ hold. Namely, for every $\delta > 0$, there exists k_0 to make $\theta_{k_0} \in (\theta - \delta, \theta + \delta)$ hold. Then it is obvious that the closure of the set composed of all the periodic points is S. So the periodic points of the equation are dense. Let $f^n(\theta) = 2^n\theta$, if θ is a periodic point, then $2^n\theta = \theta + 2k\pi$, so the periodic point of the equation is $\theta = 2k\pi/(2^n - 1)$, $(0 \leq k \leq 2^n)$. For every $\theta \in S$, $\forall\delta > 0$, obviously, there exists n_0 to make $\theta_1 = 2\pi/(2^{n_0} - 1) < \delta$. Let $\theta_k = 2k\pi/(2^{n_0} - 1)$, $k = 1, 2, \ldots, 2^{n_0}$, obviously, they are all periodic points of the equation. Then it is obvious that there exists k_0 to make $\theta_{k_0} = 2k_0\pi/(2^{n_0} - 1) \in (\theta - \delta, \theta + \delta)$. So, the periodic points of the equation are dense.

Now we can present and prove the complex number equation.

Proposition 1 The equation

$$x_{n+1} = \frac{x_n^2 + 1}{2x_n} \quad (2)$$

is chaotic in the imaginary axis.

Proof Firstly, we make a variable substitution, let $z_n = (x_n + 1)/(x_n - 1)$, then

$$x_n = \frac{z_n - 1}{z_n + 1}. \quad (3)$$

Put Eq. (3) into Eq. (2), we have

$$\frac{z_{n+1} - 1}{z_{n+1} + 1} = \frac{[(z_n - 1)/(z_n + 1)]^2 + 1}{2(z_n - 1)/(z_n + 1)} = \frac{z_n^2 + 1}{z_n^2 - 1}. \quad (4)$$

So, we obtain

$$(z_{n+1}-1)(z_n^2-1)=(z_{n+1}+1)(z_n^2+1). \tag{5}$$

Then there is

$$z_{n+1}=-z_n^2. \tag{6}$$

Now, let us take account of the relationship between x_n and z_n. For simplicity, we leave out the subscripts, namely, x_n and z_n are given by x and z, respectively. Since x and z are both complex numbers, we let $x=p+q\mathrm{i}$ and $z=r+s\mathrm{i}$, then

$$\begin{aligned} x &= p+q\mathrm{i} \\ &= \frac{z-1}{z+1} \\ &= \frac{(r-1)+s\mathrm{i}}{(r+1)+s\mathrm{i}} \\ &= \frac{[(r-1)+s\mathrm{i}][(r+1)-s\mathrm{i}]}{[(r+1)+s\mathrm{i}][(r+1)-s\mathrm{i}]} \\ &= \frac{r^2+s^2-1+2s\mathrm{i}}{(r+1)^2+s^2} \\ &= \frac{r^2+s^2-1}{(r+1)^2+s^2}+\frac{2s}{(r+1)^2+s^2}\mathrm{i}. \end{aligned} \tag{7}$$

Obviously, when $r^2+s^2=1$, there is $p=0$, which means that the imaginary axis of the original plane (let it be the x plane) is turned into the unit circle in a new plane (let it be the z plane) via the variable substitution.

Now we prove that equation (2) is chaotic in the imaginary axis. From the previous derivation, we know this is equivalent to prove that equation (6) is chaotic in the unit circle. We express equation (6) in the common function form $f(t)=-t^2$. Without loss of generality, we can remove the minus sign from the function. Namely, we only need to prove function $g(t)=t^2$ is chaotic in the unit circle.

Let S be the unit circle, an arbitrary point in S given in the polar coordinate is $\mathrm{e}^{\mathrm{i}\theta}$, then

$$g(\mathrm{e}^{\mathrm{i}\theta})=\mathrm{e}^{2\mathrm{i}\theta}. \tag{8}$$

If we denote the point in S with a radian number, then equation (8) becomes

$$g(\theta)=2\theta. \tag{9}$$

From Lemma 1, we know $g(\theta)$ is chaotic in the unit circle. Consequently, the complex number equation (2) is chaotic in the imaginary axis.

3. Construction of pseudo-random number generator

In this section, a pseudorandom number generator is constructed based on the complex number chaotic equation.

We divide the imaginary axis of the x plane into four sets, $E_1=\{b\mathrm{i}|b<-1\}$, $E_2=\{b\mathrm{i}|-1<b<0\}$, $E_3=\{b\mathrm{i}|0<b<1\}$, and $E_4=\{b\mathrm{i}|b>1\}$. Let Q_1, Q_2, Q_3, and Q_4 indicate the first, the second, the third, and the fourth quadrants in the z plane, respectively, and then we also divide the unit circle in the z plane into four parts, $I_1=\{S|S\in Q_1\}$, $I_2=\{S|S\in Q_2\}$, $I_3=\{S|S\in Q_3\}$, and $I_4=\{S|S\in Q_4\}$. From the proof of Proposition 1, we know that the imaginary axis in the x plane is mapped into the unit circle in the z plane. And from Eq. (3), it is easy to obtain that E_1, E_2, E_3, and E_4 are mapped into I_1, I_2, I_3, and I_4, respectively, as shown in Fig. 1.

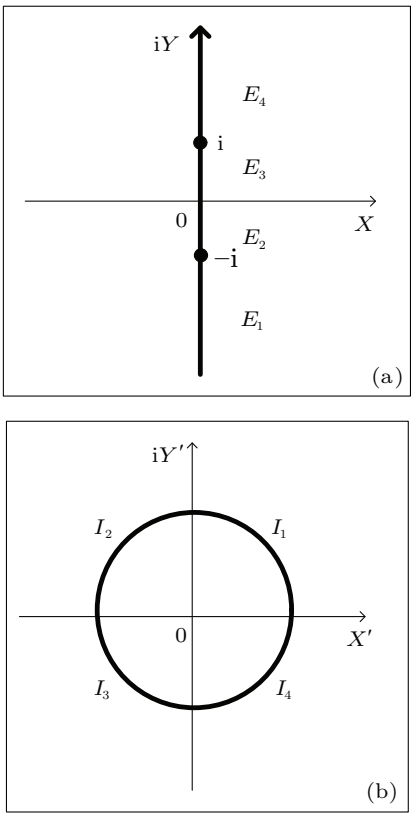


Fig. 1. Map from (a) the imaginary axis in the x plane to (b) the unit circle in the z plane.

Arbitrary initial point $x_0=b_0\mathrm{i}$ ($b_0\in\mathbf{R}$, $b_0\neq 0,\pm1$) in the imaginary axis iterated with Eq. (2) can lead to a sequence $x_1=b_1\mathrm{i}$, $x_2=b_2\mathrm{i},\ldots$, $x_k=b_k\mathrm{i},\ldots$. Let $\Delta=\{x_0,x_1,x_2,\ldots,x_k,\ldots\}$, $A=$

$\{x_t|x_t \in E_1\}$, $B = \{x_t|x_t \in E_2\}$, $C = \{x_t|x_t \in E_3\}$, $D = \{x_t|x_t \in E_4\}$, it is obvious that sets A, B, C, D are a partition of Δ, namely, the equalities $A \cap B \cap C \cap D = \phi$ and $A \cup B \cup C \cup D = \Delta$ hold.

For 100 sequences obtained with different initial values, we have counted the numbers of every sequence $\{x_t\}$, $t \in \{0, 1, 2, \ldots, k\}$ in the four sets A, B, C, D respectively, and have calculated the average values of the 100 sequences for different iteration times, see Table 1. We propose the following distance function D to measure the statistic properties of the sequence generated by the complex number chaotic equation:

$$D(P, P^{\mathrm{e}}) = \frac{1}{N} \sum\nolimits_{i=1}^{N} \left| p_i - p_i^{\mathrm{e}} \right|, \tag{10}$$

where P is the practical probability distribution, P^{e} is the ideal probability distribution, N is the number of the sets that the sequence has been divided into, p_i is the frequency of the sequence in the i-th subset, and p_i^{e} is the corresponding ideal frequency. Because P^{e} is the ideal probability distribution, we have $p_i^{\mathrm{e}} = 1/N$. Obviously, this distance function can present the difference between P and P^{e}, so $D(P, P^{\mathrm{e}})$ should be close to zero in an optimal situation. We calculate $D(P, P^{\mathrm{e}})$, and the whole set is divided into four subsets A, B, C, D. The average values of the 100 times are shown in Table 1. Table 1 indicates that the distributions of the four sets are close to equal, namely, $P(A) = P(B) = P(C) = P(D) = 1/4$.

Based on the above analysis, we can encode the complex number sequence now.

A complex number sequence $\Delta = \{x_0, x_1, x_2, \ldots, x_k, \ldots\}$ can be obtained by using the complex number chaotic equation (2), where $x_0 = b_0\mathrm{i}$, $x_1 = b_1\mathrm{i}$, $x_2 = b_2\mathrm{i}, \ldots$, $x_k = b_k\mathrm{i}, \ldots$ To obtain the binary sequence, we encode the complex number sequence as follows:

$$a_t = \begin{cases} 0, & x_t \in A \cup C, \\ 1, & x_t \in B \cup D, \end{cases} \quad t \in \{0, 1, 2, ..., k, ...\}. \tag{11}$$

In this way, a pseudorandom number generator based on the complex number chaotic equation is constructed.

Table 1. Distributions of sequences in four subsets.

Length of sequence	Number of points in A	Number of points in B	Number of points in C	Number of points in D	$D(P, P^{\mathrm{e}})$
1000	255	247	238	260	0.00525
10000	2491	2495	2513	2501	0.00070
50000	12493	12506	12496	12505	0.00035
100000	24997	24990	25004	25009	0.00026
500000	125009	125001	124996	124994	0.00004

4. Analysis of pseudorandom sequence

This section is devoted to analyzing the properties of binary sequences generated by the proposed pseudorandom number generator.

4.1. Statistic characteristics

4.1.1. Theoretical analysis

The statistic characteristics of the binary sequence are as follows.

Proposition 2 Distributions of 0 and 1 in the binary sequence produced by Eq. (11) are equal, namely, $P(0) = P(1) = 1/2$.

Proof Obviously, $P(a_t = 0) = P(x_t \in A) + P(x_t \in C)$, $P(a_t = 1) = P(x_t \in B) + P(x_t \in D)$. From Section 3, we have $P(A) = P(B) = P(C) = P(D) = 1/4$, so $P(a_t = 0) = 1/2$, $P(a_t = 1) = 1/2$. Namely, $P(0) = P(1) = 1/2$.

Proposition 3 The expectation of the binary sequence is 1/2.

Proof Obviously, a_t is a random variable valued in {0,1}. Then the expectation of a_t is

$$\begin{aligned} E(a_t) &= 0P(0) + 1P(1) \\ &= 0 \times \frac{1}{2} + 1 \times \frac{1}{2} \\ &= \frac{1}{2}. \end{aligned}$$

Proposition 4 The entropy of the binary sequence is 1.

Proof The binary sequence can be seen as a single signal discrete information source X, and then the entropy is

$$\begin{aligned} H(X) &= -\sum_{i=1}^{2} p(x_i)\log p(x_i) \\ &= -[p(0)\log p(0) + p(1)\log p(1)] \\ &= 1. \end{aligned}$$

These properties represent the good randomness of the binary sequence.

4.1.2. Numerical analysis

We have tested the binary sequences with different initial values for 500 times, where the length of the sequence is 100000 at least.

As an example of distributions of 0 and 1, consider a sequence $\{l_t\}_{t=0}^{N-1}$ with $N = 200000$ obtained by the above-mentioned method with initial value $x_0 = 0.3\mathrm{i}$. Figure 2 shows that the ratio of 1 to 0 in $\{l_t\}_{t=0}^{N-1}$ is close to 1 (as expected for a truly random sequence).

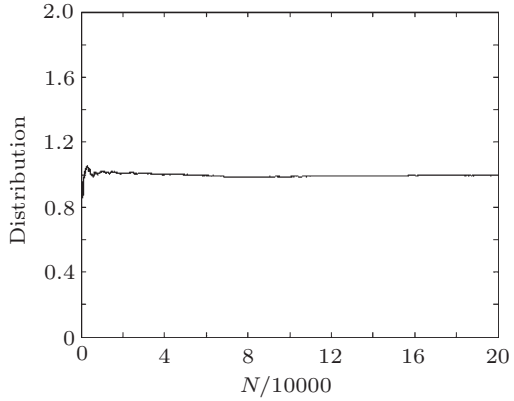


Fig. 2. Distributions of 0 and 1 in a sequence, where $N = 200000$ and $x_0 = 0.3\mathrm{i}$.

The autocorrelation function[13] Ψ of sequence $\{l_t\}_{t=0}^{N-1}$ measures the amount of similarity between $\{l_t\}_{t=0}^{N-1}$ and a shift version of $\{l_t\}_{t=0}^{N-1}$. For $j = 0, 1, \ldots, N-1$,

$$\Psi\left(\{l_t\}_{t=0}^{N-1}, \{l_t\}_{t=j}^{N+j-1}\right) = \frac{A-D}{N}, \qquad (12)$$

where A and D are the numbers of bit-by-bit agreements and disagreements between $\{l_t\}_{t=0}^{N-1}$ and $\{l_t\}_{t=j}^{N+j-1}$, respectively. The value of the autocorrelation function Ψ should be close to 0 in a truly random sequence. While in the binary sequences generated by the complex number chaotic equation, the values of Ψ are all close to 0. Figure 3 shows the result of an example with $N = 100000$, initial value $x_0 = -0.2\mathrm{i}$, and $j = 100$.

The cross-correlation measures the amount of similarity between different sequences. For a truly random sequence, the value is close to 0. Figure 4 shows the cross-correlation value of two sequences with initial values $x_0 = -0.2\mathrm{i}$ and $y_0 = -0.200000000000001\mathrm{i}$ respectively. Obviously, the cross-correlation value is close to 0 in Fig. 4.

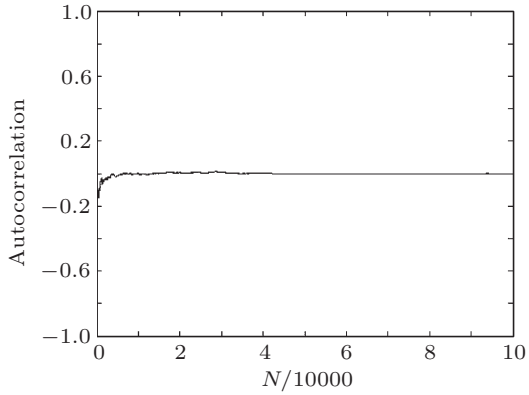


Fig. 3. The autocorrelation value of a sequence, where $N = 100000$, $x_0 = -0.2\mathrm{i}$, and $j = 100$.

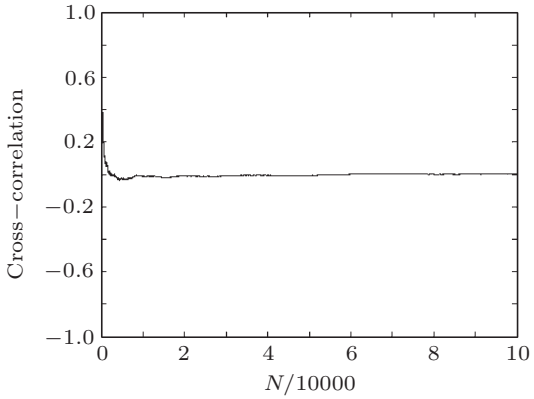


Fig. 4. The cross-correlation value of two sequences with initial values $x_0 = -0.2\mathrm{i}$ and $y_0 = -0.200000000000001\mathrm{i}$, respectively, and $N = 100000$.

4.2. NIST tests

The NIST tests[17] are used to detect deviations of a binary sequence from the true randomness. For each test, a P value is computed from the binary sequence. If this value is greater than a predefined threshold α, it is considered that the sequence passes the test successfully. Usually, α is set to be 0.01. In the experiments, 100 sequences, 1000000 bits each, are generated with our scheme. The test results are shown in Table 2.

In Table 2, prop. denotes the proportion of the sequences that pass the test. And if there is more than one statistical value in a test, the P value denotes the average value. The test results show the good statistic characteristics of the binary sequences.

4.3. Security analysis

4.3.1. Analysis of key space

The brute-force attack to our pseudorandom number generator requires finding the initial condition b. In the complex number chaotic equation, the initial value b belongs to $\mathbf{R}$, where $\mathbf{R}$ is the set of all real numbers. Obviously, to ensure that the complex number chaotic equation is meaningful, there should be $b \neq 0, \pm 1$. So the key b lies in the set $J = \{b \in \mathbf{R} | b \neq 0, \pm 1\}$. Such a large key space can resist the brute-force attack.

Table 2. Results of NIST tests.

Test	P	Prop.
Frequency	0.495000	1.00
Block-frequency	0.517249	1.00
Cumulative sums	0.492596	0.99
Runs	0.447331	1.00
Longest run	0.487530	1.00
Rank	0.565011	1.00
FFT	0.514842	1.00
Overlapping templates	0.444320	1.00
Non-overlapping templates ($B = 000000001$)	0.503238	1.00
Universal	0.467056	0.99
Approximate entropy ($m = 10$)	0.504711	1.00
Random excursions ($x = 1$)	0.514166	0.99
Random excursions variant ($x = 8$)	0.520510	1.00
Serial	0.495331	1.00
Linear complexity ($m = 500$)	0.482491	1.00

4.3.2. Analysis of key sensitivity

For any pseudorandom number generator, the key sensitivity, i.e., the sensitivity to the variation of key parameters, is important.[5] From Section 2, we know that our pseudorandom number generator is provided with good key sensitivity.

4.3.3. Analysis of linear complexity

The linear complexity measures the (linear) unpredictability of a sequence (finite or periodic) by using the length of the shortest linear feedback shift register (LFSR) that is able to generate the given sequence.[18,19] The Berlekamp–Massey algorithm[20] is an effective scheme to calculate the linear complexity. The expected linear complexity of a sequence of N independent and uniformly distributed binary random variables is very close to $N/2$. We have tested 1000 binary sequences generated by the proposed pseudorandom number generator, and the results are all satisfactory. Table 3 is the outcome of the sequence with the initial value 0.5i.

Table 3. Linear complexity of a sequence.

Length of sequence	Linear complexity
200	103
500	252
1000	501
5000	2501
10000	5000
20000	10000

4.4. Speed analysis

The proposed algorithm is implemented using GCC, and the speed performance is measured on a personal computer with 2.1 GHz Pentium(R) Dual-Core CPU, 2.00 GB RAM, and with Ubuntu as the operating system. In Table 4, we have compared our scheme with the other schemes in terms of speed.

Table 4. Speeds of the proposed scheme and some other schemes.

Generator	Speed/Mbit·s^{-1}
Proposed	0.4844
Ref. [8]	0.3798
Ref. [14]	0.2897
Ref. [21]	0.2385

When the randomness and the security requirement are fulfilled, the running speed becomes an important factor for practical applications. From Table 4, we find the proposed pseudorandom number generator is better.

5. Conclusion

In this paper, a new chaotic equation has been presented and proved, where the definitional domain of the equation is the imaginary axis. The difference from the conventional real number field provides a new approach to the construction of chaotic equations. Based on this equation, a pseudorandom number generator has been constructed. The randomness, the

security, and the speed of the binary sequences generated by the pseudorandom number generator are satisfactory.

References

[1] Li P, Li Z, Halang W A and Chen G R 2006 *Phys. Lett.* A **349** 467

[2] Wang K, Pei W J, Xia H S and Cheung Y M 2008 *Phys. Lett.* A **372** 4388

[3] Wang X Y and Yu Q 2009 *Commun. Nonlinear Sci. Numer. Simulat.* **14** 574

[4] Raj S K, Rajesh G K and Vyasa S 2010 *IEEE T. Circuits* II **57** 203

[5] Wang S H and Li D 2010 *Chin. Phys.* B **19** 080505

[6] Wang Y, Wong K W, Liao X F and Chen G R 2011 *Appl. Soft. Comput.* **11** 514

[7] Ali K and Nejib S 2009 *Chaos Soliton. Fract.* **40** 2557

[8] Michael J W 1998 *IEEE T. Circuits* II **45** 227

[9] He D, He C, Jiang L G, Zhu H W and Hu G R 2001 *IEEE T. Circuits* I **48** 900

[10] Ljupco K and Goce J 2003 *IEEE T. Circuits* I **50** 123

[11] Barash L and Shchur L N 2006 *Phys. Rev.* E **73** 036701

[12] Mieczyslaw J 2006 *IEEE T. Circuits* I **53** 1140

[13] Ali K 2011 *Commun. Nonlinear Sci. Numer. Simulat.* **16** 822

[14] Zhang X F and Fan J L 2010 *Acta Phys. Sin.* **59** 2289 (in Chinese)

[15] Zhao H, Ma Y J, Liu S J, Gao S G and Zhong D 2011 *Acta Phys. Sin.* **60** 120501 (in Chinese)

[16] Lu K 1990 *Chaos Dynamics* (Shanghai: Shanghai Translation Publishing Company) pp. 48–53 (in Chinese)

[17] http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf [2011-12-18]

[18] Rueppel R 1986 *Proceedings of a Workshop on the Theory and Application of Cryptographic Techniques* (Berlin: Springer-Verlag) p. 167

[19] Sun K H, He S B and Sheng L Y 2011 *Acta Phys. Sin.* **60** 020505 (in Chinese)

[20] Msssey J L 1969 *IEEE T. Inform. Theory* **15** 122

[21] Tong X J and Cui M G 2010 *Sci. China Inf. Sci.* **53** 191