Information Processing Letters 116 (2016) 674–681

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

A pseudorandom bit generator based on new multi-delayed Chebyshev map

Lingfeng Liu [a,*], Suoxia Miao [b], Mengfan Cheng [c], Xiaojing Gao [d]

[a] School of Software, Nanchang University, Nanchang, 330031, PR China
[b] Faculty of Science, Nanchang Institute of Technology, Nanchang, 330029, PR China
[c] School of Optical and Electronic Information, Huazhong University of Science & Technology, Wuhan, 430074, PR China
[d] School of Automation, Huazhong University of Science & Technology, Wuhan, 430074, PR China

ARTICLE INFO

Article history:
Received 27 October 2015
Received in revised form 15 April 2016
Accepted 25 June 2016
Available online 30 June 2016
Communicated by X. Wu

Keywords:
Cryptography
Safety/security in digital systems
Algorithm

ABSTRACT

Chaotic map is regarded as an important pseudorandom source in the design of pseudorandom bit generators due to its excellent properties, such as unpredictability, randomness, aperiodicity, sensitive dependence on initial conditions and parameters. One-dimensional Chebyshev map is one of the most popular maps in designing pseudorandom bit generator. In order to improve its security, in this paper, we will first construct a new multi-delayed Chebyshev map. The dynamics analysis shows that this new map is more complex than the original Chebyshev map. Furthermore, we propose a new pseudorandom bit generator based on this multi-delayed Chebyshev map; the statistics and security analysis show that our pseudorandom bit generator has good pseudorandom characteristics and is highly capable to withstand attacks.

© 2016 Elsevier B.V. All rights reserved.

1. Introduction

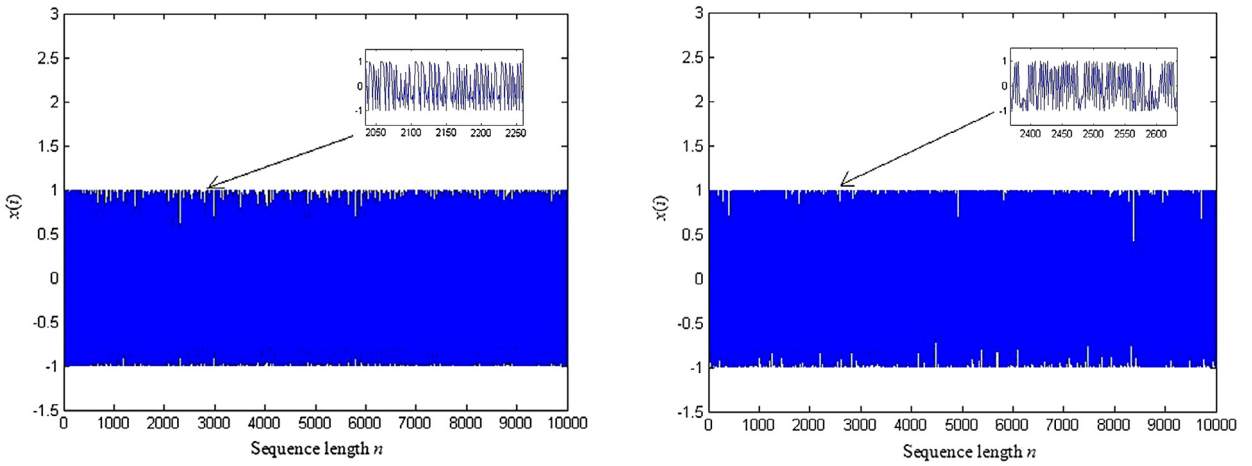
Chaos is a common nonlinear phenomenon in nature which has been studied for decades. The first mathematical definition of chaos was introduced by Li and Yorke in the 1970s [1]. After this, many chaotic theories, such as bifurcation diagrams, basin of attraction, Julia sets, or fractal attractors were widely been studied [2–4]. And for their random-like behavior, in spite of being deterministic, the chaotic maps were made attractive both for theoreticians and practitioners. In recent decades, chaotic map is regarded as an important pseudorandom source in the design of pseudorandom bit generators (PRBGs).

The first idea of designing a pseudorandom number generator by making use of chaotic map was proposed by Oishi and Inoue [5] in 1982. In recent years, a large number of chaotic pseudorandom sequence generators were proposed. Due to that the high-dimensional chaotic maps are often difficult to implement, among all the chaotic PRBGs, one-dimensional chaotic maps were most widely used [6–15]. Gonzalez and Pino generalized the logistic map and designed a truly unpredictable random function, which helped in the generation of truly random numbers [6]. Kocarev and Stojanovski et al. analyzed the application of a chaotic piecewise-linear one-dimensional map as random number generator [7]. Furthermore, Li did a theoretical analysis, which suggests that piecewise linear chaotic maps have perfect cryptographic properties [8]. In 2004, Huaping et al. used one-way coupled chaotic map lattice for generating pseudorandom numbers [9]. In 2006, Wang et al. proposed a pseudorandom number generator based on z-logistic map [10]. Very recently, Liu analyzed the statistics and complexity of chaotic pseudorandom sequences generated by Chebyshev map [11], et al.

However, classical one-dimensional chaotic map is not secure to be used as a PRBG for its simple structure. Short use of the phase space reconstruction method, successfully

* Corresponding author.
E-mail address: vatanoilcy@163.com (L. Liu).

http://dx.doi.org/10.1016/j.ipl.2016.06.011
0020-0190/© 2016 Elsevier B.V. All rights reserved.



(a) Original Chebyshev map (b) Multi-delayed Chebyshev map

Fig. 1. The trajectories of Original Chebyshev map and Multi-delayed Chebyshev map.

attacked almost all the one-dimensional chaotic maps [16]. For a classical one-dimensional chaotic map, the current state is completely determined by its previous state. This inner structure is rather simple and is easily to be revealed. In order to improve its security, motivated by the time-delayed dynamical system, we can lead other pre-order states into the chaotic iteration equation. In this paper, we will construct a new kind of chaotic map based on classical Chebyshev map. Our new map is a multi-delayed chaotic map, with its iteration based on multiple previous states. The dynamics analysis shows that our new chaotic map is more complex than the Chebyshev map. After then, we propose a new PRBG based on this multi-delayed chaotic map; the statistics and security analysis show that our PRBG has good pseudorandom characteristics and is highly capable to withstand attacks.

The rest of this paper is organized as follows. The new multi-delayed Chebyshev map and its dynamical characteristics are introduced in Section 2. In Section 3, we will propose our new PRBG based on multi-delayed Chebyshev maps. The statistical test and security analysis of the generated binary sequences are proposed in Section 4 and 5, respectively. Section 6 concludes the whole paper.

2. Multi-delayed Chebyshev map and its dynamical characteristics

The Chebyshev map is one of typical one-dimensional chaotic maps [17]. The equation of the Chebyshev map can be written as follows:

$$x(i+1) = \cos\big(a \cdot \arccos\big(x(i)\big)\big) \quad -1 \le x \le 1, \tag{1}$$

here, a is the degree of the Chebyshev map. If $a \ge 2$, the Chebyshev maps have the positive Lyapunov exponents for almost any initial state value, and have good properties with mixture and ergodicity. The map comes to be chaotic.

From Eq. (1) we have that, the current state of Chebyshev map is completely determined by its previous one. This inner structure is rather simple and can be easily revealed by some chaos theory methods and statistical methods. In order to improve its security, here, we proposed a new chaotic map, which is called multi-delayed Chebyshev map. The equation of our new multi-delayed Chebyshev map is as follows.

$$x(i+1) = \cos\Bigg(a \cdot \arccos\big(x(i)\big) + \sum_{j=1}^{k} b_j \cdot \arccos\big(x(i-j)\big)\Bigg) \quad -1 \le x \le 1, \tag{2}$$

where, b_j, $j = 1, 2, \ldots, k$, are the coefficients of the multi-delayed Chebyshev map, and k is the maximum delay time. In this paper, we just set $k = 1$, and Eq. (2) can be simplified as:

$$x(i+1) = \cos\big(a \cdot \arccos\big(x(i)\big) + b \cdot \arccos\big(x(i-1)\big)\big) \quad -1 \le x \le 1. \tag{3}$$

Next, we will compare the dynamical properties of our multi-delayed Chebyshev map shown in Eq. (3) with the original Chebyshev map shown in Eq. (1).

(a) Trajectory and attractor

Let the parameters be $a = 2$ and $b = 2$, and the initial values be $x(0) = 0.4214$ and $x(1) = -0.6448$. Fig. 1 shows that both trajectories of these two chaotic maps are random-like. Fig. 2 shows the attractors of these two chaotic maps. From Fig. 2 we can see that the attractor of original Chebyshev map has a particular shape, like a parabola, while the attractor of multi-delayed Chebyshev map has a fractal structure, which means that our multi-delayed Chebyshev map disrupt the original phase space of Chebyshev map, and is much more complex in its inner structure.

(b) Bifurcation

Here, we analyze the bifurcation behaviors of degree a for these two chaotic maps. Fig. 3(a) shows the bifurcation behavior of the original Chebyshev map. Fig. 3(b) shows the bifurcation behavior of the multi-delayed Chebyshev

Download English Version:

https://daneshyari.com/en/article/426997

Download Persian Version:

https://daneshyari.com/article/426997

Daneshyari.com