Pseudo-Random Bit Generator Based on Couple Chaotic Systems and its Applications in Stream-Cipher Cryptography*

Li Shujun[a], Mou Xuanqin[b], and Cai Yuanlong[c]

Institute of Image Processing, School of Electronics and Information Engineering,
Xi'an Jiaotong University, Xi'an, Shaanxi 710049, P. R. China

Abstract. Chaotic cryptology is widely investigated recently. This paper reviews the progress in this area and points out some existent problems in digital chaotic ciphers. As a comprehensive solution to these problems, a novel pseudo-random bit generator based on a couple of chaotic systems called CCS-PRBG is presented. Detailed theoretical analyses show that it has perfect cryptographic properties, and can be used to construct stream ciphers with higher security than other chaotic ciphers. Some experiments are made for confirmation. Finally, several examples of stream ciphers based on digital CCS-PRBG are given, and their security is discussed.

1 Introduction

Chaotic cryptography has received much attention in recent years, both digital and analog chaotic encryption methods have been proposed and analyzed [1–30]. Most analog chaotic ciphers are designed to realize secure communications through noisy channel using chaotic synchronization technique [1]. This paper chiefly focuses on the digital chaotic ciphers.

The tight relationship between chaos theory and cryptography has been pointed out by some researchers [1, 2, 16, 31]. Many fundamental characteristics of chaos, such as mixing and sensitivity to initial conditions, can be connected with those of good ciphers, such as confusion and diffusion. Since chaos theory has developed well in recent decades, and numerous chaotic systems can be employed in ciphers, chaos should be a new rich source of cryptography.

Generally speaking, there are two chief ways to design digital chaotic ciphers: 1) using chaotic systems to generate pseudo-random keystream to encrypt plaintext [3, 5–8, 10–12]; 2) using plaintext and/or secret key as the initial conditions and/or control parameters, iterating/counter-iterating chaotic systems n times to obtain ciphertext [2,9,13–16]. The first way corresponds to the stream ciphers

* This paper was published in *Progress in Cryptology - INDOCRYPT 2001, the 2nd International Conference on Cryptology in India* (INDOCRYPT'2001, 16-20 December, 2001, Indian Institute of Technology, Madras, Chennai, India), LNCS, vol. 2247, pp. 316-329, Springer-Verlag, Berlin, 2001.
The corresponding author is Shujun Li, personal web site: `http://www.hooklee.com`.

and the second does to the block ciphers. Some other ways also have been proposed [17–19]. Meanwhile, some efficient attacks have been presented [20–25]. In the following of this section, we will give a brief survey of the proposed digital chaotic ciphers, and discuss some problems existing in them.

1.1 Overview

Digital chaotic stream ciphers: Many different chaotic systems have been employed to generate pseudo-random keystream, 2-D Hénon attractor in [3], logistic map in [10], generalized logistic map in [6], quasi-chaotic nonlinear filter in [7], piecewise linear chaotic map in [4, 5, 8, 19], and first-order nonuniformly sampling digital phase-locked loop (DPLL) circuits in [11]. In [12] multiple different chaotic maps are suggested, Bernoulli shift and logistic map are used for demonstration. The algorithms generating chaotic pseudo-random keystreams can be divided into three classes: A1) – extracting from some bits of the chaotic orbits [4–6, 12]; A2) – determining by which interval the chaotic orbits reach [3, 8, 10, 11]; A3) – just equaling the chaotic orbits themselves [7]. It should be noticed that some algorithms in A2) [8, 10, 11] can be considered as the corresponding ones in A1), and A3) can be deemed as a special case of A1). Several chaotic stream ciphers [3, 6, 7] have been known not secure enough [20–23].

Digital chaotic block ciphers: Inverse tent map is used by T. Habutsu et al. in a chaotic cryptosystem [13], in which the plaintext represents the initial condition of the inverse tent map and the ciphertext is obtained by iterating this map N times. Because of the weakness of piecewise linearity of tent map and the use of 75 random bits, E. Biham presented a known-plaintext attack and a chosen-plaintext attack to break it [24]. Zbigniew Kotulski and Janusz Szczepanski generalized the method presented in [13] using other chaotic systems [14, 15]. In Jiri Fridrich's chaotic cipher [16], 2-D digital Barker map is introduced to realize secure pseudo-random permutation of 2-D plaintext such as digital images. A discrete version of chaotic inverse system encryption approach is presented by Zhou Hong et al. in [9].

Other digital chaotic ciphers: M. S. Baptista suggested a new encryption method in [17]: a chaotic attractor is divided into S units representing different plaintexts, the ciphertext is the number of iteration from an initial value to the unit representing the plaintext, logistic map is used for demonstration. In [18], such an idea is introduced: run a chaotic system, and use a threshold to generate a pseudo-random sequence from its orbit, find the position that plaintext occurs in the sequence and take the corresponding information about the position as the ciphertext, tent map is used as an example. G. Alvarez et al. pointed out that it is not secure at all if the tent map is used [25]. Li Shujun et al. improve the original chaotic cryptosystem to resist the proposed attacks [19].

1.2 Problems

Although many digital chaotic ciphers have been proposed and some of them have not been confronted with effective attacks, there are still many problems existing in them. To design a really good digital chaotic cipher, they must be carefully considered. The following is brief discussions on these problems:

1) Discrete Dynamics: When chaotic systems are realized discretely in finite computing precision, their discrete dynamics will be far different from continuous ones. Some severe degradation will arise, such as short cycle-length, non-ideal distribution and correlation, etc. This problem has been firstly noticed by J. Palmore, C. Herring [32] and D. Wheeler [21, 22], and then Ghobad Heidari-Bateni [33]. Up till now, there is not an established theory to measure the discrete dynamics of chaos exactly, and to indicate how to improve such degradation (we have proved some limited theoretical results in [34] recently). Only several engineering methods are suggested: using higher finite precision [21, 22], perturbation-based algorithm [4, 5, 35], and cascading multiple chaotic systems [33]. Actually, this problem is neglected in most digital chaotic ciphers [3, 8–15, 17, 18], so their security cannot be adequately ensured.

2) Employed Chaotic Systems: Because logistic map has been widely investigated in chaos theory and is very simple to be realized, it has been used by some digital chaotic ciphers [6,10,12,17]. However, only when control parameters r is 4.0, logistic map is a surjective function and has perfect chaotic properties. So r must be selected near 4.0 in these ciphers, which makes the key space much smaller. Other good candidates for simple realization are piecewise linear chaotic maps, such as tent map [13, 18] and the ones used in [4, 5, 8, 9, 19]. But we must be very careful to use them since there exist some weaknesses for their piecewise linearity [24, 25, 34]. In fact, it is desired that a digital chaotic cipher can work well with a large number of chaotic systems; such a property is called *chaotic-system-free* in this paper. Several chaotic ciphers are chaotic-system-free to some extent [12, 15, 17, 18]. Some others can be chaotic-system-free since different chaotic systems are not essentially excluded by their design [10, 11].

3) Encryption Speed: Some digital chaotic ciphers work so slowly that they are infeasible for real-time encryption [13–15, 17–19]. While the chaotic systems are running in finite precision, the floating-point or fixed-point arithmetic must be employed. Since the floating-point arithmetic is much slower than the fixed-point one, we suggest using fixed-point arithmetic as possible. But several chaotic systems defined by some complicated functions [6, 15] must run under floating-point arithmetic, they should be avoided in chaotic ciphers. The piecewise linear chaotic maps are the fastest chaotic systems, since only one division and several additions are needed in one iteration. Another problem about the encryption speed is: in order to enhance security, many ciphers need multiple chaotic iterations to generate one ciphertext [9–19], which will lower the encryption speed. In addition, some ciphers [17–19] have time-variant speed, so they cannot encrypt plaintext with constant bit-rate, such as MPEG video stream.

4) Practical Security: Most digital chaotic ciphers are claimed to be secure by the authors, but many of them are actually not. Because chaotic systems are deterministic systems, there are some tools in chaos theory to discern chaos. Once an intruder finds some information about the chaotic systems from their orbits, he might use such information to lessen the complexity of finding the secure key. For almost all digital chaotic ciphers [1–11, 13–19], the ciphertext directly depends on the chaotic orbit of a single chaotic system, so the extraction of such information may be possible. In fact, based on such a fact, many cryptanalysis methods [26–30] have been developed to break the analog secure communication approaches. If multiple chaotic systems are used [12, 33], the cryptanalysis of chaotic ciphers will be more difficult since the output is determined by many different mixed chaotic orbits.

5) Realization: Simple realization by hardware and software at low cost is a very important requirement for a good digital cipher. In consideration of the above fact, the fixed-point arithmetic is better than the floating-point one since the latter needs more cost. Another desired requirement is the extensible security with considerably more cost and complexity. In fact, problems of realization are the crucial factors influencing the use of a cipher in many final applications, since there are so many kinds of ciphers that can provide enough security.

Although many problems have not been settled in most digital chaotic ciphers, we still believe that the chaotic and conventional cryptology will benefit each other from the mutual relationship between them; some other researchers hold the same opinion [1,2,16,31]. In this paper, we suggest a comprehensive solution to the existent problems. A novel pseudo-random bit generator (PRBG) based on a couple of chaotic systems, called CCS-PRBG, is presented, which has perfect cryptographic properties and can be used to construct stream ciphers with high security. In these ciphers, most above-mentioned problems can be overcome satisfactorily.

The outline of this paper is as follows. In Sect. 2, CCS-PRBG and its digital realization with finite precision are introduced. Analyses on cryptographic properties of CCS-PRBG, including some experimental results, are given in Sect. 3. In Sect. 4, several examples of chaotic stream ciphers based on CCS-PRBG are established; discussion on the security is also given. The conclusion is given and some open research topics are pointed out in the last section.

2 Couple Chaotic Systems Based PRBG (CCS-PRBG)

As mentioned in Sect. 1, using chaos to generate pseudo-random numbers (PRN) is a general way to design digital chaotic stream ciphers. Besides in chaotic cryptography area, chaotic pseudo-random number generators (PRNG) have also attracted much attention in other research areas, such as communications [33,36, 37] and physics [38]. Most chaotic PRNG-s are based on single chaotic system and generate PRN directly from its orbit. In Sect. 1.2, we have discussed that such chaotic PRNG-s are potentially insecure, since the output PRN may expose some information about chaotic systems. In this paper, we present a novel pseudo-random bit generator (PRBG) based on a couple of chaotic systems, which can provide higher security than other ciphers because **two** chaotic systems are employed to generate PRN. Here, we call it CCS-PRBG as abbreviation. Since the PRN is generated by comparing two different chaotic orbits, it is difficult for an eavesdropper to extract information about both chaotic systems. More detailed discussions on security will be given in Sect. 4, after some chaotic stream ciphers based on CCS-PRBG are described.

2.1 Definition

Assume there are two different one-dimensional chaotic maps $F_1(x_1, p_1)$ and $F_2(x_2, p_2)$: $x_1(i+1) = F_1(x_1(i), p_1)$, $x_2(i+1) = F_2(x_2(i), p_2)$, where p_1, p_2 are control parameters, $x_1(0), x_2(0)$ are initial conditions, and $\{x_1(i)\}$, $\{x_2(i)\}$ denote the two chaotic orbits.

Define a pseudo-random bit sequence $k(i) = g(x_1(i), x_2(i))$, where

$$g(x_1, x_2) = \begin{cases} 1 & , x_1 > x_2 \\ \text{no output} & , x_1 = x_2 \\ 0 & , x_1 < x_2 \end{cases} . \tag{1}$$

When some requirements are satisfied, the chaotic PRBG will have perfect cryptographic properties and be called "a **C**ouple of **C**haotic **S**ystems based **P**seudo-**R**andom **B**it **G**enerator" (CCS-PRBG). These requirements are: *R1*) – $F_1(x_1, p_1)$ and $F_2(x_2, p_2)$ are surjective maps defined on a same interval $I = [a, b]$; *R2*) – $F_1(x_1, p_1)$ and $F_2(x_2, p_2)$ are ergodic on I, with unique invariant density functions $f_1(x)$ and $f_2(x)$; *R3*) – One of the following conditions holds: $f_1(x) = f_2(x) = f(x)$, or $f_1(x), f_2(x)$ are both even symmetrical to $x = (a+b)/2$; *R4*) – $\{x_1(i)\}, \{x_2(i)\}$ are asymptotically independent as $i \to \infty$.

If one of chaotic map is replaced by a constant $c \in I$, $k(i)$ will be simplified to the pseudo-random sequence in [11] and the chaotic threshold sequence in [36]. From such a viewpoint, CCS-PRBG can be regarded as the generalized version of them with "pseudo-random and time-variant threshold parameter" [1].

2.2 Digital Realization with Perturbation

It is obvious that CCS-PRBG can be applied to both analog and digital chaotic ciphers. We will only consider digital CCS-PRBG in this paper. The perturbation-based algorithm in [4] is suggested improving statistical properties of digital CCS-PRBG. The algorithm can be described as follows.

Use two PRNG-s to generate two pseudo-random distributed signals [2], which are used to perturb l lowest bits of $\{x_1(i)\}, \{x_2(i)\}$, with intervals Δ_1, Δ_2 [4]. The maximal length linear feedback shift registers (m-LFSR) are the best perturbing PRNG-s for hardware realization, and the linear congruential generators for

[1] $g(x_1, x_2)$ can be considered as follows: one chaotic orbit is binarized by anther chaotic orbit, the second chaotic orbit behaves like the threshold constant in [11, 36].

[2] Please see [4] for more details on how to generate the perturbing signals. Of course, we can use some other generation algorithms, the only requirement is that the generated signals should be pseudo-randomly distributed.

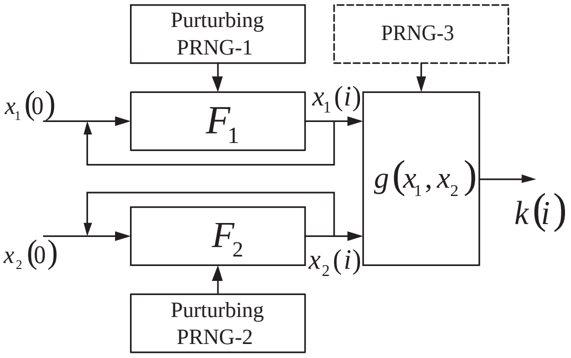


Fig. 1. The digital CCS-PRBG with perturbation

software realization [39]. Different from [4], this paper suggests determining l as follows: $l \geq \lceil \lambda \cdot \log_2 e \rceil = \lceil 1.44\lambda \rceil$, where λ is Lyapunov exponent of the perturbed chaotic map and $\lceil x \rceil$ denotes the least integer not less than x. It is based on such a fact: when the finite computing precision is n (bits), the least difference between two signals 2^{-n} will become $e^{\lambda} \cdot 2^{-n}$ after one iteration averagely (under fixed-point arithmetic). To keep the characteristics of the chaotic systems, $l \ll n$ should also be satisfied. Although the perturbing signal is much smaller than chaotic signal, it can still drive $\{x_1(i)\}, \{x_2(i)\}$ to a very complex way since chaos is sensitive to initial conditions. The combination of digital chaos and pseudo-randomness of PRNG-s will make both chaos-theory-based and conventional cryptanalysis difficult.

Another trivial problem existing in digital CCS-PRBG is: when $x_1 = x_2$, $g(x_1, x_2)$ will not output pseudo-random bit. An extra simple PRNG-3 can be introduced to determine $k(i)$. The digital CCS-PRBG with perturbation is shown in Fig. 1. We can see that it can be easily realized by both hardware and software.

3 Cryptographic Properties of Digital CCS-PRBG

For $\{k(i)\}$ generated by digital CCS-PRBG, the following cryptographic properties are satisfied: 1) balance on $\{0, 1\}$; 2) long cycle-length; 3) high linear complexity approximating to half of the cycle-length; 4) δ-like auto-correlation; 5) cross-correlation near to zero; 6) chaotic-system-free (see Sect. 1.2). Detailed discussions are given as follows, with some experimental results.

3.1 Balance

Theorem 1. *If two chaotic maps satisfy the above requirement R1–R4, we can get* $P\{k(i) = 0\} = P\{k(i) = 1\}$*, i.e.,* $k(i)$ *is balanced on* $\{0, 1\}$.

Proof. Because $F_1(x_1, p_1)$ and $F_2(x_2, p_2)$ are ergodic on $I = [a, b]$ (requirement *R2*), the orbits generated from almost all initial conditions will lead to the same distribution functions $f_1(x), f_2(x)$ [40]. From requirement *R4*, the orbits $\{x_1(i)\}, \{x_2(i)\}$ are asymptotically independent, so the probabilities of $x_1 > x_2$ and $x_1 < x_2$ as $i \to \infty$ will be:

$$P\{x_1 > x_2\} = \int_a^b \int_a^x f_1(x) f_2(y) \, \mathrm{d}y \, \mathrm{d}x \tag{2}$$

$$P\{x_1 < x_2\} = \int_a^b \int_a^x f_2(x) f_1(y) \, \mathrm{d}y \, \mathrm{d}x \tag{3}$$

When requirement *R3* holds, we can prove $P\{x_1 > x_2\} = P\{x_1 < x_2\}$:
***R3*–1)** $f_1(x) = f_2(x) = f(x)$:

$$P\{x_1 > x_2\} = P\{x_1 < x_2\} = \int_a^b \int_a^b f(x) f(y) \, \mathrm{d}y \, \mathrm{d}x. \tag{4}$$

***R3*–2)** $f_1(x), f_2(x)$ are both even symmetrical to $x = (a+b)/2$:
Define the mirror orbits of x_1, x_2 as $x'_1 = b - x_1, x'_2 = b - x_2$. From the symmetry of $f_1(x), f_2(x)$, x'_1, x'_2 will have the same distribution $f_1(x), f_2(x)$, then we have:

$$P\{x_1 > x_2\} = P\{x'_1 < x'_2\} = \int_a^b \int_a^{x'} f_2(x') f_1(y') \, \mathrm{d}y \, \mathrm{d}x = P\{x_1 < x_2\}. \tag{5}$$

Consider $x_1 > x_2 \to k(i) = 1$ and $x_1 < x_2 \to k(i) = 0$, $P\{x_1 > x_2\} = P\{x_1 < x_2\} \Rightarrow P\{k(i) = 0\} = P\{k(i) = 1\}$. The proof is complete.

Apparently, the above deduction is still based on the continuous conditions. When chaotic systems are discretely realized with perturbation, every chaotic orbit will be perturbed timely to a certain neighbor orbit by the small perturbing signal. Consequently, almost all orbits reach to the discrete versions of $f_1(x), f_2(x)$ with a little smoothing. For the discrete versions of $f_1(x), f_2(x)$, the above deduction also holds if $\int$ is replaced by $\sum$ [3]. Therefore, the balance will be approximately preserved in the digital CCS-PRBG with perturbation.

3.2 Long Cycle-Length

When the ergodic chaotic systems are realized continuously, the cycle-length will be infinite for the orbit beginning at almost every initial condition [40]. However, as we have pointed out in Sect. 1, when they are discretely realized with finite precision, the short cycle-length problem will arise. Employing perturbation can solve this problem. Without loss of generality, assume two m-LFSR-s are used as the perturbing PRNG-s, whose degrees are L_1, L_2, and perturbing intervals are

[3] Equation (2) and (3) are replaced by $P\{x_1 > x_2\} = \sum_{x=a}^{b} \sum_{y=a}^{x} P_1\{x_1 = x\} \cdot P_2\{x_2 = y\}$ and $P\{x_2 > x_1\} = \sum_{x=a}^{b} \sum_{y=a}^{x} P_2\{x_1 = x\} \cdot P_1\{x_2 = y\}$. From the approximate symmetry to $x = 1/2$ of x_1, x_2 when a digital CCS-PRBG is realized with perturbation, we can obtain the following result $P\{x_1 > x_2\} \approx P\{x_1 < x_2\}$.

$\varDelta_1, \varDelta_2$. Then the cycle-length of $x_1(i)\}, \{x_2(i)\}$ are $\sigma_1\varDelta_1(2^{L_1}-1), \sigma_2\varDelta_2(2^{L_2}-1)$, where σ_1, σ_2 are two positive integers [4]. So the cycle-length of $\{k(i)\}$ will be:

$$\mathrm{lcm}(\sigma_1\varDelta_1(2^{L_1}-1), \sigma_2\varDelta_2(2^{L_2}-1)). \tag{6}$$

When $\varDelta_1, \varDelta_2$ and L_1, L_2 are selected to satisfy $\gcd(\varDelta_1, \varDelta_2) = 1$ and $\gcd(2^{L_1}-1, 2^{L_2}-1) = 1$, the cycle-length of $\{k(i)\}$ will be:

$$\mathrm{lcm}(\sigma_1, \sigma_2) \cdot \varDelta_1\varDelta_2(2^{L_1}-1)(2^{L_2}-1) \approx \mathrm{lcm}(\sigma_1, \sigma_2) \cdot \varDelta_1\varDelta_2 2^{L_1+L_2}. \tag{7}$$

Such a cycle length is long enough for most secure applications. Furthermore, there are still some methods that can be used to further prolong the cycle length, such as the one in [5].

3.3 High Linear Complexity and Good Correlation Properties

Actually, the requirement *R4* and the balance of $\{k(i)\}$ imply that $\{k(i)\}$ is an independent and identically distributed (i.i.d.) bit sequence as $i \to \infty$. Therefore, it will have δ-like auto-correlation and near-to-zero cross-correlation. What's more, it has been proved (see [41]) that i.i.d. binary sequence has half-length linear complexity, so $\{k(i)\}_{i=1}^{n}$ will also have high linear complexity approximating to $n/2$ [4]. So let us discuss under what condition requirement *R4* will be satisfied for digital CCS-PRBG.

For any chaotic maps, even if the initial conditions or the control parameters have a very small difference, their orbits will become entirely different after limited iterations. If there is some initial information about the orbits, the information will decrease to zero as $i \to \infty$. The relation between two chaotic orbits can be considered as such information. In chaos theory, Kolmogorov entropy is defined to measure the decreasing rate of the information. For one-dimensional chaotic maps, Kolmogorov entropy is equal to Lyapunov exponent [42]. If the initially known information is H, it will lose completely after $\eta \approx H/\lambda$ iterations [11], where λ is Lyapunov exponent. When chaotic systems are realized discretely, the information will decrease even faster since the quantization errors and small perturbing signals makes two orbits depart faster. So we can see, as long as there is initial difference between two chaotic orbits, they will become asymptotically independent as $i \to \infty$. Therefore, the equivalent requirement of *R4* is $\{x_1(i)\} \neq \{x_2(i)\}$, that is to say, $F_1 \neq F_2$, or $x_1(0) \neq x_2(0)$, or $p_1 \neq p_2$.

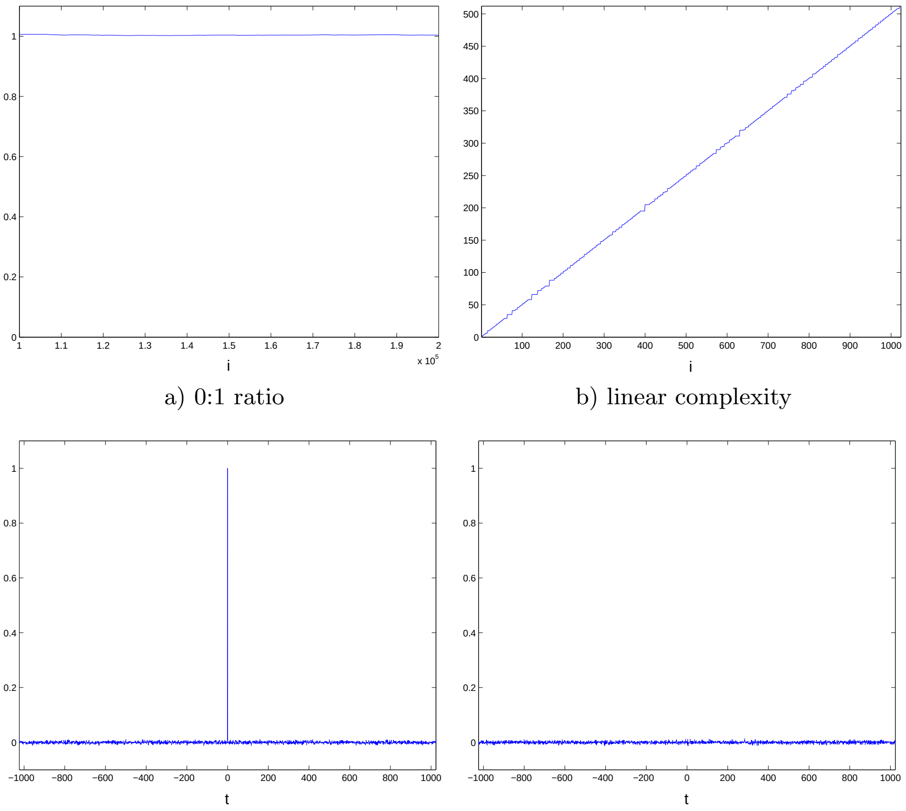
Because the independence of $\{x_1(i)\}, \{x_2(i)\}$ holds after η iterations, we suggest discarding the first m bits of $\{k(i)\}$, where $m > \eta$. It means m pre-iterations for the two chaotic maps should be done before $\{k(i)\}$ is output. Since m is not very large, such pre-iterations need only a little extra computation.

Although analyses given here are entirely theoretic, the experiments strongly support the theoretical results (see the following Fig. 2. and Sect. 3.5 for more details). In the future research, we will try to find the strict proof of $\{k(i)\}$ generated by CCS-PRBG is real i.i.d. binary sequence.

[4] The cycle-length of $\{k(i)\}$ is $L = \mathrm{lcm}(\sigma_1\varDelta_1(2^{L_1}-1), \sigma_2\varDelta_2(2^{L_2}-1))$, not infinity. Hence, the linear complexity of $\{k(i)\}_{i=1}^{\infty}$ should be about $L/2$, not infinity either.

3.4 Chaotic-System-Free Property

Consider there are many chaotic maps satisfy the requirements *R1* and *R2*, and the requirement *R3* and *R4* just restrict the relation between the two chaotic systems, CCS-PRBG is chaotic-system-free obviously. Since piecewise linear chaotic maps satisfy the requirements *R1*–*R4*, they are strongly suggested being used, from the viewpoint of the encryption speed and realization (recall section 1.2).



a) 0:1 ratio

b) linear complexity

c) auto-correlation

d) cross-correlation

Fig. 2. Cryptographic properties of digital CCS-PRBG

3.5 Experimental Results

In order to verify the theoretical results on cryptographic properties of digital CCS-PRBG with perturbation, some experiments are made. The two chaotic maps are both selected as the following piecewise linear maps define on $I = [0, 1]$, which are used in [9] and detailed analyzed in [34]:

$$F_1(x,p) = F_2(x,p) = F(x,p) = \begin{cases} x/p, & x \in [0,p) \\ (x-p)/(\frac{1}{2}-p), & x \in [p,\frac{1}{2}] \\ F(1-x,p), & x \in [\frac{1}{2},1] \end{cases} , \qquad (8)$$

The finite computing precision is $n = 32$ (bits). The perturbing PRNG-s are selected as two m-LFSR-s, whose degrees are $L_1 = 16$, $L_2 = 17$ and whose perturbing intervals are $\Delta_1 = 99$, $\Delta_2 = 101$. The number of pre-iteration m is 16. Both initial conditions and control parameters are generated randomly, and a large number of sub-sequences of $k(i)$ are extracted from random positions to test the cryptographic properties. The 0:1 ratio, linear complexity and auto-correlation of one sub-sequence are shown in Fig. 2a–c respectively. In Fig. 2d, the cross-correlation of two sub-sequences with identical initial conditions but slightly different (2^{-n}) control parameters is given. We can see the experimental results coincide well with the theoretical analyses.

4 Construct Stream Ciphers Using Digital CCS-PRBG

Based on digital CCS-PRBG, many different practical stream ciphers can be constructed. We will see these stream ciphers can provide feasible solutions to the problems existing in other digital chaotic ciphers. Using different configurations of CCS-PRBG, many stream ciphers can be obtained conveniently with considerably low cost and simple realization. Here, digital CCS-PRBG replaces the kernel role of LFSR in conventional stream-cipher cryptography.

4.1 Some Examples of Stream Ciphers

• **Cipher 1:** Give a digital CCS-PRBG with perturbation, initial conditions $x_1(0), x_2(0)$ and control parameters p_1, p_2 are the secure key. $\{k(i)\}$ is directly used to encrypt (generally XOR) plaintext and decrypt ciphertext.

The above Cipher 1 is the simplest stream cipher based on digital CCS-PRBG. If finite computing precision is n (bits), the key entropy will be $4n$. Moreover, it is easy to be realized by hardware or software with rather low cost. On a Pentium III 800MHz PC, a software version based on piecewise linear chaotic map (8) is developed with Turbo C 2.0 for test. The actual encryption speed reaches 9 Mbps under fixed-point arithmetic. Such a speed is faster than many other chaotic ciphers and can be acceptable in many secure applications. Under hardware realization, the speed will be promoted much.

If some simple modifications are made on cipher 1, some enhanced stream ciphers with larger key entropy (higher security), faster speed can be obtained with a little extra complexity and cost. Two examples are given as follows.

• **Cipher 2:** Give four one-dimensional chaotic systems $CS_0 \sim CS_3$, and five m-LFSR-s $m\text{-}LFSR_0 \sim m\text{-}LFSR_4$, in which $m\text{-}LFSR_0 \sim m\text{-}LFSR_3$ are used to perturb $CS_0 \sim CS_3$. Before each iteration of $CS_0 \sim CS_3$, firstly use $m\text{-}LFSR_4$

to generate two 2-bits pseudo-random numbers $pn1(i)$ and $pn2(i)$. If $pn2(i) = pn1(i)$, do $pn2(i) = pn1(i) \oplus 1$. Then select $CS_{pn1(i)}$ and $CS_{pn2(i)}$ to compose the digital CCS-PRBG to generate $k(i)$. The secure key contains the initial conditions and control parameters of the four chaotic systems.

The key entropy will be $8n$ under n (bits) computing precision. $m\text{-}LFSR_4$ adds more complexity to the cryptanalysis so such a cipher is securer, with only double cost of realization and approximate encryption speed to cipher 1.

- **Cipher 3:** For piecewise linear chaotic maps defined on $I = [0, 1]$, such as the map (8), the invariant density functions are $f(x) = 1$. When they are realized discretely, every bit of the orbits will be balanced on $\{0, 1\}$. Based on such a fact, we can define a generalized version of digital CCS-PRBG. Here assume finite computing precision is n (bits). For one iteration of $F_1(x_1, p_1)$ and $F_2(x_2, p_2)$, generate n bits $K(i) = k_0(i) \dots k_{n-1}(i)$ as follows:

```
for $j = 0$ to $n - 1$ do
    $x_1(i, j) = x_1(i) \gg j$
    $x_2(i, j) = x_2(i) \ll j$
    $k_j(i) = g(x_1(i, j), x_2(i, j))$
end
```

Where $\gg$ ($\ll$) denotes circular right (left) shift operation. Apparently, a stream cipher based on generalized CCS-PRBG will run nearly n times faster than the one based on common CCS-PRBG, without loss of high security. When cipher 3 is realized by hardware with parallel arithmetic technique, the encryption speed of cipher 3 will close to s Mbps when the clock frequency is s MHz [5]. Such a speed approximately equals to the speed of many conventional stream ciphers based on LFSR-s, such as Geffe generator and clock-controlled generator, and faster than some complicated stream ciphers [39]. If we combine cipher 2 and cipher 3, both the security and the encryption speed can be improved much. Actually, in order to further enhance the security of Cipher 3, we can introduce another $m\text{-}LFSR_5$ to pseudo-randomly control the direction of the circular shift operation of x_1 and x_2.

4.2 Security

Generally speaking, the security of the above ciphers can be ensured by the perfect cryptographic properties of digital CCS-PRBG. But we have known that many chaotic ciphers are not secure although they have some “good” statistical properties. So we should still investigate whether or not the ciphers based on digital CCS-PRBG is secure enough to known cryptanalysis methods.

Many methods have been proposed to break analog chaotic encryption schemes, such as chaotic masking, switching and modulating approaches [26–30]. They work well because chaotic synchronization makes it possible to extract dynamical information of the chaotic systems. Since the transmitted signal must be

[5] Apparently, the speed is chiefly determined by the fixed-point divisions needed in chaotic iterations. Since a n-bit digital divider consumes about n clock cycles for one n-bit division, the encryption speed of cipher 3 will be close to $\frac{s}{n} \cdot n = s$ Mbps.

used to realize synchronization of the transmitter and receiver, such information may be useful to restore the chaotic orbit and then extract the hidden message. For digital CCS-PRBG, because chaotic synchronization is not used and two different chaotic orbits are employed to make pseudo-random keystream $k(i)$, the dynamics of the two chaotic systems cannot be obtained from the ciphertext. In addition, the pseudo-random perturbation also makes the cryptanalysis more difficult. Even if the plaintext is known, it is impossible to extract the two chaotic orbits just from $k(i)$. Hence, those methods, which are available to break secure communication approaches based on chaotic synchronization, cannot be used to break the ciphers based on digital CCS-PRBG.

Other known cryptanalysis methods aim at different weaknesses of concerned chaotic ciphers. The one in [21,22] is available because of the degraded statistical properties of discrete chaotic systems, which has been considered carefully and been avoided by perturbation-based algorithm in digital CCS-PRBG. The one in [20] is based on a specific weakness of 2-D Hénon map and cannot be generalized to other chaotic systems. The ones in [23–25] can work well for the special weaknesses in the corresponding ciphers and also cannot be extended to break CCS-PRBG based ciphers with entirely different encryption structure.

We can see the ciphers based on digital CCS-PRBG are secure to all known cryptanalysis methods of chaotic ciphers. Of course, before we can finally say "digital CCS-PRBG based ciphers are secure enough", further research on cryptanalysis of digital CCS-PRBG should be done. But the above discussion implies that digital CCS-PRBG may be a new promising candidate to construct stream ciphers with high security and low cost.

There is one notable defect in digital CCS-PRBG that should be mentioned here. Assume $x_1(0) = x_2(0)$, when the control parameters are p_1, p_2, the generated pseudo-random bit sequence is $k(i)$; exchange the control parameters of the two chaotic maps, the generated pseudo-random bit sequence is $k'(i)$. If the two chaotic maps are perturbed with identical perturbing PRNG-s and identical perturbing intervals ($\varDelta_1 = \varDelta_2$), it is obvious that $k'(i) = \overline{k(i)}$, which is the natural result of $g(x_2, x_1) = \overline{g(x_1, x_2)}$. Such an effect will cause the key space size of the ciphers decrease $1/2$. To avoid this defect, different perturbing PRNG-s or perturbing intervals should be used, and $m > \max(\varDelta_1, \varDelta_2)$ is suggested.

5 Conclusion

Nowaday digital chaotic ciphers are surveyed, and some existent problems in them are discussed in this paper. A novel chaotic PRBG called CCS-PRBG is proposed to solve these problems. Theoretical analyses and experiments show that digital CCS-PRBG has perfect cryptographic properties. The digital CCS-PRBG can be a kernel part in the design of new stream ciphers. In the future, some details on hardware realization of CCS-PRBG based stream ciphers will be concerned. As we have mentioned in Sect. 3.3, the strict proof of $\{k(i)\}$ is i.i.d. sequence will be further studied, too. Possible cryptanalysis methods of the digital CCS-PRBG will be another open topic.

Acknowledgement

The authors would like thank the anonymous reviewers for their helpful comments, Miss Han Lu at Xi'an Foreign Language University and Miss Cao Yanghui at Xi'an Jiaotong University for their helps in the preparation of this paper.

References

1. G. Alvarez, G. Pastor F. Monotoya, and M. Romera. Chaotic cryptosystems. In *Proc. IEEE Int. Carnahan Conf. Security Technology*, pages 332–338. IEEE, 1998.
2. Ljupčo Kocarev, Goce Jakimoski, Toni Stojanovski, and Ulrich Parlitz. From chaotic maps to encryption schemes. In *Proc. IEEE Int. Symposium Circuits and Systems*, volume 4, pages 514–517. IEEE, 1998.
3. R. Forré. The Hénon attractor as a keystream generator. In *Advances in Cryptology – EuroCrypt'91*, Lecture Notes in Computer Science 0547, pages 76–81, Berlin, 1991. Spinger-Verlag.
4. Sang Tao, Wang Ruili, and Yan Yixun. Perturbance-based algorithm to expand cycle length of chaotic key stream. *Electronics Letters*, 34(9):873–874, 1998.
5. Sang Tao, Wang Ruili, and Yan Yixun. Clock-controlled chaotic keystream generators. *Electronics Letters*, 34(20):1932–1934, 1998.
6. R. Matthews. On the derivation of a 'chaotic' encryption algorithm. *Cryptologia*, XIII(1):29–42, 1989.
7. D. R. Frey. Chaotic digital encoding: An approach to secure communication. *IEEE Trans. Circuits and Systems II*, 40(10):660–666, 1993.
8. Zhou Hong and Ling Xieting. Generating chaotic secure sequences with desired statistical properties and high security. *Int. J. Bifurcation and Chaos*, 7(1):205–213, 1997.
9. Hong Zhou and Xie-Ting Ling. Problems with the chaotic inverse system encryption approach. *IEEE Trans. Circuits and Systems I*, 44(3):268–271, 1997.
10. M. E. Bianco and D. A. Reed. Encryption system based on chaos theory. US Patent No. 5048086, 1991.
11. G. M. Bernstein and M. A. Lieberman. Secure random number generation using chaotic circuits. *IEEE Trans. Circuits and Systems*, 37(9):1157–1164, 1990.
12. V. A. Protopopescu, R. T. Santoro, and J. S. Tollover. Fast and secure encryption – decryption method based on chaotic dynamics. US Patent No. 5479513, 1995.
13. T. Habutsu, Y. Nishio, I. Sasase, and S. Mori. A secret key cryptosystem by iterating a chaotic map. In *Advances in Cryptology - EuroCrypt'91*, Lecture Notes in Computer Science 0547, pages 127–140, Berlin, 1991. Spinger-Verlag.
14. Zbigniew Kotulski and Janusz Szczepanski. Application of discrete chaotic dynamical systems in cryptography – dcc method. *Int. J. Bifurcation and Chaos*, 9(6):1121–1135, 1999.
15. Zbigniew Kotulski and Janusz Szczepanski. Discrete chaotic cryptography. *Annalen der Physik*, 6(5):381–394, 1997.
16. Jiri Fridrich. Symmetric ciphers based on two-dimensional chaotic maps. *Int. J. Bifurcation and Chaos*, 8(6):1259–1284, 1998.
17. M. S. Baptista. Cryptography with chaos. *Physics Letters A*, 240:50–54, 1998.
18. E. Alvarez, A. Fernández, P. García, J. Jiménez, and A. Marcano. New approach to chaotic encryption. *Physics Letters A*, 263:373–375, 1999.

19. Li Shujun, Mou Xuanqin, and Cai Yuanlong. Improving security of a chaotic encryption approach. *Physics Letters A (to be published)*.
20. D. Erdmann and S. Murphy. Hénon stream cipher. *Electronics Letters*, 28(9):893–895, 1992.
21. D. D. Wheeler. Problems with chaotic cryptosystems. *Cryptologia*, XIII(3):243–250, 1989.
22. D. D. Wheeler and R. Matthews. Supercomputer investigations of a chaotic encryption algorithm. *Cryptologia*, XV(2):140–151, 1991.
23. W. G. Chambers. Comments on 'chaotic digital encoding: An approach to secure communication'. *IEEE Trans. Circuits and Systems II*, 46(11):1445–1447, 1993.
24. E. Biham. Cryptoanalysis of the chaotic-map cryptosystem suggested at EuroCrypt'91. In *Advances in Cryptology - EuroCrypt'91*, Lecture Notes in Computer Science 0547, pages 532–534, Berlin, 1991. Spinger-Verlag.
25. G. Alvarez, F. Montoya, M. Romera, and G. Pastor. Cryptanalysis of a chaotic encryption system. *Physics Letters A*, 276:191–196, 2000.
26. Kevin M. Short. Signal extraction from chaotic communications. *Int. J. Bifurcation and Chaos*, 7(7):1579–1597, 1997.
27. Tao Yang, Lin-Bao Yang, and Chun-Mei Yang. Cryptanalyzing chaotic secure communications using return maps. *Physics Letters A*, 245:495–510, 1998.
28. Maciej J. Ogorzatek and Hervé Dedieu. Some tools for attacking secure communication systems employing chaotic carriers. In *Proc. IEEE Int. Symposium Circuits and Systems 1998*, volume 4, pages 522–525. IEEE, 1998.
29. Chang-Song Zhou and Tian-Lun Chen. Extracting information masked by chaos and contaminated with noise: Some considerations on the security of communication approaches using chaos. *Physics Letters A*, 234:429–435, 1997.
30. Th. Beth, D. E. Lazic, and A. Mathias. Cryptanalysis of cryptosystems based on remote chaos replication. In *Advances in Cryptology - EuroCrypt'94*, Lecture Notes in Computer Science 0950, pages 318–331, Berlin, 1994. Spinger-Verlag.
31. R. Brown and L. O. Chua. Clarifying chaos: Examples and counterexamples. *Int. J. Bifurcation and Chaos*, 6(2):219–249, 1996.
32. Julian Palmore and Charles Herring. Computer arithmetic, chaos and fractals. *Physica D*, 42:99–110, 1990.
33. Ghobad Heidari-Bateni and Clare D. McGillem. A chaotic direct-sequence spread-spectrum communication system. *IEEE Trans. Communications*, 42(2/3/4):1524–1527, 1994.
34. Li Shujun, Li Qi, Li Wenmin, Mou Xuanqin, and Cai Yuanlong. Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-random coding. In *Cryptography and Coding - 8th IMA Int. Conf. Proc. (to be published)*, Lecture Notes in Computer Science, Berlin, 2001. Springer-Verlag.
35. Zhou Hong and Ling Xieting. Realizing finite precision chaotic systems via perturbation of m-sequences. *Acta Eletronica Sinica* (In Chinese), 25(7):95–97, 1997.
36. Tohru Kohda and Akio Tsuneda. Statistics of chaotic binary sequences. *IEEE Trans. Information Theory*, 43(1):104–112, 1997.
37. Shin'ichi Oishi and Hajime Inoue. Pseudo-random number generators and chaos. *Trans. IECE Japan*, E 65(9):534–541, 1982.
38. Jorge A. González and Ramiro Pino. A random number generator based on unpredictable chaotic functions. *Computer Physics Communications*, 120:109–114, 1999.
39. Bruce Schneier. *Applied Cryptography – Protocols, algorithms, and souce code in C.* John Wiley & Sons, Inc., New York, second edition, 1996.

40. Andrzej Lasota and Michael C. Mackey. *Chaos, Fractals, and Noise - Stochastic Aspects of Dynamics*. Springer-Verlag, New York, second edition, 1997.
41. Yang Yixian and Lin Xuduan. *Coding Theory and Cryptology* (In Chinese). People's Post and Telecommunications Press, Beijing, China, 1992.
42. Hao Bai-Lin. *Starting with Parabolas: An Introduction to Chaotic Dynamics* (In Chinese). Shanghai Scientific and Technological Education Publishing House, Shanghai, China, 1993.