Security analysis of a multiple pseudorandom-bit generator based on a spatiotemporal chaotic map*

Wang Shi-Hong(王世红)[a)b)†] and Li Da(李 达)[a)]

[a)] *School of Science, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*

[b)] *Key Laboratory of Optical Communication and Lightwave, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*

(Received 9 December 2009; revised manuscript received 7 April 2010)

In this paper we analyse the security of a multiple pseudorandom-bit generator based on the coupled map lattice and suggest an improved model. Utilizing the error function attack, the multiple pseudorandom-bit generators which can be realized by the three digitization methods are analysed and the effective key spaces are estimated. We suggest an improved multiple pseudorandom-bit generator with 128-bit secret key, and analyse the key sensitivity and statistical properties of the system.

Keywords: coupled map lattice, cryptoanalysis, pseudorandom-bit generator

PACC: 0545

1. Introduction

Due to the random behaviour of chaos and the sensitivity of chaotic trajectories to the initial conditions and the parameters, chaos dynamics have been investigated and applied to the information security fields. Many chaos-based cryptosystems are presented and analysed.[1−7] To enhance the complexity and security of the cryptosystems, spatiotemporal chaos dynamics have usually been used.[8−14] Chaos dynamics work in real number field, therefore, some methods of digitizing chaotic signals have been suggested for digital communications. A multiple pseudorandom-bit generator (MPRBG) based on the coupled map lattice (CML–MPRBG) is proposed in Ref. [15]. In Ref. [15] the authors investigated three digitization methods and suggested that the digitization method 2 is better than the other two used in the CML–MPRBG.

This work aims to analyse the CML–MPRBG in Ref. [15] by the error function attack (EFA)[5,13] and suggest an improved CML–MPRBG. The paper is arranged as follows. The coupled map lattice (CML) dynamics and the three methods of digitizing chaotic signals[15] are introduced in Section 2. In Section 3 we analyse the key sensitivity of the CML–MPRBG and estimate the effective spaces of secret keys. In Section 4 we suggest an improved CML–MPRBG, and analyse the key sensitivity and the correlation of output sequences. The last section finishes with some concluding remarks.

2. An MPRBG based on CML

The CML dynamics of the CML–MPRBG in Ref. [15] is

$$x_{n+1,i} = (1-\varepsilon)f(x_{n,i}) + \frac{\varepsilon}{2}[f(x_{n,i-1}) + f(x_{n,i+1})], \quad (1)$$

where n is the time index, and i, $i = 1, 2, \ldots, L$, is the lattice site index. Periodic boundary conditions are used. Parameter ε is a coupling constant. $f(x) = rx(1-x)$, $r \in [0, 4]$, $x \in [0, 1]$. $f(x)$ is the local map. The parameters ε and r are used as two secret keys. According to the first IEEE Standard for Binary Floating-Point Arithmetic (IEEE 754-1985), a double-precision 64-bit real number includes three parts, 1-bit sign, 52-bit fraction, and 11-bit exponent. For the parameters ε and r, key space comes to 104-bit.

The CML–MPRB is generated by digitizing the chaotic signals $x_{n,i}$ defined in Eq. (1). Through digitizing $x_{n,i}$ to $s_{n,i}$, the i-th pseudorandom-bit generator (PRBG), $S_i = \{s_{1,i}, s_{2,i}, s_{3,i}, \ldots, s_{n,i}\}$, can be

*Project supported by the National Natural Science Foundation of China (Grant No. 60973109).

†Corresponding author. E-mail: shwang@bupt.edu.cn

© 2010 Chinese Physical Society and IOP Publishing Ltd

generated from the output of the i-th site of the CML. Three digitization methods in Ref. [15] are simply introduced as follows.

Method 1 Given different thresholds to digitize chaotic signals. For example, given one threshold c, $x_{n,i}$ can be digitized as

$$s_{n,i} = \begin{cases} 0, & x_{n,i} \in [a, c], \\ 1, & x_{n,i} \in (c, b]. \end{cases} \tag{2}$$

Method 2 $x_{n,i}$ can be presented as a binary sequence $x_{n,i} = 0.b_{n,i,1}b_{n,i,2\ldots}\, b_{n,i,m} \ldots b_{n,i,p}$, $b_{n,i,m} \in \{0, 1\}$, p stands for a certain precision. $x_{n,i}$ can be digitized as

$$s_{n,i} = b_{n,i,m},\ 1 \le m \le p. \tag{3}$$

Method 3 $x_{n,i}$ can be digitized as follows:

$$\begin{aligned} s_{n,i} &= b_{n,i,m_1} \oplus b_{n,i,m_1+1} \oplus \ldots \\ &\quad \oplus b_{n,i,m_2-1} \oplus b_{n,i,m_2}, \\ &\quad m_1 \ge 1, \quad \text{and} \quad m_2 \le p, \end{aligned} \tag{4}$$

where the operation $\oplus$ stands for an exclusive XOR operation. If $m_1 = 1$, $m_2 = p$, equation (4) becomes $s_{n,i} = b_{n,i,1} \oplus b_{n,i,2} \oplus \cdots \oplus b_{n,i,p}$.[15]

3. Security analysis

For any PRBG the key sensitivity, i.e., the sensitivity to variation of key parameters, is of importance for evaluating the security of systems. The EFA is a method suggested for analysing the key sensitivity of self-synchronizing stream ciphers.[5,13] In this section we utilize the EFA to analyse the CML–PRBG with the three digitization methods and estimate actual key spaces.

3.1. The EFA on the digitization Method 2

Fix the secret keys r_0 and ε_0, and the corresponding key differences Δr and $\Delta\varepsilon$, then test keys r_0, ε_0, and r', ε' in Eq. (1), with $r' = r_0 + \Delta r$, $\varepsilon' = \varepsilon_0 + \Delta\varepsilon$. Two chaotic outputs from Eq. (1) can be attained,

$$\begin{aligned} x_{n+1,i} &= (1-\varepsilon_0)f(x_{n,i}) + \frac{\varepsilon_0}{2}[f(x_{n,i-1}) + f(x_{n,i+1})] \\ &= (1-\varepsilon_0)r_0x_{n,i}(1-x_{n,i}) + \frac{\varepsilon_0}{2}[r_0x_{n,i-1}(1-x_{n,i-1}) + r_0x_{n,i+1}(1-x_{n,i+1})], \end{aligned} \tag{5}$$

$$\begin{aligned} x'_{n+1,i} &= (1-\varepsilon')f(x_{n,i}) + \frac{\varepsilon'}{2}[f(x_{n,i-1}) + f(x_{n,i+1})] \\ &= (1-\varepsilon')r'x_{n,i}(1-x_{n,i}) + \frac{\varepsilon'}{2}[r'x_{n,i-1}(1-x_{n,i-1}) + r'x_{n,i+1}(1-x_{n,i+1})] \\ &= (1-\varepsilon_0)r_0x_{n,i}(1-x_{n,i}) + \frac{\varepsilon_0}{2}[r_0x_{n,i-1}(1-x_{n,i-1}) + r_0x_{n,i+1}(1-x_{n,i+1})] + \Delta x_{n+1,i}, \end{aligned} \tag{6}$$

where $\Delta x_{n+1,i}$ is the difference between $x_{n+1,i}$ and $x'_{n+1,i}$. $\Delta x_{n+1,i}$ reads

$$\begin{aligned} \Delta x_{n+1,i} &= [-r_0\Delta\varepsilon + (1-\varepsilon_0)\Delta r - \Delta r\Delta\varepsilon]\, x_{n,i}(1-x_{n,i}) \\ &\quad + \frac{1}{2}(r_0\Delta\varepsilon + \varepsilon_0\Delta r - \Delta r\Delta\varepsilon)x_{n,i-1}(1-x_{n,i-1}) \\ &\quad + \frac{1}{2}(r_0\Delta\varepsilon + \varepsilon_0\Delta r - \Delta r\Delta\varepsilon)x_{n,i+1}(1-x_{n,i+1}), \end{aligned} \tag{7}$$

$|\Delta x_{n+1,i}|$ can be presented as a binary sequence, $|\Delta x_{n+1,i}| = 0.b_{n+1,i,1}b_{n+1,i,2\ldots}\, b_{n+1,i,m} \ldots b_{n+1,i,p}$. According the digitization Method 2, we define the output difference of the i-th pseudorandom-bit generator, $\Delta s_{n+1,i}$

$$\Delta s_{n+1,i} = b_{n+1,i,m},\ 1 \le m \le p. \tag{8}$$

Without loss of universality, we fix $m = 26$ in Eq. (8) (This is a given example in Ref. [15]), and analyse Eq. (7). Suppose $\Delta\varepsilon = 0$ and keep $\Delta r \le 2^{-24}$. We know $r_{0\max} = 2^2$, $\varepsilon_{0\max} = 1$, $\varepsilon_{\min} = 0$, and the maximum product of $x(1-x)$ is 2^{-2}, therefore, $|\Delta x_{n+1,i}|$ must be smaller than 2^{-26}. Then we have $\Delta s_{n+1,i} = b_{n+1,i,26} = 0$. The above analyses show that only 25 higher significant bits of the parameter r

are able to affect the 26-th binary output of $x_{n+1,i}$ (the parameter r can only be chosen between 3.57 and 4 for chaotic outputs). We numerically compute Eq. (7) with $\varepsilon_0 = 0.6$, $r_0 = 3.998765432$ throughout the paper, and calculate the average values of $\Delta s_{n+1,i}$,

$$p(\Delta s_{n+1,i}) = \frac{1}{T}\sum_{j=1}^{T} \Delta s_{n+1,i},\ i = 1, 2, \ldots, L. \quad (9)$$

Figure 1(a) shows the curve of the average value of $\Delta s_{n+1,i}$ vs. the parameter difference Δr with $T = 10^4$. Initial conditions of the system $x_{0,i}$ are randomly chosen, $x_{0,i} \in [0, 1]$, $i = 1, 2, \ldots, L$. The circles and dots in Fig. 1(a) correspond to the 1-st and 10-th lattice sites, respectively. In Fig. 1(a) we can observe that $p(\Delta s_{n+1,i})$ is zero with $\Delta r \leq 2^{-24}$, and near to 0.5 with $\Delta r > 2^{-24}$, and the simulation coincides with the above analytical results.

Fixing $\Delta r = 0$ and keeping $\Delta\varepsilon \leq 2^{-26}$, we analyse Eq. (7), and find $\Delta s_{n+1,i} = b_{n+1,i,26} = 0$. For the variable of the coupling coefficient ε, only 27 high significant bits can affect the output of the PRBG. In Fig. 1(b) we plot $p(\Delta s_{n+1,i})$ vs. $\Delta\varepsilon$ and we can see that $p(\Delta s_{n+1,i})$ is zero with $\Delta\varepsilon \leq 2^{-26}$ and near to 0.5 with $\Delta\varepsilon > 2^{-20}$.

In Figs. 1(c) and 1(d) we plot $p(\Delta s_{n+1,i})$ vs. $\Delta\varepsilon$ and Δr (1(c) and 1(d) for the 1-st and 10-th sites, respectively) and find that $p(\Delta s_{n+1,i})$ is zero with $\Delta r \leq 2^{-24}$ and 0.5 with $\Delta r > 2^{-24}$ and $\Delta\varepsilon > 2^{-20}$. Through the above analyses and numerical simulations, the secure key space of the digitization Method 2 is around $2^{m-1}2^{m-5} = 2^{2m-6}$, which depends on the digitizing bit site of output. While choosing $m = 10$, the effective key space is around 2^{14}, which is much smaller than the variable space 2^{108}.

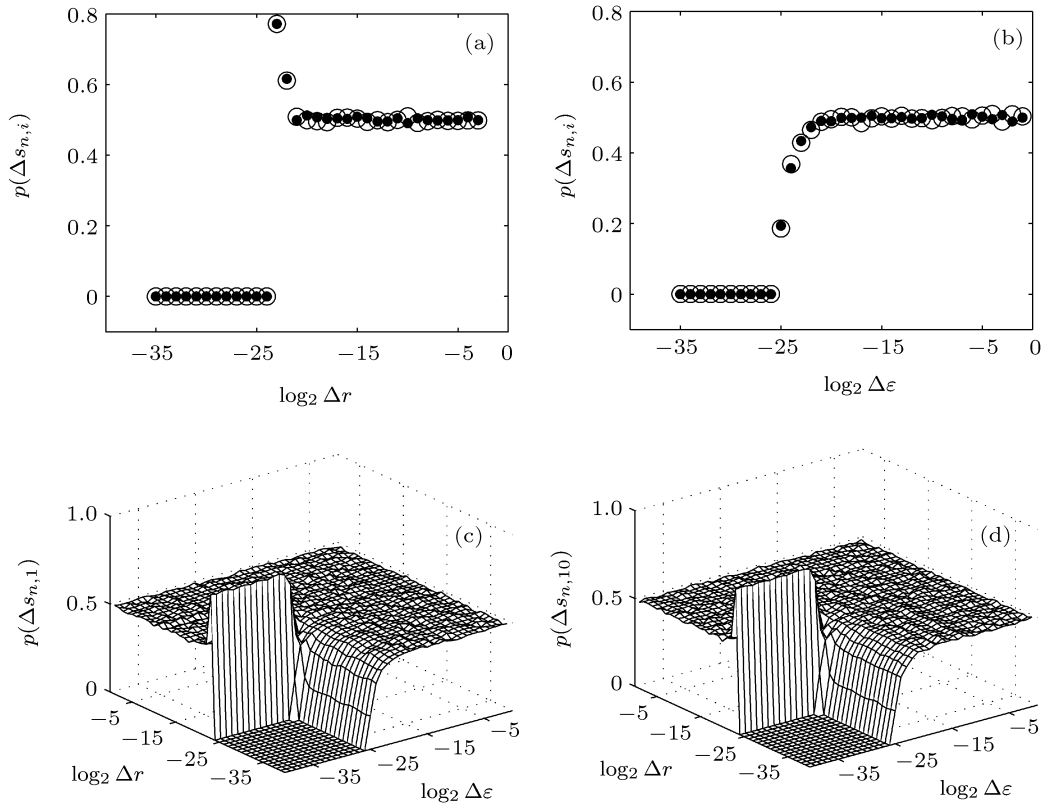


Fig. 1. $p(\Delta s_{n+1,i})$ defined in Eqs. (8) and (9). $T = 10^4$, $\varepsilon_0 = 0.6$, $r_0 = 3.998765432$, $m = 26$. (a) $p(\Delta s_{n+1,i})$ vs. Δr with $\Delta\varepsilon = 0$. We can observe that $p(\Delta s_{n+1,i})$ is zero with $\Delta r \leq 2^{-24}$, and near to 0.5 with $\Delta r > 2^{-24}$. (b) $p(\Delta s_{n+1,i})$ vs. $\Delta\varepsilon$ with $\Delta r = 0$. $p(\Delta s_{n+1,i})$ is zero with $\Delta\varepsilon \leq 2^{-26}$, and near to 0.5 with $\Delta\varepsilon > 2^{-20}$. The circles and dots stand for the 1-st and 10-th lattice sites, respectively in figures (a) and (b). Figures (c) and (d) are $p(\Delta s_{n+1,i})$ plotted in the Δr–$\Delta\varepsilon$ plan, and stand for the 1-st and 10-th lattice sites, respectively.

3.2. The EFA on the digitization Method 3

Considering both the above analyses and the digitization Method 3 of Eq. (4), we numerically calculate the output differences with $m_1 = 20$, $m_2 = 26$ in Eq. (4). According the digitization Method 3, the output

difference of the i-th site is given as

$$\Delta s_{n+1,i} = b_{n+1,i,20} \oplus b_{n+1,i,21} \oplus \cdots b_{n+1,i,26}. \tag{10}$$

In Fig. 2 we do the same as in Fig. 1. We can find that $p(\Delta s_{n+1,i})$ is near to 0.5 with $\Delta r > 2^{-24}$ and $\Delta\varepsilon = 0$ in Fig. 2(a), and equal to zero with $\Delta\varepsilon \leq 2^{-26}$ and $\Delta r = 0$ in Fig. 2(b), and zero with $\Delta r \leq 2^{-24}$ and $\Delta\varepsilon \leq 2^{-26}$ in Figs. 2(c) and 2(d). Through the above results the estimation of the actual key space is about $r \cdot \varepsilon \approx 2^{m_2-1}2^{m_2+1} = 2^{2m_2}$, with $m_1 = 20$ and $m_2 = 26$. Utilizing the digitizing method with $m_1 = 1$ and $m_2 = p$, the effective key space is about 2^{2p}, that directly depends on the precision of computer realizations. Comparing with the digitization Method 2, the efficiency of the PRBG by the digitization Method 3 slows down a little.

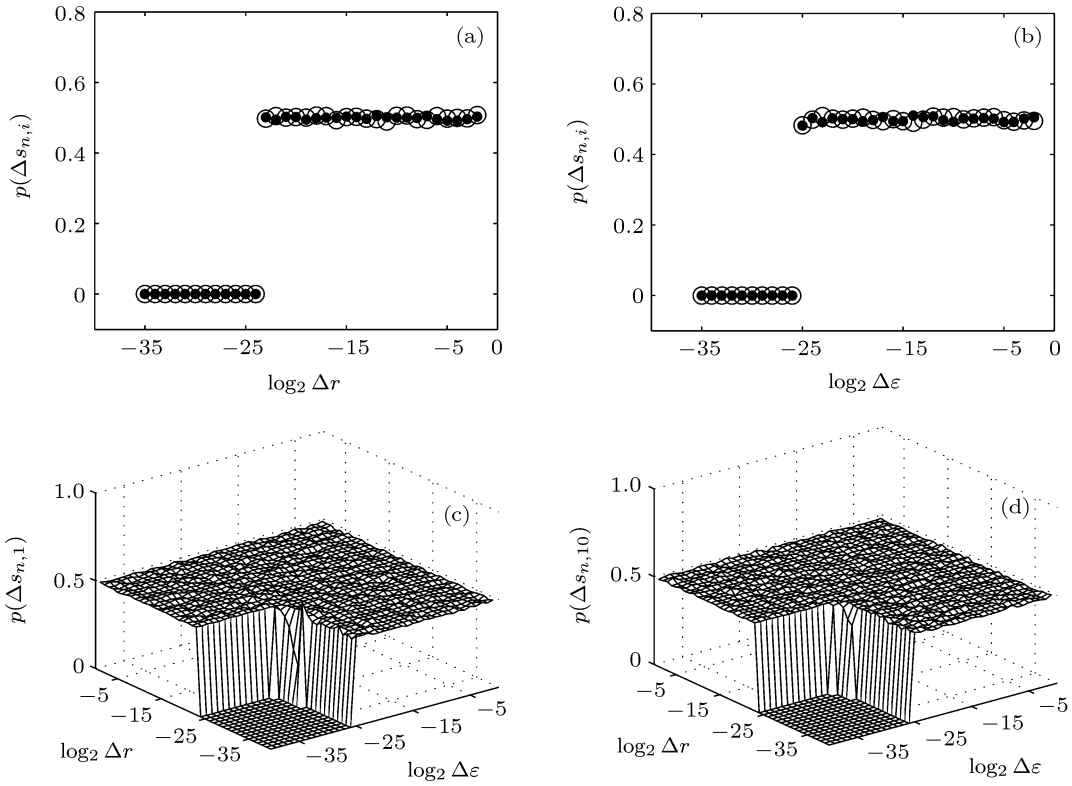


Fig. 2. $p(\Delta s_{n+1,i})$ defined in Eqs. (9) and (10) with $m_1 = 20$, $m_2 = 26$ in Eq. (4). Figures 2(a)–2(d) are the same as those in Figs. 1(a)–1(d), respectively.

3.3. The EFA on the digitization Method 1

For the digitization Method 1, without losing its universality, a threshold value is fixed at $c = 0.5$ in Eq. (2). Directly digitize the outputs $x_{n+1,i}$ and $x'_{n+1,i}$ to $s_{n+1,i}$ and $s'_{n+1,i}$, and calculate the average value of the output differences

$$p(\Delta s_{n+1,i}) = \frac{1}{T}\sum_{j=1}^{T}(s_{n+1,i} \oplus s'_{n+1,i}),\ i = 1, 2, \ldots, L. \tag{11}$$

Figure 3 shows the numerical results of Eq. (11). Figures 3(a)–3(d) are the same as those in Figs. 1(a)–1(d), respectively. In Fig. 3 we can observe that the average values of the output differences have bad statistical property, and the maximum average value is much smaller than 0.5 while the key variables, $\Delta r \to 1$ and $\Delta\varepsilon \to 1$. For the parameter variables $\Delta r \leq 2^{-10}$ and $\Delta\varepsilon \leq 2^{-10}$, $p(\Delta s_{n+1,i}) \equiv 0$. Therefore the effective key space is near 2^{20}. In the key space such as 2^{20}, we can trace the minimal value of $p(\Delta s_{n+1,i})$ to find the secret key with the cost much less than 2^{20}.[5,13]

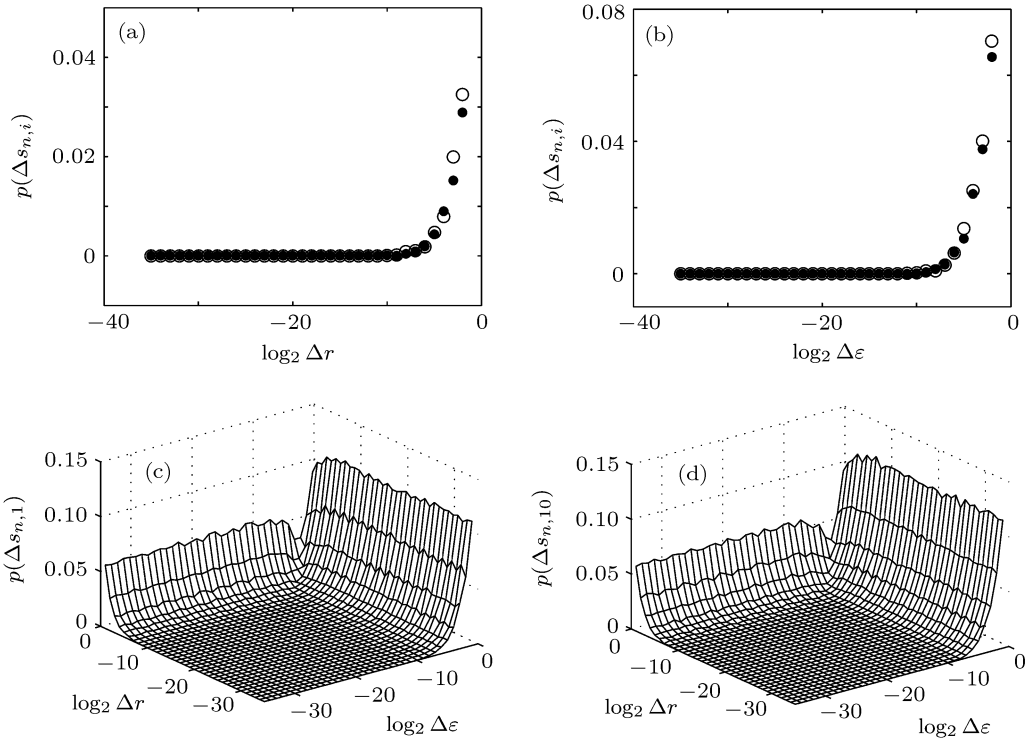


Fig. 3. Figures 3(a)–3(d) are the same as those in Figs. 1(a)–1(d), respectively. $p(\Delta s_{n+1,i})$ defined in Eq. (11) with the threshold value $c = 0.5$.

4. An improved MPRBG

To enhance the security of above CML–MPRBG, we suggest an improved MPRBG which is based on an asymmetrical CML. The improved MPRBG has 128-bit-long key k_i, $k_i \in [0, 2^{32} - 1]$, $i = 1, 2, 3, 4$.

4.1. Model of the improved MPRBG

The biased CML of the improved MPRBG reads

$$x_{n+1,i} = (1 - \varepsilon_1 - \varepsilon_2) f(x_{n,i}) + \varepsilon_1 f(x_{n,i-1}) + \varepsilon_2 f(x_{n,i+1}), \quad i = 1, 2, \ldots, L \tag{12}$$

with the subscript n and i being the iteration and the lattice site indexes. Periodic boundary conditions are used. ε_1 and ε_2 are coupling constants and $f(x)$ is logistic map, $f(x) = (3.75 + r)x(1 - x)$, $r \in [0, 0.25]$. For odd and even site lattices, the local maps are with different parameters r_1 and r_2, respectively. All parameters of CML are generated from the secret keys of MPRBG, and calculated as

$$r_1 = \frac{k_1}{2^{34}}, \quad r_2 = \frac{k_2}{2^{34}}, \quad r_1, r_2 \in [0, 0.25], \tag{13}$$

$$\varepsilon_1 = 0.25 + \frac{k_3}{2^{34}},$$

$$\varepsilon_2 = 0.25 + \frac{k_4}{2^{34}}, \quad \varepsilon_1, \varepsilon_2 \in [0.25, 0.50]. \tag{14}$$

For the improved MPRBG, pseudorandom-bit signals are generated when the iteration numbers are even. Given a chaotic signal of the i-th lattice, $x_{2n,i} = 0.b_{2n,i,1}b_{2n,i,2\ldots}\, b_{2n,i,m} \ldots b_{2n,i,52}$, the digitization method is represented as

$$s_{2n,i} = b_{2n,i,43}b_{2n,i,44} \ldots b_{2n,i,50}, \tag{15}$$

where each lattice is able to put out 8-bit binary number every two iterations.

Our MPRBG has the following novel characteristics:

(i) The improved system utilizes an asymmetric CML (through coupling constants ε_1 and ε_2 in Eqs. (12) and (14)). The asymmetrical coupling structure increases the parameter numbers, and enlarges the space of the secret keys.

(ii) The coupled lattices are divided into two types by the number of lattice sites (corresponding to the different parameters r_1 and r_2). The change of MPRBG also increases the parameter numbers and the key space.

(iii) The system adopts the low significant 8-bit digits of the system variables as output. Compared with the high significant bits of the system variables, these bits are more correlated to the system parameters due to the floating point computation. Therefore,

the sensitivity of the key is largely improved. Meanwhile, an 8-bit-digit maintains the system efficiency.

(iv) To enhance the bit confusion and diffusion rates of CML, our system calculates two iterations to produce one time output. The change guarantees the randomness of binary outputs, and the confusion and diffusion between the secret keys.

(v) To use this model, the initial values of MPRBG should be specified by users, who take the same initial values which are not secret. We suggest to take random real numbers between 0 and 1 as the initial. To weaken the effect of the initial conditions, we suggest that MPRBG begins to generate bit output after it proceeds to iterate some steps.

Due to the above characteristics, the improved system has two advantages over the original one. First, the improved system has stronger security. Through adding the system parameters, generating bit outputs every two iterations, adopting the last 8-bit of the system variables as output, and adding temporal iterations before producing bit output, the space of the secret keys is enlarged and the confusion and diffusion rates of CML are enhanced. The second advantage of the system is its efficiency in producing bits. Although random bits having been generated every two iterations, 8-bit output of each chaotic signal makes the efficiency of the improved system up to four times as before.

4.2. The key sensitivity and the correlation property of output bits

After we revised the MPRBG, the improved system still keeps the good dynamic properties of the CML and cryptographic properties, such as long period, good balance, and large linear complexity of output bits.[15] In this subsection, we will emphatically study the key sensitivity and the correlation of output bits. In the following simulations we fix $L = 64$ in Eq. (12).

4.2.1. The key sensitivity

First we compute two sets of outputs $s_{2n,i}$ and $s'_{2n,i}$ in Eq. (15) through Eqs. (12)–(15) with two different secret keys (k_1, k_2, k_3, k_4) and (k'_1, k'_2, k'_3, k'_4), and an identical initial conditions of the systems, $x'_{0,i} = x_{0,i}$, $i = 1, 2, \ldots, 64$. Then we calculate the difference $\Delta s_{2n,i} = s_{2n,i} \oplus s'_{2n,i}$, and the average of all 8-bit $\Delta s_{2n,i} = \Delta s_{2n,i,1}\Delta s_{2n,i,2} \ldots \Delta s_{2n,i,7}\Delta s_{2n,i,8}$

$$p(\Delta s_{2n,i,j}) = \frac{1}{T}\sum_{n=1}^{T} \Delta s_{2n,i,j},$$
$$j = 1, 2, \ldots, 8,\ i = 1, 2, \ldots, 64. \qquad (16)$$

In Fig. 4(a) we fix $k'_2 = k_2$, $k'_3 = k_3$, $k'_4 = k_4$, and $k_1 = 0$, $k'_1 = 1$ arbitrarily choosing the initial conditions, and plot $p(\Delta s_{2n,i,j})$ for 80 bits from 1-st to 10-th site with $T = 10^6$, $i = 1, 2, \ldots 10$, $j = 1, 2, \ldots, 8$. It is clearly shown that $p(\Delta s_{2n,i,j})$ is near to 0.5 with very small fluctuation. In Fig. 4(b) we plot $|p_{\max}(\Delta s_{2n,i,j}) - 0.5|$ (circles) and $|p_{\min}(\Delta s_{2n,i,j}) - 0.5|$ (dots) against T for 80 bits. In Fig. 4(b) we can see that the fluctuation $|p_{\max,\min}(\Delta s_{2n,i,j}) - 0.5|$ is proportional to $1/\sqrt{T}$. The same behaviour can be observed as well for changing k'_2 and k_2. The excellent key sensitivity (i.e., the sensitivity of the parameters r_1 and r_2) and satisfactory behaviour of random-like are shown in Fig. 4.

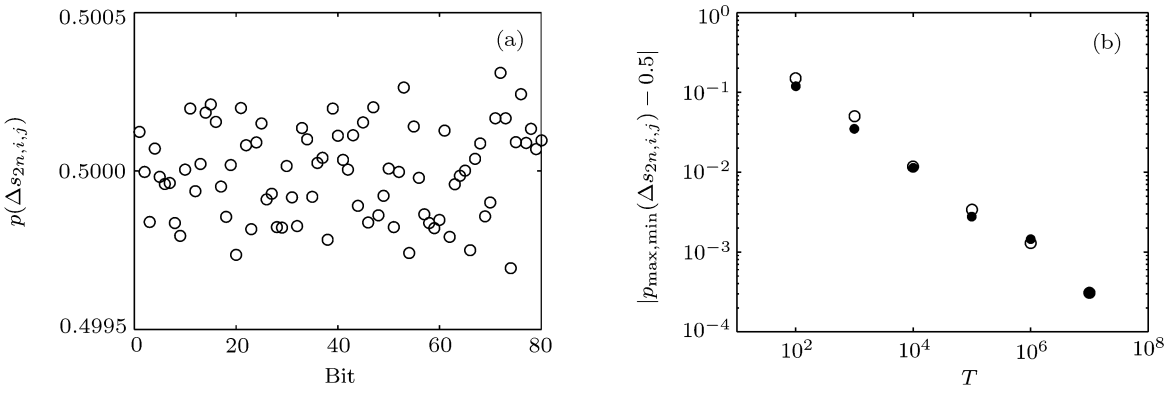


Fig. 4. $k'_2 = k_2$, $k'_3 = k_3$, $k'_4 = k_4$, and $k_1 = 0$, $k'_1 = 1$. Arbitrarily choose the initial conditions $x'_{0,i} = x_{0,i}$. (a) $p(\Delta s_{2n,i,j})$ defined in Eq. (16) for 80 bits from 1-st to 10-th site with $T = 10^6$. (b) $|p_{\max}(\Delta s_{2n,i,j}) - 0.5|$ (circles) and $|p_{\min}(\Delta s_{2n,i,j}) - 0.5|$ (dots) vs. T.

In Figs. 5(a) and 5(b) we do the same as those in Figs. 4(a) and 4(b) with $k'_1 = k_1$, $k'_2 = k_2$, $k'_4 = k_4$, and $k_3 = 0$, $k'_3 = 1$. We can observe the same behaviour as that in Fig. 4. In the above investigations we consider the output from 1-st to 10-th lattices. It is found that the outputs from all other sites have the same properties of key sensitivity and random-like statistics.

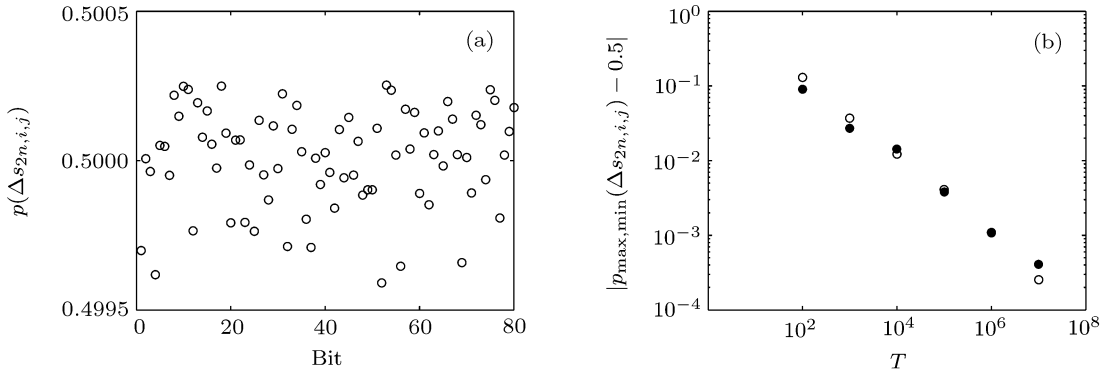


Fig. 5. Figures 5(a) and 5(b) are the same as those in Figs. 4(a) and 4(b) with $k'_1 = k_1$, $k'_2 = k_2$, $k'_4 = k_4$, and $k_3 = 0$, $k'_3 = 1$.

4.2.2. Autocorrelation and cross-correlation

In Fig. 6 we compute the correlations between various sites and various time distances. In Fig. 6(a) the autocorrelation of the 8-bit integer $s_{2n,5}$ from the 5-th site, $c_{55}(\tau)$

$$c_{55}(\tau) = \widehat{c}_{55}(\tau)/\widehat{c}_{55}(0)\,,$$
$$\widehat{c}_{55}(\tau) = \frac{1}{T}\sum_{n=1}^{T}(s_{2n,5} - \overline{s}_{2n,5})(s_{2n+\tau,5} - \overline{s}_{2n,5}) \quad (17)$$

is plotted vs. τ for $T = 10^6$, where $\overline{s}_{2n,5}$ is the average of the $s_{2n,5}$ in T iterations. It is clear that $c_{55}(\tau)$ is equal to 1 for $\tau = 0$, and equal to zero (with small fluctuations) for any nonzero τ. It demonstrates random-like property of the output sequences.

In Fig. 6(b) we plot the cross-correlation function between the two outputs of the two successive sites 4 and 5, $c_{45}(\tau)$

$$c_{45}(\tau) = \frac{\widehat{c}_{45}(\tau)}{\sqrt{\widehat{c}_{44}(0)\widehat{c}_{55}(0)}},$$
$$\widehat{c}_{45}(\tau) = \frac{1}{T}\sum_{n=1}^{T}(s_{2n,4} - \overline{s}_{2n,4})(s_{2n+\tau,5} - \overline{s}_{2n,5})\,. \quad (18)$$

In Fig. 6(b) the circles and the dots correspond to the cross-correlation $c_{45}(\tau)$ from sites 4 and 5, and $c_{56}(\tau)$ from sites 5 and 6, respectively. We find that the cross-correlation is identically approximately equal to zero for all τ detected. That shows a typical behaviour of two completely uncorrelated random sequences from two successive sites.

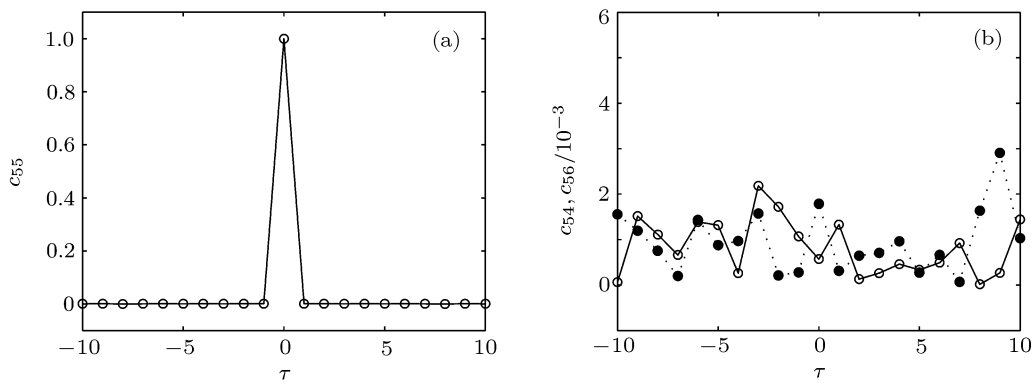


Fig. 6. (a) Autocorrelation function of the output sequence $s_{2n,5}$, $c_{55}(\tau)$ defined in Eq. (17). $T = 10^6$. (b) Cross-correlation function between the two output sequences from the two successive sites, defined in Eq. (18). Circles and dots in the figure correspond to $c_{45}(\tau)$ from sites 4 and 5, and $c_{56}(\tau)$ from sites 5 and 6, respectively.

5. Conclusions

In conclusion we have analysed the PRBG based on CML, incorporating the three digitization methods. Numerical results showed that the CML–MPRBG, incorporating with the digitization Method 1, cannot be used as a secure PRBG, as its secure key can be found easily by attackers. And theoretical analyses and simulations showed that the effective key spaces of CML–MPRBG with the digitization Method 2 and Method 3 depend on the output bit sites of the chaotic signal, and the key spaces are able to reach the largest parameter spaces, 2^{108}, smaller than 2^{128}. To increase effective key space, we suggest increasing the system parameters as the key, i.e., choosing asymmetrical coupling constants (ε_1 and ε_2 in Eq. (12)) and the non-uniform parameter distribution of the local dynamics (r_1 and r_2 in Eq. (13)). Meanwhile, we adopt the low significant 8-bit of the system variables as the output. The numerical and theoretical investigation shows that the improved system has excellent key sensitivity. We estimate its security up to 2^{128} although we have not proved it.

References

[1] Cuomo L M and Oppenheim A V 1993 *Phys. Rev. Lett.* **71** 65
[2] Kocarev L and Parlitz U 1995 *Phys. Rev. Lett.* **74** 5028
[3] Chen G, Mao Y and Chui C K 2003 *Chaos, Solitons and Fractals* **21** 749
[4] Zheng Y F, Chen G and Zhu C Y 2005 *Int. J. Bifurcation and Chaos* **15** 2569
[5] Wang X, Zhan M, Lai C H and Hu G 2004 *Chaos* **14** 128
[6] Wang Y, Liao X, Xiang T, Wong K W and Yang D 2007 *Phys. Lett.* A **363** 277
[7] Wang J, Xu S and Yang S 2008 *Chin. Phys.* B **17** 4027
[8] White J K and Moloney J V 1999 *Phys. Rev.* A **59** 2422
[9] Garcia-Ojalvo J and Roy R 2001 *Phys. Rev. Lett.* **86** 5204
[10] Sundar S and Minai A 2000 *Phys. Rev. Lett.* **85** 5456
[11] Kim C, Rim S and Kye W 2002 *Phys. Rev. Lett.* **88** 014103
[12] Wang S H, Kuang J Y, Li J H, Luo Y L, Lu H P and Hu G 2002 *Phys. Rev.* E **66** 065202
[13] Lu H P, Wang S H, Li X W, Tang G N, Kuang J Y, Ye W P and Hu G 2004 *Chaos* **14** 617
[14] Liu S B, Sun J, Xu Z Q and Liu J S 2009 *Chin. Phys.* B **18** 5219
[15] Li P, Li Z H, Halang W A and Chen G 2006 *Phys. Lett.* A **349** 467