A NOVEL MULTIPLE PSEUDO RANDOM BITS GENERATOR BASED ON SPATIOTEMPORAL CHAOS

Ping Li [*,1] **Zhong Li** [*] **Wolfgang. A. Halang** [*]
Guanrong Chen [**]

[*] *Faculty of Electrical and Computer Engineering, FernUniversität in Hagen, 58084 Hagen, Germany*
[**] *Department of Electronic Engineering, City University of Hong Kong, Kowloon, Hong Kong SAR, P. R. China*

Abstract: An approach of generating multiple pseudo random bits from a single spatiotemporal chaotic system is proposed in this paper. A coupled map lattice is adopted as a prototype of a spatiotemporal chaotic system. The cryptographic properties of the pseudo random bits generator based on the coupled map lattice (CML-MPRBG) are analyzed, and simulation results show that the CML-MPRBG is a good candidate for generating keystreams in cryptography.

Keywords: Spatiotemporal chaos, pseudo random bits generator, coupled map lattice, cryptography

1. INTRODUCTION

Recently, spatiotemporal chaos has been attracting more and more interests from researchers in the fields of mathematics, physics and computer engineering. Much research has been devoted to controlling and synchronizing spatiotemporal chaos using various methods. Especially, synchronization of spatiotemporal chaos has been applied to secure communication (Wang *et al.*, 2002; Tang *et al.*, 2003), where the information are masked and transmitted simultaneously, and as a result, the communication efficiency is greatly enhanced. It motivates the research of applying spatiotemporal chaos to generate multiple Pseudo Random Bit Sequences (PRBSes) at one time, thus to provide a fast Multiple PseudoRandom Bit Generator (MPRBG) with good cryptographic properties for cryptography.

In fact, spatiotemporal chaos has its evident advantages in cryptography. It is well known that any chaotic orbit will eventually be periodic in computer realizations with a finite precision. However, since the period of an chaotic orbit with a sufficiently large number of chaotic coupled oscillators is too long to be reached in the realistic communications, periodicity is practically avoided in spatiotemporal chaotic systems. Moreover, since spatiotemporal chaotic systems have large numbers of positive Lyapunov exponents, bit diffusion and confusion are conducted in multiple directions and high dimensional variable spaces, thus become very strong (Tang *et al.*, 2003).

Most chaos-based pseudo random bit generators are obtained directly by sampling the orbit of a single chaotic system, where the PRBS exposes

[1] Thanks Dr. Shujun. Li at City University of HongKong for the fruitful discussion and for his valuable comments to the paper. Thanks also go to Dr. F.H. Willeboordse at the National University of Singapore for his help in the simulation of the paper.

some information about the chaotic system, consequently, it may be not so appropriate for cryptography. From this point of view, spatiotemporal chaotic systems as high dimensional chaotic systems have potential to be used to generate more secure PRBS. In addition, chaos-based pseudo random bit generators mostly generate only one PRBS, however, a number of PRBSes can be obtained simultaneously from a spatiotemporal chaotic system, which provides a more secure and faster solution for generating keystreams in cryptography. In this paper, an algorithm of generating a multiple pseudo random bits generator based on spatiotemporal chaos is proposed. It possesses very good cryptographic properties, such as long period, balance, large linear complexity, δ-like auto-correlation and close-to-zero cross-correlation, all of which will be analyzed in this paper. Therefore, the MPRBG can generate good keystreams for cryptography.

The rest of the paper is organized as follows. Section 2 describes the construction of the CML-MPRBG. In section 3, cryptographic properties of the CML-MPRBG are analyzed numerically, and the results show the CML-MPRSG is fit to be applied in cryptography. Finally, conclusion is drawn in section 4.

2. CONSTRUCTING A MPRBG BASED ON SPATIOTEMPORAL CHAOS

2.1 A Spatiotemporal Chaotic System

Spatiotemporal chaotic systems are often modeled by partial differential equations (PDE), coupled ordinary differential equations (CODE), or coupled map lattices (CML) (Schuster(ed.), 1999). These systems exhibit chaotic properties both in time and space.

In this paper, CML is adopted as the model of a spatiotemporal chaotic system. There are two main merits of using CML. One is that CML captures the essential of spatiotemporal chaos. Another is that CML can be easily handled both analytically and numerically (Schuster(ed.), 1999).

The spatiotemporal chaos in CML is created by local nonlinear dynamics and spatial diffusion. By adopting various nonlinear mappings for local chaos and various discretized diffusion processes, which are also regarded as coupling, various forms of CML can be obtained. The logistic map as the local map and the nearest-neighbor coupling are popularly used.

A general nearest-neighbor coupling CML can be described as

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

Where $n = 1, 2, ...$ is the time index, $i = 1, 2, ...L$ is the lattice site index with a periodic boundary condition, f is a local chaotic map in the interval I and $\epsilon \in [0, 1]$ is a coupling constant. Here, the logistic map is taken as the local map, that is,

$$f(x) = rx(1-x), \quad (2)$$

where $r \in (0, 4]$ is a constant.

2.2 Construction of the MPRBG via Digitization

A PRBS is generated by digitizing the chaotic output of a lattice site of the CML. Define the chaotic orbit generated from ith lattice site as $\{x_{n,i}\}$. By digitizing $\{x_{n,i}\}$, a PRBS, $S_i = \{s_{n,i}, n = 1, 2, ..., \}$, can be generated. Varieties of digitization methods have been proposed. One of them has been proposed in literature and is applied in the paper.

$x_{n,i}$ can be represented as a binary sequence $x_{n,i} = (0.b_{n,i,1}, b_{n,i,2}, ..., b_{n,i,P})$, P stands for a certain precision. Therefore, $\{b_{1,i,m}, b_{2,i,m}, ...b_{n,i,m} ...\}$, $1 \leq m \leq P$, consist a PRBS. In this method, P chaotic binary sequences can be derived (Sang *et al.*, 1998; Argenti *et al.*, 2000; Pareek *et al.*, 2003; Kocarev and Jakimoski, 2003).

Based on the digitization method, a PRBS can be generated from the output of a lattice site of the CML. By simultaneously obtaining L PRBSes from the outputs of L lattice sites, a MPRBG can be constructed based on the CML.

3. PROPERTIES OF THE MPRBG

To get cryptographically good PRBS, the CML must satisfy the following requirements from chaos theory and cryptographic points of view, respectively.

3.1 Chaotic Properties

- Positive Leading Lyapunov exponent

  To get chaotic outputs of CML, the largest Lyapunov exponent of CML must be positive. The ith Lyapunov exponent is defined as,

  $$\lambda_i = \lim_{n\to\infty} \frac{1}{n} \ln[i\text{th eigenvalue of} J_{n-1}J_{n-2}...J_0], \quad (3)$$

  where J_n is the Jacobian matrix at time n. The (i, j)th element of J_n is $J_n(i, j)$, which is obtained as,

  $$(J_n)_{i,j} = \frac{\partial x_{n+1,i}}{\partial x_{n,j}}, \quad (4)$$

The nth Jacobian matrix of (1) is derived as,

$$\begin{aligned} J_n(i,j) = & f'(x_{n,j})((1-\epsilon)\delta_{i,j} + \frac{\epsilon}{2}(\delta_{i,j-1} + \\ & \delta_{i,1}\delta_{j,L} + \delta_{i,j+1} + \delta_{i,L}\delta_{j,1})), \\ \delta_{i,j} = & \begin{cases} 1, \ if & i = j \\ 0, \ if & i \neq j \end{cases} \\ i,j = & 1,2,...,L. \end{aligned} \quad (5)$$

For the CML (1), the parameters of CML such as r, ϵ and the dimension of system, L, should be selected within certain ranges where the largest Lyapunov exponent of the CML is positive. In terms of (3), (5)and (1), we calculate the largest Lyapunov exponent of the CML with regard to varieties of r, ϵ and L, respectively, as shown in Fig. 1. As we can see, CML operates chaotically with $r = 4$, $\epsilon = 0.9$, $L = 64$.

- Ergodicity

  As a chaotic system, the CML can exhibit ergodicity. The ergodic property of chaotic maps is closely related to the property of diffusion in encryption algorithms.

  A chaotic system is called ergodic if the time average of a typical orbit are the same as the state space average, which is weighted by the probability that a trajectory visits a particular portion of the state space (Hilborn, 2000). The Frobenius-Perron (FP) operator P associated with iterated sequence $\{x_n\}$ can be used as a criterion for judging ergodicity, that is to say, if there is a stationary probability density function $\rho^*(x)$ of P and $\rho^*(x) > 0$, then $\{x_n\}$ is ergodic in I (Lasota and Mackey, 1997). Since a PRBS is derived from a site of the CML, we concern the probability density function of a single site, $\rho(x)$, which can be measured based on the probability density function of L-dimensional CML, $\rho(\vec{x})$. With the notation $\vec{x}_n = (x_{n,1}, ..., x_{n,L})$ and $f(\vec{x}_n) = (f(x_{n,1}), ..., f(x_{n,L}))$, a compact form of the CML (1) reads,

$$\begin{aligned} & \vec{x}_n = \mathbf{A}f(\vec{x}_n), \\ & \mathbf{A}_{ij} = (1-\epsilon)\delta_{i,j} + \frac{\epsilon}{2}(\delta_{i,j-1} + \delta_{i,1}\delta_{j,L} \\ & \quad + \delta_{i,j+1} + \delta_{i,L}\delta_{j,1}) \end{aligned} \quad (6)$$

The Frobenius-Perron operator for the N-dimensional probability density ρ is defined as,

$$P\rho(\vec{x}) = \frac{1}{\det\mathbf{A}} \sum_{\vec{y}} \frac{1}{\prod_i |f'(y_i)|} \rho(\vec{y}) \quad (7)$$

where $\vec{y}$ is the solution given by (Kaneko(ed.), 1993),

$$y_i = f^{-1}(\sum_j A_{ij}^{-1} x_i) \quad (8)$$

In terms of (7), the probability density of a single site can be self-consistently derived as (Kaneko, 1989):

$$\begin{aligned} & P^{SPF}\rho(x) \\ & = (1-\epsilon)^{-1} \int\int_{y_1} \frac{\rho(y_1)\rho(y_0)\rho(y_2)}{|f'(y_1)|} dy_0 dy_2, \end{aligned} \quad (9)$$

where $y_1 \in f^{-1}([0, \hat{x}])$, $\hat{x} = x - \frac{\epsilon(y_0+y_2)}{2(1-\epsilon)}$, $f^{-1}([0,x]) = [0, \frac{1}{2} - \frac{1}{2}\sqrt{1-x}] \cup [\frac{1}{2} + \frac{1}{2}\sqrt{1-x}, 1]$. In general, probability distribution can only be solved numerically based on (9). In Fig. 2, numerical results show that r has influence on distribution, while neither ϵ nor L have significant influence. The bigger r is, the closer to a stationary one the probability density is. Therefore, r should be chosen as 4.

3.2 Cryptographic Properties

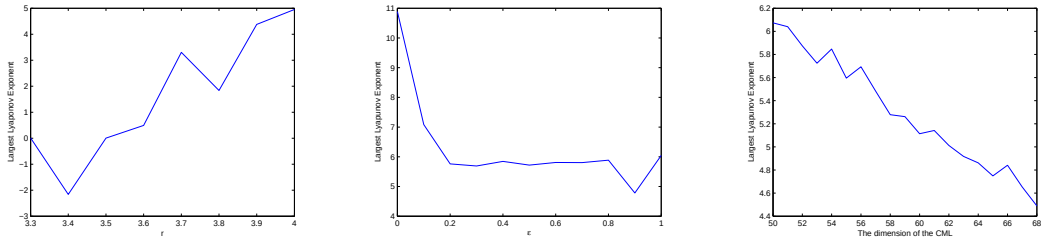
To generate secure keystreams, the CML-MPRBG should have good cryptographic properties (Sang *et al.*, 1998; Li, 2003).

- Long period

  Since chaotic maps are realized in computer with a finite precision, the short period problem of chaotic orbits is inevitable. However, the period of CML with L lattices is about $10^{-0.4L}2^{52\times 0.47L} \approx 10^{7L}$ (Wang *et al.*, n.d.), and the period of PRBS generated from CML-MPRBG is about 10^{7L}, Therefore, when $L > 5$, the period of CML-MPRBG satisfies the requirement of cryptography since a length of order $O(2^{100})$ is cryptographically long.
- Balance

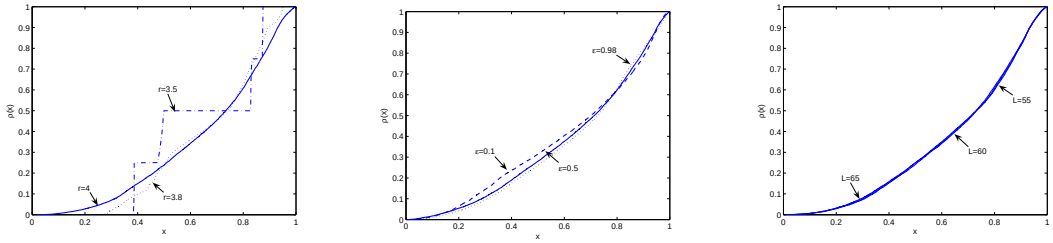
  Since $S_N = \{s_1, s_2, ...s_i, ..., s_N\}$, where N stands for iteration times, generated from the CML-MPRBG, is a binary sequence, uniform distribution function, namely balance, of S_N means $P(s_i = 0) = P(s_i = 1)$, in other words, the ratio between the number of $\{s_i = 0\}$ and that of $\{s_i = 1\}$ equals to 1.
- Large linear complexity

  Let L_n denote the linear complexity of S_N, the sequence $\{L_n, n = 1, 2, ...N\}$ is called the linear complexity profile of S_N, which can be computed using the Berlekamp-Massey algorithm and be graphed by plotting the points (n, L_n) in the $n \times L$ plane and joining the successive points by a horizontal line followed by a vertical line, if necessary. The expected linear complexity of a random sequence should close to $L = N/2$ (Menezes *et al.*, 1997).
- Close-to-zero cross-correlation



(a) $r(\epsilon = 0.9,\ L = 64)$ (b) $\epsilon(r = 4,\ L = 64)$ (c) $L(r = 4,\ \epsilon = 0.9)$

Fig. 1. Largest Lyapunov exponents



(a) r (b) ϵ (c) L

Fig. 2. Distribution

PRBSes can be generated simultaneously from CML-MPRBG. If being independent of each other with zero-value cross-correlation, they can be used to encrypt many plaintexts at one time. The cross-correlation function between two PRBSes is defined as a normalized cross-covariance function (Xiao *et al.*, 1996):

$$\begin{aligned} &C_{ij}(\tau) = \hat{C}_{ij}(\tau)/\sqrt{\hat{C}_{ii}(0)\hat{C}_{jj}(0)}, \\ &\hat{C}_{ij}(\tau) = \frac{1}{N}\sum_{n=1}^{N-|\tau|}(b_{n,i} - b_{A,i})(b_{n+|\tau|,j} - b_{A,j}), \\ &|\tau| = 1, ..., 2N-1, \end{aligned} \tag{10}$$

where C_{ij} stands for the cross-covariance between the ith PRBS and the jth PRBS, $b_{n,i}$ is the nth bit of the ith PRBS, and $b_{A,i}$ is the average value of $b_{n,i}$.

- δ-like auto-correlation

  The autocorrelation of S_N measures the amount of similarity between the sequences S_N and a shift of S_N by t positions. δ-like auto-correlation is required for a good PRBS. The definition of auto-correlation is a special case of cross-correlation with the form as:

$$\begin{aligned} &C_{ii}(\tau) = \hat{C}_{ii}(\tau)/\hat{C}_{ii}(0), \\ &\hat{C}_{ii}(\tau) = \frac{1}{N}\sum_{n=1}^{N-|\tau|}(b_{n,i} - b_{A,i})(b_{n+|\tau|,i} - b_{A,i}), \\ &|\tau| = 1, ..., 2N-1, \end{aligned} \tag{11}$$

Using the digitization method described in section 2.2 can obtain a MPRBG. Its cryptographic properties are shown in Fig. 3. Here, one of 64 PRBSes is randomly chosen for testing its distribution, linear complexity and auto-correlation. Additionally, two of 64 PRBSes are randomly chosen for testing their cross-correlation.

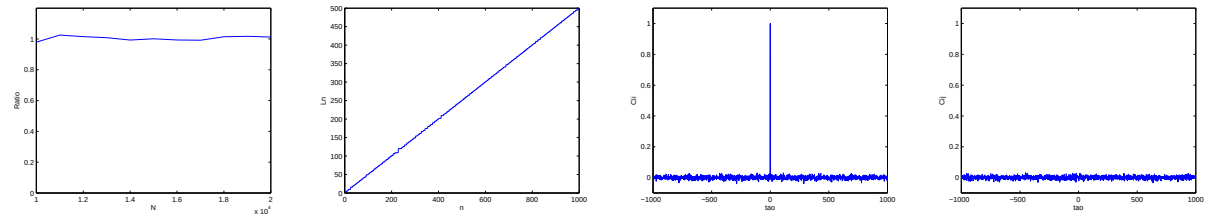
As we can see, the PRBS is almost balance, the linear complexity of the PRBS is about $N/2$, the auto-correlation of the PRBS is δ-like, and the cross-correlation of the PRBS is close to zero. Therefore, CML-MPRBG has good cryptographic properties.

4. CONCLUSION

A novel pseudo random bits generator based on spatiotemporal chaos has been presented in this paper. By constructing an appropriate coupled map lattice system, multiple chaotic numbers can be simultaneously obtained from lattices of the CML. With a suitable digitization method, many PRBSes are derived at one time. Numerical results have shown that the CML-MPRBG has perfect cryptographic properties. Moreover, multiple PRBSes can be used to encrypt many plaintexts at one time or to serve as keys in block ciphers. In a word, regarding the CML-MPRBG as the keystream generator in a cipher, the security and speed of encryption can be considerably improved. The application of the CML-MPRBG in cryptography and its security analysis will be carried out further.

REFERENCES

Argenti, F., S. Benzi, E.D. Re and R. Genesio (2000). Stream cipher system based on



(a) 0:1 Ratio (b) Linear Complexity (c) Auto-correlation (d) Cross-Correlation

Fig. 3. Cryptographic Properties of PRBG

chaotic maps. In: *Proceeding of Mathematics and Applications of Data/Image Coding, Compression, and Encryption III*. Vol. 4122. SPIE. pp. 10–17.

Hilborn, R.C. (2000). *Chaos and Nonlinear Dynamics*. Chap. 9, p. 334. Second ed.. OXFORD University Press.

Kaneko, K. (1989). Towards thermodynamics of spatiotemporal chaos. *Prog. Theor. Phys.* **supplement**, 263–287.

Kaneko(ed.), K. (1993). *Theory and Application of Coupled Map Lattices*. Chap. 3, p. 100. John Wiley and Sons.

Kocarev, L. and G. Jakimoski (2003). Pseudorandom bits generated by chaotic maps. *IEEE Trans. Circuits and Syst-I* **50**, 123–126.

Lasota, A. and M.C. Mackey (1997). *Chaos, Fractals, and Noise: stochastic aspects of dynamics*. Chap. 4, p. 61. Second ed.. Spinger-Verlag.

Li, S. (2003). Analyses and New Designs of Digital Chaotic Ciphers. Ph.D. thesis. School of Electronics and Information Engineering, Xi'an Jiaotong University. Xi'an, China.

Menezes, A., P.V. Oorschot and S. Vanstone (1997). *Handbook of Applied Cryptography*. Chap. 6, p. 199. CRC Press.

Pareek, N.K., V. Patidar and K.K. Sud (2003). Discrete chaotic cryptography using external key. *Physics Letters A* **309**, 75–82.

Sang, T., R. Wang and Y. Yan (1998). Perturbance-based algorithm to expand cycle length of chaotic key stream. *Electronics Letters* **34**, 873–874.

Schuster(ed.), H.G. (1999). *Handbook of Chaos Control*. Chap. 3. WILEY-VCH.

Tang, G., S. Wang, H. L and G. Hu (2003). Chaos-based cryptograph incorporated with s-box algebraic operation. *Physics Letters A* **318**, 388–398.

Wang, S., J. Kuang, J. Li, Y. Luo, H. L and G. Hu (2002). Chaos-based secure communications in a large community. *Physical Review E* **66**, 065202.

Wang, S., W Liu, H. Lu, J. Kuang and G. Hu (n.d.). Periodicity of chaotic trajectories in realizations of finite computer precisions and its implication in chaos communications. *arXiv:nlin.CD/0309005 v2 20 Feb 2004*.

Xiao, J., G. Hu and Z Qu (1996). Synchronization of spatiotemporal chaos and its application to multichannel spread spectrum communication.. *Phys. Rev. Lett.* **77**, 4162–4165.