Available online at www.sciencedirect.com
SCIENCE DIRECT
Physics Letters A 349 (2006) 467–473
PHYSICS LETTERS A
www.elsevier.com/locate/pla

A multiple pseudorandom-bit generator based on a spatiotemporal chaotic map

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

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

Received 21 October 2004; received in revised form 22 September 2005; accepted 23 September 2005

Available online 4 October 2005

Communicated by A.R. Bishop

Abstract

An approach to generate multiple pseudorandom-bit sequences from a single spatiotemporal chaotic system is proposed in this Letter. A coupled map lattice is adopted as a prototype of a spatiotemporal chaotic system. The cryptographic properties of the pseudorandom-bit generator based on the coupled map lattice (CML–MPRBG) are analyzed. It is observed from simulation results that the CML–MPRBG has good cryptographic properties. Basic security analysis of a stream cipher based on the CML–MPRBG is also discussed. The results show that the CML–MPRBG can be a good candidate for constructing a secure cipher.

Keywords: Spatiotemporal chaos; Pseudorandom-bit 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 communications [1–3], where the information is masked and transmitted simultaneously, and as a result, the communication efficiency is greatly enhanced. This motivates the research of applying spatiotemporal chaos to generate multiple pseudorandom-bit sequences (PRBSs) at one time, thus to provide a fast multiple pseudorandom-bit generator (MPRBG) with good cryptographic properties for encryption.

In fact, spatiotemporal chaos has its evident advantages in cryptography. It is well known that any chaotic orbit will eventually become periodic in computer realizations with a finite precision. However, since the period of a chaotic orbit with a sufficiently large number of chaotic coupled oscillators is too long to be reached in real 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 of high-dimensional variable spaces, therefore ciphers based on spatiotemporal chaos can be made very strong [2].

Most chaos-based pseudorandom-bit generators are obtained directly by sampling the orbit of a single continuous chaotic system, where the PRBS exposes some information about the chaotic system; consequently, it becomes not so appropriate for encryption. 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 pseudorandom-bit generators mostly generate only one PRBS. On the contrary, a number of PRBSs can be obtained simultaneously from a spatiotemporal chaotic system, which provides a more secure and faster solution for generating keystreams in cryptosystems. In this Letter, an algorithm for a multiple pseudorandom-bit generator based on couple map lattice

* Corresponding author. Tel.: +49 2331 987 1732; fax: +49 2331 987 375.
E-mail address: ping.li@fernuni-hagen.de (P. Li).

0375-9601/$ – see front matter
doi:10.1016/j.physleta.2005.09.060

(CML–MPRBG) 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 Letter.

The rest of the Letter is organized as follows. Section 2 describes the construction of the CML–MPRBG. In Section 3, cryptographic properties of the CML–MPRBG are investigated numerically, and the security of a stream cipher based on the CML–MPRBG is analyzed. 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) [4]. These systems exhibit chaotic properties both in time and in space.

In this Letter, CML is adopted as the basic model of a spatiotemporal chaotic system. There are two main merits in using CML: one is that CML captures the essential features of spatiotemporal chaos; another is that CML can be easily handled both analytically and numerically [4].

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

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

where $n = 1, 2, \ldots$ is the time index, $i = 1, 2, \ldots, L$ 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,

$$f(x) = rx(1-x), \tag{2}$$

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

2.2. Construction of the MPRBG via digitization

A PRBS is generated here by digitizing the chaotic output of a lattice site of the CML. Define the chaotic orbit generated from the ith lattice site as $\{x_{n,i}\}$. By digitizing $\{x_{n,i}\}$, a PRBS, $S_i = \{s_{n,i}, n = 1, 2, \ldots\}$, can be generated. Three digitization methods proposed in the literature are applied in the Letter.

Method 1 By dividing the interval visited by the chaotic orbit into m parts and labeling them with definite integers belonging to $[0, m-1]$, a pseudorandom number takes an integer $r \in [0, m-1]$ when $x_{n,i}$ enters the rth subinterval [5–11]. A special case is $m = 2$, that is, the interval $[a, b]$ is divided into two parts $[a, C]$ and $[C, b]$, where $x_{n,i} \in [a, b]$ and C is a threshold. Then, a PRBS is defined as [5,12]

$$s_{n,i} = \begin{cases} 1, & \text{if } x_{n,i} \in [a, C], \\ 0, & \text{if } x_{n,i} \in [C, b]. \end{cases} \tag{3}$$

Method 2 $x_{n,i}$ can be represented as a binary sequence $x_{n,i} = (0.b_{n,i,1}, b_{n,i,2}, \ldots, b_{n,i,P})$, P stands for a certain precision. Therefore, $\{b_{1,i,m}, b_{2,i,m}, \ldots, b_{n,i,m}, \ldots\}$, $1 \leqslant m \leqslant P$, consist a PRBS. In this method, P chaotic binary sequences can be derived [8,13–23]. In the case that the chaotic orbit is ergodic, the PRBS, which is generated by digitizing the original chaotic numbers in this method, has a uniform distribution [15].

Method 3 For $x_{n,i} = (0.b_{n,i,1}, b_{n,i,2}, \ldots, b_{n,i,P})$, a PRBS can be generated as follow:

$$s_{n,i} = b_{n,i,1} \oplus b_{n,i,2} \oplus \cdots \oplus b_{n,i,P}, \tag{4}$$

where $\oplus$ means an exclusive OR operation. The method is similar to that of [23].

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

3. Properties of the MPRBG

To get a cryptographically good PRBS, the CML must satisfy some basic requirements from both chaotic dynamics theory and cryptographic analysis.

3.1. Some good dynamic properties of the CML

Since the CML is used to generate multiple PRBSs, it should have suitable dynamic properties as follows.

- *Avoiding chaos synchronization*
  All local maps of the CML must avoid being synchronized, otherwise, the PRBSs generated from all the sites will be same. The chaos synchronization of the CML has been investigated by using Lyapunov exponent spectrum [24].
  As we know, the Lyapunov exponent for the logistic map is $\ln(r/2)$, the Lyapunov exponent sectrum for the synchronous chaos of Eq. (1) are derived as [24]

$$\begin{aligned} &\lambda_1 = \ln(r/2), \\ &\lambda_2 = \lambda_1 + \ln\big[1 - \epsilon + \epsilon \cdot \cos(2\pi/L)\big], \\ &\vdots \\ &\lambda_L = \begin{cases} \lambda_1 + \ln(1-2\epsilon), & \text{if } L \text{ even}, \\ \lambda_1 + \ln[(1-\epsilon-\epsilon \cdot \cos(2\pi/L)], & \text{if } L \text{ odd}. \end{cases} \end{aligned} \tag{5}$$

  To avoid the coupled maps getting into synchronization, λ_2 must be bigger than 0, that is,

$$\lambda_1 + \ln\big[1 - \epsilon + \epsilon \cdot \cos(2\pi/L)\big] > 0, \tag{6}$$