International Journal of Bifurcation and Chaos, Vol. 27, No. 3 (2017) 1750046 (17 pages)
© World Scientific Publishing Company
DOI: 10.1142/S0218127417500468

Int. J. Bifurcation Chaos 2017.27. Downloaded from www.worldscientific.com
by CITY UNIVERSITY OF HONG KONG on 04/09/17. For personal use only.

Discrete Chaotic Systems with One-Line Equilibria and Their Application to Image Encryption

E. Chen* and Lequan Min†
University of Science and Technology Beijing,
Beijing 100083, P. R. China
**chene5546@163.com*
†minlequan@sina.com

Guanrong Chen
Department of Electronic Engineering,
City University of Hong Kong,
Hong Kong SAR, P. R. China
gchen@ee.city.edu.hk

Received December 3, 2016

This paper introduces nine four-dimensional discrete chaotic systems with one-line equilibria (DCSLE), consisting of some simple sine functions. Based on the generalized chaos synchronization (GCS) theorem, a DCSLE is used to construct an eight-dimensional DCSLE GCS system. The new DCSLE GCS system is verified by numerical simulation and then used to design a chaotic pseudorandom number generator (CPRNG). The randomness of ten 100-key streams generated by the CPRNG, two GCS-based CPRNGs, the RC4 PRNG and the ZUC PRNG are tested by the SP800-22/FIPS 140-2 tests. The test results confirm that the randomness performances of the three CPRNGs are promising, for there are no significant correlations between a keystream and any perturbed keystream generated by such CPRNG. Also, the key space of the CPRNG is larger than 2^{1170}. Finally, the CPRNG is used with an avalanche-effect encryption scheme to encrypt an RGB image, demonstrating that the CPRNG is able to generate the avalanche effects which are similar to those generated by ideal CPRNGs.

Keywords: Discrete chaotic map; one-line equilibria; pseudorandom number generator; randomness test; avalanche-effect encryption.

1. Introduction

The complex chaotic dynamical systems generate seemingly random but actually deterministic behaviors, thereby becoming useful in some applications requiring manageable randomness. Chaotic orbits are extremely sensitive to initial conditions and system parameters, very difficult or even impossible to predict in a long duration [Li & Yorke, 1975; Chen & Dong, 1998; Sprott, 2003], because a small difference in the initial conditions will lead to significantly different outcomes after a lengthy evolution of the system dynamics [Zhou *et al.*, 2015]. Typical examples of continuous-time and discrete-time chaotic systems include the Lorenz system [Lorenz, 1995], Chua circuit [Chua, 1994], logistic map [Law *et al.*, 2003] and cat map [Wu *et al.*, 2015], to name just a few.

Recently, some chaotic systems were found to have no equilibrium or have only stable equilibria. This kind of systems were rare [Sprott, 1994;

†Author for correspondence

Int. J. Bifurcation Chaos 2017.27. Downloaded from www.worldscientific.com by CITY UNIVERSITY OF HONG KONG on 04/09/17. For personal use only.

Jafari *et al.*, 2013; Yang *et al.*, 2015]. Likewise, it is unusual to see dynamic systems having one-line equilibria, with or without chaotic behaviors [Fiedler *et al.*, 2000a; Fiedler & Liebscher, 2000; Fiedler *et al.*, 2000b]. For this kind of systems, there are some reports on bifurcation analysis of two-memristor oscillatory models, described by three-dimensional five-parameter piecewise-linear or cubic systems of ordinary differential equations [Messias *et al.*, 2010]. The periodic orbits of these systems arise from changes in local stability of equilibrium points on the line of equilibria, for a fixed set of parameter values. There is also a report on a four-dimensional fractional-order chaotic system with one-line equilibria [Zhou *et al.*, 2013]. Moreover, by exhaustive computer search, nine simple chaotic flows were found to have one-line equilibria [Jafari & Sprott, 2013]. Most, if not all, of the above-mentioned dynamical systems have hidden chaotic attractors [Leonov & Kuznetsov, 2011]. It is expected that such chaotic systems with one-line equilibria are relatively more complicated, and more useful when being applied to cryptography.

Regarding cryptography, a common perception is that if designed appropriately, chaos synchronization may provide some new tools for cryptography (see, e.g. [Zang *et al.*, 2007; Wang *et al.*, 2011; Kanso & Ghebleh, 2012; Liu & Min, 2014; Yang *et al.*, 2015]) and secure communications (see, e.g. [Chen *et al.*, 2003; Alvarez *et al.*, 2004; Wu, 2006; Xia & Cao, 2008; Nana *et al.*, 2009; Sun *et al.*, 2013; Wu *et al.*, 2014]). Since the seminal paper [Pecora & Carroll, 1990], research on chaos-synchronization-based communications has seen rapid developments. Furthermore, (generalized) chaos synchronization has been proved useful in some applications to engineering systems (see, e.g. [Yang *et al.*, 2012; Kili, 2006; Matouk, 2011; Pehlivan *et al.*, 2014; Wang & Liu, 2006]), physical systems (e.g. [Senator, 2006; Ge *et al.*, 2008; Gross *et al.*, 2006; Shahverdiev & Shore, 2009; Li *et al.*, 2014]), biological systems (e.g. [Aguirre *et al.*, 2006; Sausedo-Solorio & Pisarchik, 2014]), and particularly cryptosystems — as will be further elaborated below.

In cryptography studies, moreover, avalanche effect in complex dynamics has been proven effective [Feistel, 1973], which means that a tiny change in the plaintext or the key will cause a drastic change in the ciphertext just like an avalanche. Strict key avalanche criterion requires that each binary bit of the ciphertext should have a change with the probability of one half in reacting to any single bit change of the key [Spillman, 2004]. Based on this technique, we recently presented a multibit segment stream encryption scheme with avalanche effect (SESAE) in [Min & Chen, 2013]. The main feature of SESAE is to ensure that each bit of the decrypted plaintext will be changed to 1 with probability of $(2^d - 1)/2^d$, where d is the bit number in a segment stream.

The FIPS 140-2 test suite issued by the American National Institute of Standards and Technology (NIST) [NIST, 2001] is a US government computer standard used to accredit cryptographic modules. It has been widely used for verifying the statistical properties of the randomness of the pseudorandom numbers generated by e.g. PRNGs. In a previous paper [Min *et al.*, 2013], a randomness test suite for the 2^d word keystream streams was presented based on the FIPS 140-2 randomness test suite. The SP800-22 test suite of NIST [NIST, 2001] is stricter than the FIPS 140-2 test suite. A binary sequence that could pass the tests of FIPS 140-2 test suite may not be able to pass the tests offered by the NIST 800-22 test suite, which will therefore be used in the present study.

The present paper proposes some new four-dimensional discrete chaotic systems with one-line equilibria (DCSLE), consisting of simple sine functions. The complex dynamics of such systems are simulated and analyzed. Then, an eight-dimensional discrete chaotic generalized synchronization system with one-line equilibria will be introduced, and an eight-dimensional DCSLE-based 2^d word CPRNG will be designed.

To that end, the SP800-22 test suite and the FIPS 140-2 test suite will be used to test and compare the randomness of five PRNGs, i.e. the DCSLE-based CPRNG, the RC4 algorithm PRNG, the ZUC algorithm PRNG [ETSI/SAGE Specification, 2011], and the other two CPRNGs developed in [Han *et al.*, 2016; Zhang *et al.*, 2015]. All the results imply that the three CPRNGs have very large key spaces and very significant pseudorandomness.

Finally, the DCSLE-based CPRNG and the SESAE [Min & Chen, 2013] are used to encrypt an RGB image, with computer simulation and numerical analysis, to demonstrate their effectiveness.

The rest of the paper is organized as follows. Section 2 proposes a general parametric form of a

Int. J. Bifurcation Chaos 2017.27. Downloaded from www.worldscientific.com
by CITY UNIVERSITY OF HONG KONG on 04/09/17. For personal use only.

four-dimensional DCSLE and constructs nine maps of this kind. Relevant concepts and the generalized synchronization theorem for discrete systems are introduced in Sec. 3. Section 4 presents an eight-dimensional DCSLE GCS system, and simulates its complex dynamics. Section 5 designs the DCSLE-based CPRNG and performs statistical tests on five PRNGs, respectively. Section 6 illustrates an image encryption example by using the DCSLE-based CPRNG and the SESAE. Finally, Sec. 7 concludes the investigation.

2. Some Discrete Chaotic Maps with One-Line Equilibria

This section presents nine four-dimensional discrete-time systems with one-line equilibria, denoted as DCSLE.

The DCSLEs have a general form as follows:

$$\begin{cases} x_1(k+1) = k_1 \sin(x_i(k)) + p_1 \sin(x_1(k)x_3(k) + x_1(k) + x_2(k)) \\ x_2(k+1) = k_2 \sin(x_j(k)) - \sin(x_l(k)) \\ x_3(k+1) = k_3 \sin(x_v(k)) + p_2 \sin(x_1(k)x_3(k)) \\ x_4(k+1) = k_4 \sin(x_m(k) + x_n(k)) \end{cases} \tag{1}$$

where $i, j, l, v, m, n \in \{1, 2, 4\}$. This form has one-line equilibria:

$$E_q = (0, 0, x_3, 0). \tag{2}$$

To obtain some sufficient conditions for the one-line equilibria to be unstable, the Jacobi matrix of the general form is first evaluated on the line equilibria (2), leading to

$$\mathbf{A}_0 = \begin{pmatrix} k_1 + p_1(x_3+1) & p_1 & 0 & 0 \\ -1 & k_2 & 0 & 0 \\ k_3 + p_2 x_3 & 0 & 0 & 0 \\ 0 & k_4 & 0 & k_4 \end{pmatrix}. \tag{3}$$

The matrix (3) has the following eigenvalues:

$$\begin{cases} \lambda_1 = 0 \\ \lambda_2 = k_4 \\ \lambda_3 = \dfrac{1}{2}[k_1 + k_2 + p_1 x_3 + p_1 + (k_1^2 - 2k_1k_2 + 2k_1p_1x_3 + 2k_1p_1 + k_2^2 - 2k_2p_1x_3 - 2k_2p_1 \\ \qquad + p_1^2x_3^2 + 2p_1^2x_3 + p_1^2 - 4p_1)^{1/2}] \\ \lambda_4 = \dfrac{1}{2}[k_1 + k_2 + p_1 x_3 + p_1 - (k_1^2 - 2k_1k_2 + 2k_1p_1x_3 + 2k_1p_1 + k_2^2 - 2k_2p_1x_3 - 2k_2p_1 \\ \qquad + p_1^2x_3^2 + 2p_1^2x_3 + p_1^2 - 4p_1)^{1/2}] \end{cases} \tag{4}$$

which yields

$$\lambda_3\lambda_4 = k_1k_2 + k_2p_1 + k_2p_1x_3 + p_1.$$

It follows that:

Case 1. If $|k_4| > 1$, then system (1) has unstable line equilibria.

Case 2. If $|\lambda_3\lambda_4| = |k_1k_2 + k_2p_1 + k_2p_1x_3 + p_1| > 1$, then system (1) has unstable line equilibria.

Next, let $k_1 = 1$, $k_2 = 1$, $k_3 = 1$, $k_4 = 2$, $p_1 = \pm 1$, $p_2 = \pm 1$. A total of nine different DCSLEs have unstable line equilibria, as summarized in Table 1. Then, an exhaustive computer search was performed by using different combinations of the variation $x_1 \sim x_4$, with sine functions having plus or minus signs. The Lyapunov exponents (LEs) and the equilibria (Eq) of the nine DCSLEs are listed in the third and fourth columns in Table 1, respectively.

Int. J. Bifurcation Chaos 2017.27. Downloaded from www.worldscientific.com
by CITY UNIVERSITY OF HONG KONG on 04/09/17. For personal use only.

Table 1. Nine simple discrete chaos systems with one-line equilibria.

No.	Equations	LEs	Eq
1	$x_1(k+1) = \sin(x_1(k)) + \sin(x_1(k)x_3(k) + x_1(k) + x_2(k))$	0.2543	0
	$x_2(k+1) = \sin(x_2(k)) - \sin(x_1(k))$	0.1411	0
	$x_3(k+1) = \sin(x_1(k)) + \sin(x_1(k)x_3(k))$	−0.7363	x_3
	$x_4(k+1) = 2\sin(x_2(k) + x_4(k))$	−1.6339	0
2	$x_1(k+1) = \sin(x_1(k)) + \sin(x_1(k)x_3(k) + x_1(k) + x_2(k))$	0.2222	0
	$x_2(k+1) = \sin(x_2(k)) - \sin(x_1(k))$	0.1445	0
	$x_3(k+1) = \sin(x_1(k)) - \sin(x_1(k)x_3(k))$	−0.6082	x_3
	$x_4(k+1) = 2\sin(x_2(k) + x_4(k))$	−1.3837	0
3	$x_1(k+1) = \sin(x_2(k)) + \sin(x_1(k)x_3(k) + x_1(k) + x_2(k))$	0.1962	0
	$x_2(k+1) = \sin(x_2(k)) - \sin(x_1(k))$	−0.1067	0
	$x_3(k+1) = \sin(x_1(k)) + \sin(x_1(k)x_3(k))$	−0.1355	x_3
	$x_4(k+1) = 2\sin(x_2(k) + x_4(k))$	−1.3976	0
4	$x_1(k+1) = \sin(x_4(k)) + \sin(x_1(k)x_3(k) + x_1(k) + x_2(k))$	0.3028	0
	$x_2(k+1) = \sin(x_2(k)) - \sin(x_1(k))$	0.0640	0
	$x_3(k+1) = \sin(x_1(k)) + \sin(x_1(k)x_3(k))$	−0.5668	x_3
	$x_4(k+1) = 2\sin(x_2(k) + x_4(k))$	−1.7692	0
5	$x_1(k+1) = \sin(x_1(k)) + \sin(x_1(k)x_3(k) + x_1(k) + x_2(k))$	0.2077	0
	$x_2(k+1) = \sin(x_2(k)) - \sin(x_4(k))$	0.1348	0
	$x_3(k+1) = \sin(x_1(k)) + \sin(x_1(k)x_3(k))$	−0.3291	x_3
	$x_4(k+1) = 2\sin(x_2(k) + x_4(k))$	−1.4684	0
6	$x_1(k+1) = \sin(x_1(k)) + \sin(x_1(k)x_3(k) + x_1(k) + x_2(k))$	0.3988	0
	$x_2(k+1) = \sin(x_4(k)) - \sin(x_1(k))$	−0.1750	0
	$x_3(k+1) = \sin(x_1(k)) + \sin(x_1(k)x_3(k))$	−1.0761	x_3
	$x_4(k+1) = 2\sin(x_2(k) + x_4(k))$	−1.6881	0
7	$x_1(k+1) = \sin(x_1(k)) + \sin(x_1(k)x_3(k) + x_1(k) + x_2(k))$	0.2912	0
	$x_2(k+1) = \sin(x_2(k)) - \sin(x_1(k))$	0.0824	0
	$x_3(k+1) = \sin(x_4(k)) + \sin(x_1(k)x_3(k))$	−0.5467	x_3
	$x_4(k+1) = 2\sin(x_2(k) + x_4(k))$	−1.3329	0
8	$x_1(k+1) = \sin(x_1(k)) + \sin(x_1(k)x_3(k) + x_1(k) + x_2(k))$	0.2544	0
	$x_2(k+1) = \sin(x_2(k)) - \sin(x_1(k))$	0.1210	0
	$x_3(k+1) = \sin(x_1(k)) + \sin(x_1(k)x_3(k))$	−0.7363	x_3
	$x_4(k+1) = 2\sin(x_1(k) + x_4(k))$	−1.6338	0
9	$x_1(k+1) = \sin(x_1(k)) + \sin(x_1(k)x_3(k) + x_1(k) + x_2(k))$	0.2542	0
	$x_2(k+1) = \sin(x_2(k)) - \sin(x_1(k))$	−0.7618	0
	$x_3(k+1) = \sin(x_1(k)) + \sin(x_1(k)x_3(k))$	−1.6648	x_3
	$x_4(k+1) = 2\sin(x_1(k) + x_2(k))$	−36.5264	0

Int. J. Bifurcation Chaos 2017.27. Downloaded from www.worldscientific.com
by CITY UNIVERSITY OF HONG KONG on 04/09/17. For personal use only.

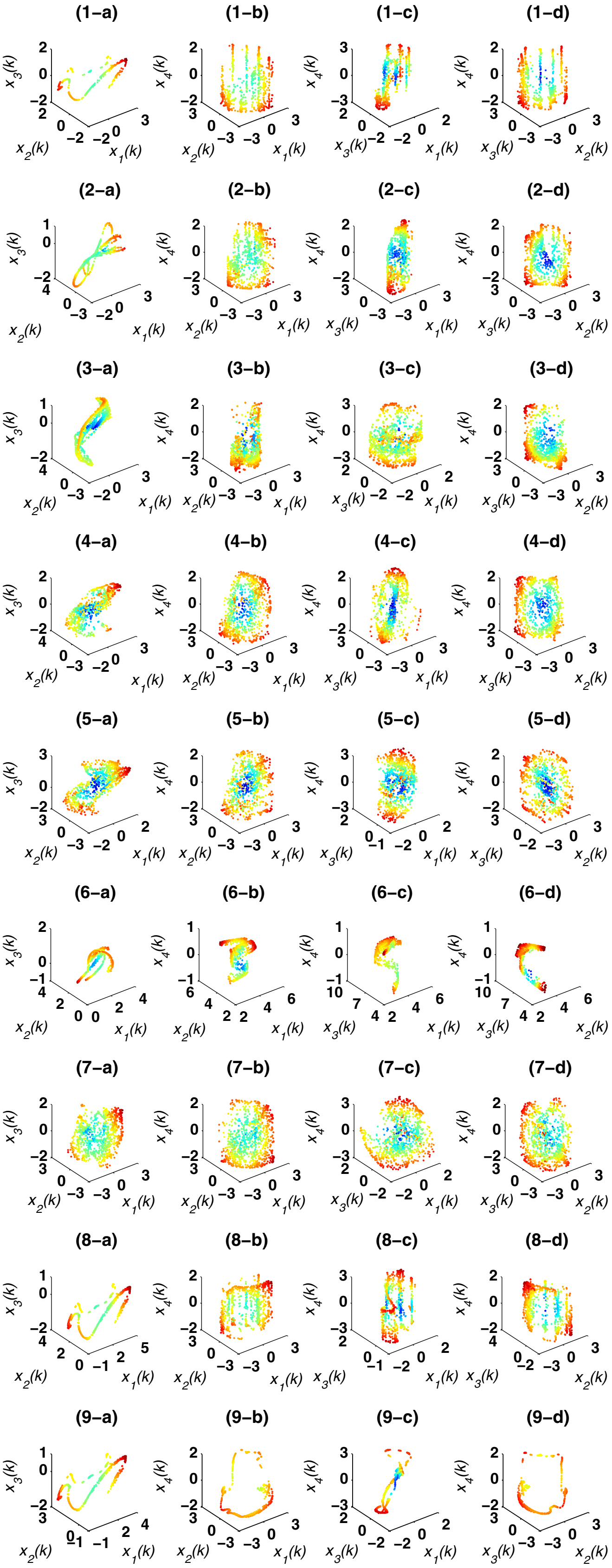


Fig. 1. Chaotic orbits of the variables of the nine equations listed in Table 1: (1-a) $x_1(k)$–$x_2(k)$–$x_3(k)$, (1-b) $x_1(k)$–$x_2(k)$–$x_4(k)$, (1-c) $x_1(k)$–$x_3(k)$–$x_4(k)$ and (1-d) $x_2(k)$–$x_3(k)$–$x_4(k)$, $(i = 1, 2, \ldots, 9)$.

Int. J. Bifurcation Chaos 2017.27. Downloaded from www.worldscientific.com
by CITY UNIVERSITY OF HONG KONG on 04/09/17. For personal use only.

To generate system orbits, select the following same initial conditions for all nine DCSLEs:

$$\begin{aligned}\mathbf{X}(0) = (&0.0769727234, 0.084649211,\\ &0.090481564, 0.084548456)^{\mathrm{T}}.\end{aligned} \tag{5}$$

Figure 1 shows the chaotic orbits of different combinations of the state variables $x_1(k)$, $x_2(k)$, $x_3(k)$ and $x_4(k)$ of the nine DCSLEs. Observation found that although their initial conditions are the same, the nine chaotic maps have different dynamic behaviors.

3. Some Concepts and the GCS Theorem

First, recall the concept of generalized synchronization (GS) [Kocarev & Parlitz, 1996; Breve *et al.*, 2009]. Let

$$\mathbf{X}(k+1) = F(\mathbf{X}(k)), \tag{6}$$

where

$$\mathbf{X}(k) = (x_1(k), \ldots, x_n(k))^{\mathrm{T}}, \tag{7}$$

$$F(\mathbf{X}(k)) = (f_1(\mathbf{X}(k)), \ldots, f_n(\mathbf{X}(k)))^{\mathrm{T}}. \tag{8}$$

System (6) is referred to as the driving system.

$$\mathbf{Y}(k+1) = G(\mathbf{Y}(k), \mathbf{X}(k)), \tag{9}$$

where

$$\mathbf{Y}(k) = (y_1(k), \ldots, y_m(k))^{\mathrm{T}}, \quad m \le n \tag{10}$$

$$\begin{aligned}G(\mathbf{Y}(k), \mathbf{X}(k)) = (&g_1(\mathbf{Y}(k), \mathbf{X}(k)), \ldots,\\ &g_m(\mathbf{Y}(k), \mathbf{X}(k)))^{\mathrm{T}}.\end{aligned} \tag{11}$$

System (9) is referred to as the driven system.

If there exists a transformation

$$H : \mathbb{R}^n \to \mathbb{R}^m \tag{12}$$

$$H(\mathbf{X}(k)) = (h_1(\mathbf{X}(k)), \ldots, h_m(\mathbf{X}(k)))^{\mathrm{T}} \tag{13}$$

and $(\mathbf{X}_0, \mathbf{Y}_0) \in \mathbb{R}^n \times \mathbb{R}^m$, there exist $\delta_1 > 0$ and $\delta_2 > 0$ such that all orbits of (6) and (9) with initial conditions $(\mathbf{X}(0), \mathbf{Y}(0)) \in B(\mathbf{X}_0, \delta_1) \times B(\mathbf{Y}_0, \delta_2) \subset \mathbb{R}^n \times \mathbb{R}^n$ satisfy

$$\lim_{k \to +\infty} \|H(\mathbf{X}(k)) - \mathbf{Y}(k)\| = 0,$$

then the two systems (6) and (9) are said to be in GS with respect to the transformation H.

Furthermore, if the two systems are chaotic, then the GS is referred to as generalized chaos synchronization (GCS).

To construct a new discrete chaotic map for GCS, the following result is needed.

Theorem 1 [Zang *et al.*, 2007]. *Let $\mathbf{X}, \mathbf{Y}, F(\mathbf{X})$ and $G(\mathbf{Y}, \mathbf{X})$ be defined by (7)–(11), and*

$$\mathbf{X}_m = (x_1(k), \ldots, x_m(k))^{\mathrm{T}}.$$

Suppose that

$$H(\mathbf{X}_m) = (y_1(k), y_2(k), \ldots, y_m(k))^{\mathrm{T}} \tag{14}$$

is an invertible transformation. If the two systems (6) and (9) are in GCS via the transformation $\mathbf{Y} = H(\mathbf{X}_m)$, then the function $G(\mathbf{Y}, \mathbf{X})$ given in (9) will be in the following form:

$$G(\mathbf{Y}, \mathbf{X}) = H(F_m(\mathbf{X})) - q(\mathbf{X}_m, \mathbf{Y}), \tag{15}$$

where

$$F_m(\mathbf{X}) = (f_1(\mathbf{X}), f_2(\mathbf{X}), \ldots, f_m(\mathbf{X}))^{\mathrm{T}}$$

and the function

$$\begin{aligned}q(\mathbf{X}_m, \mathbf{Y}) = (&q_1(\mathbf{X}_m, \mathbf{Y}), q_2(\mathbf{X}_m, \mathbf{Y}), \ldots,\\ &q_m(\mathbf{X}_m, \mathbf{Y}))^{\mathrm{T}}\end{aligned}$$

guarantees that the zero solution of the following error equation is asymptotically stable:

$$\begin{aligned}\mathbf{e}(k+1) &= H(\mathbf{X}_m(k+1)) - \mathbf{Y}(k+1)\\ &= q(\mathbf{X}_m, \mathbf{Y}).\end{aligned} \tag{16}$$

4. A Novel Chaotic Map and the DCSLE GCS System

Now, based on the DCSLE, an eight-dimensional DCSLE is introduced for the GCS. The system 2 listed in Table 1 is arbitrarily selected as the driving system of the DCSLE.

Construct an invertible matrix as follows:

$$\mathbf{A} = \begin{pmatrix} 0.2 & 0.5 & 0.1 & -0.3 \\ -0.5 & 0.5 & 0.5 & -0.3 \\ 0.2 & -0.3 & 0.5 & 0.4 \\ -0.3 & -0.3 & 0.5 & 0 \end{pmatrix}, \tag{17}$$

with the transformation $H : \mathbb{R}^4 \to \mathbb{R}^4$ defined by

$$H(\mathbf{X}) = \mathbf{A}\mathbf{X} \triangleq (h_1(\mathbf{X}), h_2(\mathbf{X}), h_3(\mathbf{X}), h_4(\mathbf{X}))^{\mathrm{T}}. \tag{18}$$

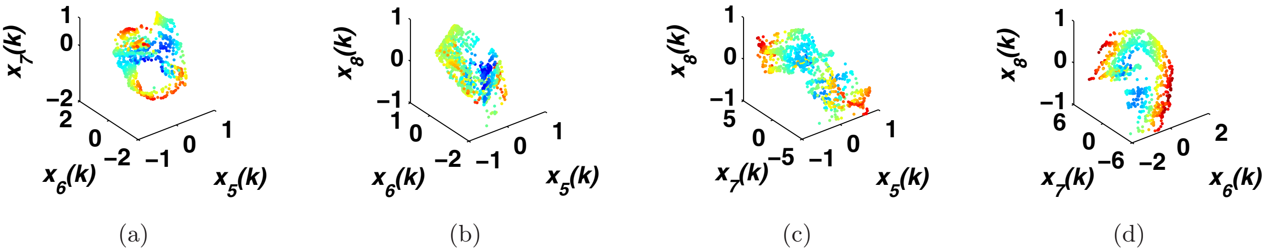


Fig. 2. Chaotic orbits of the variables of system (19): (a) $x_5(k)$–$x_6(k)$–$x_7(k)$, (b) $x_5(k)$–$x_6(k)$–$x_8(k)$, (c) $x_5(k)$–$x_7(k)$–$x_8(k)$ and (d) $x_6(k)$–$x_7(k)$–$x_8(k)$.

Based on Theorem 1, one can construct the driven system as

$$\mathbf{Y}(k+1) = \begin{pmatrix} x_5(k+1) \\ x_6(k+1) \\ x_7(k+1) \\ x_8(k+1) \end{pmatrix}$$

$$= \mathbf{A}[F(\mathbf{X}(k))] - q(\mathbf{X}(k), \mathbf{Y}(k)), \qquad (19)$$

where

$$q(\mathbf{X}, \mathbf{Y}) = \frac{1}{8}(\mathbf{AX} - \mathbf{Y}). \qquad (20)$$

Thus, $q(\mathbf{X}, \mathbf{Y})$ can ensure the zero solution of the error equation (16) to be asymptotically stable.

Hence, system 2 given in Table 1 and system (19) are in GCS with respect to the transformation (18), for any initial value $(\mathbf{X}(0), \mathbf{Y}(0)) \in \mathbb{R}^4 \times \mathbb{R}^4$.

Furthermore, choose (5) and the following as initial conditions:

$$\mathbf{Y}(0) = \mathbf{AX}(0). \qquad (21)$$

The chaotic orbits of different combinations of the state variables x_1, x_2, x_3 and x_4 are the same as those shown in the second row in Fig. 1.

Figure 2 shows the chaotic orbits of different combinations of the state variables x_5, x_6, x_7 and x_8. Figure 3 shows the evolution of the state variables $k - x_1(k), k - x_2(k), \ldots, k - x_8(k)$. Figure 4 shows that $\mathbf{X}(k)$ and $\mathbf{Y}(k)$ are in GS with respect

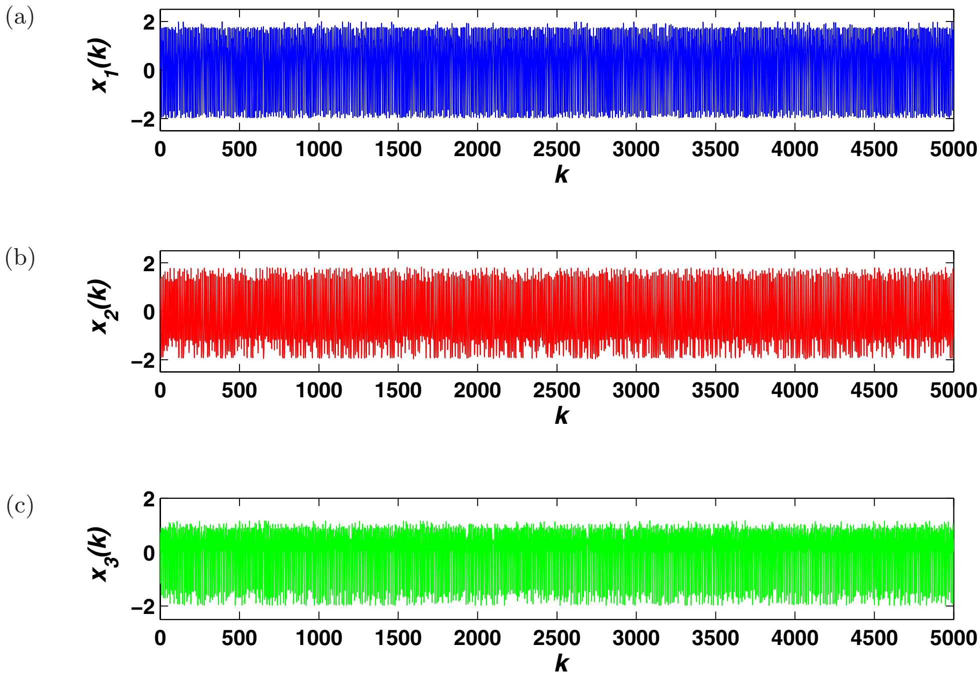


Fig. 3. The evolution of the state variables of the GCS system 2 given in Table 1 and (15): (a) k–$x_1(k)$, (b) k–$x_2(k)$, (c) k–$x_3(k)$, (d) k–$x_4(k)$, (e) k–$x_5(k)$, (f) k–$x_6(k)$, (g) k–$x_7(k)$ and (h) k–$x_8(k)$.

Int. J. Bifurcation Chaos 2017.27. Downloaded from www.worldscientific.com
by CITY UNIVERSITY OF HONG KONG on 04/09/17. For personal use only.

Int. J. Bifurcation Chaos 2017.27. Downloaded from www.worldscientific.com by CITY UNIVERSITY OF HONG KONG on 04/09/17. For personal use only.

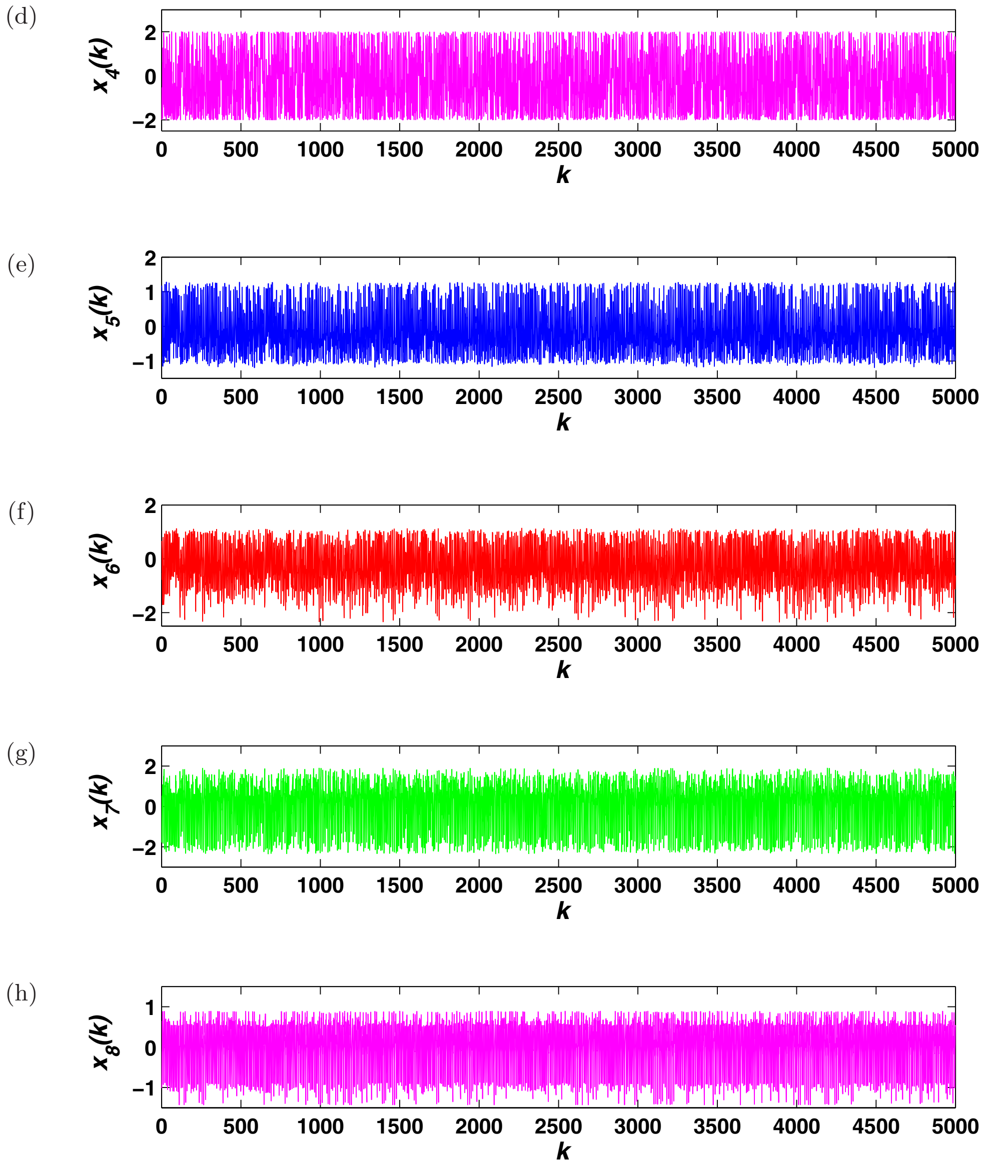
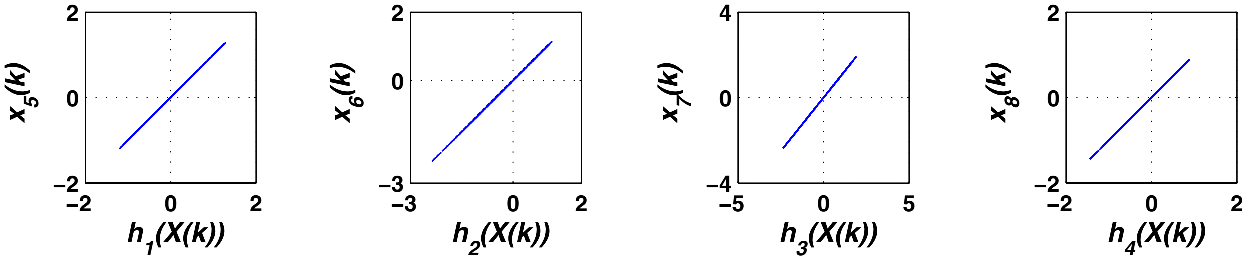


Fig. 3. (*Continued*)



(a) (b) (c) (d)

Fig. 4. The state vectors $\mathbf{X}(k)$ and $\mathbf{Y}(k)$ are in GS with respect to the transformation H: (a) $h_1(\mathbf{X}(k))$–$x_5(k)$, (b) $h_2(\mathbf{X}(k))$–$x_6(k)$, (c) $h_3(\mathbf{X}(k))$–$x_7(k)$ and (d) $h_4(\mathbf{X}(k))$–$x_8(k)$.

to the transformation $H = A$, as predicted by Theorem 1.

5. Chaotic Pseudorandom Number Generator and Pseudorandomness Tests

5.1. 2^d *word pseudorandom number generator*

Let

$$\mathbf{X}_i = \{x_i(k) \,|\, k = 1, 2, \ldots, 8\}, \tag{22}$$

where x_i is defined by system 2 listed in Table 1 and system (19).

Firstly, introduce a transformation $T_1 : \mathbb{R} \to \{0, 1, \ldots, 2^{16} - 1\}$. It is used to transform the chaotic streams of systems (22) into keystreams. Let

$$\begin{aligned}\mathbf{Y}_1 &= T_1(\mathbf{X}_1)\\ &= \mathrm{mod}\left(\mathrm{round}\left(\frac{10^{15}(\mathbf{X}_1 - \min(\mathbf{X}_1))}{(\max(\mathbf{X}_1) - \min(\mathbf{X}_1))}\right), 2^{16}\right)\end{aligned}$$

and

$$\begin{aligned}\mathbf{Y}_2 &= T_1(\mathbf{X}_6)\\ &= \mathrm{mod}\left(\mathrm{round}\left(\frac{10^{15}(\mathbf{X}_6 - \min(\mathbf{X}_6))}{(\max(\mathbf{X}_6) - \min(\mathbf{X}_6))}\right), 2^{16}\right).\end{aligned}$$

Then, define the CPRNG T by

$$T(\mathbf{X}_1, \mathbf{X}_6) = \mathrm{mod}(\mathrm{round}(\mathbf{Y}_1 + \mathbf{Y}_2), 2^{16}). \tag{23}$$

The initial conditions of the DCSLE GCS systems will be used as the seeds for the CPRNG, which can be generated by a 2^d word PRNG.

5.2. *SP800-22 test*

The NIST SP800-22 test suite [Rukhin *et al.*, 2001] consists of 15 statistical tests (see the first column in Table 2). Each statistical test is used to test a specific null hypothesis H_0, and the sequence to be tested is random.

When applying the NIST test suit, a significance level $\alpha = 0.01$ is chosen for testing. If P-value $\geq \alpha$, then the null hypothesis is accepted, namely the sequence being tested is considered to be random.

SP800-22 test suite is used to test the 100 keystreams of length 10^6, produced by the CPRNG designed in this paper with randomly perturbed initial conditions (5) and (21), and randomly perturbed matrix (17) in the range of $|\epsilon| \in [10^{-16}, 10^{-2}]$. In so doing, one has to change the keystreams with values of $\{0, 1, \ldots, 2^{16} - 1\}$ generated by the CPRNG into binary keystreams. For this purpose, the following transformation

Table 2. The calculated mean p-values of SP800-22 statistical tests for the 100 binary sequences with length 10^6 produced by the CPRNG, CPRNG1 [Han *et al.*, 2016], CPRNG2 [Zhang *et al.*, 2015], RC4 algorithm PRNG, and ZUC algorithm PRNG, respectively. Select a significance level $\alpha = 0.01$.

	Mean p-Value				
Statistical Test	CPRNG	CPRNG1	CPRNG2	RC4	ZUC
1. Frequency	0.55674	0.51988	0.5254	0.49598	0.46669
2. Block Frequency	0.51217	0.57812	0.4764	0.47781	0.48780
3. Runs	0.47272	0.51240	0.5667	0.46958	0.45937
4. Long Runs of Ones	0.51647	0.50567	0.5144	0.53504	0.45351
5. Binary Matrix Rank	0.50685	0.50621	0.5020	0.50302	0.47611
6. Spectral DFT	0.54170	0.51909	0.5219	0.47094	0.50207
7. Nonoverlapping Template	0.49795	0.49964	0.5037	0.49385	0.50045
8. The Overlapping Template	0.49728	0.48047	0.4812	0.50478	0.46822
9. Maurer's Universal Test	0.51832	0.46277	0.5084	0.48780	0.45006
10. Linear Complexity	0.49346	0.51841	0.5150	0.51639	0.46828
11. Serial ($m = 5$, $\nabla\Psi_m^2$)	0.49824	0.45204	0.4721	0.47546	0.4837
Serial ($m = 5$, $\nabla^2\Psi_m$)	0.49687	0.45997	0.4726	0.48377	0.50556
12. Approximate Entropy	0.4922	0.47617	0.5158	0.48344	0.45022
13. Cumulative Sums +1	0.54616	0.53895	0.5133	0.45873	0.46031
Cumulative Sums −1	0.56159	0.53518	0.5040	0.47298	0.47543
14. Random Excursions	0.36288	0.37138	0.3481	0.31615	0.29159
15. Random Excursions Variant	0.34621	0.37753	0.3367	0.30332	0.32560

Int. J. Bifurcation Chaos 2017.27. Downloaded from www.worldscientific.com
by CITY UNIVERSITY OF HONG KONG on 04/09/17. For personal use only.

Int. J. Bifurcation Chaos 2017.27. Downloaded from www.worldscientific.com
by CITY UNIVERSITY OF HONG KONG on 04/09/17. For personal use only.

Table 3. Acceptance rates of SP800-22 [Rukhin *et al.*, 2001] statistical tests for 100 binary sequences of length 10^6 generated by the designed CPRNG, CPRNG1 [Han *et al.*, 2016], CPRNG2 [Zhang *et al.*, 2015], RC4 PRNG, ZUC PRNG [ETSI/SAGE Specification, 2011], respectively. The significance level is selected as $\alpha = 0.01$.

	Acceptance Rate (%)				
Statistical Test	CPRNG	CPRNG1	CPRNG2	RC4	ZUC
1. Frequency	99	100	100	98	100
2. Block Frequency	99	100	100	98	100
3. Runs	99	99	100	98	100
4. Long Runs of Ones	99	99	99	97	99
5. Binary Matrix Rank	99	99	99	97	99
6. Spectral DFT	100	99	100	98	99
7. Nonoverlapping Template	95–100	96–100	97–100	94–98	96–100
8. The Overlapping Template	100	100	100	97	100
9. Maurer's Universal Test	100	98	99	97	100
10. Linear Complexity	99	99	99	98	98
11. Serial ($m = 5$, $\nabla\Psi_m^2$)	99	98	98	98	98
Serial ($m = 5$, $\nabla^2\Psi_m$)	98	100	97	96	99
12. Approximate Entropy	98	100	99	98	99
13. Cumulative Sums +1	99	100	99	98	98
Cumulative Sums −1	99	100	100	98	98
14. Random Excursions	67–69	69–72	65–68	57–58	57–58
15. Random Excursions Variant	67–69	69–72	66–68	56–58	56–58

is used:

$$\tilde{T} : \{0, 1, \ldots, 2^{16} - 1\} \to \{0, 1\},$$

which is defined by

$$\tilde{T} = T_{22} \circ T_{21}, \tag{24}$$

such that, for any $\mathbf{y} \in \{0, 1, \ldots, 2^{16} - 1\}^N$,

$$T_{21}(\mathbf{y}) = \text{dec2bin}(\mathbf{y}).$$

Denote $\mathbf{z}$ and define dec2bin$(T_{21}(\mathbf{y}))$ and

$$T_{22}(\mathbf{z}) = \mathbf{z}(:),$$

where dec2bin and $\mathbf{z}(:)$ are both Matlab commands.

The SP800-22 test suite is used to test the 100 keystreams of length 10^6 produced by the CPRNG with perturbed keys in the range $|\epsilon| \in [10^{-16}, 10^{-13}]$. The results are shown in the second columns of Tables 2 and 3.

Now, use the SP800-22 test suite to test the CPRNG1 introduced in [Han *et al.*, 2016], the CPRNG2 presented in [Zhang *et al.*, 2015], the RC4 algorithm PRNG widely used in protocols, and the ZUC algorithm PRNG accepted by the 3GPP LTE as the international encryption standard for the 4G mobile communication. The results are shown in the third–seventh columns of Tables 2 and 3 (see also [Han *et al.*, 2016]), respectively. From the statistical properties of the pseudorandomness of the sequences generated by the five PRNGs, it can be observed that all the CPRNGs have very good randomness.

5.3. 2^d *word FIPS 140-2 test*

The FIPS 140-2 randomness test consists of four subtests: Monobit Test, Poker Test, Runs Test and Long Runs Test. Each test needs a single stream of 20 000 one- and zero-bits from the keystream generator. If the first three tests corresponding to the quantity of the sequences fall out of the required intervals listed in the second column in Table 4, or if there are runs of length 26 or more, then the stream of 20 000 bits pass the test.

In a previous paper [Min *et al.*, 2013], we have pointed out that the required intervals of the monobit test, the poker test and the runs test correspond to the confidence interval with significant levels: $\alpha = 10^{-4}$, and 1.6×10^{-7} (approximately), respectively. Therefore the required intervals of the runs tests given by FIPS are not reasonable. The accepted intervals of the runs test with significant levels: $\alpha = 10^{-4}$ are listed in the third column in Table 4. We call the accepted intervals as generalized FIPS 140-2 test (criterions). According to Golomb's three postulates [Golomb, 1982], the ideal values of the Monobit test and the Runs test are listed in the fourth column in Table 4.

Int. J. Bifurcation Chaos 2017.27. Downloaded from www.worldscientific.com
by CITY UNIVERSITY OF HONG KONG on 04/09/17. For personal use only.

Table 4. The required intervals of the FIPS 140-2 Monobit Test, the Poker Test, the Runs Test. Here, MT, PT, and LT represent the Monobit Test, the Poker Test and the Long Runs Test, respectively. k represents the length of the run of a tested sequence. χ^2 DT represents χ^2 distribution.

Test Item	FIPS 140-2 Required Intervals	$\alpha = 10^{-4}$ Required Intervals	Golomb's Postulates
MT	9725∼10 275	9725∼10 275	10 000
PT	2.16∼46.17	2.16∼46.17	χ^2 DT
LT	< 26	< 26	—
k	Run Test	Run Test	Run Test
1	2315∼2685	2362∼2638	2500
2	1114∼1386	1153∼1347	1250
3	527∼723	556∼694	625
4	240∼384	264∼361	313
5	103∼209	122∼191	156
6+	103∼209	122∼191	156

Based on the FIPS 140-2 test and Golomb's three postulates on the randomness that pseudorandom sequences should satisfy [Golomb, 1982], in [Min *et al.*, 2013], we have generalized the monobit test, the poker test, the runs test and the longest runs test to 2^d word sequences. The procedures are described as follows.

(1) Denote a 2^d word sequence with length n by
$$\epsilon = \epsilon_1\epsilon_2\cdots\epsilon_n. \tag{25}$$

(2) For any $\epsilon_i \in \epsilon$, denote $2^d - 1 - \epsilon_i$ by $\sim \epsilon_i$.

(3) For each fixed i, take ϵ_i and $\sim \epsilon_i$ consecutively from ϵ, so as to obtain $2^d/2$ new sequences and denote them as
$$E_i = E_{n_1}E_{n_2}\cdots E_{n_i}, \quad i = 1, 2, \ldots, \frac{2^d}{2}. \tag{26}$$

(4) For any fixed i and E_i, replace $\epsilon_i \in E_i$ by 0, and $\sim \epsilon_i$ by 1. Denote the new sequences by
$$\tilde{\epsilon}_i = \tilde{\epsilon}_{n_1}\tilde{\epsilon}_{n_2}\cdots\tilde{\epsilon}_{n_i}, \quad i = 1, \ldots, \frac{2^d}{2}. \tag{27}$$

(5) For the case of $n = 10\,000 \times 2^d$, one can use the generalized FIPS 140-2 criteria to test the $\{0, 1\}$ sequence $\tilde{\epsilon}_i' s$. If the significant level $\alpha = 0.0001$ is taken, then the accepted intervals for the tests are the same as those listed in the third column of Table 4 (see [Min *et al.*, 2013] for more details).

Now, the 2^d word FIPS 140-2 test is used to verify the randomness of five 2^{16} word PRNGs.

(a) 2^{16} Word RC4 PRNG. Generally, a 2^d word RC4 PRNG can be designed by using the following Matlab commands:

```
d= 16;  N = 10000*2^d;
K=randi([0 2^d-1],1,2^d);
S=[0:2^d-1];j=0;
for i=1:2^d
      j=mod(j+S(i)+K(i),2^d);
         Sk=S(j+1);
           S(j+1)=S(i);
              S(i)=Sk;
end
     C=zeros(1,N); j=0;i=0; k=1;
for l=1:N
       i=mod(i+1,2^d);
         j=mod(j+S(i+1),2^d);
           Sk=S(j+1);
             S(j+1)=S(i+1);
               S(i+1)=Sk;
 C(l)=S(mod(S(j+1)+S(i+1),2^d)+1);
 end
```

Here, "randi$([0, 2^d], 1, 2^d)$" generates a vector of uniformly distributed random integers $\{0, 1, \ldots, 2^d\}$ of dimension 2^d; "mod" means taking modulus after division; "zeros$(1, N)$" is a zero row vector of dimension N. Consequently, the RC4 algorithm-based PRNG is designed.

(b) 2^{16} Word ZUC PRNG. The ZUC PRNG is actually a 2^{32} word PRNG [ETSI/SAGE Specification, 2011]. Practically, the 2^{32} word keystreams generated via the ZUC PRNG have been changed into binary keystreams for encryptions. Now, one can reshape the binary keystreams generated via the ZUC PRNG to a 16-bit sequence, thereby obtaining a 2^{16} word PRNG.

(c) 2^{16} Word CPRNGs. The first 2^{16} word CPRNG is the one defined by formula (23). The second 2^{16} word CPRNG (denoted by CPRN1) is the one defined by formula (37) given in [Han *et al.*, 2016]. The third 2^{16} word CPRNG (denoted by CPRN2) is the one defined by formula (25) presented in [Zhang *et al.*, 2015].

Now, use the 2^d word FIPS 140-2 criterions to test the 100 keystream of length $10\,000 \times 2^{16}$ generated by the five PRNGs via randomly perturbed seeds, respectively. The results are listed in Tables 5 and 6, in which the statistic results are described by the mean value ± standard deviation (denoted by Mean ± SD). Observe that there are no significant differences in the randomness performances among them.

Int. J. Bifurcation Chaos 2017.27. Downloaded from www.worldscientific.com by CITY UNIVERSITY OF HONG KONG on 04/09/17. For personal use only.

Table 5. The tested Mean ± SD of all $E_i's$ defined by (26) for the 100×2^{16} word (16-bit) key streams of length $10\,000 \times 2^{16}$ generated by the RC4 PRNG, the ZUC PRNG and the three CPRNGs, respectively.

Test Item	Bits $\{\varepsilon_i, \sim\varepsilon_i\}$	RC4 Mean ± SD	ZUC Mean ± SD	CPRNG Mean ± SD	CPRNG1 Mean ± SD	CPRNG2 Mean ± SD
MT	ε_i	$10\,000 \pm 100.01$	9999.9 ± 100	9999.9 ± 99.957	$10\,000 \pm 100.03$	$10\,000 \pm 99.892$
	$\sim\varepsilon_i$	$10\,000 \pm 100$	9999.9 ± 100.3	$10\,000.0 \pm 99.925$	$10\,000 \pm 99.999$	9999.9 ± 100.02
PT	—	15.003 ± 5.478	15 ± 5.5	14.999 ± 5.477	14.999 ± 5.4756	15 ± 5.4778
LT	ε_i	13.62 ± 1.873	13.6 ± 1.9	13.619 ± 1.871	13.621 ± 1.8731	13.621 ± 1.8717
	$\sim\varepsilon_i$	13.62 ± 1.871	13.6 ± 1.9	13.620 ± 1.872	13.621 ± 1.8737	13.622 ± 1.8728
k		Runs Test				
1	ε_i	2500.1 ± 49.995	2500 ± 50	2500.1 ± 49.999	2500.0 ± 49.991	2500.1 ± 49.967
	$\sim\varepsilon_i$	2500.2 ± 50.023	2499.9 ± 49.9	2500.1 ± 49.982	2500.2 ± 50.005	2500.2 ± 50.01
2	ε_i	1249.8 ± 33.1	1250 ± 33.0	1249.9 ± 33.074	1250 ± 33.070	1250 ± 33.079
	$\sim\varepsilon_i$	1250 ± 33.098	1250 ± 33.058	1250.0 ± 33.054	1250 ± 33.072	1250.1 ± 33.045
3	ε_i	624.96 ± 23.391	625 ± 22.4	624.95 ± 23.380	624.96 ± 23.377	624.96 ± 23.393
	$\sim\varepsilon_i$	624.99 ± 23.385	625 ± 23.4	624.99 ± 23.364	624.99 ± 23.411	624.98 ± 23.38
4	ε_i	312.47 ± 16.825	312.5 ± 16.8	312.45 ± 16.819	312.47 ± 16.822	312.48 ± 16.832
	$\sim\varepsilon_i$	312.47 ± 16.822	312.5 ± 16.8	312.46 ± 16.832	312.47 ± 16.827	312.48 ± 16.834
5	ε_i	156.22 ± 12.093	156.2 ± 12.1	156.2 ± 12.100	156.23 ± 12.100	156.22 ± 12.104
	$\sim\varepsilon_i$	156.24 ± 12.103	156.3 ± 12.1	156.2 ± 12.104	156.23 ± 12.101	156.23 ± 12.098
6^+	ε_i	156.21 ± 11.894	156.3 ± 11.9	156.2 ± 11.901	156.22 ± 11.902	156.21 ± 11.901
	$\sim\varepsilon_i$	156.22 ± 11.905	156.2 ± 11.9	156.2 ± 11.900	156.22 ± 11.893	156.2 ± 11.900

5.4. *Key space*

For the proposed CPRNG, the key parameter set includes the initial conditions $\mathbf{X}(0), \mathbf{Y}(0)$ and the matrix $\mathbf{A} = (\alpha_{i,j})$. Hence, the CPRNG has $4 + 4 + 16$ key parameters, which are denoted by

$$\mathbf{K}_s = \{k_1, k_2, \ldots, k_{24}\}. \tag{28}$$

In the new design, the first eight keys are taken from the initial conditions $\mathbf{X}(0)$ and $\mathbf{Y}(0)$, and the other 16 keys from the parameters of the matrix $\mathbf{A}$.

The perturbed keys have the following forms:

$$k_i + \delta_i, \quad i = 1, 2, \ldots, 8. \tag{29}$$

The Matlab platform uses double-precision decimal computations, so each computed decimal number has 16 bits of accuracy. Thus, one can select

$$|\delta_i| \in [10^{-16}, 1), \quad i = 1, 2, \ldots, 8.$$

Table 6. The percentages of failure to pass G FIPS 140-2 for the $\{\epsilon, \sim\epsilon\}$ sequence in the 100×2^{16} word (16-bit) key streams of length $10\,000 \times 2^{16}$ generated by the RC4 PRNG, the ZUC PRNG and the designed three CPRNGs, respectively.

PRNG Test	RC4 %	ZUC %	CPRNG %	CPRNG1 %	CPRNG2 %
G FIPS	0.31090	0.31801	0.31093	0.30931	0.30617

It can be proved that if the elements of the perturbation matrix $\Delta = (\sigma_{i,j})_{4\times 4}$ satisfy

$$|\sigma_{i,j}| < 0.043095, \quad i, j = 1, \ldots, 4,$$

then the matrix $A + \Delta$ remains to be invertible. Thus, for the key k_i ($i = 9, 10, \ldots, 24$), one can select

$$\delta_i \in [10^{-16}, 10^{-2}),$$

namely,

$$\delta_i = 0.0a_2a_3 \cdots a_{16},$$

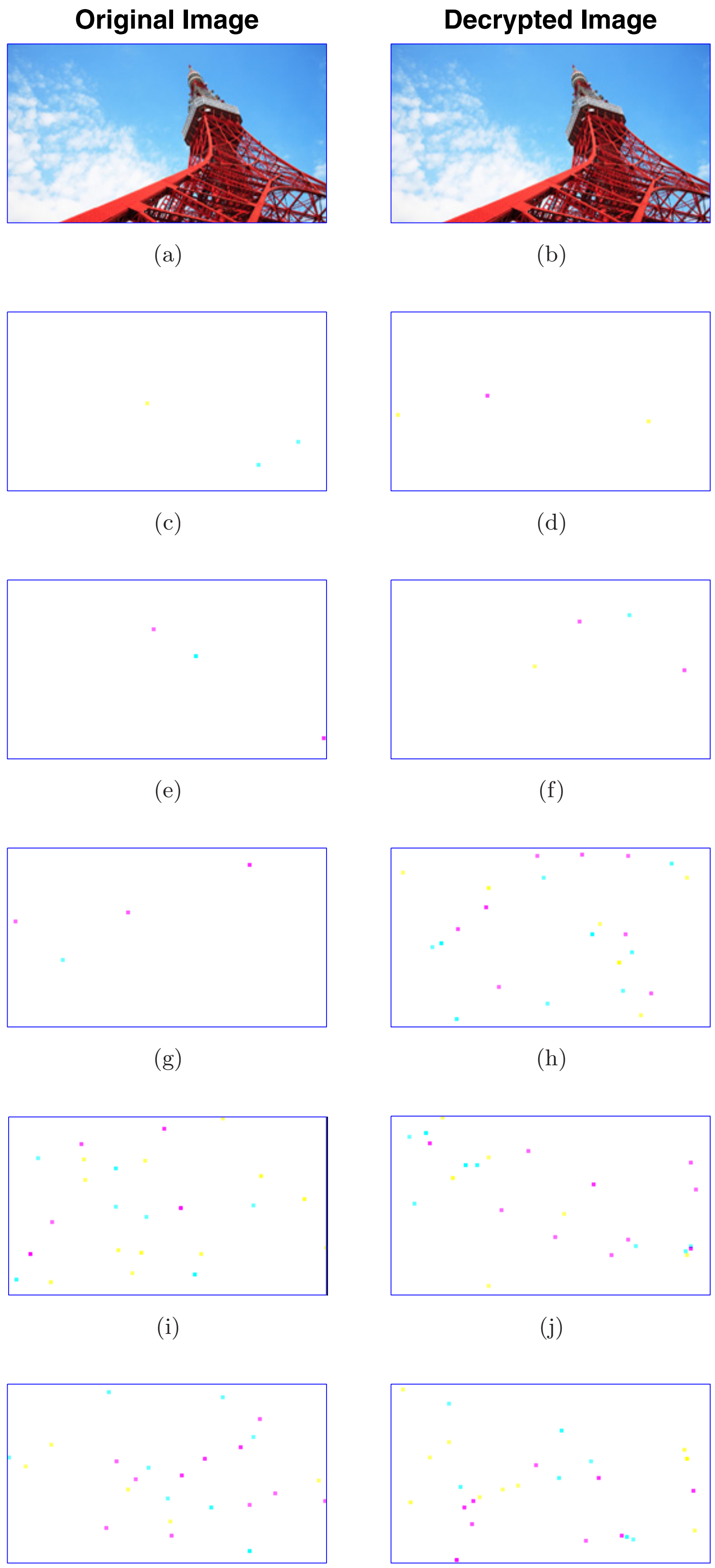
where

$$a_i \in [0, 1, \ldots, 9].$$

Table 7. Percentages of the differences and the correlation parameters of the keystream variations between S and S_p, S and S_m, respectively.

Item	SV	S, S_p	S, S_m
DC	Min	48.645%	48.910%
	Mean	50.006%	49.982%
	Max	51.240%	51.060%
CC	Min	7.0401×10^{-6}	1.1440×10^{-5}
	Mean	5.4137×10^{-3}	5.6992×10^{-3}
	Max	2.7095×10^{-3}	2.1807×10^{-3}

Int. J. Bifurcation Chaos 2017.27. Downloaded from www.worldscientific.com
by CITY UNIVERSITY OF HONG KONG on 04/09/17. For personal use only.



(a) (b)

(c) (d)

(e) (f)

(g) (h)

(i) (j)

(k) (l)

Fig. 5. (a) Original image, (b) decrypted image via the keystream without perturbation. Ten decrypted images via keystreams generated with slighted perturbed initial conditions and the matrix within the range $[10^{-16}, 10^{-13}]$: (c) $G_{3,1}$, (d) $G_{3,2}$, (e) $G_{3,3}$, (f) $G_{4,1}$, (g) $G_{4,2}$, (h) $G_{23,1}$, (i) $G_{24,1}$, (j) $G_{24,2}$, (k) $G_{24,3}$ and (l) $G_{26,1}$.

Therefore, in the CPRNG, the 24 keys have an effective key space

$$2 \times 10^{8\times16} \times 10^{16\times14} > 2^{1170}.$$

Now, we compare the differences between the keystream S of 10^6 code lengths generated by the key set (28) and the keystream S_p generated by the perturbed key set (29), respectively.

The comparison results are listed in the third column of Table 7, where SV denotes statistical values, DC means different codes, and CC stands for correlation coefficients.

It can be observed that the average percentage of different codes and the average correlation coefficient are 50.006% and 0.0054137, which are very close to the ideal values of 50% and 0, respectively.

Next, we compare the differences between the same keystream S and the 1000 streams S_m generated by the Matlab function randi($[0 \quad 1], 1, 10^6$). The comparison results are listed in the fourth column of Table 7. It can be observed that the average percentage of different codes is 49.982% and the average correlation coefficient is 0.0056992, implying that the keystream S has no significant correlations with the perturbed keystream S_p and the streams S_m.

6. Simulation on SESAE

The avalanche effect of the CPRNG is discussed here, which is used to encrypt an RGB image "tower" with 250 × 140 pixels, as shown in Fig. 5(a). The simulation is implemented by using the Matlab 7.1 platform on a PC computer.

Here, the SESAE experiment procedures on CPRNG are intentionally designed to be very similar to those given in Sec. 3.1.5 in [Min & Chen, 2013]. By using the CPRNG and the SESAE to encrypt and decrypt the image given in Fig. 5(a), the results show that decrypted images can be obtained without errors.

However, if one uses 1000 keystreams generated by randomly disturbing the initial conditions (5) and (21), as well as by the matrix (17), for 1000 times in the range $|\epsilon| \in [10^{-16}, 10^{-10}]$, then all decrypted RGB images will become almost pure white-colored ones.

In these simulations, each of all decrypted images has 840 000 $\{0, 1\}$ codes. Among the decrypted images, the minimum and the maximum numbers of zeros are 3 and 26, respectively.

Table 8. Differences between the original keystream S_0 and the keystreams $S_{j,i}$, measured by norm $\|S_0 - S_{j,i}\|$.

	$\|S_0 - S_{j,i}\|$ $(\times 10^{-10})$				
	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$	$S_{4,1}$	$S_{4,2}$
S_0	2.8142	3.1824	3.2058	2.5598	2.7061
	$S_{23,1}$	$S_{24,1}$	$S_{24,2}$	$S_{24,3}$	$S_{26,1}$
S_0	3.1077	3.1989	2.9631	2.7148	3.0767

Let $G_{i,j}$ represent the jth image that has i zero codes. The first five images with a minimum number of zero codes and the last five images with a maximum number of zero codes are shown in Figs. 5(c)–5(l). Note that in order to make the pixels with brightness less than 255 be visible in the decrypted images, technically the brightness of the three color planes of these pixels has been reduced by 150, and increase the size of those pixels by 9 times.

Therefore, the percentages of the number of "1" codes in the 1000 decrypted images are within the range [0.999969, 0.999996], which are all very close to the ideal value $(2^{16} - 1)/2^{16} = 0.999985$.

Summarizing the above simulation results, the CPRNG can generate encrypted images with significant avalanche effects SESAE to encrypt RGB images.

Table 8 lists some statistical data of the deviations (denoted by "norms") between the original keystream S_0 and the keystreams $S_{i,j}$ used in the above decrypted image $G_{i,j}$. It can be seen that there are no significant correlations between the norms and the corresponding decrypted images.

7. Conclusions

The main contributions of this paper are summarized as follows:

(1) Introduced the concept of discrete chaotic maps with one-line equilibria, and proposed nine such maps consisting of sine functions

(2) Combined a four-dimensional discrete chaotic map with one-line equilibria and the GCS theorem to design an eight-dimensional DCSLE GCS system

(3) Constructed a 2^{16} word CPRNG and compared the simulation results tested by the FIPS 140-2 test suite and the NIST SP800 test suite on the keystreams generated by using the CPRNG (keyspace $> 2^{1170}$), the CPRNG1 (proposed in [Han *et al.*, 2016], keyspace $=> 2^{1195}$), the

Int. J. Bifurcation Chaos 2017.27. Downloaded from www.worldscientific.com by CITY UNIVERSITY OF HONG KONG on 04/09/17. For personal use only.

CPRNG2 (introduced in [Zhang *et al.*, 2015], keyspace => 2^{1116}), the RC4 algorithm and the ZUC algorithm (keyspace = 2^{128}), respectively. It is demonstrated that the randomness of the sequences generated via the CPRNGs have promising performances in term of the SP800-22/FIPS 140-2 tests

(4) An image encryption example has shown that the designed CPRNG is able to generate significant avalanche effects, and the percentage of "1" codes in the decrypted images for different keystreams is larger than 0.999969, which is very close to the ideal value of $(2^{16} - 1)/2^{16} = 0.999985$. This demonstrates that the proposed CPRNG is a qualified candidate for SESAE.

(5) The results may imply that if the 2^d word sequences generated by a 2^d word PRNG are able to pass the 2^d word FIPS 140-2 tests with a high percentage, then the CPRNG has good performance similar to that of ideal 2^d word PRNG [Min & Chen, 2013].

In summary, the proposed CPRNG is a promising candidate for practical applications. Further comparisons with different state-of-the-art PRNG schemes in terms of computational complexity, communication cost and storage requirement will be carried out in future research.

Int. J. Bifurcation Chaos 2017.27. Downloaded from www.worldscientific.com
by CITY UNIVERSITY OF HONG KONG on 04/09/17. For personal use only.

Acknowledgments

This project is supported by the National Natural Science Foundation of China (Grant Nos. 61074192, 61170037) and by the Hong Kong Research Grants Council under the GRF Grant CityU11208515. The calculations of the FIPS 140-2 tests are implemented via the "Nonlinear Complex System Research Platform Project" supported by the Fund of Improving Conditions of Running National Ordinary Universities of China. The authors would like to thank Mr. Longjie Hao from the Peking University Founder Group Co. Ltd for his assistance in the calculations on FIPS 140-2 tests.

References

Aguirre, C., Campos, D., Pascual, P. & Serrano, E. [2006] "Synchronization effects using a piecewise linear map-based spiking-bursting neuron model," *Neurocomput.* **69**, 1116–1119.

Alvarez, G., Montoya, F., Pastor, G. & Romera, M. [2004] "Breaking a secure communication scheme based on the phase synchronization of chaotic systems," *Chaos* **14**, 274–278.

Breve, F. A., Zhao, L., Quiles, M. G. & Macau, E. E. [2009] "Chaotic phase synchronization and desynchronization in an oscillator network for object selection," *Neur. Netw.* **22**, 728–737.

Chen, G. & Dong, X. [1998] *From Chaos to Order*: *Methodologies*, *Perspectives*, *and Applications* (World Scientific, Singapore).

Chen, J., Wong, K., Cheng, L. & Shuai, J. [2003] "A secure communication scheme based on the phase synchronization of chaotic systems," *Chaos* **13**, 508–514.

Chua, L. O. [1994] "Chua's circuit 10 years later," *Int. J. Circuit Th. Appl.* **22**, 279–305.

ETSI/SAGE Specification [2011] *Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document*: *ZUC Specification*; *Version:1.5.*

Feistel, H. [1973] "Cryptography and computer privacy," *Scient. Amer.* **228**, 15–23.

Fiedler, B. & Liebscher, S. [2000] "Generic Hopf bifurcation from lines of equilibria without parameters: II. Systems of viscous hyperbolic balance laws," *SIAM J. Math. Anal.* **31**, 1396–1404.

Fiedler, B., Liebscher, S. & Alexander, J. C. [2000a] "Generic Hopf bifurcation from lines of equilibria without parameters: I. Theory," *J. Diff. Eqs.* **167**, 16–35.

Fiedler, B., Liebscher, S. & Alexander, J. C. [2000b] "Generic Hopf bifurcation from lines of equilibria without parameters III: Binary oscillations," *Int. J. Bifurcation and Chaos* **10**, 1613–1621.

Ge, Z.-M., Li, C.-H., Li, S.-Y. & Chang, C. M. [2008] "Chaos synchronization of double duffing systems with parameters excited by a chaotic signal," *J. Sound Vibr.* **317**, 449–455.

Golomb, S. W. [1982] *Shift Register Sequences* (Aegean Park Press, Laguna Hills, CA).

Gross, N., Kinzel, W., Kanter, I., Rosenbluh, M. & Khaykovich, L. [2006] "Synchronization of mutually versus unidirectionally coupled chaotic semiconductor lasers," *Opt. Commun.* **267**, 464–468.

Han, D., Min, L. & Chen, G. [2016] "Stream encryption scheme with key and plaintext avalanche effects with application stream encryption scheme with key and plaintext," *Int. J. Bifurcation and Chaos* **26**, 1650091-1–19.

Jafari, S. & Sprott, J. [2013] "Simple chaotic flows with a line equilibrium," *Chaos Solit. Fract.* **57**, 79–84.

Jafari, S., Sprott, J. C. & Golpayegani, S. H. [2013] "Elementary quadratic chaotic flows with no equilibria," *Phys. Lett. A* **377**, 699–702.

Kanso, A. & Ghebleh, M. [2012] "A novel image encryption algorithm based on a 3D chaotic map," *Commun. Nonlin. Sci. Numer. Simul.* **17**, 2943–2959.

Int. J. Bifurcation Chaos 2017.27. Downloaded from www.worldscientific.com
by CITY UNIVERSITY OF HONG KONG on 04/09/17. For personal use only.

Kili, R. [2006] "Experimental study on impulsive synchronization between two modified Chua's circuits," *Nonlin. Anal.*: *Real World Appl.* **7**, 1298–1303.

Kocarev, L. & Parlitz, U. [1996] "Generalized synchronization, predictability and equivalence of unidirectionally coupled dynamical systems," *Phys. Rev. Lett.* **76**, 1816–1819.

Law, R., Murrell, D. J. & Dieckmann, U. [2003] "Population growth in space and time: Spatial logistic equations," *Ecology* **84**, 252–262.

Leonov, G. A. & Kuznetsov, N. V. [2011] "Analytical-numerical methods investigation of hidden oscillations in nonlinear control systems," *IFAC Proc. Vol.* **44**, 2494–2505.

Li, T. Y. & Yorke, J. A. [1975] "Period three implies chaos," *Amer. Math. Month.* **82**, 985–992.

Li, N., Pan, W., Yan, L. *et al.* [2014] "Enhanced chaos synchronization and communication in cascade-coupled semiconductor ring lasers," *Commun. Nonlin. Sci. Numer. Simul.* **19**, 1874–1883.

Liu, T. & Min, L. [2014] "Design of non-autonomous chaotic generalized synchronization based pseudorandom number generator with application in avalanche image encryption," *Proc. 17th IEEE Int. Conf. Computational Science and Engineering* (IEEE, Chengdu, China), pp. 576–582.

Lorenz, E. N. [1995] *The Essence of Chaos* (University of Washington Press, Washington).

Matouk, A. E. [2011] "Chaos, feedback control and synchronization of a fractional-order modified autonomous van der Pol–Duffing circuit," *Commun. Nonlin. Sci. Numer. Simul.* **16**, 975–986.

Messias, M., Nespoli, C. & Botta, V. A. [2010] "Hopf bifurcation from lines of equilibria without parameters in memristor oscillators," *Int. J. Bifurcation and Chaos* **20**, 437–450.

Min, L. & Chen, G. [2013] "A novel stream encryption scheme with avalanche effect," *Eur. Phys. J. B* **86**, 1–13.

Min, L., Hao, L. & Zhang, L. [2013] "Study on the statistical test for string pseudorandom number generators," *Advances in Brain Inspired Cognitive Systems. BICS 2013*, Lecture Notes in Computer Sciences, Vol. 7888 (Springer, Berlin, Heidelberg), pp. 278–287.

Nana, B., Woafo, P. & Domngang, S. [2009] "Chaotic synchronization with experimental application to secure communications," *Commun. Nonlin. Sci. Numer. Simul.* **14**, 2266–2276.

NIST [2001] *FIPS PUB 140-2*, *Security Requirements for Cryptographic Modules* (NIST, Gaithersburg, MD).

Pecora, L. M. & Carroll, T. L. [1990] "Synchronization in chaotic systems," *Phys. Rev. Lett.* **64**, 821–825.

Pehlivan, I., Moroz, I. M. & Vaidyanathan, S. [2014] "Analysis, synchronization and circuit design of a novel butterfly attractor," *J. Sound Vibr.* **333**, 5077–5096.

Rukhin, A., Soto, J., Nechvatal, J., Smid, M. & Barker, E. [2001] *A Statistical Test Suite for Random and Pseudorandom Number Generator for Cryptographic Applications* (NIST Special Publication).

Sausedo-Solorio, J. M. & Pisarchik, A. [2014] "Synchronization of map-based neurons with memory and synaptic delay," *Phys. Lett. A* **378**, 2108–2112.

Senator, M. [2006] "Synchronization of two coupled escapement-driven pendulum clocks," *J. Sound Vibr.* **291**, 566–603.

Shahverdiev, E. & Shore, K. [2009] "Impact of modulated multiple optical feedback time delays on laser diode chaos synchronization," *Opt. Commun.* **282**, 3568–3572.

Spillman, R. J. [2004] *Classical and Contemporary Cryptology* (Prentice-Hall, Inc., Upper Saddle River, NJ).

Sprott, J. C. [1994] "Some simple chaotic flows," *Phys. Rev. E* **50**, 647–650.

Sprott, J. C. [2003] *Chaos and Time-Series Analysis* (Oxford University Press, Oxford).

Sun, J., Shen, Y., Yin, Q. & Xu, C. [2013] "Compound synchronization of four memristor chaotic oscillator systems and secure communication," *Chaos* **23**, 013140-1–10.

Wang, F. & Liu, C. [2006] "A new criterion for chaos and hyperchaos synchronization using linear feedback control," *Phys. Lett. A* **360**, 274–278.

Wang, Y., Wong, K., Liao, X. & Chen, G. [2011] "A new chaos-based fast image encryption algorithm," *Appl. Soft Comput.* **11**, 514–522.

Wu, X. [2006] "A new chaotic communication scheme based on adaptive synchronization," *Chaos* **16**, 043118-1–12.

Wu, X., Bai, C. & Kan, H. [2014] "A new color image cryptosystem via hyperchaos synchronization original research," *Commun. Nonlin. Sci. Numer. Simul.* **19**, 1884–1897.

Wu, Y., Hua, Z. & Zhou, Y. [2015] "N-dimensional discrete cat map generation using Laplace expansions," *IEEE Trans. Cybern.* **46**, 2622–2633.

Xia, W. & Cao, J. [2008] "Adaptive synchronization of a switching system and its applications to secure communications," *Chaos* **18**, 023128-1–15.

Yang, C.-H., Li, S.-Y., Chang, C. M. & Ge, Z.-M. [2012] "Chaos generalized synchronization of an inertial tachometer with new Mathieu-van der Pol systems as functional system by gyc partial region stability theory," *Commun. Nonlin. Sci. Numer. Simul.* **17**, 1355–1371.

Yang, X., Min, L. & Wang, X. [2015] "A cubic map chaos criterion with applications in generalized synchronization based pseudorandom number generator and image encryption," *Chaos* **25**, 053104-1–9.

Zang, H., Min, L. & Zhao, G. [2007] "A generalized synchronization theorem for discrete-time chaos system with application in data encryption scheme," *Int. Conf. Commun. Circuits and Systems, 2007. ICCCAS 2007* (Kokura, Fukuoka Japan), pp. 1325–1329.

Zhang, M., Wang, D., Min, L. & Wang, X. [2015] "A generalized stability theorem for discrete-time nonautonomous chaos system with applications," *Math. Probl. Engin.* **2015**, 121359-1–12.

Zhou, P., Huang, K. & Yang, C. D. [2013] "A fractional-order chaotic system with an infinite number of equilibrium points," *Discr. Dyn. Nat. Soc.* **2013**, 910189-1–6.

Zhou, Y., Hua, Z., Pun, C.-M. & Chen, C. L. P. [2015] "Cascade chaotic system with applications," *IEEE Trans. Cybern.* **45**, 2001–2012.

Int. J. Bifurcation Chaos 2017.27. Downloaded from www.worldscientific.com
by CITY UNIVERSITY OF HONG KONG on 04/09/17. For personal use only.