Generalized Stability Theorems for Bidirectional Discrete Systems and Differential Equations with Application

Xiuping Yang, Lequan Min, and Mei Zhang

***Abstract*—Chaos synchronization and generalized chaos synchronization (GCS) are of essential importance for many physical, circuit, biological, and engineering systems. This paper introduces the definitions of generalized stability (GST) in bidirectional discrete and differentiable systems, which are the extensions for the definitions of chaos generalized synchronization of corresponding bidirectional discrete and differentiable chaos systems. Two constructive generalized stability (GST) theorems for bidirectional discrete systems and bidirectional differential equations (BDS and BDE) are introduced, which give general representations for GST BDS and GST BDE. Using the two theorems, one can easily construct new chaos systems to make the system variables be in GST. Two 8-dimensional GST systems are presented to illustrate the effectiveness of the theoretical results. By combining the 8-dimensional systems with the GCS theorem, two 12- dimensional GCS systems are designed. Numerical simulations verify the chaotic dynamics of such discrete systems and differential equations. Using the two 12-dimensional GCS systems designs two chaotic pseudorandom number generators (CPRNGs). The FIPS 140-2/SP800-22 test suite are used to test the randomness of the four 1,000/100 key-streams consisting of 20,000 bits generated by our CPRNGs, the RC4 algorithm, the ZUC algorithm, respectively. The results show that the randomness performances of our CPRNGs are promising. In addition, theoretically the key space of the each CPRNG is larger than 2^{1196}.**

***Index Terms*—Generalized stability, bidirectional systems, numerical simulation, RANDOMNESS test.**

I. Introduction

Chaos was first formally introduced into mathematics in connection with an interval map by Li and Yorke in 1975 [1]. Chaotic dynamics are intrinsically sensitive to initial conditions, as well as system parameters, with random-like unpredictable long-term behaviors [2], [3].

The problem of chaotic synchronization was first studied by Yamada and Fujisaka in 1983 [4], then studied by Afraimovich *et al*. in 1986 [5]. Since the pioneering work by Pecora and Carroll in 1990 [6], now commonly termed the Pecora-Carroll method, much attention has been devoted to research on chaos synchronization. Chaos synchronization is of essential importance for much synchronization is of essential importance for many physical, circuits, biological and engineering systems ([7]–[12]). Chaos synchronization systems may provide new tools in cryptography and communication fields ([13]–[18]). Along this line of thoughts, we recently studied in-depth a generalized chaos synchronization (GCS) scheme [19] (see also [13], [20]–[22]).

First, this paper introduces the definitions of generalized stability (GST) in bidirectional discrete and differentiable chaos system, which are extensions the definitions of chaos generalized synchronization for corresponding bidirectional discrete and differentiable chaos systems. Second, this study sets up two constructive GST theorems for bidirectional discrete systems and differential equations. Two numerical simulations aim our theoretical results. Third, using two 12-dimensional GCS systems designs two CPRNGs. The FIPS 140-2 test suite and SP800-22 test suite are used to test the randomness of the two CPRNGs, the RC4 algorithm and the ZUC [23] algorithm.

The rest of this paper is organized as follows. Section II introduces the definition and the theorem on GST for BDS. Section III proposes the definition and the theorem on GST for BDE. Section IV presents one 12-dimensional GCS discrete system, and one 12-dimensional GCS continuous system, simulates the dynamic behaviors of these systems. Section V designs two CPRNGs, and implements and compares the randomness tests for the two CPRNGs and the RC4 algorithm and the ZUC algorithm. Finally, some concluding remarks are given in Section VI.

II. GS Theorem for Bidirectional Discrete Systems

In this section, motivated by the bidirectional discrete generalized chaotic synchronization (GCS) (for example see [24] and [25]), this study introduces the following:

Definition 1: Consider two systems

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

$$Y(k+1) = G(Y(k), X(k)), \tag{2}$$

where

$$X(k) = (x_1(k), \ldots, x_n(k))^T, \tag{3}$$

$$Y(k) = (y_1(k), \ldots, y_m(k))^T, m \le n \tag{4}$$

$$F(X(k), Y(k)) = (f_1(X(k), Y(k)), \ldots, f_n(X(k), Y(k)))^T \tag{5}$$

$$G(Y(k), X(k)) = (g_1(Y(k), X(k)), \ldots, g_m(Y(k), X(k)))^T \tag{6}$$

If there exists a transformation

$$H : R^n \to R^m,$$

Manuscript received June 1, 2015; revised August 11, 2015. This work was supported in part by the National Natural Science Foundations of China (Grant Nos. 61074192, 61170037)

The authors are with the School of Mathematics and Physics, University of Science and Technology Beijing, Beijing 100083, PR China (e-mail: yangxiuping_1990@163.com, minlequan@sina.com, Zhangmei_math@163.com).

DOI: 10.7763/IJMO.2015.V5.471

$$H(X_m(k)) = (h_1(X_m(k)),\ldots,h_m(X_m(k)))^T \quad (7)$$

and for $\forall \varepsilon > 0$ there exists $\delta_1 > 0, \delta_2 > 0$

$$B = B(X_0,\delta_1)\times B(Y_0,\delta_2) \subset R^n \times R^m,$$

Such that all initial conditions satisfy $(X(0),Y(0)) \in B$, and all trajectories of (1) and (2) satisfy.

$$\| H(X_m(k)) - Y(k) \| < \varepsilon, \quad k = 1,2,3\cdots \quad (8)$$

where

$$X_m(k) = (x_1(k),\ldots,x_m(k))^T .$$

Then the systems in (1) and (2) are said to be in GST with respect to the transformation H.

Theorem 1: Let $X, Y, X_m, F(X,Y)$ and $G(Y,X)$ be defined by (3)-(6),

$$X_m(k) = (x_1(k),\ldots,x_m(k))^T$$

Suppose that

$$H\ (x_1,\ x_2,\ \cdots,\ x_m) = (y_1,\ y_2,\ \cdots,\ y_m).$$

If the two systems (1) and (2) are in GST via the transformation $Y = H(X_m)$, if, and only if, the function $G(Y,X)$ given in (2) has the following form:

$$G(Y,X) = H[F_m(X,Y)] - q(X_m,Y)$$

where

$$F_m(X,Y) = (f_1(X,Y),\ f_2(X,Y),\ldots,\ f_m(X,Y))^T$$

and the function

$$q(X_m,Y) = (q_1(X_m,Y), q_2(X_m,Y),\ldots,q_m(X_m,Y))^T$$

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

$$\begin{aligned} e(k+1) &= H(X_m(k+1)) - Y(k+1) \\ &= q(X_m,Y). \end{aligned} \quad (9)$$

Proof: Denote

$$G(Y,X) - H[F_m(X,Y)] = -q(X_m,Y),$$

Then

$$\begin{aligned} e(k+1) &= H(X_m(k+1)) - Y(k+1) \\ &= q(X_m,Y). \end{aligned}$$

Therefore, two dynamic systems (1) and (2) are in GST via the transformations H if, and only if, the function $q(X_m,Y)$ makes the trajectory in (9) tends to zero solution stably. This completes the proof.

Remark 1. Theorem 1 is constructive. It provides a general approach to construct bidirectional discrete generalized stability systems.

III. GST Theorem for Bidirectional Differential Systems

Motivated by GCS of differential systems ([24] and [25]), this paper introduces the following

Definition 2: Consider two systems

$$\frac{d(X(t))}{dt} = F(X(t),Y(t)), \quad (10)$$

$$\frac{d(Y(t))}{dt} = G(Y(t),X(t)), \quad (11)$$

where

$$X(t) = (x_1(t),\ldots,x_n(t))^T \quad (12)$$

$$Y(t) = (y_1(t),\ldots,y_m(t))^T, m \le n \quad (13)$$

$$F(X(t),Y(t)) = (f_1(X(t),Y(t)),\ldots,\ f_n(X(t),Y(t)))^T \quad (14)$$

$$G(Y(t),X(t)) = (g_1(Y(t),X(t)),\ldots,g_m(Y(t),X(t)))^T . \quad (15)$$

If there exists a transformation

$$H: R^n \to R^m,$$
$$H(X_m(t)) = (h_1(X_m(t)),\ldots,h_m(X_m(t)))^T \quad (16)$$

and for $\forall \varepsilon > 0$ there exists $\delta_1 > 0, \delta_2 > 0$ and

$$B = B(X_0,\delta_1)\times B(Y_0,\delta_2) \subset R^n \times R^m,$$

Such that all initial conditions satisfy $(X(0),Y(0)) \in B$, and all trajectories of (1) and (2) satisfy

$$\| H(X(t,X(0))) - Y(t,Y(0)) \| < \varepsilon,\ t \to \infty, \quad (17)$$

where

$$X_m(t) = (x_1(t),\ldots,x_m(t))^T$$

Then the systems in (10) and (11) are said to be in GST with respect to the transformation H.

Theorem 2: If two bidirectional differential systems (10) and (11) are in GST with respect to the transformation $Y = H(X_m)$ given by (16). Then the driven system function $G(Y,X)$ in (11) has the following form:

$$G(Y,X) = H'(X_m)F_m(X,Y) - q(X_m,Y) \quad (18)$$

where

$$H'(X_m) = \begin{pmatrix} \frac{\partial h_1}{\partial x_1} & \frac{\partial h_1}{\partial x_2} & \cdots & \frac{\partial h_1}{\partial x_m} \\ \frac{\partial h_2}{\partial x_1} & \frac{\partial h_2}{\partial x_2} & \cdots & \frac{\partial h_2}{\partial x_m} \\ \vdots & \vdots & \vdots & \vdots \\ \frac{\partial h_m}{\partial x_1} & \frac{\partial h_m}{\partial x_2} & \cdots & \frac{\partial h_m}{\partial x_m} \end{pmatrix}$$

and

$$F_m(X,Y) = (f_1(X,Y),\ f_2(X,Y),\ldots,\ f_m(X,Y))^T .$$

The function

$$q(X_m,Y) = (q_1(X_m,Y), q_2(X_m,Y),\ldots,q_m(X_m,Y))^T$$

guarantees that the zero solution of the following

errorequation is stable on the open set B.

$$\dot{e} = \frac{d(H(X_m) - Y)}{dt} = q(X_m, Y). \quad (19)$$

Proof: Since $H'(X_m)$ is an invertible matrix, the function $G(Y, X_m)$ can be expressed as the form given in (18). Denote

$$\begin{aligned} e &= H(X_m) - Y \\ &= (h_1(X_m) - y_1, h_2(X_m) - y_2, \cdots, h_m(X_m) - y_m)^T, \end{aligned}$$

Then

$$\begin{aligned} \dot{e} &= \frac{d(H(X_m)}{dt} - \frac{dY}{dt} \\ &= (\sum_{i=1}^{m} \frac{\partial h_1(X_m)}{\partial x_i} \frac{dx_i}{dt}, \sum_{i=1}^{m} \frac{\partial h_2(X_m)}{\partial x_i} \frac{dx_i}{dt}, \cdots, \\ &\quad \sum_{i=1}^{m} \frac{\partial h_m(X_m)}{\partial x_i} \frac{dx_i}{dt})^T - G(Y, X) \\ &= H'(X_m) F_m(X, Y) - G(Y, X). \\ &= q(X_m, Y). \end{aligned}$$

Therefore two dynamic systems (10) and (11) are in GST via the transformations H. if, and only if, the function $q(X_m, Y)$ makes the trajectory in (19) tends to zero stably. This completes the proof.

Remark 2. Theorem 2 is constructive. It provides a general approach to construct bidirectional differential generalized stability systems.

IV. Novel Chaotic Systems Based GST Theorems

A. Discrete GST Systems

This subsection presents an 8-dimensional bidirectional discrete chaotic map (8DBDCM) with the GST property, and designs a 12-dimensional discrete chaotic map (12DDCM) based on the GCS theorem and the 8DBDCM, which is the driving system of the 12DDCM.

Step (1): Introduce the 8DBDCM.

The first part of the 8DBDCM is in the following form:

$$X(k+1) = \begin{pmatrix} x_1(k+1) \\ x_2(k+1) \\ x_3(k+1) \\ x_4(k+1) \end{pmatrix}$$

$$= \begin{cases} 0.98x_1(k) + 0.02x_2(k) \\ x_2(k) + 0.01(x_4(k) - x_1(k)x_3(k)) \\ 0.01(x_1(k)x_2(k) + 0.1x_6(k)) + x_3(k) - 0.1 \\ 0.001(x_1(k)^2 - x_2(k)(x_1(k) + 1)) + x_4(k) \end{cases} \quad (20)$$

Secondly, construct an invertible matrix

$$A = \begin{pmatrix} -1 & 0 & 4 & 6 \\ -3 & -2 & 0 & -4 \\ 0 & 5 & -4 & 2 \\ 0 & -1 & 0 & -6 \end{pmatrix} \quad (21)$$

and define the transformation $H: R^4 \to R^4$ as follows

$$H(X) = AX \triangleq (h_1(X), h_2(X), h_3(X), h_4(X))^T. \quad (22)$$

Select $q(X, Y)$ in Theorem 1 to have the form

$$q(X, Y) = e(k+1) = Be(k). \quad (23)$$

where

$$B = \begin{pmatrix} -0.1 & 0 & 0 & 0 \\ 0 & 0.2 & 0 & 0 \\ 0 & 0 & -0.2 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \quad (24)$$

The following Theorem guarantees error equation (9) be zero stable.

Theorem 3: [26] Let B be an $m \times m$ matrix with $\rho(B) \le 1$ and assume that each eigenvalue of B with $|\lambda| = 1$ is simple. Then there is a constant C such that

$$\| e(k) \| \le C \| e(0) \|$$

for every $k \in N$ and $e(0) \in R^m$, where $e(k)$ is solution of

$$e(k+1) = Be(k).$$

In fact, the spectral radius $\rho(B) \le 1$ and each eigenvalue of matrix B with $|\lambda| = 1$ is simple. According to Theorem 3, taking $\| e(k) \| < \frac{\varepsilon}{C}$ gives

$$\| e(k) \| \le C \frac{\varepsilon}{C} < \varepsilon.$$

Therefore the equation (23) is zero stable.

By Theorem 1, we can select the second part of the 8DBDCM to have the form:

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

$$= A[F(X(k), Y(k))] - q(X(k), Y(k)). \quad (25)$$

Moreover, choose the initial conditions as follows:

$$X(0) = (-0.2, 0.2, 0.2, 0.2)^T, \quad (26)$$

$$Y(0) = AX(0). \quad (27)$$

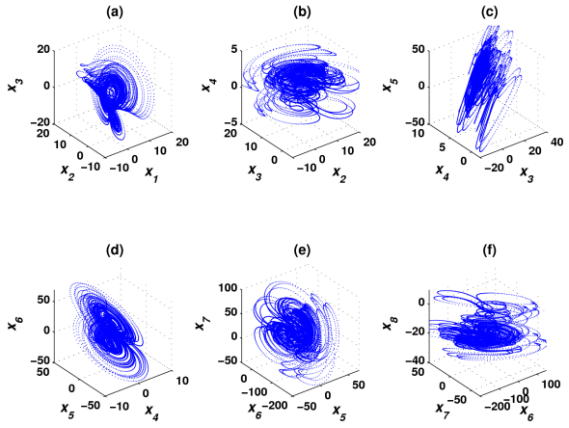

Fig. 1. Chaotic trajectories of variables: (a) $x_1 - x_2 - x_3$, (b) $x_2 - x_3 - x_4$, (c) $x_3 - x_4 - x_5$, (d) $x_4 - x_5 - x_6$, (e) $x_5 - x_6 - x_7$, and (f) $x_6 - x_7 - x_8$.

The calculated Lyapunov exponents of chaotic systems (20) and (25) are {0.00431, 0.00012, 0, 0, - 0.02398, - 1.6095, -1.6095, -2.3022}. This means that systems (20) and (25) are chaotic.

The chaotic trajectories of the state variables $x_1, x_2, x_3, x_4, x_5, x_6, x_7$, and x_8 for the first 20000 iterations are shown in Figs. 1(a)-(f). The evolution of the state variables $k-x_1, k-x_2, k-x_3, k-x_4, k-x_5, k-x_6, k-x_7$, and $k-x_8$ are shown in Fig. 2(a1) - (b4).

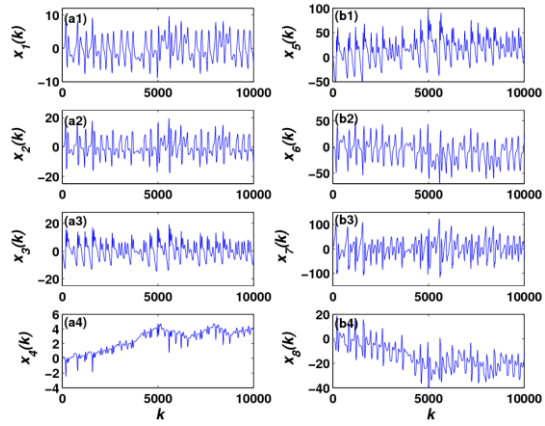

Fig. 2. The evolution of the state variables: (a1) $k-x_1(k)$, (a2) $k-x_2(k)$, (a3) $k-x_3(k)$, (a4) $k-x_4(k)$, (b1) $k-x_5(k)$, (b2) $k-x_6(k)$, (b3) $k-x_7(k)$, and (b4) $k-x_8(k)$.

Fig. 3 (a)-(d) show that $X(k)$ and $Y(k)$ are in generalized synchronization with respect to transformation $H=A$, as the theory predict

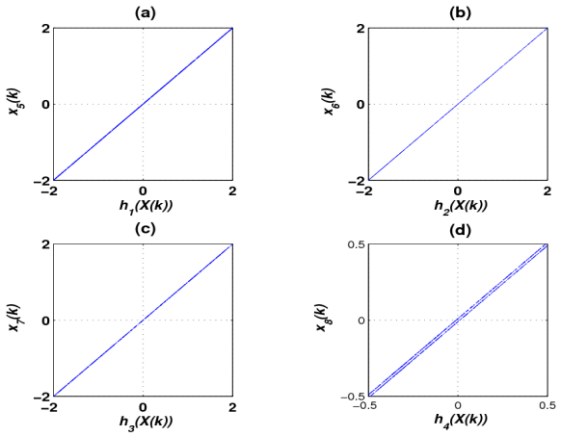

Fig. 3. The state vectors X and Y are in GST with respect to the transformation H. (a) $h_1(X(k))-x_5(k)$, (b) $h_2(X(k))-x_6(k)$, (c) $h_3(X(k))-x_7(k)$, and (d) $h_4(X(k))-x_8(k)$.

Step 2. Introduce a driven system via the 8DBDCM. An invertible matrix C is constructed as follows:

$$C=\begin{pmatrix} -5 & 4 & -1 & -7 \\ -10 & -4 & -2 & 0 \\ -8 & 9 & 6 & -1 \\ 7 & -10 & 6 & 3 \end{pmatrix} \tag{28}$$

Design a transformation $H: R^4 \to R^4$ as follows:

$$H(X)=CX \triangleq (h_1(X), h_2(X), h_3(X), h_4(X))^T. \tag{29}$$

Let

$$q(X_m, Z)=\frac{1}{6}(CX-Z). \tag{30}$$

Select the driven system has the form:

$$Z(k+1)=\begin{pmatrix} z_1(k+1) \\ z_2(k+1) \\ z_3(k+1) \\ z_4(k+1) \end{pmatrix} \tag{31}$$

Then, $q(X_m, Z)$ ensures the error equation

$$\begin{aligned} e(k+1) &= H(X_m(k+1))-Z(k+1) \\ &= q(X_m, Z). \end{aligned} \tag{32}$$

be asymptotically stable. From Theorem 1 in [14] which in a special case of Theorem 1 proposed in section II, it follows that systems (20) and (25) as well as system (31) are GS with respect to the transformation H. Therefore, one can construct a 12DDCM with the GS property.

Moreover, choose (26), (27) and (33) as initial conditions, and choose (33) as follows:

$$Z(0)=AX(0) \tag{33}$$

The chaotic trajectories of the state variables $z_1-z_2-z_3$, $z_1-z_2-z_4$, $z_2-z_3-z_4$, and $z_1-z_3-z_4$ for the first 20000 iterations are shown in Figs. 4(a)-(d). The evolution of the state variables $k-z_1, k-z_2$, $k-z_3$, and $k-z_4$ are shown in Figs. 5(a) - (d).

Fig. 6 (a)-(d) show that $X(k)$ and $Z(k)$ are in generalized synchronization with respect to transformation $H=C$, as the theory predicts.

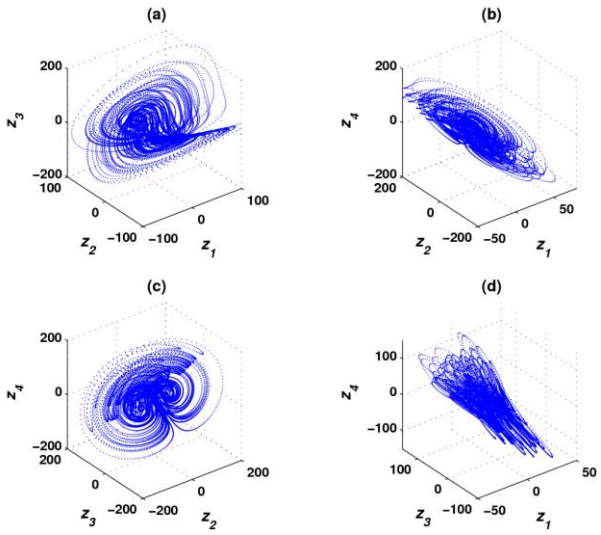

Fig. 4. Chaotic trajectories of variables: (a) $z_1-z_2-z_3$, (b) $z_1-z_2-z_4$, , (c) $z_2-z_3-z_4$, and (d) $z_1-z_3-z_4$.

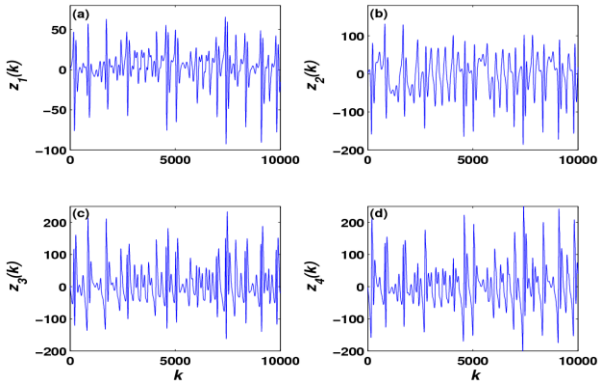

Fig. 5. The evolution of the state variables: (a) $k-z_1(k)$, (b) $k-z_2(k)$, (c) $k-z_3(k)$, and (d) $k-z_4(k)$.

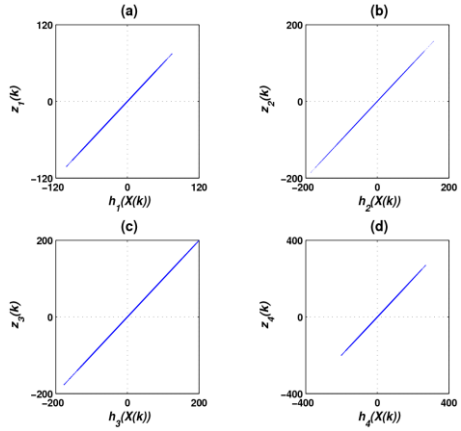

Fig. 6. The state vectors X and Z are in generalizedsynchronization with respect to the transformation H. (a) $h_1(X(k))-z_1(k)$, (b) $h_2(X(k))-z_2(k)$, (c) $h_3(X(k))-z_3(k)$, and (d) $h_4(X(k))-z_4(k)$.

B. *Differential GST Systems*

This subsection presents an 8-dimensional bidirectional continuous chaotic map (8DBCCM) with the GST property, and designs a 12-dimensional continuous chaotic map (12DCCM) based on the GCS theorem and the 8DBCCM, which is the driving system of the 12DCCM.

Step (1): Introduce the 8DBCCM, which is the driving system of the 12DCCM.

The driving system of the 8DBCCM is in the following form:

$$\dot{X}=\begin{cases}\dot{x}_1=20(-x_1+x_2)\\ \dot{x}_2=-x_1x_3+x_4\\ \dot{x}_3=x_1x_2+10\sin(x_6)-80\\ \dot{x}_4=2x_1-4x_2+\cos(x_8)\end{cases} \tag{34}$$

Then, an invertible matrix is constructed:

$$A=\begin{pmatrix}0.6 & 1.6 & 1.4 & 1.6\\ -0.6 & 0.8 & 0 & 1.4\\ 1.2 & -0.2 & 1 & 0\\ 0.2 & 1 & 1.8 & 1.8\end{pmatrix} \tag{35}$$

with the transformation $H:R^4\to R^4$ defined as follows:

$$\begin{aligned}H(X)&=AX\\ &\triangleq(h_1(X),h_2(X),h_3(X),h_4(X))^T.\end{aligned} \tag{36}$$

Let

$$\dot{e}_1=-e_1^3+e_2+2e_3,\ \dot{e}_2=-e_1+e_2^3+2e_4$$
$$\dot{e}_3=-2e_1-e_4,\ \dot{e}_4=-2e_2+e_3$$

Then

$$\dot{e}=(\dot{e}_1,\dot{e}_2,\dot{e}_3,\dot{e}_4)=q(X,Y) \tag{37}$$

makes the error equation (19) be zero stable. In order to proof the equation (37) is zero stable, we can construct Lyapunov function

$$V=e_1^2+e_2^2+e_3^2+e_4^2$$

Then

$$\begin{aligned}\dot{V}&=2e_1\dot{e}_1+2e_2\dot{e}_2+2e_3\dot{e}_3+2e_4\dot{e}_4\\ &=2e_1(-e_1^3+e_2+2e_3)+2e_2(-e_1+e_2^3+2e_4)\\ &\quad+2e_3(-2e_1-e_4)+2e_4(-2e_2+e_3)\\ &=-2(e_1^4+e_2^4)\le 0,\quad (e\ne 0)\end{aligned}$$

Therefore, the equation (37) is zero stable.

Then by Theorem 2, the driven system has the form

$$\begin{aligned}\dot{Y}&=\dot{H}(X)\dot{X}-q(X,Y)\\ &=A[F(X,Y)]-q(X,Y).\end{aligned} \tag{38}$$

Moreover, choose the initial conditions (41) and (42) as

$$X(0)=(1.1,0.2,1,-0.5)^T, \tag{39}$$
$$Y(0)=AX(0). \tag{40}$$

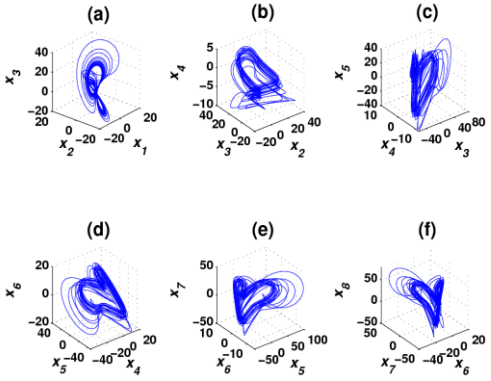

Fig. 7. Chaotic trajectories of variables: (a) $x_1-x_2-x_3$, (b) $x_2-x_3-x_4$, (c) $x_3-x_4-x_5$, (d) $x_4-x_5-x_6$, (e) $x_5-x_6-x_7$, and (f) $x_6-x_7-x_8$.

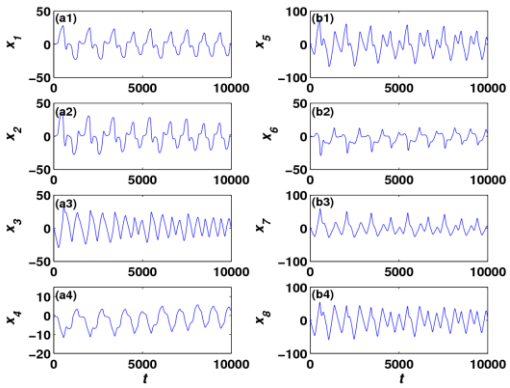

Fig. 8. The evolution of the state variables: (a1) $t-x_1$, (a2) $t-x_2$, (a3) $t-x_3$, (a4) $t-x_4$, (b1) $t-x_5$, (b2) $t-x_6$, (b3) $t-x_7$, and (b4) $t-x_8$.

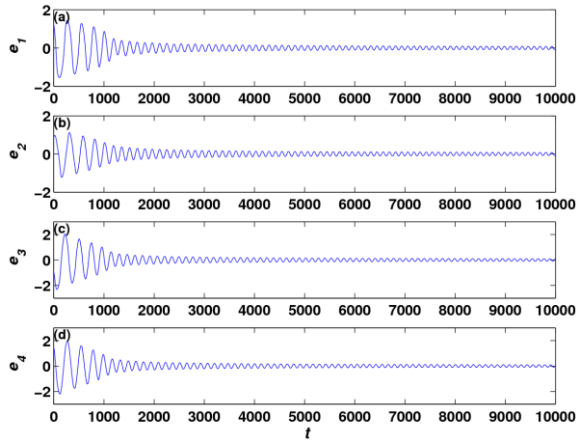

Fig. 9. The evolution of the state variables: (a) $t-e_1$, (b) $t-e_2$, (c) $t-e_3$, (d) $t-e_4$.

The calculated Lyapunov exponents of chaotic systems (34) and (38) are {0.13242, 0.00006, - 0.00072, - 0.00077, - 0.00124, - 0.00357, - 0.38513, - 19.7369}. This means that systems (34) and (38) are chaotic.

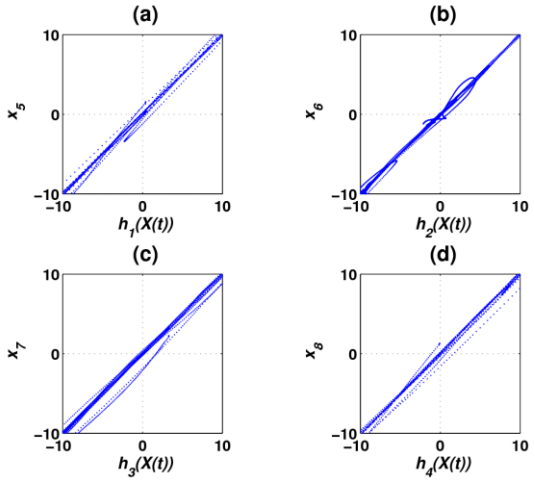

Fig. 10. The state vectors X and Y are in GST with respect to the transformation H .(a) $h_1(X(t))-x_5(t)$, (b) $h_2(X(t))-x_6(t)$, (c) $h_3(X(t))-x_7(t)$, and (d) $h_4(X(t))-x_8(t)$.

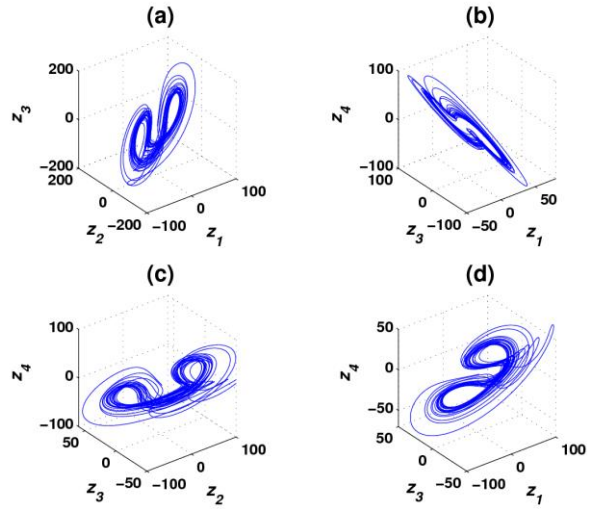

Fig. 11. Chaotic trajectories of variables: (a) $z_1-z_2-z_3$, (b) $z_1-z_2-z_4$, , (c) $z_2-z_3-z_4$, and (d) $z_1-z_3-z_4$.

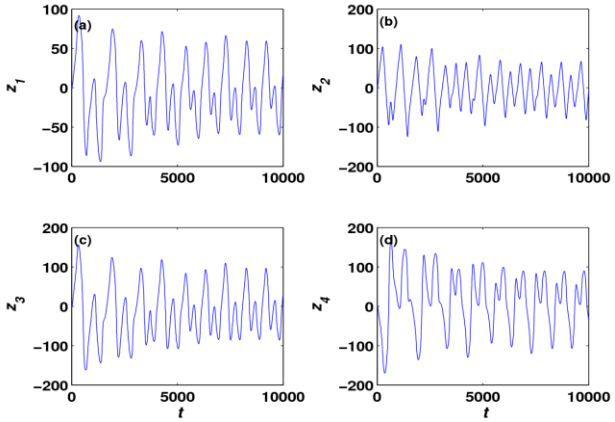

Fig. 12. The evolution of the state variables: (a) $t-z_1(t)$, (b) $t-z_2(t)$, (c) $t-z_3(t)$, and (d) $t-z_4(t)$.

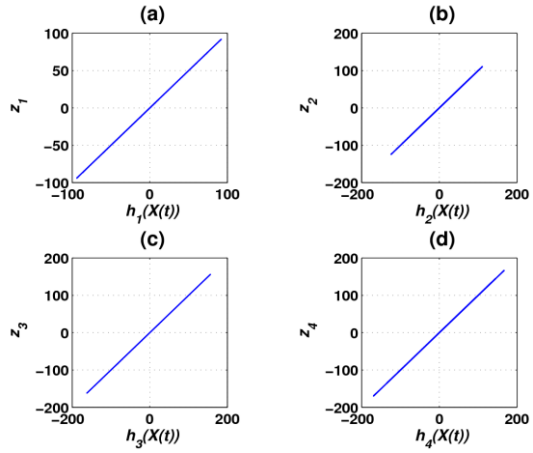

Fig. 13. The state vectors X and Z are in generalized synchronization with respect to the transformation H. (a) $h_1(X(t))-z_1(t)$, (b) $h_2(X(t))-z_2(t)$, (c) $h_3(X(t))-z_3(t)$, and (d) $h_4(X(t))-z_4(t)$.

The chaotic trajectories of the state variables x_1, x_2, x_3, x_4, x_5, x_6, x_7, and x_8 for the first 20000 iterations are shown in Fig. 7 (a)-(f). The evolution of the state variables $t-x_1$, $t-x_2, t-x_3, t-x_4, t-x_5, t-x_6, t-x_7$, and $t-x_8$ are shown in Figs. 8(a1) - (b4). The evolution of the state variables $t-e_1, t-e_2, t-e_3$, and $t-e_4$ are shown in Figs. 9(a) - (d).

Fig. 10 (a)-(d) show that X and Y are in GST with respect to transformation $H=A$, as the theory predicts.

Step 2. Introduce a driven system via the 8DBCCM.

An invertible matrix B is constructed as follows:

$$B=\begin{pmatrix} 2 & 1 & -2 & 2 \\ 2 & -3 & -4 & -2 \\ 2 & 2 & -4 & 4 \\ -1 & -4 & 3 & -4 \end{pmatrix} \tag{41}$$

Design a transformation $H: R^4 \to R^4$ as follows:

$$H(X)=BX \triangleq (h_1(X), h_2(X), h_3(X), h_4(X))^T. \tag{42}$$

Let

$$q(X_m, Z)=\frac{1}{4}(BX-Z). \tag{43}$$

Select the driven system has follows:

$$Z(k+1)=\begin{pmatrix} z_1(k+1) \\ z_2(k+1) \\ z_3(k+1) \\ z_4(k+1) \end{pmatrix} \tag{44}$$

Then, $q(X_m, Z)$ ensures the error equation

$$\begin{aligned} \dot{e} &= \frac{d(H(X_m)-Z)}{dt} \\ &= q(X_m, Z). \end{aligned} \tag{45}$$

be asymptotically stable. Similar to Theorem 2 cited above, we can draw a conclusion that systems (34) and (38) as well as system (44) are GS with respect to the transformation H. Therefore, one can construct a 12DCCM with the GS property.

Moreover, choose (39), (40) and (46) as initial conditions, and choose (46) as follows:

$$Z(0)=AX(0) \tag{46}$$

The chaotic trajectories of the state variables $z_1-z_2-z_3$, $z_1-z_2-z_4$, $z_2-z_3-z_4$, and $z_1-z_3-z_4$ for the first 20000 iterations are shown in Figs. 11(a)-(d). The evolution of the state variables $t-z_1, t-z_2$, $t-z_3$, and $t-z_4$ are shown in Figs. 12 (a) - (d).

Fig. 13 (a)-(d) show that $X(k)$ and $Z(k)$ are in generalized synchronization with respect to transformation $H=B$, as the theory predicts。

V. Chaotic Psuedorandom Number Generator and Psuedorandomness tests

A. Pseudorandom Number Generator

In this section two chaotic psuedorandom number generators (CPRNGs) are designed. The CPRNG1 and CPRNG2 are based on the first discrete system and the differential system in section IV, respectively.

Denote

$$X_i=\{x_i(k)\,|\,k=1,2,3,4\}, \tag{47}$$

$$Y_i=\{y_i(k)\,|\,k=1,2,3,4\}, \tag{48}$$

$$Z_i=\{z_i(k)\,|\,k=1,2,3,4\}, \tag{49}$$

$$W_i=\{w_i(k)\,|\,k=1,2,3,4\}, \tag{50}$$

where $x_i's$, $y_i's$, $z_i's$ and $w_i's$ are defined by (20), (31), (34), and (44).

First, introduce a transformation $T_1: R\to\{0,1,\cdots,2^{16}-1\}$ which transforms the chaotic streams of GST systems (47), (48), (49), and (50) into key streams. Denote

$$S=X_3+Y_2 \tag{51}$$

$$R=Z_2+W_1 \tag{52}$$

Then T_1 is defined by

$$\begin{aligned} T_1(S)=\mathrm{mod}(&round((L(S-\min(S))\\ &/(\max(S)-\min(S))),2^{16}) \end{aligned} \tag{53}$$

$$\begin{aligned} T_1(R)=\mathrm{mod}(&round((L(R-\min(R))\\ &/(\max(R)-\min(R))),2^{16}) \end{aligned} \tag{54}$$

Second, construct a transform $T_2:\{0,1,\cdots,2^{16}-1\}\to\{0,1\}$ which is defined by

$$\begin{aligned} &T_2=T_{22}\circ T_{21} \\ &\text{s.t. } \forall y\in\{0,1,\cdots,2^{16}-1\}^N \\ &T_{21}(y)=dec2bin(y). \end{aligned} \tag{55}$$

Let $u=dec2bin(y)$, then

$$T_{22}(u)=u(:),$$

where $dec2bin$ and $u(:)$ are both Matlab commands.

Finally the transformation $T: R\to\{0,1\}$ is defined via

$$T=T_2\circ T_1 \tag{56}$$

Now we can design a CPRNG based on the transformations (51)-(56) and systems (20) and (31) or systems (34) and (44).

$$S=T(S) \tag{57}$$

is the key stream generated via the CPRNG1.

$$R=T(R) \tag{58}$$

is the key stream generated via the CPRNG2.

The seeds of the CPRNGs are the initial conditions of the GST systems, which can be chosen via random number generators. Therefore the output key streams of the CPRNGs can be obtained via the transformation (56) acting on the chaotic streams of the GST systems (20) and (31) or systems (34) and (44).

B. Pseudorandomness Tests

The FIPS 140-2 test consists of four sub-tests: Monobit Test, Poker Test, Run Test and Long Run Test. Each test needs a single stream of 20,000 one and zero bits from the keystream generator. Any failure in the first three tests means that the corresponding quantity of the sequences falls out the required intervals listed in the second column in Table I. The Long Run test is passed if there are no runs of length 26 or more.

It has been pointed out that the required intervals of the Monotone test and the Pork test correspond significant $\alpha=10^{-4}$ for the normal cumulative distribution and the χ distribution, respectively, and the required intervals of the Run tests correspond approximately the significant $\alpha=1.6\times10^{-7}$ for the normal cumulative distribution ([27], [28]). If we select the significant $\alpha=10^{-4}$ of all tests, the correspond accepted intervals are listed in the third column in Table I.

According to Golomb's three postulates on the

randomness that ideal pseudorandom sequences should satisfy [29], the ideal values of the first three tests should be those listed in the 4th column in Table I.

TABLE I: THE REQUIRED INTERVALS OF THE FIPS 140-2 MONOBIT TEST, PORK TESTS, RUN TEST

Test Item	FIPS140-2 Required Intervals	$\alpha = 10^{-4}$ Required Intervals	Golomb's Postulates
MT	9,725~10,275	9,725~10,275	10000
PT	2.16~46.17	2.16~46.17	χ2 DT
LT	<26	<26	—
k	Run Test	Run Test	Run Test
1	2,315~2,685	2,362~2,638	2,500
2	1,114~1,386	1,153~1,347	1,250
3	527~723	556~694	625
4	240~384	264~361	313
5	103~209	122~191	156
6+	103~209	122~191	156

Here, MT, PT, and LT represent the Monobit test, the pork test and the long run test, respectively. k represents the length of the run of A tested sequence. χ^2 DT represents χ^2 distribution.

TABLE II: THE CONFIDENT INTERVALS OF THE FIPS 140-2 TESTED VALUES OF 1,000 KEY STREAMS GENERATED BY THE CPRNG1, CPRNG2, RC4 PRNG AND ZUC PRNG

Test Item	bits	CPRNG1 Mean ± SD	CPRNG2 Mean ± SD	RC4 Mean ± SD	ZUC Mean ± SD
MT	0	10000 ±73.980	10008 ±71.134	9999.7 ±70.092	9998.4 ±71.843
	1	9999.8 ±73.980	10007 ±71.135	10000 ±70.092	9998.4 ±71.843
PT	-	15.020 ±5.3399	15.047 ±5.3595	14.870 ±5.4330	15.043 ±5.5491
LT	0	13.710 ±1.862	13.549 ±1.782	13.60 ±1.8214	13.488 ±1.829
	1	13.629 ±1.824	13.599 ±1.856	13.642 ±1.931	13.595 ±1.931
k	bits	Run test	Run test	Run test	Run test
1	0	2499.6 ±47.407	2502.2 ±45.778	2500.9 ±45.568	2501.9 ±45.735
	1	2499.9 ±47.627	2502.3 ±47.759	2501.4 ±46.398	2502.7 ±46.121
2	0	1249.9 ±16.394	1250.6 ±32.261	1250.5 ±31.372	1252.1 ±32.606
	1	1248.8 ±33.617	1250.8 ±33.612	1249 ±31.048	1249.5 ±32.221
3	0	625.19 ±23.357	624.89 ±22.706	624.95 ±22.964	624.09 ±22.648
	1	624.96 ±23.181	624.47 ±22.201	625.65 ±22.93	624.64 ±23.455
4	0	311.73 ±16.394	312.27 ±16.485	311.71 ±16.548	312.56 ±16.748
	1	313.15 ±16.561	312.83 ±16.485	312.17 ±16.822	312.72 ±16.506
5	0	156.48 ±11.680	156.55 ±11.776	156.41 ±12.069	155.65 ±12.097
	1	156.82 ±12.453	156.57 ±12.533	156.60 ±11.958	156.66 ±12.369
6+	0	156.40 ±11.807	156.83 ±12.188	156.15 ±11.792	155.75 ±11.719
	1	155.73 ±11.875	156.43 ±11.989	155.79 ±11.979	155.82 ±11.497

Here, SD represents the standard Diviation. *k* represents the length of the run.

The NIST SP800-22 Test Suite [30] consists of 15 statistical tests (see the first column of Table I), which were set for testing the randomness of binary sequences produced by hardware or software-based cryptographic random or pseudorandom number generators [30]. Each statistical test is formulated to test a specific null hypothesis H_0: the sequence being tested is random. A significance level (α) can be chosen for the tests. If $P-value \geq \alpha$, then the null hypothesis is accepted; i.e., the sequence is considered to be random. Typically, α is chosen in the range [0.001, 0.01]. The NIST SP800-22 test suite is more strictly than the FIPS140-2 test suite, NIST; namely, a binary sequence that can pass all tests of FIPS140-2 test suite may not pass all tests in the NIST SP800-22 test suite.

The FIPS 140-2 / SP800-22 test is used to check 1,000 / 100 keystreams, which are randomly generated by CPRNG1 with perturbed randomly initial conditions (26), (33) and the parameters of matrix (28) and CPRNG2 with perturbed randomly initial conditions (39), (46) and the parameters of matrix (41) , respectively. The tested results are shown in the Tables II, III, and IV.

For CPRNG1, there is no sequence failing to pass the FIPS 140-2 test, and there are 12 sequences failing to pass the G FIPS 140-2 test. The statistic test results are listed in the 3th column in Table II. And for CPRNG2, there is no sequence failing to pass the FIPS 140-2 test, and there are 15 sequences failing to pass the G FIPS 140-2 test. The statistic test results are listed in the 4th column of Table II. In Table II the statistic results of the Pork test and the Long Run test are described by mean values ± standard deviation (Mean ± SD). The SP800-22 tested results for CPRNG1 and CPRNG2 are shown in the 2th and 3th columns of Tables III and IV.

ZUC is a stream cipher that forms the heart of the third generation partnership project (3GPP) confidentiality algorithm 128-EEA3 and the 3GPP integrity algorithm 128-EIA3. Using FIPS 140-2 test tests the 1,000 keystreams randomly generated by the ZUC algorithm program (see

Appendix A in [23]). Results show that the 1000 sequences all passed the FIPS 140-2 test criterions, and there are 21 sequences failing to pass the G F140-2 test criterions. The statistic test results are listed in the 6th column in Table II. And using the SP800-22 test tests the 100 keystreams randomly generated by the ZUC suite algorithm. The tested results are shown in the 5th column of Tables III and IV.

TABLE III: THE CALCULATED MEAN *P*-VALUES OF SP800-22 [30] TESTS FOR 100 BINARY SEQUENCES OF LENGTH 10^6 PRODUCED BY THE RC4 PRNG, THE ZUC ALGORITHM [23], THE CPRNG1 AND CPRNG2 PROPOSED IN THIS PAPER, RESPECTIVELY. SELECT THE SIGNIFICANCE LEVEL TO BE A = 0.01

Statistical Test	Mean *p*-value CPRNG1	Mean *p*-value CPRNG2	Mean *p*-value RC4	Mean *p*-value ZUC
1. Frequency	0.49195	0.49790	0.49598	0.46669
2. Block Frequency	0.50943	0.48222	0.47781	0.48780
3. Runs	0.51660	0.50656	0.46958	0.45937
4. Long Runs of Ones	0.53508	0.50755	0.53504	0.45351
5. Binary Matrix Rank	0.51860	0.47726	0.50302	0.47611
6. Spectral DFT	0.48271	0.50772	0.47094	0.50207
7. Non-overlapping Template	0.50058	0.49426	0.49385	0.50045
8. Overlapping Template	0.48686	0.50201	0.50478	0.46822
9. Maurer's Universal Test	0.45849	0.51229	0.48780	0.45006
10. Linear Complexity	0.52159	0.50975	0.51639	0.46828
11. Serial $(m=5,\nabla\Psi^2_m)$	0.54287	0.52256	0.47546	0.48370
Serial $(m=5,\nabla^2\Psi_m)$	0.55143	0.52292	0.48377	0.50556
12. Approximate Entropy	0.57906	0.50284	0.48344	0.45022
13. Cumulative Sum +1	0.52003	0.52161	0.45873	0.46031
Cumulative Sum -1	0.48541	0.50313	0.47298	0.47543
14. Random Excursion	0.32165	0.32664	0.31615	0.29159
15. Random Excursion Variant	0.31142	0.30775	0.30332	0.29350

TABLE IV: ACCEPTANCE RATES OF THE SP800-22 [27] STATISTICAL TESTS FOR 100 BINARY SEQUENCES OF LENGTH 10^6 PRODUCED BY THE RC4 PRNG, THE ZUC ALGORITHM [23], THE CPRNG1 AND CPRNG2 PROPOSED IN THIS PAPER, RESPECTIVELY. SELECT THE SIGNIFICANCE LEVEL TO BE A = 0.01

Statistical Test	Mean *p*-value CPRNG1	Mean *p*-value CPRNG2	Mean *p*-value RC4	Mean *p*-value ZUC
1. Frequency	100	99	98	100
2. Block Frequency	99	100	98	100
3. Runs	99	100	98	100
4. Long Runs of Ones	100	100	97	99
5. Binary Matrix Rank	97	99	97	99
6. Spectral DFT	97	99	98	99
7. Non-overlapping Template	95-100	95-100	94-98	96-100
8. Overlapping Template	98	100	97	100
9. Maurer's Universal Test	99	99	97	100
10. Linear Complexity	99	99	98	98
11. Serial $(m=5,\nabla\Psi^2_m)$	99	100	98	98
Serial $(m=5,\nabla^2\Psi_m)$	99	100	96	99
12. Approximate Entropy	100	100	98	99
13. Cumulative Sum +1	100	99	98	98
Cumulative Sum -1	100	99	98	98
14. Random Excursion	64-66	63-64	57-58	57-58
15. Random Excursion Variant	65-66	63-64	56-58	56-58

TABLE V: THE STATISTIC DATA FOR THE PERCENTAGES OF THE CODES OF THE KEY STREAM CPRNG1 VARIATIONS BETWEEN S AND $S'_p s$ AND S AND $S'_m s$

Item	SV	$S'_p s$	$S'_m s$
DC	min	48.860%	48.890%
	mean	49.999%	49.995%
	max	51.000%	50.985%
CC	min	0.0000042	0.0000005
	mean	0.0055970	0.0057483
	max	0.0228107	0.0221622

The RC4 was designed by Rivest of the RSA Security in 1987, which has been widely used in popular protocols such as Secure Sockets. The RC4 Algorithm based 8-bit segment PRNG can be designed via Matlab commands.

TABLE VI: THE STATISTIC DATA FOR THE PERCENTAGES OF THE CODES OF THE KEY STREAM CPRNG2 VARIATIONS BETWEEN R AND $R'_p s$ AND R AND $R'_m s$

Item	SV	$S'_p s$	$S'_m s$
DC	min	48.965%	48.905%
	mean	50.048%	50.015%
	max	51.090%	51.375%
CC	min	0.0000029	0.0000010
	mean	0.0053481	0.0055299
	max	0.0215035	0.0275045

```
 N = 20000;
K=randint(1,2^L,[0 2^L-1]);
S=[0:2^L-1];j=0;
for i=1:2^L
      j=mod(j+S(i)+K(i),2^L);
         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/L
       i=mod(i+1,2^L);
         j=mod(j+S(i+1),2^L);
           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^L)+1);
end
 C=(dec2bin(C))';
    C=C(:);
      C=bin2dec(C);
```

Here, " $2\wedge L$ " represents 2^L; "randint $(1,2\wedge L,[0,2\wedge L-1])$" generates a vector of uniformly distributed random integers $\{0,1,\cdots,2\wedge L-1\}$ of dimension 2L; "mod" means modulus after division; "zeros(1,N)" is a zero raw vector of dimension N.

Consequently, the RC4 Algorithm Based L-bit segment PRNG is designed. The FIPS 140-2 test is used to test the 1,000 keystreams randomly generated by RC4. There is only one sequence failing to pass the FIPS 140-2 test and there are only 12 sequences failing to pass the G FIPS 140-2 test. The statistic test results are listed in the 5th column in Table II. And using the NIST SP800-22 test tests the 100 keystreams randomly generated by the ZUC algorithm. The tested results are shown in the 4th column of Tables III and IV.

Observe the statistical properties of the pseudorandomness of the sequences generated via the CPRNG1, CPRNG2, RC4 algorithm, and the ZUC algorithm, it follows that the statistical properties of the pseudorandomness of the two CPRNGs are promising.

C. Key Space

The key set parameters of CPRNG1 includes the initial conditions (26) and (33) and the matrix (28) is $C=(c_{i,j})$. It can be proved that if the perturbation matrix $\Delta_1=(c_{i,j})$ satisfies

$$|c_{i,j}|<1.29$$

the matrix $C+\Delta_1$ is still invertible.

The key set parameters of CPRNG2 includes the initial conditions (39) and (46) and the matrix (41) is $B=(\beta_{i,j})$. It can be proved that if the perturbation matrix $\Delta_2=(\beta_{i,j})$ satisfies

$$|\beta_{i,j}|<0.16$$

The matrix $B+\Delta_2$ is still invertible.

Therefore the CPRNG1 and CPRNG2 have 4 + 4 + 16 key parameters denoted by

$$K_S=\{k_1,k_2,\cdots,k_{24}\}. \tag{59}$$

Let the key set be perturbed by

$$K_s(\Delta)=K_s+\{\delta_1,\delta_2,\cdots,\delta_{24}\} \tag{60}$$

where

$$10^{-16}\le|\delta_i|\le 10^{-1},\quad i=1,2,\cdots,24$$

Now we compare the difference between the key stream $S=T(S)$ and $R=T(R)$ with 20000 code length generated by the key set (59) with the 1000 key streams $S_p's$ and $R_p's$ generated by the perturbed key set (60) from our two CPRNGs, respectively.

Comparing the results that are shown in the second row in Table III, and Table IV, respectively. For CPRNG1, the average percent of the different codes is about 49.999%. And for CPRNG2, the average percent of the different codes is about 50.048%. They are very closed to the ideal different value 50%.

Now let us to compare the same key stream S / R with the 1000 stream $S_m's$ / $R_m's$ generated by the function of Matlab command *randi*$([0,1],1,20000)$. The comparing results are shown in Table III and IV. The average percent is about $49.995\%/50.015\%$. The results may suggest that there are no significant correlations between the key stream S / R and the perturbed key streams $S_m's$ / $R_m's$. In summary the key space of each CPRNG is larger than $2\times10^{24\times15}>2^{1196}$.

VI. Concluding Remarks

This study introduces the definitions of GST in bidirectional discrete and differential systems and proposes two constructive GST theorems. They describe the general forms of bidirectional discrete systems or differential equations which are in GST with respect to some given transformations.

Two new 8-dimensional bidirectional GST systems are introduced, and designs two 12-dimensional generalized chaos synchronization (GCS) systems based on the 8-dimensional bidirectional GST systems and the GCS theorem. Numerical simulations suggest that their trajectories display chaotic attractor characteristics.

Two CPRNGs are constructed based on the 12-dimensional GCS systems. Comparing the results of the FIPS 140-2 test and the SP800-22 test for the keystreams generated via the CPRNG1, CPRNG2, the RC4 algorithm and the ZUC algorithm shows that the randomness of the sequences generated via our two CPRNGs are promising. The simulations suggest that the key space of each CPRNG is larger than 2^{1196}. The key space is large enough to against brute-force attacks.

In summary, the GST theorems may describe dynamic behaviors of wider nature phenomena than chaos synchronization (CS) and generalized chaos synchronization (GCS), and provide new tools for various purposes. And the two GST theorems make us be able to design CPRNGs with large key space. Research along this line is promising.

ACKNOWLEDGMENT

This project is supported by the National Natural Science Foundation of China (Grant Nos. 61074192, 61170037).

REFERENCES

[1] T. Y. Li and J. A. Yorke, "Period three implies chaos," *Amer Math Monthly*, vol. 82, pp. 985–992, 1975.
[2] G. Chen and X. Dong, *From Chaos to Order: Methodologies, Perspectives, and Applications*, Singapore: World Scientific, 1998.
[3] J. G. Sprott., *Chaos and Time-Sries Analysis*, Oxford: Oxford University Press, 2003.
[4] T. Yamada and H. Fujisaka, "Stability theory of synchronized motion in coupled-oscillator systems," *II, Progr. Theoret. Phys*, vol. 70, no. 5, pp. 1240–1248, 1983.
[5] V. S. Afraimovich, N. N. Verichev, and M. I. Rabinovich, "Stochastic synchronization of oscillations in dissipative systems," *Izv Vuzov, Radiofiz*, vol. 29, pp. 795–803, 1986.
[6] M. Pecora and L. Carroll, "Synchronization in chaotic systems," *Physical Review Letters*, vol. 64, no. 8, pp. 821–825, 1990.
[7] M. Senator, "Synchronization of two coupled escapement-driven pendulum clocks," *Journal of Sound and Vibration*, vol. 291, no. 3-5, pp. 566–603, 2006.
[8] Z.-M. Ge, C.-H. Li, S.-Y. Li, and C. M. Chang, "Chaos synchronization of double duffing systems with parameters excited by a chaotic signal," *Journal of Sound and Vibration*, vol. 317, no. 3-5, pp. 449–455, 2008.
[9] A. E. Matouk, "Chaos, feedback control and synchronization of a fractional-order modified autonomous van derpolcduffing circuit," *Communications in Nonlinear Science and Numerical Simulation*, vol. 16, no. 2, pp. 975–986, 2011.
[10] F. Rogister, "Impact of modulated multiple optical feedback time delays on laser diode chaos synchronization," *Optics Communications*, vol. 284, no. 13, pp. 3399–3402, 2011.
[11] I. Pehlivan, I. M. Moroz, and S. Vaidyanathan, "Analysis, synchronization and circuit design of a novel butterfly attractor," *Journal of Sound and Vibration*, vol. 333, no. 20, pp. 5077–5096, 2014.
[12] N. Li, W. Pan, L. Yan *et al*., "Enhanced chaos synchronization and communication in cascade-coupled semiconductor ring lasers," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 6, pp. 1874–1883, 2013.
[13] K. Murali and M. Laskshmanan, "Secure communication using a compound signal from generalized synchronizable systems," *Phys. Lett*, vol. 241, pp. 303–310, 1998.
[14] H. Zang, L. Min, and G. Zhao, "A generalized synchronization theorem for discrete-time chaos system with application in data encryption scheme," in *Proc. the 2007 Int. Conference on Communications*, Kokura, Fukuoka Japan: Circuit and Systems, 2007, pp. 1325–1329.
[15] W. Xia and J. Cao, "Adaptive synchronization of a switching system and its applications to secure communications," *Chaos*, vol. 18, p. 023128, 2008.
[16] A. Kanso and M. Ghebleh, "A novel image encryption algorithm based on a 3d chaotic map," *Commun Nonlinear Sci Numer Simulat*, no. 17, pp. 2943–2959, 2012.
[17] J. Sun, Y. Shen, and Q. Yin *et al*., "Compound synchronization of four memristor chaotic oscillator systems and secure communication," *Chaos*, vol. 23, p. 013140, 2013.
[18] L. Min, K. Hu, L. Zhang, and Y. Zhang, "Study on pseudo randomness of some pseudorandom number generators with application," in *Proc. the 9th International Conference on Computational Intelligence and Security*, Leshan, China: IEEE, 2013, pp. 569–574.
[19] L. Min and G. Chen, "Generalized synchronization in an array of nonlinear dynamic systems with applications to chaotic cnn," *J. Bifurcat. Chaos*, vol. 23, no. 1, pp. 1350 016–1-1350 016–53, 2013.
[20] A. Kadir, X. Wang, and Y. Zhao, "Generalized synchronization of diverse structure chaotic systems," *Chinese Physics Letters*, vol. 28, no. 9, pp. 90 503–90 506, 2011.
[21] A. Margheri, "Generalized synchronization in linearly coupled time periodic systems," *Journal of Differential Equations*, vol. 249, no. 12, pp. 3215–3232, 2011.
[22] A. Koronovskii, O. Moskalenko, and A. Hramov, "Generalized synchronization in complex networks," *Technical Physics Letters*, vol. 38, no. 10, pp. 924–927, 2012.
[23] ETSI/SAGE Specification, *Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128- EIA3. Document 2: ZUC Specification; Version: 1.5*, Date: 4th January 2011.
[24] L. Kocarev and U. Parlitz, "Generalized synchronization, predictability and equivalence of unidirectionally coupled dynamical systems," *Phys. Rev. Lett*, vol. 76, pp. 1816–1819, 1996.
[25] Y. Ji, T. Liu, and L. Min, "Generalized chaos synchronization theorems for bidirectional differential equations and discrete systems with applications," *Phys Lett A*, vol. 372, pp. 3645–3652, 2008.
[26] M. Barbarossa, "Stability of discrete dynamical systems," 2011.
[27] L. Min, T. Chen, and H. Zang, "Analysis of fips 140-2 test and chaos-based pseudorandom number generator," in *Proc. the 5th Chaotic Modeling and Simulation International Conference*, Antens, Greece, June 2012, pp. 345–352.
[28] L. Min, T. Chen, and H. Zang, "Analysis of fips 140-2 test and chaos-based pseudorandom number generator," *Chaotic Modeling and Simulation*, no. 2, pp. 273–280, 2013.
[29] S. Golomb, *Shift Register Sequences*, Aegean Park, CA: Laguna Hills, 1982.
[30] R. Rukhin, J. Soto, J. Nechvatal *et al*., *A Statistical Test Suite for Random and Pseudorandom Number Generator for Cryptographic Applications (NIST Special Publication)*, 2001.

Xiuping Yang is currently a master science candidate of School of Mathematics and Physics at the University of Science and Technology Beijing. Her current research interest is chaos generalized synchronization (CGS), pseudorandom number generator and image encryption. She has co-authored to publish three SCI or EI cited papers.

Lequan Min is currently a professor of the Department of Information and Computer Sciences, School of Mathematics and Physics at the University of Science and Technology Beijing. His current research interests are in the areas of image processing, chaos generalized synchronization, chaos cryptography and modeling virus infection dynamics. He is the author and coauthor of over three hundred scientific papers.

Mei Zhang is currently a master science candidate of School of Mathematics and Physics at the University of Science and Technology Beijing. Her current research interest is chaos generalized synchronization, pseudorandom number generator and image encryption.