八维广义同步系统在伪随机数发生器中的应用

韩丹丹*① 闵乐泉② 赵 耿③
①(北京科技大学自动化学院 北京 100083)
②(北京科技大学数理学院 北京 100083)
③(北京电子科技学院 北京 100070)

摘 要：该文提出一类 4 维离散系统。利用系统平衡点处 Jacobi 矩阵的特征值来分析系统在平衡点处的稳定性，建立了一个判别这类系统为周期或混沌的定理。依据该定理构造了一个新的 4 维离散系统。该系统具有正的 Lyapunov 指数，数值模拟显示该系统的动力学行为具有混沌特性。结合该系统和系统广义同步定理构造了一个 8 维广义同步混沌系统。利用该系统构造了一个 16 bit 混沌伪随机数发生器 (CPRNG)，其密钥空间大于 2^{1245}。利用 FIPS 140-2 检测/广义 FIPS 140-2 检测判别标准分别检测由 CPRNG, Narendra RBG, RC4 PRNG 和 ZUC PRNG 生成的 1000 个长度为 20000 bit 的密钥流的随机性。检测结果表明，分别有 100%/99%, 100%/82.9%, 99.9%/98.8%和 100%/97.9%密钥流通过 FIPS 140-2 检测/广义 FIPS 140-2 检测标准。数值仿真显示不同密钥流之间有平均 50.004%不同码。结果说明设计的伪随机数发生器有好的随机性，可以抵抗穷尽攻击。该文提出的 CPRNG 为密码安全的研究与发展提供了新的工具。

关键词：伪随机数发生器；混沌系统；收敛性；广义同步；随机性检测
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2016)05-1158-08
DOI: 10.11999/JEIT150899

Application of 8-dimensional Generalized Synchronization System in Pseudorandom Number Generator

HAN Dandan① MIN Lequan② ZHAO Geng③
①(*School of Automation and Electrical Engineering*, *University of Science and Technology Beijing*, *Beijing* 100083, *China*)
②(*School of Mathematics and Physics*, *University of Science and Technology Beijing*, *Beijing* 100083, *China*)
③(*Beijing Electronic Science and Technology Institute*, *Beijing* 100070, *China*)

Abstract: This paper proposes a class of 4-Dimensional Discrete Systems (4DDSs). Using the eigenvalues of Jacobian matrix of the system at the equilibrium, the stability of the system at the equilibrium is analyzed. A theorem is set up, which is used to determine whether the class systems are periodic or chaotic. Based on the theorem, a 4DDS is constructed. The 4DDS has positive Lyapunov exponent. Numerical simulations show that the dynamic behaviors of the 4DDS have chaotic attractor characteristics as they expects. Combining the 4DDS with Generalized Synchronization (GS) theorem, an 8-Dimensional GS Chaotic System (8DGSCS) is designed. Using this system, this paper designs a 16 bit string Chaotic Pseudo Random Number Generator (CPRNG). Theoretically the key space of the CPRNG is larger than 2^{1245}. The FIPS 140-2 test suit/Generalized FIPS 140-2 test suit are used to test the randomness of the 1000-key streams consisting of 20000 bit generated by the CPRNG, Narendra RBG, RC4 PRNG and ZUC PRNG, respectively. The results show that there are 100%/99%, 100%/82.9%, 99.9%/98.8% and 100%/97.9% key streams passing the FIPS 140-2 test suit/Generalized FIPS 140-2 test suit, respectively. Numerical simulations show that the different key-streams have 50.004% different codes. The results show that the generated CPRNG has good randomness properties, can better resist the brute attack. The designed CPRNG provides a novel tool for the research and development of cryptography.

Key words: Pseudo-Random Number Generator (PRNG); Chaotic system; Convergence; Generalized synchronization; Randomness test

1 引言

混沌是一类在确定性系统中显示类似随机事件的复杂动态行为。混沌系统主要定义在连续或离散的相空间中。它们表现出一些特性，如对初始条件和系统参数的敏感性，遍历性及对长时间混乱行为的无法预测性[1]。1975 年，文献[2]中首次使用到“混沌”。

伪随机数在很多领域有着广泛的应用，如计算

收稿日期：2015-07-30；改回日期：2015-12-18；网络出版：2016-02-19
*通信作者：韩丹丹 hxu1204@163.com
基金项目：国家自然科学基金(61074192, 61170037)
Foundation Items: The National Natural Science Foundation of China (61074192, 61170037)

机仿真[3−6]和信息加密[7−11]等。伪随机数发生器产生不可预知、不可再现的密钥数字串，对信息加密有着重要的作用。知名的伪随机数发生器(PRNGs)统计检测标准包括 DIEHARD 检测[12]，FIPS140 检测[13]和 SP800-22 检测[14]，它们是由美国国家标准与技术研究院(NIST)公布的。

近年来，利用混沌的良好特性来构造伪随机数发生器已成为一个研究的热点[15−19]。较早之前线性同余发生器、移位寄存器序列发生器等随机数发生器相继出现，但这些随机数发生器存在明显的缺陷，即密钥空间小，序列存在长周期等相关现象。基于混沌对初始条件和系统参数的敏感性设计的伪随机数发生器在一定程度上改善了这一缺陷，而且可以增大伪随机数发生器的密钥空间。

利用三角函数，本文提出了一类 4 维离散系统。对离散系统平衡点处 Jacobi 矩阵的特征值进行分析并给出定理及证明，系统在平衡点处不是收敛而是发散的。在离散系统性质定理前提下，构造了一个新的 4 维离散系统。数值模拟说明系统在平衡点处不收敛，不是周期的，是混沌的。基于离散系统广义同步定理构造了一个 8 维混沌系统。利用 8 维混沌系统，本文设计了一个 16 bit 的伪随机数发生器(CPRNG)，其随机性检测结果说明新提出的 CPRNG 具有较好的随机性能。

本文其余部分安排如下：第 2 节提出一类新的 4 维离散系统，并对其平衡点处收敛性进行分析，给出系统的性质定理；第 3 节构造一个新的 4 维离散系统，说明系统的混沌特性。依据离散系统广义同步定理，本文构造一个 8 维广义同步混沌系统；第 4 节利用 8 维混沌系统设计了一个 16 bit 伪随机数发生器，并对其进行了随机性检测和密钥分析；最后，第 5 节总结全文。

2　一类 4 维离散系统

首先，本文提出一类 4 维离散系统，形式为

$$\left.\begin{aligned} x_1(k+1)&=\cos(x_1(k)x_2(k)x_4(k))\\ x_2(k+1)&=\sin(ax_2(k))\\ x_3(k+1)&=\cos(x_3(k))\sin(x_4(k))\\ x_4(k+1)&=\sin(x_2(k)) \end{aligned}\right\} \tag{1}$$

其中 a 为系统参数。下面对离散系统式(1)平衡点处的收敛性进行分析，并给出定理 1 及证明。

定理 1　当参数取值 $\sqrt{\pi^2+1}<a<3.55$ 时，离散系统式(1)是周期或混沌的。

证明　已知在有界空间内的离散系统不是收敛到平衡点，就是周期或混沌的。由系统式(1)基于三角函数构造而成，显然有

$$\sup_{0\le k<\infty}\|x(k)\|\le 1+1+1+1<\infty \tag{2}$$

则 $x(k)$ 是全局有界。

已知系统式(1)的 Jacobi 矩阵为

$$\boldsymbol{J}=\begin{pmatrix} -x_2x_4\sin(x_1x_2x_4) & -x_1x_4\sin(x_1x_2x_4) & 0 & -x_1x_2\sin(x_1x_2x_4)\\ 0 & a\cos(ax_2) & 0 & 0\\ 0 & 0 & -\sin(x_3)\sin(x_4) & \cos(x_3)\cos(x_4)\\ 0 & \cos(x_2) & 0 & 0 \end{pmatrix} \tag{3}$$

解 Jacobi 行列式：

$$|\lambda I-\boldsymbol{J}|=0$$

得系统 Jacobi 矩阵的特征值为

$$\begin{aligned}\lambda=(&-x_2x_4\sin(x_1x_2x_4),a\cos(ax_2),\\ &-\sin(x_3)\sin(x_4),0)\end{aligned} \tag{4}$$

下面求解系统式(1)的平衡点并对平衡点处系统 Jacobi 矩阵的特征值进行分析。设存在平衡点 $c=(c_1,c_2,c_3,c_4)$，且满足

$$c_2=\sin(ac_2) \tag{5}$$

显然 $c_2=0$ 满足条件式(5)，代入系统可得一平衡点 $(1,0,0,0)$，此处系统 Jacobi 矩阵存在一特征值：

$$\lambda_2=a\cos(ac_2)=a \tag{6}$$

已知 $1<\sqrt{\pi^2+1}<a$，则系统 Jacobi 矩阵在平衡点 $(1,0,0,0)$ 处存在一特征值，且特征值大于 1。

又令函数 $y=f(x)=x-\sin(ax)$，$y'=1-a\cos(ax)$，$x\in[-1,1]$。显然函数 $f(x)$ 是一奇函数，且 $f(0)=0$，$f(1)=1-\sin(a)\ge 0$，$f'(0)=1-a$。下面我们只需在区间 $[0,1]$ 内对系统进行讨论。

已知 $1<\sqrt{\pi^2+1}<a$，则 $f'(0)=1-a<0$，由函数连续性可知在区间 $(0,1)$ 上必存在函数值小于 0 的点。又 $f(1)\ge 0$，则由连续函数中值定理，函数 $f(x)$ 在区间 $(0,1)$ 内必存在一零点，则设点为 c_2，即满足 $c_2=\sin(ac_2)$。说明存在平衡点 c。

易知 $\sin(a\cdot\pi/2a)=1$，$\sin(a\cdot\pi/a)=0$。由 $\pi<\sqrt{\pi^2+1}<a$，则 $\pi/2a<1$，$y=f(\pi/2a)=\pi/2a-1<0$，$y=f(\pi/a)=\pi/a>0$，点 $c_2\in(\pi/2a,\pi/a)$。

由式(4)和式(5)可知，在平衡点 c 处的一特征值满足：

$$\begin{aligned}\lambda_2^2&=a^2\cos^2(ac_2)=a^2\left(1-\sin^2(ac_2)\right)\\ &=a^2\left(1-c_2^2\right)>a^2\left(1-\pi^2/a^2\right)=a^2-\pi^2\end{aligned} \tag{7}$$

已知 $a>\sqrt{\pi^2+1}$，则 $a^2>\pi^2+1$，$|\lambda_2|>1$。则系统 Jacobi 矩阵在平衡点 c 处存在一特征值，且特征值大于 1。

由系统 Jacobi 矩阵的特征值 $\lambda_2^2=a^2(1-c_2^2)$，满足 $\lambda_2^2>1$。必须满足 $c_2^2\neq 1$ 才有意义。由式(5)，则 $a\neq \pi/2+k\pi$。已知 $\sqrt{\pi^2+1}<a<3.55$，则 $a\in(\pi/2,\pi/2+\pi)$ 有意义。

综上，系统式(1)存在平衡点，且在平衡点处其 Jacobi 矩阵存在绝对值大于 1 的特征值，则系统在平衡点处不收敛，是发散的。又由系统是全局有界的，则系统在参数 $a\in(\pi^2+1,3.55)$ 上不是周期就是混沌的。 证毕

3 8 维离散混沌广义同步系统

取定系统式(1)的参数 $a=3.5$，得到一个新的 4 维离散系统：

$$\boldsymbol{X}(k+1)=\begin{cases}x_1(k+1)=\cos(x_1(k)x_2(k)x_4(k))\\ x_2(k+1)=\sin(3.5x_2(k))\\ x_3(k+1)=\cos(x_3(k))\sin(x_4(k))\\ x_4(k+1)=\sin(x_2(k))\end{cases} \tag{8}$$

由定理 1 可知系统式(8)不是周期就是混沌的。通过计算，系统 Lyapunov 指数为

$$\{0.78192,-2.3778,-4.1548,-36.984\}$$

存在正的 Lyapunov 指数，说明系统是混沌的。

取定初始值：

$$\boldsymbol{X}(0)=(0.43885,0.22104,0.22495,0.49370)^{\mathrm{T}} \tag{9}$$

状态变量 $\{x_1,x_2,x_3,x_4\}$ 前 5000 次的迭代轨迹图如图 1 所示。

下面取混沌系统式(8)作为广义同步系统的驱动系统，构造一可逆矩阵：

$$\boldsymbol{A}=\begin{pmatrix}-8 & 8 & -5 & 0\\ -4 & 4 & 0 & -5\\ 6 & 0 & 9 & 0\\ -9 & 1 & 0 & 2\end{pmatrix} \tag{10}$$

并定义可逆变换 $\boldsymbol{H}:\mathbb{R}^4\to\mathbb{R}^4$

$$\boldsymbol{H}(\boldsymbol{X})=\boldsymbol{A}\boldsymbol{X}\triangleq\big(h_1(\boldsymbol{X}),h_2(\boldsymbol{X}),h_3(\boldsymbol{X}),h_4(\boldsymbol{X})\big) \tag{11}$$

令

$$\boldsymbol{q}(\boldsymbol{X},\boldsymbol{Y})=\frac{1}{9}\big(\boldsymbol{A}\boldsymbol{X}(k)-\boldsymbol{Y}(k)\big) \tag{12}$$

则由离散系统广义同步定理[20]，得到响应系统，有式(13)形式：

$$\boldsymbol{Y}(k+1)=\boldsymbol{A}\big[\boldsymbol{F}\boldsymbol{X}(k)\big]-\boldsymbol{q}(\boldsymbol{X},\boldsymbol{Y}) \tag{13}$$

由式(12)可保证误差方程渐进稳定，则由离散系统广义同步定义及定理[20]，系统式(8)和式(13)关于变换 $\boldsymbol{H}=\boldsymbol{A}$ 广义同步。

选择初始条件：

$$\boldsymbol{Y}(0)=\boldsymbol{A}\boldsymbol{X}(0)+\boldsymbol{1} \tag{14}$$

状态变量 $\{y_1,y_2,y_3,y_4\}$ 前 5000 次的迭代轨迹图如图 2 所示。混沌映射的动力学行为说明了混沌吸引子特性。由图 3 所示，即使初始条件式(14)有微小扰动，$\boldsymbol{X}(k)$ 和 $\boldsymbol{Y}(k)$ 也会如广义同步定理预测的一样会迅速转变成广义同步的。

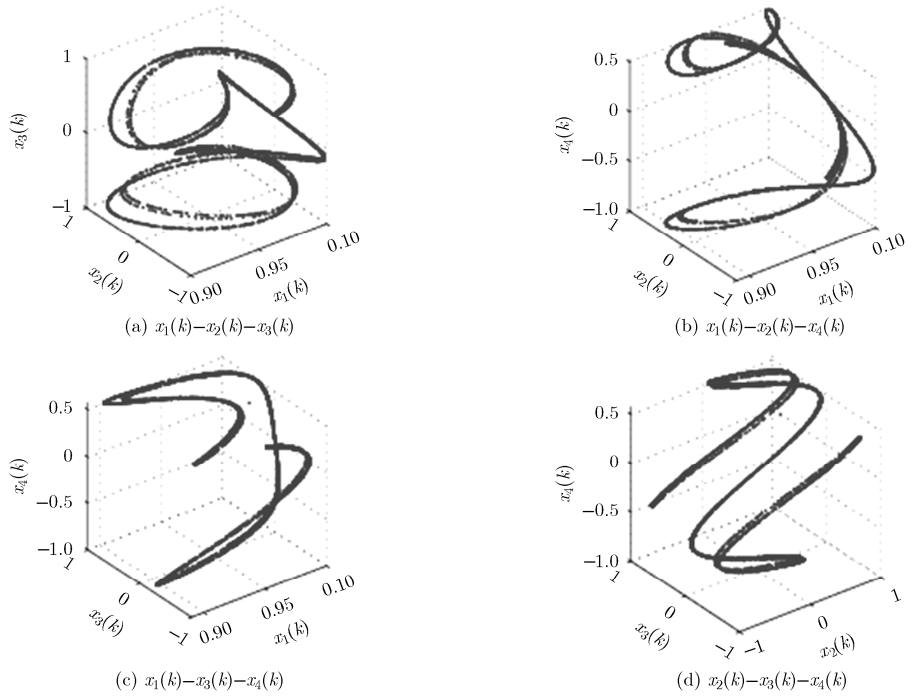

图 1 状态变量 $\{x_1,x_2,x_3,x_4\}$ 的轨迹图

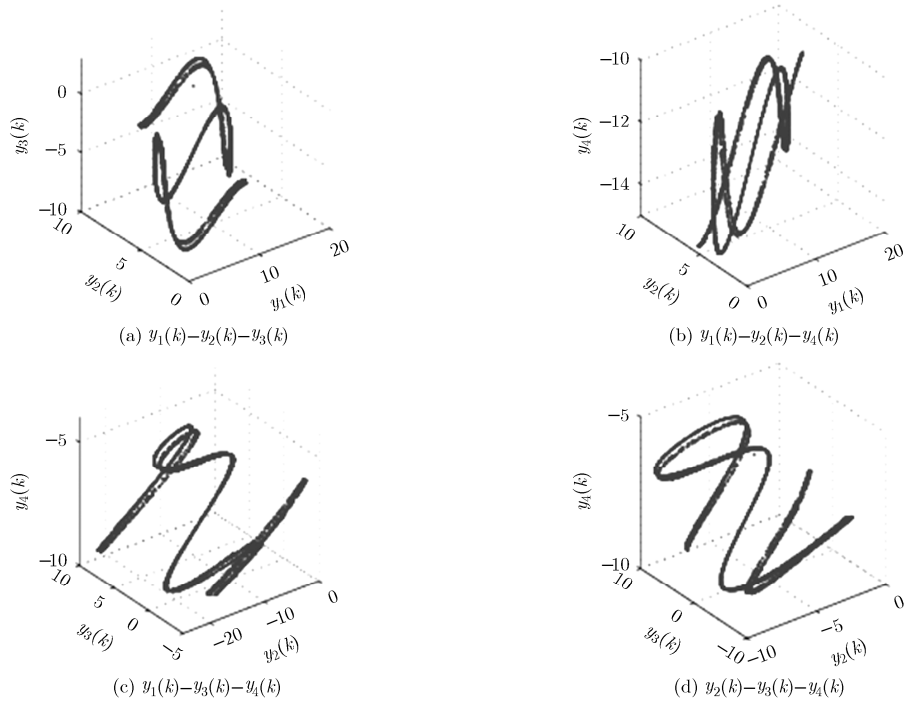

图 2　状态变量 $\{y_1, y_2, y_3, y_4\}$ 的轨迹图

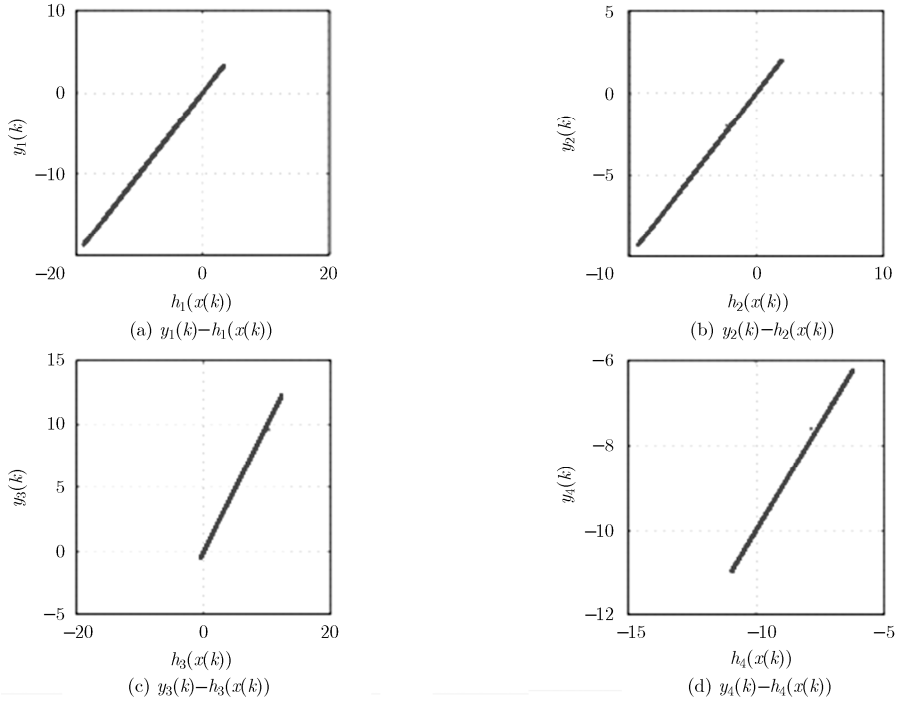

图 3　状态向量 $\boldsymbol{X}$ 和 $\boldsymbol{Y}$ 关于变换 $\boldsymbol{H}$ 广义同步

4　伪随机数发生器及随机性检测

4.1 基于混沌系统的伪随机数发生器

设

$$\boldsymbol{X}_i = \{x_i(k) | k = 1,2,\cdots,N\} \tag{15}$$

$$\boldsymbol{Y}_i = \{y_i(k) | k = 1,2,\cdots,N\} \tag{16}$$

其中 $i = 1,2,3,4$，$x_i's$ 和 $y_i's$ 由广义同步系统式(8)和式(13) 生成。引入变换 $\boldsymbol{T}_1 : \mathbb{R} \to \{0,1,\cdots,2^{16}-1\}$ 将系统式(8)和式(13)的混沌流转变成密钥流：

$$\boldsymbol{T}_1(\boldsymbol{S}) = \mathrm{mod}\left(\mathrm{round}\left(L\frac{S-\min(S)}{\max(S)-\min(S)}\right),\ 2^{16}\right) \tag{17}$$

$$\boldsymbol{S} = \boldsymbol{X}_3 + \boldsymbol{X}_4 + \boldsymbol{Y}_1 + \boldsymbol{Y}_4 \tag{18}$$

其中 $L = 10^{15}$。

基于变换式(17)，式(18)和广义同步系统式(8)和式(13)，我们设计了一个伪随机发生器(CPRNG)。CPRNG 的种子为广义同步系统的初始条件，它们可以通过随机数发生器选定。因此 CPRNG 输出的密钥流是通过变换式(17)，广义同步系统式(8)和式(13)生成的。

4.2 随机性检测

FIPS 140-2 检测包括 4 类检测：Monobit 检测，Poker 检测，Runs 检测和 Long Runs 检测。每种检测都需要密钥流发生器生成 20000 个 0,1 比特流。3 种检测中的任意一次失败都意味着序列的相应检测值没有落入表 1 第 2 列所要求的区间内。如果没有超过长度 26 的游程说明通过 Long Runs 检测。

Monobit 检测和 Poker 检测的接受区间分别对应 α 取值为 10^{-4} 时标准正态分布和 χ^2 分布的置信区间，Runs 检测的相应接受区间对应 α 取值为 1.6×10^{-7} 时标准正态分布的置信区间[21,22]。当对所有的检测选定 $\alpha = 10^{-4}$ 时，相应的接受区间见表 1 的第 3 列(称为 G FIPS 140-2 检测)。根据 Golomb 的 3 个假设[23]，理想随机序列需满足：前 3 种检测的理想值应如表 1 的第 4 列所示。其中，MT, PT 和 LT 分别代表 Monobit 检测，Poker 检测和 Long Runs 检测。k 代表检测序列的游程长度，χ^2 DT 代表 χ^2 分布。

为了检测 CPRNG 的伪随机性能，我们将式(17)定义的 16 bit 密钥流转换成{0,1}比特流。利用 FIPS 140-2 检测包来检测 CPRNG 产生的 1000 个密钥流，密钥流是通过在区间 $|\varepsilon| \in [10^{-16},10^{-1}]$ 内随机扰动初始条件 $X(0)$，$Y(0)$，参数 $\{a\}$ 和矩阵参数 $\boldsymbol{A} = (a_{i,j})$ 产生的。检测结果表明，CPRNG 的所有序列均通过了 FIPS 140-2 检测，有 10 个序列没有通过 GFIPS 140-2 检测。检测结果见表 2 的第 3 列，其中统计结果由均值和标准差 (Mean ± SD)，Mean 代表均值，SD 代表标准差。

表 1 FIPS 140-2 Monobit 检测，Poker 检测，Runs 检测的接受区间

检测项目	FIPS 140-2 接受区间	$\alpha = 10^{-4}$ 接受区间	Golomb's 假设
MT	9,725~10,275	9,725~10,275	10000
PT	2.16~46.17	2.16~46.17	χ^2 DT
LT	<26	<26	–
k	游程检测	游程检测	游程检测
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

文献[17]利用分段线性映射和交叉耦合设计了随机比特发生器 (RBG)。对产生的比特随机序列进行 FIPS 140-2 检测，所有序列均通过了 FIPS 140-2 检测，有 171 个序列没有通过 GFIPS 140-2 检测，结果见表 2 的第 4 列。

RC4 是 1987 年由 RSA 安全的 Rivest 设计的，它被广泛用于协议如网络协议。利用 FIPS 140-2 来检测由 RC4 PRNG 随机生成的 1000 个密钥流。结果显示有 1 个序列没有通过 FIPS 140-2 检测, 有 12 个序列没有通过 GFIPS 140-2 检测。检测结果见表 2 第 5 列。

ZUC 是流密码，它构成了第 3 代合作伙伴计划 (3GPP) 保密算法 128-EEA3 和完整算法 128-EIA3 的核心部分[24]。利用 FIPS 140-2 来检测由 ZUC 算法随机生成的 1000 个密钥流。结果显示 1000 个序列全部通过 FIPS 140-2 检测，有 21 个序列没有通过 G FIPS 140-2 检测。检测结果见表 2 第 6 列。

通过检测 CPRNG, RC4 算法，ZUC 算法和 RGB 生成序列的伪随机性，结果显示本文设计的 CPRNG 随机性能明显更优。

4.3 密钥空间

CPRNG 的参数密钥集包括初始条件 $X(0)$，$Y(0)$，参数 $\{a\}$ 和矩阵参数 $\boldsymbol{A} = (a_{i,j})$。若扰动矩阵 $\boldsymbol{\Delta} = (\delta_{i,j})$ 满足

$$\left|\delta_{i,j}\right| < 0.9822$$

矩阵 $\boldsymbol{A} + \boldsymbol{\Delta}$ 仍然是可逆的。则 CPRNG 有 4+4+1+16 个密钥参数，标记为

$$\boldsymbol{K}_s = \{k_1, k_2, \cdots, k_{25}\} \tag{19}$$

令密钥集做如下扰动：

$$\boldsymbol{K}_s(\boldsymbol{\Delta}) = \boldsymbol{K}_s + [\delta_1, \delta_2, \cdots, \delta_{25}] \tag{20}$$

其中 $10^{-16} \le \left|\delta_i\right| \le 10^{-1}$，$i = 1,2,\cdots,25$。Matlab 使用的是双精度十进制运算。这就意味着每个用于计算的十进制数有 16 bit 精确度。则对每个扰动的密钥参数 $k_i + \delta_i$ (见式(20))，$\left|\delta_i\right| \in [10^{-16},10^{-1}]$，$\delta_i$ 有表达式 $\delta_i = 0.0a_2a_3\cdots a_{16}$，其中 $a_i \in [0,1,\cdots,9]$。根据排列组合理论，我们有 25 个密钥，其密钥空间大于 $10^{15\times25} > 2^{1245}$。

表 2　CPRNG, RBG, RC4 算法和 ZUC 算法生成的 1000 个密钥流的 FIPS140-2 检测值 Mean ± SD

检测项目	比特	CPRNG Mean ± SD	RBG Mean ± SD	RC4 Mean ± SD	ZUC Mean ± SD
MT	0	10000 ± 73.381	10016 ± 21.386	10000 ± 71.472	9998.4 ± 71.843
	1	9999.3 ± 73.381	9983.0 ± 20.379	9998.5 ± 71.278	10002 ± 71.390
PT	–	14.842 ± 5.5091	30.886 ± 5.3596	15.022 ± 5.4730	15.043 ± 5.5491
LT	0	13.625 ± 1.8606	13.000 ± 0	14.004 ± 2.0635	13.488 ± 1.8290
	1	13.669 ± 1.8430	14.000 ± 0	13.596 ± 1.8759	13.595 ± 1.9305
k	比特	游程检测	游程检测	游程检测	游程检测
1	0	2497.3 ± 46.247	2314.4 ± 4.7743	2502.1 ± 49.008	2501.9 ± 45.735
	1	2498.8 ± 46.660	2323.2 ± 8.5951	2499.9 ± 46.437	2502.7 ± 46.121
2	0	1251.1 ± 31.657	1230.2 ± 2.7826	1251.2 ± 31.473	1252.1 ± 32.606
	1	1250.5 ± 31.520	1194.6 ± 3.2024	1249.8 ± 32.095	1249.5 ± 32.221
3	0	625.61 ± 22.490	611.02 ± 3.8995	625.67 ± 22.545	624.09 ± 22.648
	1	625.13 ± 22.450	645.26 ± 2.4608	625.35 ± 23.071	624.64 ± 23.455
4	0	312.65 ± 16.965	304.45 ± 1.8775	312.50 ± 16.961	312.56 ± 16.748
	1	312.21 ± 16.932	323.70 ± 2.0689	312.04 ± 16.874	312.72 ± 16.506
5	0	156.35 ± 12.407	169.58 ± 1.2158	156.00 ± 12.713	155.65 ± 12.097
	1	156.14 ± 11.992	143.21 ± 2.5148	155.94 ± 12.245	156.66 ± 12.369
6+	0	155.93 ± 11.628	189.58 ± 1.2408	156.21 ± 12.331	155.75 ± 11.719
	1	156.13 ± 12.136	189.30 ± 2.3613	156.29 ± 12.372	155.82 ± 11.497

4.4 密钥流的相关性

本节比较长度为 20000 的密钥流 $\boldsymbol{S}=\boldsymbol{T}(\boldsymbol{S})$ 和 $\boldsymbol{S}_p's$ 的不同，其中密钥流 $\boldsymbol{S}$ 和 $\boldsymbol{S}_p's$ 分别由密钥集式(19)和扰动密钥集式(20)生成。分析结果见表 3 的第 3 列，不同码的平均百分比为 50.004%，非常接近理想值 50%。其中 SV 代表统计量，DC 代表不同码，CC 代表密钥流和扰动密钥流的相关系数。

下面来比较 1000 个长度为 20000 的密钥流 $\boldsymbol{S}_p's$，$\boldsymbol{S}_{1p}'s$，$\boldsymbol{S}_r's$ 和 $\boldsymbol{S}_z's$ 的不同码及相关系数，其中密钥流分别由 CPRNG, RBG[17], RC4 PRNG 和 ZUC PRNG 生成，结果见表 3。对 4 个发生器的未扰动密钥 $\boldsymbol{S}$，$\boldsymbol{S}_1$ [17]，$\boldsymbol{S}_{r0}$ 和 $\boldsymbol{S}_{z0}$ 与 1000 个由 Matlab 函数 randi([0,1],1,20000) 生成的密钥流 $\boldsymbol{S}_m's$ 进行比较，结果见表 4。分析结果表明本文设计的 CPRNG 的扰动密钥生成的密钥流几乎是完全独立的。

5　结论

首先，本文提出了一类 4 维离散系统，对其平衡点处收敛性进行了分析，说明系统不会收敛到平衡点。基于这一性质定理，本文得到一新的 4 维离散系统，具有正的李雅普诺夫指数。通过数值仿真说明系统不是周期而是混沌的。然后，利用离散系统广义同步定理生成了一个 8 维混沌广义同步系统。基于 8 维混沌系统，我们设计了一个 16 bit 的伪随机数发生器 (CPRNG)。利用 FIPS 140-2 检测包/广义 FIPS 140-2 检测包分别来检测由 CPRNG

表 3　密钥流 $\boldsymbol{S}$ 和 $\boldsymbol{S}_p's$，$\boldsymbol{S}_1$ 和 $\boldsymbol{S}_{1p}'s$，$\boldsymbol{S}_{r0}$ 和 $\boldsymbol{S}_r's$ 以及 $\boldsymbol{S}_{z0}$ 和 $\boldsymbol{S}_z's$ 之间的统计结果

项目	SV	$\boldsymbol{S}_p's$	$\boldsymbol{S}_{1p}'s$	$\boldsymbol{S}_r's$	$\boldsymbol{S}_z's$
DC(%)	最小值	48.845	48.755	48.850	48.845
	均值	50.004	49.990	50.001	50.014
	最大值	51.045	51.190	51.040	51.120
CC	最小值	0.000008	3.252e−18	0.000021	0.000002
	均值	0.005628	0.0005861	0.005606	0.005584
	最大值	0.023150	0.024899	0.022965	0.023097

表 4 密钥流 $\boldsymbol{S}$ 和 $\boldsymbol{S}_m^{'}\boldsymbol{s}$，$\boldsymbol{S}_1$ 和 $\boldsymbol{S}_m^{'}\boldsymbol{s}$，$\boldsymbol{S}_{r0}$ 和 $\boldsymbol{S}_m^{'}\boldsymbol{s}$ 以及 $\boldsymbol{S}_{z0}$ 和 $\boldsymbol{S}_m^{'}\boldsymbol{s}$ 之间的统计结果

项目	SV	$\boldsymbol{S}$	$\boldsymbol{S}_1$	$\boldsymbol{S}_{r0}$	$\boldsymbol{S}_{z0}$
DC(%)	最小值	48.805	48.710	48.685	49.050
	均值	49.980	49.995	50.001	50.005
	最大值	51.370	51.175	51.090	51.050
CC	最小值	0.000001	0.000003	0.000006	0.000001
	均值	0.005789	0.0005744	0.005347	0.005687
	最大值	0.027414	0.025814	0.026244	0.020992

生成的 1000 个包含 20000 bit 的密钥流的随机性。检测得 100%/99%密钥流通过 FIPS 140-2 检测包/广义 FIPS 140-2 检测包检测。

对 CPRNG 进行密钥和相关性的分析。结果显示本文设计的 CPRNG 密钥空间大于 2^{1245}，不同密钥流之间的不同码平均值为 50.004%。由 CPRNG 的扰动密钥生成的密钥流几乎是完全独立的。分析结果说明本文设计的 CPRNG 足够抵抗穷尽攻击。

参 考 文 献

[1] SPROTT J G. Chaos and Time-sries Analysis[M]. Oxford: Oxford University Press, 2003: 1–120.

[2] LI Tianyan and YORKE J A. Period three implies chaos[J]. *The American Mathematical Monthly*, 1975, 82(10): 985–992.

[3] BARBERIS G E. Non-periodic pseudo-random numbers used in Monte Carlo calculations[J]. *Physica B-Condensed Matter*, 2007, 398: 468–471. doi: 10.1016/j.physb.2007.04.088.

[4] DIAZ N C, GIL A V, and VARGAS M J. Assessment of the suitability of different random number generators for Monte Carlo simulations in gamma-ray spectrometry[J]. *Applied Radiation and Isotopes*, 2010, 68(3): 469–473. doi: 10.1016/j.apradiso.2009.11.037

[5] JOAN M S, JOAQUIN G A, and JORDI H J. J3Gen: a PRNG for low-cost passive RFID[J]. *Sensors*, 2013, 13(3): 3816–3830. doi: 10.3390/s130303816.

[6] HARASE S. On the F2-linear relations of Mersenne Twister pseudorandom number generators[J]. *Mathematics and Computers in Simulation*, 2014, 100(1): 103–113. doi: 10.1016/j.matcom.2014.02.002.

[7] PATIDAR V, PAREEK N K, PUROHIT G, *et al*. A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption[J]. *Optics Communications*, 2011, 284(19): 4331–4339. doi: 10.1016/j.optcom.2011.05.028.

[8] TIAN Hui, ZHOU Ke, and LU Jing. A VoIP-based covert communication scheme using compounded pseudorandom sequence[J]. *International Journal of Advancements in Computing Technology*, 2012, 4(1): 223–230. doi: 10.4156/ijact.vol4.issue1.25.

[9] MIN Lequan and CHEN Guanrong. A novel stream encryption scheme with avalanche effect[J]. *The European Physical Journal B*, 2013, 86(11): 459–472. doi: 10.1140/epjb/e2013-40199-7.

[10] HAZARIKA N and SAIKIA M. A novel partial image encryption using chaotic logistic map[C]. Proceedings of 2014 International Conference on Signal Processing and Integrated Networks (SPIN), Noida, 2014: 231–236.

[11] WANG Xingyuan, LIU Lintao, and ZHANG Yingqian. A novel chaotic block image encryption algorithm based on dynamic random growth technique[J]. *Optics and Lasers in Engineering*, 2015, 66(1): 10–18. doi: 10.1016/j.optlaseng.2014.08.005.

[12] MARSAGLIA G. The marsaglia random number CDROM including the Diehard[OL]. http://www.stat.fsu.edu/pub/diehard/, 1995.

[13] NIST. Fips-pub-140 Security Requirements for Cryptographic Modules[M]. Gaithersburg: NIST Special Publication, 2001: 1–30.

[14] RUKHIN R, SOTO J, NECHVATAL J, *et al*. SP800-22-2001. a statistical test suite for random and pseudorandom number generator for cryptographic applications[S]. 2001.

[15] 王蕾, 汪芙平, 王赞基. 一种新型的混沌伪随机数发生器[J]. 物理学报, 2006, 55(8): 3964–3968.
WANG Lei, WANG Fuping, and WANG Zanji. A novel chaos based pseudorandom number generator[J]. *Acta Physica Sinica*, 2006, 55(8): 3964–3968.

[16] 王华伟. 无理数发生器及确定性随机数发生器[J]. 武汉理工大学学报(交通科学与工程版), 2012, 36(1): 215–218.
WANG Huawei. Irrational number generator and deterministic random bit generator[J]. *Journal of Wuhan University of Technology* (*Transportation Science and Engineering*), 2012, 36(1): 215–218.

[17] NARENDRA K P, VINOD P, and KRISHAN K S. A random

bit generator using chaotic maps[J]. *International Journal of Network Security*, 2010, 10(1): 32–38.

[18] FRANCOIS M, GROSGES T, and BARCHIESI D. Pseudo-random number generator based on mixing of three chaotic maps[J]. *Communications in Nonlinear Science and Numerical Simulation*, 2014, 19(4): 887–895. doi: 10.1016/j.cnsns.2013.08.032.

[19] AKHSHANI A, AKHAVAN A, and MOBARAKI A. Pseudo random number generator based on quantum chaotic map[J]. *Communications in Nonlinear Science and Numerical Simulation*, 2014, 19(1): 101–111. doi: 10.1016/j.cnsns.2013.06.017.

[20] ZANG Hongyan, MIN Lequan, and ZHAO Geng. A generalized synchronization theorem for discrete-time chaos system with application in data encryption scheme[C]. Proceedings of 2007 International Conference on Communications, Kokura, Fukuoka Japan, 2007: 1325–1329.

[21] MIN Lequan, HAO Longjie, and ZHANG Lijiao. Study on the statistical test for string pseudorandom number generators[J]. *Advances in Brain Inspired Cognitive Systems*, 2013, 7888(1): 278–287. doi: 10.1007/978-3-642-38786-9_32.

[22] MIN Lequan, CHEN Tianyu, and ZANG Hongyan. Analysis of Fips 140-2 test and chaos- based pseudorandom number generator[J]. *Chaotic Modeling and Simulation*, 2013, 2(1): 273–280.

[23] GOLOMB S. Shift Register Sequences[M]. Laguna Hills: Aegean Park Press, 1981: 1–100.

[24] ETSI/SAGE TS 35.222-2011. Specification of the 3GPP confidentiality and integrity algorithms 128-EEA3 & 128-EIA3. Document 2: ZUC Specification[S]. 2011.

韩丹丹：女，1989 年生，博士生，研究方向为复杂混沌动力学系统和通信安全.

闵乐泉：男，1951 年生，教授，博士生导师，研究方向为混沌系统的广义同步与安全通信、 复杂系统建模、 细胞神经网络.

赵　耿：男，1972 年生，博士，副教授，研究方向为混沌安全通信.