基于离散广义混沌同步定理的伪随机数生成器设计及性能分析*

韩双霜[1a,2], 闵乐泉[1a,1b], 臧鸿雁[1b]
(1. 北京科技大学 a. 自动化学院; b. 数理学院, 北京 100083; 2. 武警北京指挥学院 信息管理中心, 北京 100012)

摘　要: 为了设计性能较好的伪随机数生成器,基于 3D-Lorenz 系统和离散系统广义同步定理构造了一个具有广义混沌同步性质的新的 6 维离散混沌系统。在此基础上设计了一个混沌伪随机数生成器(CPNG)。利用美国国家标准技术研究院(NIST)提出的 FIPS 140-2 标准对 CPNG 产生的 1 000 个二进制码序列的随机性进行了检测。结果表明,所有的序列都通过了检测。置信区间分析表明设计的 CPNG 产生的伪随机序列具有良好的随机性,比较适合用于信息安全领域。

关键词: 广义同步; 伪随机序列; FIPS 140-2 标准
中图分类号: TN918　　**文献标志码**: A　　**文章编号**: 1001-3695(2013)05-1511-04
doi:10.3969/j.issn.1001-3695.2013.05.059

Generalized synchronization theorem-based chaotic pseudo-random number generator and performance analysis

HAN Shuang-shuang[1a, 2], MIN Le-quan[1a, 1b], ZANG Hong-yan[1b]
(1. *a. School of Automation, b. School of Mathematics & Physics, University of Science & Technology Beijing, Beijing* 100083, *China*; 2. *Information Management Center, Beijing Command College of Chinese People's Armed Police Force, Beijing* 100012, *China*)

Abstract: In order to design good pseudorandom number generator, using a generalized synchronization theorem for discrete chaos system, this paper introduced a new 6-dimensional generalized chaos synchronization system based on 3D-Lorenz map. It designed a chaos-based pseudo-random number generator (CPNG) by the new system. Using the FIPS 140-2 tests issued by the NIST, it verified the random properties of the 1 000 binary number sequences generated via the CPNG. The results show that all the tested sequences passed the FIPS 140-2 test. The confidence interval analysis shows that the sequences have sound random properties. The CPNG is suitable to be used in the information security field.

Key words: generalized synchronization; pseudo-random sequence; FIPS 140-2 tests

0　引言

混沌作为一种特有的非线性动力学现象,具有遍历性、初始状态敏感性、轨道长期不可预测性等特性[1]。近年来混沌学的研究十分活跃[2~4],已经被广泛应用于保密通信中[5~7]。作为混沌学研究范畴中具有巨大应用潜力的混沌同步理论同样已成为各国高科技竞争的一个热点[1]。在此基础上的广义同步混沌理论的发展为构造安全通信系统提供了新的工具[8~13]。

基于文献[10]中的离散系统广义同步理论(generalized chaos synchronization,GCS)理论和 3D-Lorenz 系统[14],本文构造了一个新的 6 维广义混沌同步系统。通过一个从 R^3 到整数域的变换 T, 将该系统产生的混沌流转换为二进制码。利用变换 T 和广义混沌系统设计一个 CPNG,该生成器的种子为混沌广义同步系统的初始条件,密钥为广义混沌系统的参数。

衡量 PNG 性能的两个重要指标是:

a) PNG 产生的伪随机序列的随机性;

b) PNG 的密钥空间。

对于指标 a),可以用伪随机序列的标准对 PNG 产生的大量伪随机序列进行检测,用通过率来衡量 PNG 的性能。对于指标 b),可通过比较 PNG 的不同密钥产生的密钥流间的相关性和不同比特的百分比来确定 PNG 的密钥空间。

用 PNG 产生的优质伪随机序列加密信息,使得攻击者只能通过穷举攻击来破解密文;而同时具有大密钥空间的 PNG,使得攻击者不能在有效时间内通过穷举使攻击解出明文。

本文以 $10^{-16} < |\Delta| < 10^{-5}$ 的精度扰动 CPNG 的种子(初始条件)和密钥(系统参数)1 000 次,用 FIPS 140-2 标准对 CPNG 产生的这 1 000 个密钥流(伪随机{0,1}序列)进行检测, 分析其置信区间,比较不同密钥流的相关性和不同比特的百分比。结果表明序列通过率为 100%。置信区间分析表明该伪随机序列具有良好的随机性。

1　离散广义同步系统和定理

考虑两个系统

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

收稿日期: 2012-08-29; **修回日期**: 2012-10-08　　**基金项目**: 国家自然科学基金资助项目(61074192,61170037)

作者简介:韩双霜(1982-),女,安徽颍上人,讲师,博士研究生,主要研究方向为信息安全(shuangert1@126.com);闵乐泉(1951-),男,教授,主要研究方向为信息安全、图像处理;臧鸿雁(1973-),女,副教授,博士,主要研究方向为信息安全.

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

其中：
$$X(k)=(x_1(k),\cdots,x_n(k))^{\mathrm{T}}\in \mathrm{R}^n, Y(k)\in \mathrm{R}^m \tag{3}$$
$$X_m(k)=(x_1(k),\cdots,x_m(k))^{\mathrm{T}}, m\leqslant n \tag{4}$$
$$F_m(X(k))=(f_1(X(k)),\cdots,f_m(X(k)))^{\mathrm{T}} \tag{5}$$
$$G(X(k),Y(k))=(g_1(X_m(k),Y(k)),\cdots,g_m(X_m(k),Y(k)))^{\mathrm{T}} \tag{6}$$

如果存在一个变换 $H:\mathrm{R}^m\to\mathrm{R}^m$ 和一个集合 $B=B_X\times B_Y\subset \mathrm{R}^n\times\mathrm{R}^m$ 使得当初始条件 $(X(0),Y(0))\in B$ 时，式(1)(2)的解 $(X(k),Y(k))$ 满足 $\lim\limits_{k\to+\infty}\|H(X(k))-Y(k)\|=0$，则称式(1)和(2)关于变换 $H(X(k))$ 在 B 上离散广义混沌同步。且称式(1)为驱动系统，式(2)为响应系统。

定理 1[10] 设 $X,Y,F(X)$ 和 $G(X,Y)$ 定义如式(3)~(6)，$H:\mathrm{R}^m\to\mathrm{R}^m$ 是可逆变换，且 $X_m=V(Y)=H^{-1}(Y)$。如果系统(1)和(2)通过变换 $Y=H(X_m)$ 达到广义混沌同步，那么式(2)中的函数 $G(X,Y)$ 将有以下形式：

$$G(X,Y)=H(F_m(X)-q(X_m,Y)) \tag{7}$$

其中，$F_m(X)=(f_1(X),f_2(X),\cdots,f_m(X))^{\mathrm{T}}$，且 $q(X_m,Y)=(q_1(X_m,Y),q_2(X_m,Y),\cdots,q_m(X_m,Y))^{\mathrm{T}}$ 使得下面的误差方程的零解渐近稳定：

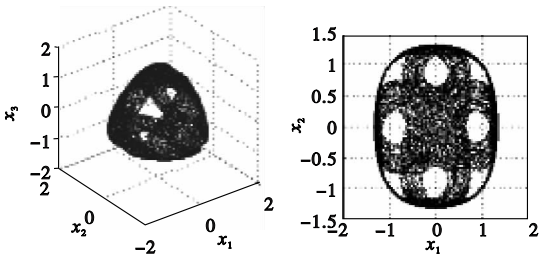
$$e(k+1)=X_m(k+1)-V(Y(k+1))=q(X_m,Y)$$

2 离散广义混沌同步系统

利用定理 1 构造一个新的离散广义混沌同步系统。设离散混沌系统 $X(k+1)=F(X(k))$ 为 3D-Lorenz 系统，其形式为[14]

$$\begin{cases} x_1(k+1)=x_1(k)x_2(k)-x_3(k)\\ x_2(k+1)=x_1(k)\\ x_3(k+1)=x_2(k)\end{cases} \tag{8}$$

该系统的 Lyapunov 指数为：0.07456，0，−0.07456，因此是混沌系统。当 $x_1(0)=0.5, x_2(0)=0.5, x_3(0)=-1$ 时，系统产生的轨道如图 1 所示。



(a) x_1、x_2和x_3 (b) x_1-x_2

图1 3D-Lorenz系统动力学轨道

2.1 构造可逆变换 H

定理 2 设 $A=\begin{pmatrix} a_1 & a_2 & a_3\\ b_1 & b_2 & b_3\\ c_1 & c_2 & c_3\end{pmatrix}$，$\det A\neq 0$，且 $X(k)=(x_1(k),x_2(k),x_3(k))^{\mathrm{T}}\in\mathrm{R}^3$，$Y(k)=(y_1(k),y_2(k),y_3(k))^{\mathrm{T}}\in\mathrm{R}^3$，构造一个变换 $Y(k)=f(X(k))$ 有如下形式：

$$\begin{pmatrix} y_1(k)\\ y_2(k)\\ y_3(k)\end{pmatrix}=A^{-1}\begin{pmatrix}(x_1(k)-a_4)^m\\ (x_2(k)-b_4)^m\\ (x_3(k)-c_4)^m\end{pmatrix}$$

其中 m 为奇数，则该变换为可逆变换。

证明 对于 R^3 中的每一个元素 $Y(k)=(y_1,y_2,y_3)^{\mathrm{T}}$，可得

$$\begin{pmatrix} x_1(k)\\ x_2(k)\\ x_3(k)\end{pmatrix}=f^{-1}\left(\begin{pmatrix} y_1(k)\\ y_2(k)\\ y_3(k)\end{pmatrix}\right)=\begin{pmatrix}(a_1y_1(k)+a_2y_2(k)+a_3y_3(k))^{1/m}+a_4\\ (b_1y_1(k)+b_2y_2(k)+b_3y_3(k))^{1/m}+b_4\\ (c_1y_1(k)+c_2y_2(k)+c_3y_3(k))^{1/m}+c_4\end{pmatrix}$$

由 $f(x(k))=f\left(\begin{pmatrix}(a_1y_1(k)+a_2y_2(k)+a_3y_3(k))^{1/m}+a_4\\ (b_1y_1(k)+b_2y_2(k)+b_3y_3(k))^{1/m}+b_4\\ (c_1y_1(k)+c_2y_2(k)+c_3y_3(k))^{1/m}+c_4\end{pmatrix}\right)=$

$A^{-1}\begin{pmatrix}a_1y_1(k)+a_2y_2(k)+a_3y_3(k)\\ b_1y_1(k)+b_2y_2(k)+b_3y_3(k)\\ c_1y_1(k)+c_2y_2(k)+c_3y_3(k)\end{pmatrix}=A^{-1}A\begin{pmatrix} y_1(k)\\ y_2(k)\\ y_3(k)\end{pmatrix}=\begin{pmatrix} y_1(k)\\ y_2(k)\\ y_3(k)\end{pmatrix}$，即 (y_1,y_2,y_3) 有原像 (x_1,x_2,x_3)。

其次，若 $X(k)\in\mathrm{R}^3$，$\tilde{X}(k)\in\mathrm{R}^3$，且 $f(X(k))=f(\tilde{X}(k))$，即

$$A^{-1}\begin{pmatrix}(x_1(k)-a_4)^m\\ (x_2(k)-b_4)^m\\ (x_3(k)-c_4)^m\end{pmatrix}=A^{-1}\begin{pmatrix}(\tilde{x}_1(k)-a_4)^m\\ (\tilde{x}_2(k)-b_4)^m\\ (\tilde{x}_3(k)-c_4)^m\end{pmatrix}$$

根据矩阵相等的定义可得

$$\begin{cases}(x_1(k)-a_4)^m=(\tilde{x}_1(k)-a_4)^m\\ (x_2(k)-b_4)^m=(\tilde{x}_2(k)-b_4)^m\\ (x_3(k)-c_4)^m=(\tilde{x}_3(k)-c_4)^m\end{cases}$$

因为 m 是奇数，且任意实数开奇次方根其结果存在且唯一，可得 $\begin{cases}x_1(k)=\tilde{x}_1(k)\\ x_2(k)=\tilde{x}_2(k)\\ x_3(k)=\tilde{x}_3(k)\end{cases}$，即对于 R^3 中的不同元素经过 f 变换后得出的像不同。

综上所述文中所构造的变换 f 是可逆变换，证毕。

2.2 构造新的 6 维离散广义同步系统

本文的仿真实验中选取 f^{-1} 为映射 H，$m=3$，

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4\\ b_1 & b_2 & b_3 & b_4\\ c_1 & c_2 & c_3 & c_4\end{pmatrix}=\begin{pmatrix}-1 & 2.5 & 3 & 1\\ 2.1 & 0.3 & 1.6 & -1\\ 1 & 0 & 0.5 & 0\end{pmatrix}$$

则 H 的逆映射 V 为

$$\begin{cases}x_1(k)=0.462(y_1(k)-1)^3-3.846(y_2(k)+1)^3+9.538y_3^3(k)\\ x_2(k)=1.692(y_1(k)-1)^3-10.769(y_2(k)+1)^3+24.308y_3^3(k)\\ x_3(k)=-0.923(y_1(k)-1)^3+7.692(y_2(k)+1)^3-17.077y_3^3(k)\end{cases}$$

取 $q(X_m(k),Y(k))=1/5e(k)=1/5(X(k)-V(Y(k)))=$

$$\frac{1}{5}\begin{pmatrix}x_1(k)-0.462(y_1(k)-1)^3+3.846(y_2(k)+1)^3-9.538y_3^3(k)\\ x_2(k)-1.692(y_1(k)-1)^3+10.769(y_2(k)+1)^3-24.308y_3^3(k)\\ x_3(k)+0.923(y_1(k)-1)^3-7.692(y_2(k)+1)^3+17.077y_3^3(k)\end{pmatrix} \tag{9}$$

则 $e(k+1)=(\frac{1}{5})^{k+1}e(0)$ 使其零解渐近稳定。令响应系统

$$Y(k+1)=G(Y(k),X_m(k))=$$
$$H(F_m(X(k))-q(X_m(k),Y(k))) \tag{10}$$

则由定理 1,式(8)和(10)关于 H 大范围广义混沌同步。由式(8)和(9)可得到

$$F_m(X(k))-q(X_m(k),Y(k))=$$
$$\begin{pmatrix} x_1(k)x_2(k)-\frac{1}{5}[x_1(k)-0.462(y_1(k)-1)^3+ \\ 3.846(y_2(k)+1)^3-9.538y_3^3(k)] \\ x_1(k)-\frac{1}{5}[x_2(k)-1.692(y_1(k)-1)^3+ \\ 10.769(y_2(k)+1)^3-24.308y_3^3(k)] \\ x_2(k)-\frac{1}{5}[x_3(k)+0.923(y_1(k)-1)^3- \\ 7.692(y_2(k)+1)^3+17.077y_3^3(k)] \end{pmatrix}=\begin{pmatrix} M \\ N \\ P \end{pmatrix}$$

则 $Y(k+1)=\begin{pmatrix} \sqrt[3]{-M+2.5N+3P}+1 \\ \sqrt[3]{2.1M+0.3N+1.6P}-1 \\ \sqrt[3]{M+0.5P} \end{pmatrix}$。

取初始条件 $X(0,0,0)=(0.5,0.5,-1)$,$Y(0,0,0)=(-0.3104,-1.7368,0)$,记 $V(Y)=(V_1(Y),V_2(Y),V_3(Y))=H^{-1}(Y)$,则广义同步系统中各状态变量的轨迹如图 2 所示。其中图 2(a)为 $X(k)$ 的混沌轨迹图,(b)为 $Y(k)$ 的混沌轨迹图,(c)为 $V(Y)$ 的轨迹图。当 $q(X_m,Y)=0$ 时,X_1 与 $V_1(Y)$ 的关系如图(d)所示。可看出两者几乎是同步变化的,即关于传递函数 H 广义同步。

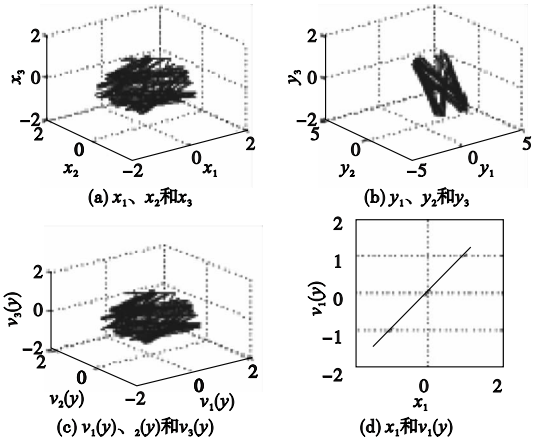


图2　GCS系统中各状态变量轨迹图

3　伪随机数生成器设计及性能分析

3.1　伪随机数生成器设计

为了把驱动系统和响应系统生成的混沌流转换为{0,1,…,255}密钥流,参照文献[12]中的方法引入变换 T。令

$$T(X(k))=\mathrm{mod}(\mathrm{round}(\frac{\sqrt{2}L255(X(k)-\min(X))}{(\max(X)-\min(X))}),256) \tag{11}$$

其中:$X(k)=\sum_{i=1}^{3}k_ix_i(k)y_i(k)$,$L=10^5$,$k_1=k_2=k_3=\sqrt{3}$;$\min(X)=\min\{X(k)\mid k=1,2,\cdots,N\}$,$\max(X)=\max\{X(k)\mid k=1,2,\cdots,N\}$,则二进制序列可以通过变换$\{T(X(k))\}$得到,即

$$s(k)=\mathrm{binary}(T(X(k)))\quad k=1,2,\cdots,N \tag{12}$$

3.2　性能分析

3.2.1　密钥空间

选择广义同步系统的变换矩阵 A 为密钥 k_1,初始条件$\{x_1(0),x_2(0),x_3(0)\}$为生成器的种子 k_2,则 CPNG 的密钥集 $k=k_1\cup k_2$。通过计算可得变换矩阵 A 的稳定性半径为 0.1048,因此以 $10^{-16}<|\Delta|<10^{-5}$ 的精度对密钥集随机扰动 1 000 次仍可保证每次迭代产生的序列都为混沌序列。对生成的 1 000 组密钥流进行相关系数和不同比特百分比的比较(表 1)。可看出 CPNG 产生的各组序列几乎完全独立,两个密钥流的平均不同率为 49.99992%,非常接近理想值 50%,从而可估计 CPNG 的密钥空间为$(10^{16}-10^5)^{12}>2^{636}$。

表 1　1 000 组密钥流间的相关系数绝对值和不同率

比较项	最小值	最大值	平均值
相关系数绝对值	2.2×10^{-20}	0.032 6	0.005 62
不同率/%	48.461 16	51.633 47	49.999 92

3.2.2　伪随机性检测

目前具有代表性的检测标准有 NIST 的 FIPS 140-2 标准、SP800-22 标准、德国资讯安全联合办公室发布的 AIS31 标准和 Marsaglia 的 Diehard battery 检测等。一般认为,通过了这些检测的伪随机序列具有良好的伪随机性能。

本文采用了目前世界上应用比较广泛的 FIPS 140-2 标准来检测所产生的二进制序列的伪随机性。检测分为四个部分:Monobit 检测(MT)、Poker 检测(PT)、游程检测和长游程检测(LT)。每项检测都需要 20 000 bit 长的{0,1}码序列。如果序列结果均在所需区间范围内(见表 2 和 3,其中 MT、PT、LT 分别代表 Monobit 检测、Poker 检测和长游程检测),则序列通过 FIPS 140-2 检测。

表 2　对密钥流的 MT、PT 和 LT 值及理想伪随机系统检测值(Golomb 假设[15])

检测	允许区间	Golomb 假设
MT	9725 ~ 10275	10000
PT	2.16 ~ 46.17	24.165
LT	<26	<26

表 3　密钥流的游程检测以及理想伪随机系统检测值

LR	允许区间	Golomb 假设	LR	允许区间	Golomb 假设
1	2315 ~ 2685	2500	4	240 ~ 384	313
2	1114 ~ 1386	1250	5	103 ~ 209	156
3	524 ~ 723	625	6 +	103 ~ 209	156

对生成器产生的 1 000 组二进制序列进行随机性测试的结果如表 4 ~ 7 所示。

表 4　系统所产生的密钥流的 MT、PT 和 LT 检测结果(1 bit)

检测	min	max	mean	置信区间 $\alpha=0.01$
MT	9792	10213	9997	[9989 10004]
PT	3.3	39	15	[14 16]
LT	10	23	14	[13 14]

表 5　系统所产生的密钥流的 MT、PT 和 LT 检测结果(0 bit)

检测	min	max	mean	置信区间 $\alpha=0.01$
MT	9787	10208	10003	[9996 10011]
PT	3.3	39	15	[14 16]
LT	10	23	14	[13 14]

表 6 系统所产生的密钥流的游程检测结果(1 bit)

LR	min	max	mean	置信区间 $\alpha=0.01$
1	2371	2629	2501	[2496 2506]
2	1141	1352	1248	[1245 1251]
3	557	696	625	[622 627]
4	256	362	313	[311 315]
5	123	194	156	[155 157]
6 +	111	200	157	[156 158]

表 7 系统所产生的密钥流的游程检测结果(0 bit)

LR	min	max	mean	置信区间 $\alpha=0.01$
1	2333	2642	2500	[2495 2505]
2	1165	1344	1250	[1246 1253]
3	551	702	625	[623 628]
4	259	363	313	[311 315]
5	119	202	156	[155 157]
6 +	122	191	156	[155 157]

结果表明新系统所产生的二进制序列都通过了 FIPS 140-2 测试。此外,定义检验的显著水平 $\alpha=0.01$,经检验 CPNG,产生的二进制序列满足正态分布,因此可利用下面的公式求得置信区间。

$$[\bar{x}-t_{n-1,1-\alpha/2}S/\sqrt{n},\bar{x}+t_{n-1,1-\alpha/2}S/\sqrt{n}] \tag{13}$$

其中:$t_{n-1,1-\alpha/2}$ 是学生分布,$\bar{x}$ 为二进制序列的均值,S 是对应的标准差,$\alpha=0.01$。由于游程中要同时对“0”和“1”进行统计分析,因此 $n=200$。置信区间分析表明,伪随机序列具有良好的随机性。

4 结束语

本文提出了一类能达到严格同步的传递函数 H。基于离散广义混沌同步定理和 3D-Lorenz 系统构造了一个新的 6 维广义同步混沌系统。通过引入变换 T 设计了一个产生二进制序列的 CPNG。计算机仿真表明该序列通过了 FIPS 140-2 标准的所有检测。置信区间分析、不同密钥流的相关性和不同比特百分比的数值分析也说明该 CPNG 可应用于信息安全领域。

参考文献:

[1] 方锦清. 驾驭混沌与发展高新技术[M]. 北京:原子能出版社,2002:31-32.

[2] LI T Y, YORKE J A. Period three implies chaos[J]. American Mathematical Monthly,1975,82(10):481-485.

[3] DVORÁKOVÁ J. Chaos in non-autonomous discrete dynamical systems[J]. Communications in Nonlinear Science and Numerical Simulation,2012,17(12):4649-5704.

[4] KARIMI A, PAUL M R. Extensive chaos in the Lorenz-96 model [J]. Chaos,2010,20(4):043105.

[5] CHEN Guan-rong, MAO Yao-bin, CHUI C K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos, Solitons and Fractals,2004,21(3):749-761.

[6] NI Xuan, LAI Ying-cheng. Transient chaos in optical metamaterials [J]. Chaos,2011,21(3):1054-1500.

[7] DENG Xiao-ping, ZHAO Dao-mu. Color component 3D Arnold transform for polychromatic pattern recognition[J]. Optics Communications,2011,284(24):5623-5629.

[8] WANG Xing-yuan, WANG Ya-qin. Adaptive generalized synchronization of hyper-chaos system[J]. International Journal of Modern Physics B,2011,25(32):4563-4571.

[9] YANG Tao, CHUA L O. Generalized synchronization of chaos via linear transformations[J]. International Journal of Bifurcation Chaos in Applied Sciences and Engineering,1999,9(1):215-219.

[10] 臧鸿雁,闵乐泉,吴春雪,等. 基于离散混沌系统广义同步定理的数字图像加密方案[J]. 北京科技大学学报,2007,29(1):97-101.

[11] XIAO Wen-xian, FU Jun-hui, LIU Zhen, *et al*. Generalized synchronization of typical fractional order chaos system[J]. Journal of Computers,2012,7(6):1519-1526.

[12] LI Pei, MIN Le-quan, ZANG Hong-yan, *et al*. A generalized chaos synchronization-based pseudo-random generator number and performance analysis[C]//Proc of International Conference on Communications, Circuits and Systems. [S. l.]:IEEE Press,2010:781-785.

[13] FERNADEZ B. Discontinuous generalized synchronization of chaos [J]. Dynamical Systems,2012,27(1):105-116.

[14] SPROTT J C. Chaos and time-series analysis[M]. Oxford: Oxford University Press, 2003:513.

[15] GOLOMB S W. Shift register sequence [M]. CA: Aegean Park Press,1982:24-59.

(上接第 1510 页)

[3] BALAKRISHNAN G. WYSINWYX: What you see is not what you exe-cute[D]. Wisconsin:University of Wisconsin, 2007.

[4] 张晓锋. 软件逆向工程相关技术研究与实现[D]. 成都:电子科技大学,2007.

[5] TAKANEN J D A, MILLER C. Fuzzing for software security testing and quality assurance [M]. London:Artech House,2008.

[6] YUAN Jing-bo, DING Shun-li. A method for detecting buffer overflow vulnerabilities[C]//Proc of the 3rd IEEE International Conference on Communication Software and Networks. 2011:188-192.

[7] RAWAT S, MOUNIER L. Finding buffer overflow inducing loops in binary executables[C]//Proc of IEEE International Conference on Software Security and Reliability. 2012:177-186.

[8] 胡定文,朱俊虎,吴灏. 基于有限状态自动机的漏洞检测模型[J]. 计算机工程与设计,2007,28(8):1804-1806.

[9] 徐有福,文伟平,万正苏. 基于漏洞模型检测的安全漏洞挖掘方法研究[J]. 信息网络安全,2011(8):72-75.

[10] SREEDHAR V C, GAO G R, LEE Y F. Identifying loops using DJ graphs[J]. ACM Trans on Programming Languages and Systems,1996,18(6):649-658.

[11] FLAKE H. More fun with graphs[K]. [S. l.]:Black Hat Federal, 2003.

[12] SILBERMAN P. Loop detection[EB/OL]. [2012-08-10]. http://old. idapalace. net/papers/loopdetection. pdf.

[13] Hex-Rays. Hex-Rays decompiler v1.0[EB/OL]. [2012-08-10]. http://www. hex-rays. com/files/hexrays_info. pdf.