基于耦合 Logistic 映射的伪随机位发生器及其在混沌序列密码算法中的应用*)

邓绍江[1] 李传东[1,2] 廖晓峰[1]

(重庆大学计算机学院 重庆400044)[1] (重庆大学数理学院 重庆400044)[2]

Pseudo-Random Bit Generator Based on Coupled Logistic Maps and its Applications in Chaotic Stream-Cipher Algorithms

DENG Shao-Jiang[1] LI Chuan-Dong[1,2] LIAO Xiao-Feng[1]

(College of Computer Sceince and Engineering, Chongqing University, Chongqing 400044)[1]

(College of Mathematics and Physics, Chongqing University, Chongqing 400044)[2]

Abstract In this paper, the recent progress on chaotic cryptography is summarized firstly. Then a novel pseudo-random bit generator based on coupled Logistic maps is proposed. Theoretical analysis and numerical experiments illustrate that it is superior to those in the literature. Finally, some examples are given to demonstrate the applications in the stream-cipher algorithms.

Keywords Chaos, Cryptography, Logistic map, Pseudo-random bit generator, Stream-cipher

1. 引言

近年来,混沌密码学得到了大量的研究,各种混沌加密算法的设计方案不可胜数,其中大多数混沌加密系统基于离散时间、离散值系统。由于连续值系统定义在连续域上,使得一些传统密码学技术(如 Shannon 熵)不能直接推广到这种系统,再加上性能分析和实现上的复杂性,人们对连续值系统的研究还较少[6]。目前,混沌密码系统主要有两种类型:混沌序列密码和混沌分组密码。

·混沌序列密码:使用混沌系统产生伪随机密钥序列加密明文得到密文。大量的混沌系统已被用作伪随机序列发生器,如: 2-D Hénon map[13], Logistic map[14], 广义 Logistic map[15], 拟混沌非线性滤波器[16], 分段线性混沌映射[2,17~20]等等。

·混沌分组密码:一种方法是用明文作为初始条件/控制参数,迭代/反迭代混沌系统产生/恢复 密文/明文[21~26]。另一种方法是将混沌吸引域分成 N 个 ε-区域,每个 ε-区域对应一个或多个字符,迭代混沌映射,以轨道点落入字符 s 对应的 ε-区域 N_S 时的迭代次数作为密文。解密时只需从相同的初始条件出发,迭代 N_S 即得明文[4]。其他方法可参见文[4]及其参考文献。

然而,现有的大多数混沌加密算法缺乏严格的安全性和性能分析,而且许多系统已被证明是不安全的[11],更多的系统则性能较差[3,6]。我们认为要从密码学的观点考虑混沌系统并对所设计的密码系统的密码学属性进行全面而仔细的分析与评价。因此,研究人员首先要清楚密码学与混沌理论的基本关系以及使用混沌系统的基本原则。

已有的研究[6]表明混沌与密码学之间有许多相似之处,也有对混沌密码学影响巨大的差别,详见表1。

表1 混沌理论与密码学之间的关系

	混沌理论	传统密码学
相似点	对初始条件和控制参数的极端敏感性	扩散
	类似随机的行为和长周期的不稳定轨道	伪随机信号
	混沌映射通过迭代,将初始域扩散到整个相空间	密码算法通过加密轮产生预期的扩散和混乱
	混沌映射的参数	加密算法的密钥
不同点	混沌映射定义在实数域内	加密算法定义在有限集上
	?	密码系统的安全性和性能

为加密算法选择混沌映射也不是一件容易的事情。我们认为选取的混沌映射应具有如下属性:混和属性、鲁棒混沌和大的参数集。需要指出具有以上属性的混沌系统不一定安全,但不具备上述属性则得到的混沌加密系统必然是弱的。

·混和属性:将明文看作初始条件域,则混和属性是指将单个明文符号的影响扩散到许多密文符号中去。显然,该属性对应密码学中的扩散属性。具有混和属性的系统具有较好的统计特性:当迭代轮数→∞时,密文的统计性质不依赖于明文的统计性质,从而由密文的统计结构不能得到明文的结构。

·鲁棒混沌:鲁棒混沌是指在小的参数扰动下,系列仍保持混沌状态。但是,一般来讲大多数混沌吸引子不是结构稳定的,而非鲁棒混沌的系统具有弱密钥。例如,Logistic 映射式(1)不是鲁棒混沌的。在 r=4附近扰动时,系统结构不稳定。因此选择混沌系统时要倍加小心。

·大的参数集:密码系统安全性的一个重要的衡量指标是 Shannon 熵,即密钥空间的测度,在离散系统中常用 $\log_2 K$ 近似,其中 K 为密钥的数目。因而,动力系统的参数空间越大,离散系统中反应的 K 就越大。

综上所述,选择混沌系统中,我们应该考虑在大的参数集

*)国家自然科学基金(60271019),教育部博士点专项基金(20020611007),重庆市科委应用基础研究(7370)和重庆大学校内基金(713411003)资助。

中具有鲁棒混沌和混和属性的系统。根据以上思想，本文基于耦合的 Logistic 映射提出了一种新颖的伪随机位发生器(PRBG)。它具有完美的密码学属性，以此构造的序列密码系统具有安全性高，加密速度快和易于实现的特点。

2. 基于耦合 Logistic 映射的伪随机位发生器(CLM—PRBG)

考虑 Logistic 映射：

$$y_{n+1}=r\cdot y_n\cdot(1-y_n) \tag{1}$$

其中 $y\in[0,1]$，$r\in[0,4]$。

Logistic 映射在混沌理论中已被广泛研究，而且易于实现，因此它被广泛用于数字混沌密码系统[4,27~29]。但是只有当控制系数 $r=4$时，Logistic 映射才是一个满射且有完美的混沌特性，因此在这些密码中 r 必须选择在 $r=4.0$附近，这就使得密钥空间非常小。其它易于实现的映射是分段线形映射，比如 Tent 映射和推广的 Tent 映射[17~20,30~31]。为了提高分段线性映射的复杂性以及克服有限精度所造成的动力学行为的退化，文[2]采用了耦合和扰动的技术。虽然，上述基于分段线性映射的密码系统易于实现，加密速度快，但终因分段线性的安全性不高。为此，我们修改非线性映射——Logistic 映射使之具有前节中列出的几种属性。在式(1)中，取 $r=4$，令 $y=x+p \pmod 1$，$x\in[0,1]$，p 为任意非负实数，得如下系统：

$$x+p \bmod(1)=4(x+p \bmod(1))(1-(x+p) \bmod(1)) \tag{2}$$

对任意给定得 $p\in R^+$。系统式(1)和系统式(2)拓扑共轭，从而系统为混沌系统，这就使得混沌系统(2)在一个大的参数空间($p\in[0,+\infty]$)内具有鲁棒混沌，而混沌系统对参数的敏感性以及由此产生的遍历性保证了系统式(2)的混和属性。

但混沌系统在有限精度下离散实现时会出现严重的退化，如短周期等，忽视这个问题必将降低密码系统的安全性。工程上已有几种方法可以解决这些精度问题，如使用较高的有效精度、基于扰动的算法以及耦合多个混沌系统。在我们的设计中，采用扰动和耦合的组合方法解决了这个问题，同时也增加了系统的分析复杂性。

我们提出如下系统：

$$\begin{cases} y_1(i+1)=4y_1(i)(1-y_1(i)) \\ y_2(i+1)=4y_2(i)(1-y_2(i)) \end{cases} \tag{3}$$

其中 $y_n=x_n+p \pmod 1$，$x_n\in[0,1]$，$p\in(0,1)$。

从而上述系统也可写成，

$$\begin{cases} (x_1(i+1)+p_1) \pmod 1=4[(x_1(i)+p_1) \pmod 1][1-(x_1(i)+p_1) \pmod 1] \\ (x_2(i+1)+p_2) \pmod 1=4[(x_2(i)+p_2) \pmod 1][1-(x_2(i)+p_2) \pmod 1] \end{cases} \tag{4}$$

$\forall p_1,p_2\in(0,1)$，取初值 $x_1(0)$，$x_2(0)$，得两个混沌轨道$\{x_1(i)\}$，$\{x_2(i)\}$。

$$\text{令：}g_1(x_1)=\begin{cases}1 & x_1+p_1 \pmod 1\geqslant 1/2\\ 0 & x_1+p_1 \pmod 1<1/2\end{cases}$$

$$g_2(x_2)=\begin{cases}1 & x_2+p_2 \pmod 1\geqslant 1/2\\ 0 & x_2+p_2 \pmod 1<1/2\end{cases}$$

$$g(x_1,x_2)=g_1(x_1)\oplus g_2(x_2) \tag{5}$$

则 $K(i)=g(x_1(i),x_2(i))\quad i=0,1,\cdots\cdots$ (6)

为一伪随机位序列。我们称上述伪随机位发生器为基于耦合 Logistic 映射的伪随机发生器，简记为 CLM－PRBG。

为了得到密码学上所要求的长周期，我们采用文[2]中的扰动算法。具体方法如下：用两个 m-LFSR 产生2个伪随机分布信号，并用这两个信号分别扰动$\{x_1(i)\}$和$\{x_2(i)\}$的最低的 L-位，扰动时间间隔分别为△1，△2，取 $L\geqslant[\lambda\cdot\log_2 e]\geqslant[1.44\cdot\lambda]$，其中 λ 为受扰混沌映射的 Lyapunov 指数，$\lceil x\rceil$表示不小于 x 的最小整数，从而，当有限计算精度为 n-位时，两个信号经一次迭代后的最小差别2^{-n}将变成 $e^{\lambda}\cdot 2^{-n}\cdot(2^{-n+l})$。带有扰动的 CLM-PRBG 如图1所示。

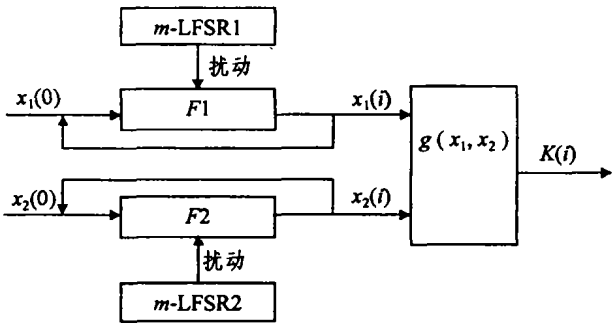

图1　带扰动的 CLM-PRBG

3. CLM-PRBG 的密码学属性

一个好的伪随机位发生器除运行速度快，易实现外，还要求它所产生的位序列$\{K(i)\}$具有一系列的密码学属性。如{0,1}上的均衡性、较长的周期、较高的线性复杂性，以及零相关和类似 δ 的自相关性等等。下面从理论上说明我们设计的 CLM-PRBG 具有所有以上属性，数值实验结果(见第4节)也进一步验证了理论分析。

3.1　0-1均衡性

容易计算 Logistic 映射式(1)在 $r=4$时的轨道点的概率密度：

$$f_Y(y)=\frac{2}{\pi}\frac{1}{\sqrt{1-(2y-1)^2}},0<y<1$$

由此，我们可以得到混沌映射式(2)的轨道点的概率密度函数：

$$f(x,p)=\begin{cases}\dfrac{2}{\pi}\cdot\dfrac{1}{\sqrt{1-[2(x+p)-3]^2}}, & 1-p<x<1\\ \dfrac{2}{\pi}\cdot\dfrac{1}{\sqrt{1-[2(x+p)-1]^2}}, & 0<x<1-p\end{cases}$$

定理1　由(4)，(5)，(6)式给出的 CLM-PRBG 满足 $P\{K(i)=0\}=P\{K(i)=1\}$，即$\{K(i)\}$在{0,1}上均衡取值。

证明：首先证明 $g_1(x_1)$和 $g_2(x_2)$所产生的序列是0－1均衡的。实际上，

$$P\{g_1(x_1)=0\}=P\{(x_1+p_1) \pmod 1<\frac{1}{2}\}$$

$$=\int_{(x+p_1) \pmod 1<1/2} f(x,p_1)dx=\int_0^{\frac{1}{2}} f_Y(y)dy$$

$$=\int_0^{\frac{1}{2}}\frac{2}{\pi}\cdot\frac{1}{\sqrt{1-(2y-1)^2}}dy=0.5$$

$$p\{g_1(x_1)=1\}=p\{(x_1+p_1) \pmod 1\geqslant\frac{1}{2}\}=$$

$$\int_{\frac{1}{2}}^1\frac{2}{\pi}\frac{1}{\sqrt{1-(2y-1)^2}}dy=0.5$$

即 $P\{g_1(x_1)=0\}=P\{g_1(x_1)=1\}=0.5$。同理可证 $P\{g_2(x_2)=0\}=P\{g_2(x_2)=1\}=0.5$

另外，根据组合操作 XOR(异或) 的定义，我们有：

$P\{K(i)=0\}=P\{g_1(x_1(i))=0\}\cdot P\{g_2(x_2(i))=0\}+P\{g_1(x_1(i))=1\}\cdot P\{g_2(x_2(i))=1\}=0.5\times 0.5+0.5\times 0.5=0.5$

同理，

$P\{K(i)=1\}=0.5$

显然，以上推导是基于连续条件的。事实上，当混沌系统在扰动下离散实现时，每个混沌轨道都会被扰动到某一个附近轨道。因此，所有的轨道都会光滑地服从于 $f(x,p)$ 的离散形式的概率密度。对 $f(x,p)$ 的离散情形，上述推导仍成立，即

$P\{K(i)=0\}\approx P\{K(i)=1\}$

3.2 长周期

当遍历混沌系统连续实现时，对几乎任意的初始条件，轨道的周期都是无限的，但是。正像第2节所指出的，当混沌系统在有限精度下实现时就会出现短周期问题。下面，我们说明加入适当的扰动可以解决这个问题。我们用两个 m-LFSR 作为扰动伪随机数发生器(PRNG)，它们的长度分别为 L_1,L_2，扰动时间间隔分别为 Δ_1,Δ_2，则 $x_1(i),x_2(i)$ 的周期分别为

$\sigma_1\Delta_1(2^{L_1}-1),\sigma_2\Delta_2(2^{L_2}-1)$

其中 σ_1,σ_2 为两个正整数[2]，这样，$\{K(i)\}$ 的周期将为：

$Lcm(\sigma_1\Delta_1(2^{L_1}-1),\sigma_2\Delta_2(2^{L_2}-1))$

其中 $Lcm(s,t)$ 表示 s,t 的最小公倍数。

若选择的 Δ_1,Δ_2 和 L_1,L_2 满足

$Gcd(\Delta_1,\Delta_2)=1, Gcd((2^{L_1}-1),(2^{L_2}-1))=1$

则 $\{K(i)\}$ 的周期将为：

$L=Lcm(\sigma_1,\sigma_2)\cdot\Delta_1\cdot\Delta_2\cdot(2^{L_1}-1)\cdot(2^{L_2}-1)\approx Lcm(\sigma_1,\sigma_2)\cdot\Delta_1\cdot\Delta_2\cdot 2^{L_1+L_2}$

其中 $Gcd(s,t)$ 表示 s,t 的最大公约数。由此可见，对大多数安全应用来说，该周期是足够长的。

3.3 复杂性及相关性分析

确定性系统的演化完全由参数空间和初始条件所决定，但是，要完全确定参数和初始条件需要无限多的信息和无限精度的测量系统，这都是不易做到的。但是混沌系统离散实现时，情况就大不一样了：这等价于将相空间分成有限个区域，观察在这些区域上的演化规律。由此导出的粗粒动力学称为符号动力学，而且 Logistic 映射式(1)的0-1符号动力学已日臻完美[32]。现有的理论表明，在混沌吸引域内，对任意的初始条件 Logistic 映射具有唯一的概率分布。因此，只要 $x_1(0)\neq x_2(0)$ 或者 $p_1\neq p_2$，动力系统式(4)所产生的混沌序列 $\{x_1(i),x_2(i)\}$ 是渐近独立的，从而 $g_1(x_1(i),p_1),g_2(x_2(i),p_2)$ 也是独立的。由此可知 $\{K(i)\}$ 独立分布。在文[33]中，作者证明了独立同分布的二进制序列有1/2序列长度的线性复杂性。这样 $\{K(i)\}(i=1,2,\cdots,n)$ 就有接近 $n/2$ 的高线性复杂性($n\leqslant L$)。同时，由于 $\{K(i)\}$ 独立同分布，它有类似 δ 的自相关性和几近于0的互相关性。

3.4 实验

选择有限计算精度 $n=32$，两个 m-LFSR 的长度分别为 $L_1=16,L_2=17$，扰动的间隔分别为 $\Delta_1=99,\Delta_2=102$。预选代次数 $m=20$，初始条件和控制参数随机产生。随机选取 $\{K(i)\}$ 的一个大的子序列(比如从 $i=10^5$ 到 $i=2\times 10^5$)来测试 CLM-PRBG 的密码学属性。图2中 a)，b)，c)分别为子序列的0，1比、线性复杂性以及自相关性，d)表示两个子序列的互相关性。我们看到实验结果与理论分析是吻合的。

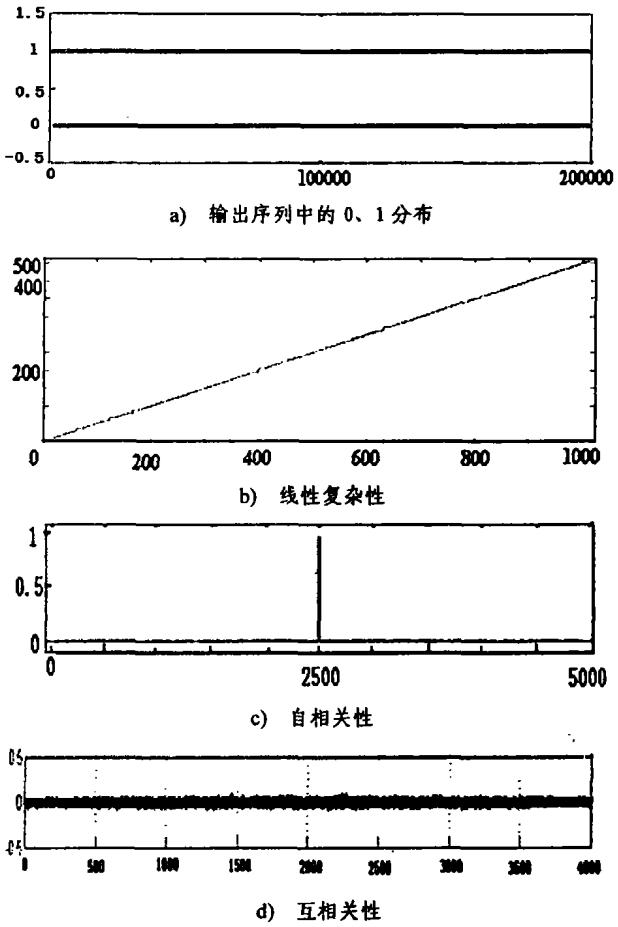

图2 CLM-PRBG 的密码学属性

4. CLM-PRBG 在序列密码中的应用

基于上述 CLM-PRBG，可以构造许多不同的实用序列密码，图3给出的序列密码也许是其中最简单的一种。在这种序列密码中，密钥空间为[0,1]×[0,1] ×(0,1)×(0,1)。

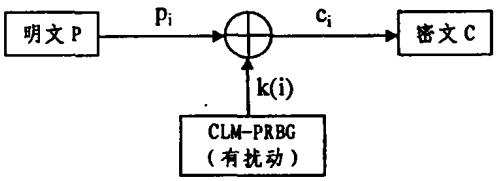

图3 基于有扰 CLM-PRBG 的一种简单的序列密码

如果有限计算精度为 n 位，则密钥熵将为 $4n$ 位。而且易于软、硬件实现，速度仅次于简单的线性和分段线性系统。只要稍微改变 CLM-PRBG 的结构，增加小的实现开销，就可以大大增加系统的密钥熵和安全性。例如，叠加上面的 CLM-PRBG，可以使密钥熵变为 $8n$(n 为有限精度)，而实现开销只增加了一倍左右，见图4。其它序列密码算法见文[2]。

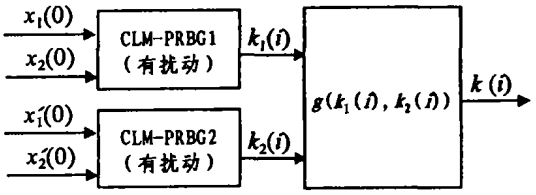

图4 两个 CLM-PRBG 叠加后的 PRNG

从第3节的分析和实验，知道图3所示的序列密码具有几近完美的密码学属性，但这只是好密码算法的必要条件，却不能保证密码系统的安全性。因此，检验一个密码系统是否安全，还要检验该系统抗各种已知攻击的能力。在传统密码学中，常用的攻击方法大致可分成两类：

·重构密钥 K：唯密文攻击、已知明文攻击以及穷举攻击等它们的最高攻击目标都是从已知的明文或密文中推导出密钥 K。

·针对系统弱点的攻击：例如差分/线性攻击，相关性攻击，各个击破以及一些攻击方法的组合方法。

显然，从由 CLM-PRBG 产生的伪随机序列 $k(i)$ 中提取或推导出密钥 K 是不可能的，而伪随机扰动也使密码分析更加困难。在混沌密码学中也出现了一些专门用于分析混沌密码系统的有效方法。例如，基于混沌同步的分析方法、基于离散混沌系统弱化的统计属性的分析方法以及一些只针对相应密码系统的分析方法。首先基于混沌同步的分析方法不适用于本文中的系统，其次在扰动情形下，用统计学方法难以奏效。而有针对性的密码分析方法不能推广。由此可见，基于 CLM-PRBG（带扰动）的数字混沌密码系统对所有的已知的分析方法都是安全的。当然，关于安全性的最终结论还有待于进一步的分析。

需要注意的一点是，在我们的 CLM-PRBG 中存在弱密钥。假使 $x_1(0)=x_2(0)$，参数分别 p_1，p_2，PRBG 产生伪随机位序列 $k(i)$。固定 $x_1(0)$，$x_2(0)$，交换两系统的参数，产生位序列 $k(i)$。如果两个子系统受到的扰动相同，扰动区间也相同，则 $k'(i)=k(i)$。这样导致密钥空间减少了1/2。为解决这个问题，应使用不同的扰动 PRNG 或扰动间隔，并使预迭代次数 $m>\max(\Delta_1,\Delta_2)$。

结论 本文提出的 CLM-PRBG 克服了现有文献中的伪随机发生器的设计中存在的缺陷，具有安全性高、速度快和易于实现等优点，可以满足大多数实际应用。但应该看到设计一个安全性高、性能优的序列加密算法并不是一件简单的事情，理论上的安全性还有待实际攻击的检验。为了提高密码系统的安全性，一种直接的方法就是采用更加复杂的混沌系统来产生伪随机序列。然而，相应地会增加实现上的困难和降低系统的运行速度。另外，从信息论的角度，系统地分析混沌理论和传统密码学之间的关系，进一步从理论上探索混沌理论在密码学上的应用价值和应用准则是混沌密码学亟需解决的问题。

参考文献

1 Kocarev L, et al. Logistic map as a block encryption algorithm. Phys. Lett. ,2001,A 289:199～206

2 Li shujun, et al. Pseudo-random bit generator based on chaotic systems and its applications in stream-cipher cryptography. Process in Cryptology,2001,2247:316～329

3 Kocarev L. Chaos-Based Cryptography: A brief overview

4 Baptista M S. Cryptography with chaos. Phys. Lett. ,1998,A 240: 50～54

5 Palacios A, et al. Cryptography with cycling chaos. Phys. Lett. , 2002,A 303:345～351

6 Dachselt F, Schwartz W. Chaos and cryptography. IEEE Trans. Circuits Sys. I,2001,48(12):1498～1509

7 Roskin K M,Casper J B. From chaos to cryptography

8 Carcia P, Jimenez J. Communication through chaotic map systems. Phys. Lett. ,2002,A 298:35～40

9 Tao Yang, et al. Phys. Cryptanalyzing chaotic secure communications. Lett. ,1998,A 245 :495～510

10 Schmitz R. Use of chaotic dynamical systems in cryptography. J. The Franklin Institute,2001,328:429～441

11 Jakimoski G, Kocarev L. Analysis of some recently proposed chaos-based encryption algorithms. Phys. Lett. ,2001,A 291:381～384

12 Chen J, Blackmore D. On the exponential self-regulating population model. Chaos, Solitons and Fractals ,2002,14: 1433～1450

13 Beth T, Lazic D E, Mathias A. in Advances in Cryptology-CRYPTO'94, Y. G. esmedt, ed. New York: Springer-Verlag, 1994, 839:318～ 331

14 Habutsu T, Nishio Y, Sasase I, Mori S. A secret key cryptosystem by iterating a chaotic map. In Advances in Cryptology-EUROCRYPT'91, D. W. Davies, Ed. New York: Springer-Verlag, 1991,547:127～140

15 Shannon C E. A mathematical theory of communication. Bell Syst. Tech. J. , 1948,27(3):379～423, 623～656

16 Shannon C E. Communication theory of secrecy systems. Bell Syst. Tech. J. ,1949,28:656～715

17 Sang Tao, Wang Ruili, Yan Yixun. Perturbance-based algorithm to expandcycle length of chaotic key stream. Electronics Letters, 1998,34(9):873～874

18 Sang Tao, Wang Ruili, Yan Yixun. Clock-controlled chaotic keystream generators. Electronics Letters, 1998,34(20):1932～1934

19 Zhou Hong, Ling Xieting. Generating chaotic secure sequences with desiredstatistical properties and high security. Int. J. Bifurcation and Chaos, 1997,7(1):205～213

20 Li Shujun, Mou Xuanqin, Cai Yuanlong. Improving security of a chaotic encryption approach. Physics Letters A (to be published)

21 Biham E. Cryptoanalysis of the chaotic-map cryptosystem suggested at Euro-Crypt'91. in Advances in Cryptology-EUROCRYPT'91, D. W. Davies, Ed. New York: Springer-Verlag, 1991, 547:532～534

22 Mitchell D W. Nonlinear key generator. Cryptologia, 1990 XIV (4):350～354

23 Pecorra L M, Carroll T L. Driving systems with chaotic signals. Phys. Rev. Lett. ,1990,64(8):821～824

24 Carroll T L, Pecorra L M. Synchronization chaotic circuits. IEEE Trans. Circuits Syst. , 1991,38:453～456

25 Pecorra L M, Carroll T L. Synchronization in chaotic systems. Phys. Rev. A,1991,44(4):2374～2383

26 de Angeli A, Genesio R. Dead-beat chaos synchronization in discretee-time systems. IEEE Trans. Circuits Syst. I, 1995,42:54～56

27 Matthews R. On the derivation of a 'chaotic' encryption algorithm. Cryptologia,1989, XIII(1):29～42

28 Bianco M E, Reed D A. Encryption system based on chaos theory. US Patent No. 5048086, 1991

29 Protopopescu V A, Santoro R T, Tollover J S. Fast and secure encryption- decryption method based on chaotic dynamics. US Patent No. 5479513, 1995

30 Zhou Hong, Ling X T. Problems with the chaotic inverse system encryption approach. IEEE Trans. Circuits and Systems I, 1997, 44(3):268～271

31 Alvarez E, et al. New approach to chaotic encryption. Physics Letters A, 1999,263:373～375

32 郑伟谋，郝柏林. 实用符号动力学. 上海：上海科技教育出版社，1994

33 Yang Yixian, Lin Xuduan. Coding Theory and Cryptology (In Chinese). People's Post and Telecommunications Press, Beijing, China, 1992