第 54 卷 第 9 期 2005 年 9 月
1000-3290/2005/54(09)/4031-07

物 理 学 报
ACTA PHYSICA SINICA

Vol.54,No.9,September,2005

基于 TD-ERCS 混沌系统的伪随机数发生器及其统计特性分析*

盛利元† 曹莉凌 孙克辉 闻 姜

(中南大学物理科学与技术学院,长沙 410083)

(2004 年 10 月 22 日收到;2004 年 12 月 22 日收到修改稿)

为了进一步分析切延迟椭圆反射腔映射系统(TD-ERCS)混沌系统的密码学意义上的安全性,采用 TD-ERCS 并行方式构造了一个结构简单的伪随机序列发生器.用户密码不再是固定不变的,可在[2^{64},2^{672}]区域内任意取值.对所产生的二值伪随机序列(即 TD-ERCS 序列)进行了均衡性、游程特性、相关性等基本统计特性初步测试,并与 m 序列、logistic 序列、Chebyshev 混沌序列、SCQC 序列作了对比分析.实验表明,TD-ERCS 序列有更好的统计特性.

关键词:混沌, TD-ERCS, PRNG, 统计特性

PACC:0545, 0540

1. 引 言

近年来,将混沌信号离散化后构造伪随机数发生器(pseudo-random number generator, PRNG)并形成新的加密算法是混沌理论应用于信息安全领域的一个新方向.这些算法采用几个著名的混沌系统,如 Logistic 映射、tent 映射等[1—4].Jakimoski 等人[5-7]对这类算法作了分析,认为这些算法与 DES(data encryption standard)相比还没有竞争力,提出了系列改进措施.Wong 等人[8—10]通过引入 Hash 函数改进算法结构,Li 等人[11]也提出了补救办法,一个原本十分简单的系统实现起来却变得越来越复杂.此外,还有基于圆映射的[12,13],基于指数映射的[14],基于分段线性映射的[15,16],基于复合离散混沌系统的[17],等等.这些算法无论怎样改进,但从密码安全和统计特性的角度来分析,它们都存在致命的缺陷.混沌系统可以构造周期任意长的 PRNG[18],但它对于密码学未必是安全的.盛利元等[19]指出,混沌系统对初始条件的敏感性仅仅是它构造密码学上安全的 PRNG 的必要条件而不是充分条件,总结了混沌安全性的 4 个充分条件,基于这些充分性条件,构造了一类新的混沌系统,即切延迟椭圆反射腔映射系统(tangent-delay ellipse reflecting cavity-map system, TD-ERCS).安全性充分条件已经给混沌系统进入信息加密领域设置了很高的门槛.作为伪随机数源,混沌系统具有其特殊的优势[20],如迭代速度快、简单易理解、灵活多变和可分析性,是其他随机数源无法相比的,吸引着越来越多的人加入其研究行列.近两年,我国密码学界也开始关注混沌加密理论[17],丘水生研究组[21]尝试将混沌加密与传统密码体制结合,提出传统密码算法的密钥由混沌系统产生的思路,这种加密算法的安全性同样完全依赖于混沌系统的安全性.

混沌加密算法的安全性本质上等价于随机序列的安全性[22],而随机序列的安全性是以随机序列的统计特性为前提的.为了全面研究 TD-ERCS 混沌系统的安全性,本文采用 DT-ERCS 并行方式构造了一个结构简单的二值伪随机序列发生器,用户密码可在[2^{64},2^{672}]区域内任意取值,完成了几个基本统计特性(均衡性、游程特性、相关性等)的数值分析,与常见的几种著名伪随机数发生器 m 序列、logistic 序列、Chebyshev 序列等进行了比较分析,表明 TD-ERCS 序列具有更好的统计特性,进一步展示了它在密码学上的应用前景.

* 湖南省自然科学基金(批准号:04JJ3077)资助的课题.

† E-mail:itpo@mail.csu.edu.cn

2. PRNG

2.1. 基本结构

本文涉及的 PRNG 是一种将混沌的数字信号流转换成一个伪随机二值序列输出的系统.主要有两种转换方法.一种方法是预先设置一个门限 c,让系统每次迭代值 x_i 与 c 比较,若 $x_i > c$,则输出"1",否则输出"0".另一种方法是将 x_i 用二进制数表示,取其中某一位或几位作为输出值.本文采用第二种方法.

PRNG 的基本结构如图 1 所示,由密码转换与种子分配器,并行 TD-ERCS,状态序列(x_{ij},k_{ij})混合器三个模块构成,其中并行 TD-ERCS 由 4 个独立的 TD-ERCS 组成.这种方案,在不降低运行速度的前提下给用户提供了巨大的自由密钥空间,使 PRNG 具有可兼容性、可扩展性,用于信息加密还具有可升级性.本文采用 C++ 软件实现 PRNG.

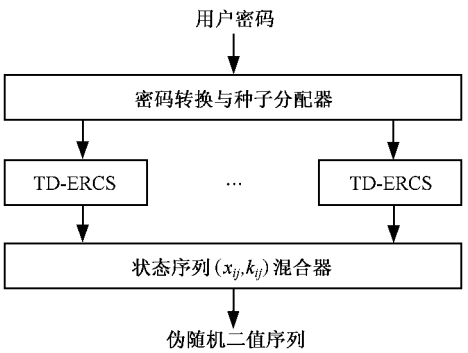

图 1 基于 TD-ERCS 的 PRNG 结构

2.2. 工作原理

2.2.1. 用户密码

用户密码用 K 表示,16 进制数字符集

$$H = \{0,1,2,3,4,5,6,7,8,9,a,b,c,d,e,f\} \quad (1)$$

为用户密码有效字符,简称 H 字符.

K 的 H 字符的个数,称为 K 的 16 进制长度,用 $L_{(h)}$ 表示.K 对应的 2 进制数字符的个数,称为 K 的 2 进制长度,用 L 表示.

K 的定义域为$[2^{64},2^{672}]$.在该区间,K 可取任意一个整数,故 K 不是固定长度的,而是一个长为 16—168 个 H 符号串,对应二进制数符号串为 64—672 bit.系统根据 K 的长度自动选择驱动 TD-ERCS 的并行数.

2.2.2. TD-ERCS[19]

给定 TD-ERCS 系统参数 $\mu(0 < \mu \leqslant 1)$,初值 x_0 $(-1 \leqslant x_0 \leqslant 1)$和 $\alpha(0 < \alpha < \pi)$,切延迟 $m(m = 2,4,5,6,\cdots)$,TD-ERCS 通过迭代关系

$$x_n = -\frac{2k_{n-1}y_{n-1} + x_{n-1}(\mu^2 - k_{n-1}^2)}{\mu^2 + k_{n-1}^2}, \quad (2)$$

$$k_n = \frac{2k'_{n-m} - k_{n-1} + k_{n-1}k'^2_{n-m}}{1 + 2k_{n-1}k'_{n-m} - k'^2_{n-m}}, \quad (3)$$

$$n = 1,2,3,\cdots,$$

将产生两个独立的实值序列

$$x_{m+1},x_{m+2},x_{m+3},\cdots, \quad (4)$$

$$k_{m+1},k_{m+2},k_{m+3},\cdots, \quad (5)$$

其中

$$k'_{n-m} = \begin{cases} -\dfrac{x_{n-1}}{y_{n-1}}\mu^2 & n < m, \\ -\dfrac{x_{n-m}}{y_{n-m}}\mu^2 & n \geqslant m, \end{cases} \quad (6)$$

$$y_n = k_{n-1}(x_n - x_{n-1}) + y_{n-1}, \quad (7)$$

$$y_0 = \mu\sqrt{1 - x_0^2}, \quad (8)$$

$$k'_0 = -\frac{x_0}{y_0}\mu^2, \quad (9)$$

$$k_0 = \frac{\tan\alpha + k'_0}{1 - k'_0\tan\alpha}, \quad (10)$$

(μ,x_0,α,m)称为 TD-ERCS 种子参数.

2.2.3. 密码转换与初值分配器

IEEE754 标准[23] 规定,一个实数的双精度二进制表示由三部分组成(图 2 所示):1-bit 符号位(用 s 表示),11-bit 有偏指数位(用 e 表示),52-bit 尾数位(用 f 表示),由

$$(-1)^S \times 2^{e-1023} \times 1.f, 0 < e < 2047 \quad (11)$$

换算到十进制数.

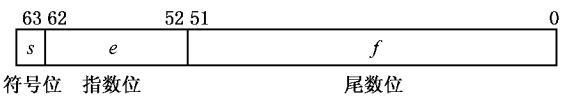

图 2 IEEE754 实数表示法

转换规则必须同时符合 C++ 的数表示法和 TD-ERCS 性质,为此引入"左移位 b 操作".

定义 如果尾数 f 中第 51-bit,50-bit,…,(51-b)-bit 均为"0",而(51-b-1)-bit 为"1",则将 f 的前 b 位依次移到 f 的右边构成一个新尾数 f,这样的操作称为左移位 b 操作.

例如

移位前 f:0000010101000011111……10,

移位后 f:1010100001111……1000000,

这里 $b=5$.经左移位 b 操作后尾数 f 中第 51-bit 始终为“1”.

TD-ERCS 并行数由用户密码长度 $L_{(h)}$ 确定,规定:$L_{(h)}=16$—42,1 个 TD-ERCS;$L_{(h)}=43$—84,2 个 TD-ERCS;$L_{(h)}=85$—126,3 个 TD-ERCS;$L_{(h)}=127$—168,4 个 TD-ERCS.

用 K_i,$i=1,2,3,4$ 表示 K 中分配给第 i 个 TD-ERCS 的密码子块,则 K 可表示为 4 个密码子块的首尾连接,定义为

$$K = K_4 K_3 K_2 K_1, \tag{12}$$

这里,K_2K_1 表示 K_2 与 K_1 首尾连接,非相乘.K_i 的二进制长度用 L_i 表示.

同理,用 K_{ij},$j=1,2,3,4$ 表示 K_i 中分配给第 j 个 TD-ERCS 的种子参数的密码子块,则 K_i 可表示为 4 个密码子块的首尾连接,定义为

$$K_i = K_{i4} K_{i3} K_{i2} K_{i1}, \quad i = 1, 2, 3, 4. \tag{13}$$

K_{ij} 与种子参数的对应关系和赋值方法如下:

1) K_{i4} 取 3 个 H 符号,长 12 bit,以整数形式按照下式赋给切延迟 m,

$$m = \begin{cases} 2 & K_{i4} = 0, \\ 4 & K_{i4} = 1, \\ K_{i4} + 3 & 2 \leqslant K_{i4} \leqslant 4095. \end{cases} \tag{14}$$

2) K_{i3} 取 13 个 H 符号,长 52 bit,作为二进制码赋给初值 x_0.

第一步,给 x_0 尾数 f 赋值,即 $K_{i3}\rightarrow f$;第二步,将 f 中的第 0-bit 的值给符号位;第三步,对 f 左移位 b 操作;第四步,给 x_0 指数 e 赋值,即 $(1022-b)\rightarrow e$ 若 $K_{i3}=0$,则 $f=+0$.

3) K_{i2} 取 13 个 H 符号,长 52 bit,作为二进制码赋给初值 α.

第一步,给 f 赋值,即 $K_{i2}\rightarrow f$;第二步,符号 s-bit 赋‘0’;第三步,对 f 左移位 b 操作;第四步,$(1022-b)\rightarrow e$ 若 $K_{i2}=0$,则 f 的第 0-bit 赋‘1’,其余位赋“0”,再按照第三步操作.赋值完毕后,其值再乘以 π 倍.

4) K_{i1} 取 13 个 H 符号,长 52 bit,作为二进制码赋给压缩系数 μ.

第一步,给 f 赋值,即 $K_{i1}\rightarrow f$;第二步,符号 s-bit 赋‘0’;第三步,对 f 左移位 b 操作;第四步,$(1022-b)\rightarrow e$ 若 $K_{i1}=0$,则 f 的第 0-bit 赋‘1’,其余位赋“0”,再按照第三步操作.

这样,K 可写成与 4 个 TD-ERCS 种子相对应的首尾连接形式

$$K = K_{44} K_{43} K_{42} K_{41} K_{34} K_{33} K_{32} K_{31} K_{24} K_{23} K_{22} K_{21} K_{14} K_{13} K_{12} K_{11}. \tag{15}$$

2.2.4. 状态序列(x_{ij},k_{ij})混合器

启用 4 个并行 TD-ERCS,实值序列(4),(5)改写成

$$\{x_{ij} \mid i = 1,2,3,4; j = 1,2,\cdots\}, \tag{16}$$

$$\{k_{ij} \mid i = 1,2,3,4; j = 1,2,\cdots\}, \tag{17}$$

其中 x_{ij} 和 k_{ij} 表示第 i 个 TD-ERCS 的第 $m+j$ 个迭代的 x 值和 k 值.再作变换并归一化处理

$$\theta_{ij} = \frac{\arccos(x_{ij})}{\pi}, (0 \leqslant \theta_{ij} \leqslant 1), \tag{18}$$

$$\beta_{ij} = 0.5 + \frac{\arctan(x_{ij})}{\pi}, (0 \leqslant \beta_{ij} \leqslant 1), \tag{19}$$

θ_{ij} 和 β_{ij} 便是对应 x_{ij} 和 k_{ij} 的归一化实值序列.

取 θ_{ij} 和 β_{ij} 的尾数 f 的二进制码为对应 θ_{ij} 和 β_{ij} 的码字序列,分别记为

$$\theta_{ij} = \theta_{ij}^1\theta_{ij}^2\theta_{ij}^3\cdots\theta_{ij}^{51}\theta_{ij}^{52}, \tag{20}$$

$$\beta_{ij} = \beta_{ij}^1\beta_{ij}^2\beta_{ij}^3\cdots\beta_{ij}^{51}\beta_{ij}^{52}, \tag{21}$$

其中 $\theta_{ij}^l = \{0,1\}$,$\beta_{ij}^l = \{0,1\}$,$l=1,2,\cdots,52$.故 θ_{ij} 和 β_{ij} 分别可用 13 个 H 符号表示.

将码字序列(20)和(21)混合,构成新的码字块,记为 κ_j,定义为

$$\kappa_j = \theta_{1j}\beta_{1j}\theta_{2j}\beta_{2j}\theta_{3j}\beta_{3j}\theta_{4j}\beta_{4j}, \tag{22}$$

最后,由 κ_j 产生的码字块流

$$\kappa_1\kappa_2\kappa_3\cdots\kappa_j\cdots, \tag{23}$$

成为 PRNG 的混沌伪随机二值序列,简称 TD-ERCS 序列.

3. TD-ERCS 序列的统计特性分析

Golomb[24] 提出了衡量伪随机二值序列性能的三条公设,按照这三条公设分析 TD-ERCS 序列(23),与其他序列性能进行比较.

3.1. 均衡性

二值序列的均衡性,是指在一段序列或一个周期序列中,0 和 1 的个数基本接近的程度,它的大小可用平衡度表示.设 N_1 和 N_0 分别表示序列中‘1’

与‘0’的个数，N 表示序列的长度，二值序列的平衡度定义[25]为

$$E = \frac{|N_1 - N_0|}{N}, \tag{24}$$

平衡度 E 越小，均衡性越好.

取 $K = abcdef12345678900987654321abcdef$，得到一个 TD-ERCS 序列，分别取 $N = 100, 200, 1000, 2000$ 统计 E，求 10000 次统计平均值 $\bar{E}$. 其结果与文献[26]关于 m 序列、logistic 序列、Chebyshev 序列和 SCQC 序列的测试结果同列于表 1. 可见 TD-ERCS 序列有均衡的 0-1 比，其均衡性远优于前 4 种序列.

表 1 “0”,“1”均衡性比较

N	100	200	1000	2000
m 序列	0.0562	0.0408	0.0506	0.0356
logistic 序列	0.0581	0.0577	0.0506	0.0554
Chebyshev 序列	0.1042	0.0792	0.1074	0.0689
SCQC 序列	0.0858	0.0388	0.0242	0.0219
TD-ERCS 序列	0.0400	0.0203	0.0160	0.0071

TD-ERCS 序列的平衡度随长度的变化如图 3 所示，结果表明，TD-ERCS 序列平衡度很快下降到 0.02 左右，实际应用中，序列长度只取 1000 以上就能满足系统对序列平衡度的要求.

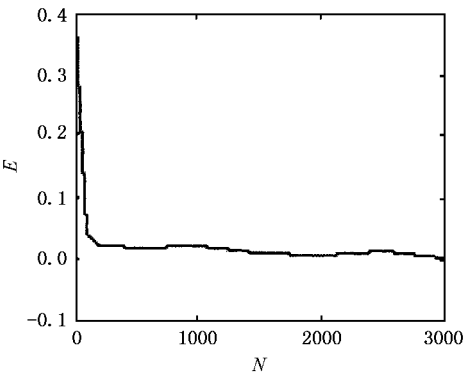

图 3 TD-ERCS 序列平衡度与序列长度的关系

3.2. 游程特性

序列中出现同样码元(0 或 1)串的长度称为游程长度. 游程特性指出，短游程长度的码元串应占优势，长为 i 的游程出现概率为 2^{-i}；0-游程和 1-游程各占游程总数的一半.

表 2 给出了用 Monte-Carlo 方法测得的 TD-ERCS 序列的游程分布比重平均值，以及 m 序列、logistic 序列、Chebyshev 混沌序列、SCQC 序列的对应值，数据表明，TD-ERCR 序列最接近理论值. 图 4 分别为不同序列长度时 SCQC[25]序列和 TD-ERCS 序列的游程长度比重值与其理论值的差值(记为 Δr)曲线. 这是一个更细致的实验比较，结果仍然表明，TD-ERCS 序列比 SCQC 序列更接近理论值.

表 2 游程分布比重平均值

序列长度	序列类别	比重值				
		1-游程	2-游程	3-游程	4-游程	短游程
100	m 序列	0.6286	0.3286	0.0286	0.0143	1.0001
	logistic	0.3636	0.3864	0.0909	0.0759	0.9168
	Chebyshev	0.5343	0.2759	0.1379	0.0345	0.9828
	SCQC	0.5490	0.1961	0.1126	0.0980	0.9607
	TD-ERCS	0.4942	0.2446	0.1239	0.0689	0.9316
200	m 序列	0.6232	0.3116	0.0580	0.0072	1.0000
	logistic	0.4316	0.3368	0.1053	0.0526	0.9263
	Chebyshev	0.5607	0.2150	0.1121	0.0918	0.9387
	SCQC	0.5204	0.2041	0.1224	0.0918	0.9387
	TD-ERCS	0.4944	0.2451	0.1240	0.0698	0.9333
1000	m 序列	0.5087	0.2126	0.2089	0.0628	0.9926
	logistic	0.5421	0.2548	0.0881	0.0479	0.9329
	Chebyshev	0.5762	0.1861	0.0792	0.0614	0.9029
	SCQC	0.4888	0.2394	0.1379	0.0771	0.9432
	TD-ERCS	0.4844	0.2513	0.1245	0.0714	0.9360
2000	m 序列	0.4773	0.2345	0.1529	0.0640	0.9287
	logistic	0.5563	0.2441	0.0861	0.0473	0.9338
	Chebyshev	0.5787	0.1843	0.0737	0.0598	0.8965
	SCQC	0.4854	0.2613	0.1276	0.0704	0.9447
	TD-ERCS	0.4857	0.2495	0.1243	0.0706	0.9301
任意长度	理论值	0.5000	0.2500	0.1250	0.0625	0.9375

3.3. 相关特性

设 $x_i, y_i, i = 0, 1, 2, \cdots$ 为两个伪随机序列，自相关函数定义为

$$R_{xx}(m) = \frac{1}{N}\sum_{i=0}^{N-1} x_i x_{i+m}, \tag{25}$$

互相关函数定义为

$$R_{xy}(m) = \frac{1}{N}\sum_{i=0}^{N-1} x_i y_{i+m}, \tag{26}$$

其中，N 为序列长度，m 为相关间隔.

取 $N = 2000$，$-500 \leqslant m \leqslant 500$，计算 TD-ERCS 序列的相关特性，结果如图 5 所示. 实验结果表明，TD-ERCS 序列的自相关函数近似于 δ 函数，互相关性函数近似为零，正如文献[19]所指出的，TD-ERCS 是一个全域零相关系统.

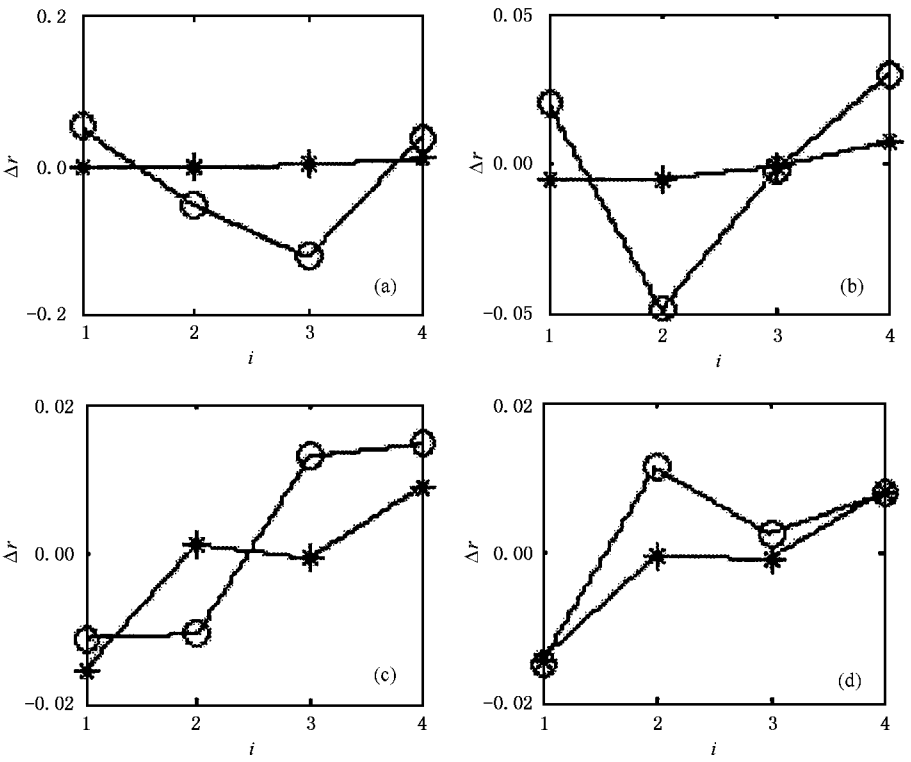

图 4　游程比重与理论的差值比较　＊ TD-ERCS 序列，○ SCQC 序列；(a) 序列长度 100；(b) 序列长度 200；(c) 序列长度 1000；(d) 序列长度 2000

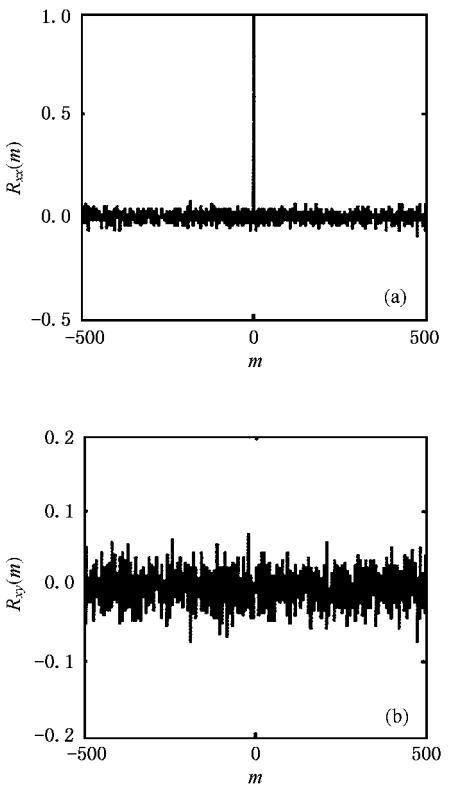

图 5　TD-ERCS 序列相关特性　(a) K = *abcdef*12345678900987654321*abcdef* 序列的自相关函数曲线；(b) K = *abcdef*123456789009876543 21*abcdef* 与 K = *bbcdef*12345678900987654321*abcdef* 序列的互相关函数曲线

在通信系统中，随机序列的自相关旁瓣及它的均方根、互相关最大值及互相关均方根是研究相关性的几个重要参量，它表征了扩频序列的多径干扰和多址干扰的大小. 这些参量越小，干扰越小，表明系统性能越好. 自相关旁瓣均方根定义为

$$\sigma(M) = \sqrt{\frac{\sum_{m=1}^{M}[R(m)]^2}{M}}, \tag{27}$$

互相关均方根定义为

$$\sigma_{xy}(M) = \sqrt{\frac{\sum_{m=-M}^{M}[R_{xy}(m)]^2}{2M+1}}, \tag{28}$$

表 3 为两种长度的 TD-ERCS 序列与 m 序列，logistic 序列的自相关旁瓣峰值和互相关函数最大值. TD-ERCS 序列相关性能远优于其他两种序

表 3　最大自相关旁瓣与最大互相关值

序列长度	序列名称	最大自相关旁瓣	最大互相关值
2047	m 序列	0.0418	0.1010
2047	logistic 序列	0.0679	0.0728
2047	TD-ERCS 序列	0.0076	0.0718
8191	m 序列	0.0108	0.0398
8191	logistic 序列	0.0370	0.0363
8191	TD-ERCS 序列	0.0016	0.0297

列.图 6 所示为 TD-ERCS 序列的自相关旁瓣均方根和互相关均方根随序列长度的变化曲线,两条曲线有相同的渐近性质.自相关旁瓣均方根和互相关均方根都随序列长度迅速减小,这一特性在通信应用中可以降低序列长度的选择限制.

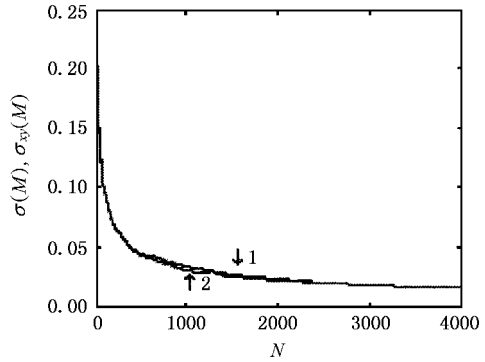

图 6 自相关旁瓣均方根与互相关均方根随序列长度的变化
1 为自相关旁瓣均方根曲线 2 为互相关均方根曲线

4. 结 论

采用 TD-ERCS 并行方式构造了一个结构简单的 PRNG,用户密码不再是固定不变的,可在 $[2^{64},2^{672}]$ 区域内任意取值.同时这种设计方案,将使 PRNG 具有可兼容性、可扩展性,用于信息加密还具有可升级性.对 TD-ERCS 序列统计特性分析表明,这种序列比传统二值序列如 m 序列、logistic 序列、Chebyshev 序列具有更良好的均衡性,游程特性和相关特性,进一步展示了它在密码学上的应用前景.

[1] Fridrich J 1998 *Int. J. Bifurc Chaos* **8** 259

[2] Baptista M S 1998 *Phys. Lett.* A **240** 50

[3] Alvarez E, Fernandez A and Garcia P 1999 *Phys. Lett.* A **263** 373

[4] Wong W K, Lee L P and Wong K W 2001 *Comput. Phys. Commun.* **138** 234

[5] Kocarev L and Jakimoski G 2001 *Phys. Lett.* A **289** 199

[6] Jakimoski G and Kocarev L 2001 *Phys. Lett.* A **291** 381

[7] Kocarev L and Jakimoski G 2001 *Patent Number*: EP 1 326 363 A1

[8] Wong W K 2002 *Phys. Lett.* A **298** 238

[9] Wong W K 2003 *Phys. Lett.* A **307** 292

[10] Wong W K, Ho S W and Yung C K 2003 *Phys. Lett.* A **310** 67

[11] Li S J, Mou X Q and Ji Z 2003 *Phys. Lett.* A **307** 22

[12] Palacios A and Juarez H 2002 *Phys. Lett.* A **303** 345

[13] Akira K and Manabu K 2002 *Patent Number*: JP2002026897

[14] Tomoaki Y, Kawamura A, Nishimura S *et al* 2003 Patent number: JP2003076272

[15] Stojanoski T and Kovarev L 2001 *IEEE Trans.* CAS-I **48** 281

[16] Wang X S and Gan J R 2002 *Chinese J. Comput.* **25** 352 (in Chinese) [王相生、甘骏人 2002 计算机学报 **25** 352]

[17] Li H D and Feng D G 2003 *Journal of Software* **14** 991 (in Chinese) [李红达、冯登国 2003 软件学报 **14** 991]

[18] Janis B 2000 *Chaos COC* (St. Petersburg, Russia) p 558

[19] Sheng L Y, Sun K H and Li C B 2004 *Acta Phys. Sin.* **53** 2871 (in Chinese) [盛利元、孙克辉、李传兵 2004 物理学报 **53** 2871]

[20] Dachselt F and Schwarz W 2001 *IEEE Trans.* CAS-I **48** 1498

[21] Qu S S, Lin T S and Chen Y F 2003 Patent number: CP02149793.1 (in Chinese) [丘水生、林士胜、陈艳峰 2003 中国专利申请号: 02149793.1]

[22] Kelsey J, Schneier, Wagner D *et al* 1998 *LNCS* **1372** 168

[23] 754-1985 *IEEE Standard for Binary Floating-Point Arithmetic* http://standards.ieee.org/

[24] Golomb S W. Shift Register Sequence 1967 Holden-Day Inc. San Francisco

[25] Yu S J, Yu C and Wang Z 2001 *J. SYIT* **20** (2) 85 (in Chinese) [于舒娟 2001 沈阳工业学院学报 **20** (2) 85]

[26] Wang H X 2002 UEST of China Doctoral Paper 15: 78 (in Chinese) [王宏霞、虞 闯、汪 铸 2002 电子科技大学 博士论文 15: 78]

[27] Yang S Y, Wang G and Gu X T 2003 *Radio Commun* **12** 19 (in Chinese) [杨莘元、王 光、谷学涛 2003 邮电设计技术 **12** 19]

Pseudo-random number generator based on TD-ERCS chaos and its statistic characteristics analysis*

Sheng Li-Yuan Cao Li-Ling Sun Ke-Hui Wen Jiang

(*School of Physics Science and Technology, Central South University, Changsha* 410083, *China*)

(Received 22 October 2004; revised manuscript received 22 December 2004)

Abstract

To analyze the security of tangent-delay ellipse reflecting cavity-map system (TD-ERCS) from the point view of cryptography, a simple pseudo-random number generator (PRNG) is proposed with parallel TD-ERCS in this paper. Users' keys are no longer fixed, and can be chosen in the interval $[2^{64}, 2^{672}]$ arbitrarily in the PRNG. By testing the basic statistic characteristics such as equilibrium, runs and correlation of the binary pseudo-random sequences (viz. TD-ERCS sequences) being generated from the PRNG, and comparing with *m*-sequences, the logistic sequences, Chebyshev sequences and SCQC sequences, the experimental results show that TD-ERCS sequences have better statistic characteristics.

Keywords: chaos, TD-ERCS, PRNG, statistic characteristics

PACC: 0545, 0540

* Project supported by the Natural Science Foundation of Hunan Provence, China (Grant No.04JJ3077).