一类可以产生独立同分布密钥流的混沌系统*

徐正光[1)] 田清[1)†] 田立[2)]

1) (北京科技大学自动化学院, 北京 100083)

2) (北京航空航天大学宇航学院, 北京 100091)

(2013年1月13日收到; 2013年2月16日收到修改稿)

构造了一类与帐篷映射拓扑同构的混沌系统, 并根据拓扑共轭变换关系给出了此类混沌系统产生独立、均匀分布密钥流序列的采样规则. 理论证明和数值模拟, 均验证了结论的有效性. 本文为产生独立同分布密钥流提供了更多的非线性系统选择. 实验结果证明利用本文定理产生的密钥流能够通过美国信息技术管理改革法案的随机数检测标准 (FIPS PUB 140-2) 和美国国家标准与技术研究院安全检测标准 (NIST SP800-22), 符合密钥流的选取标准.

关键词: 独立同分布, 混沌系统, 帐篷映射, 拓扑同构

PACS: 05.45.Ac, 05.45.Pq, 05.45.Vx **DOI:** 10.7498/aps.62.120501

1 引 言

混沌系统的基本特性, 如确定性、有界性、对初始条件的敏感性、拓扑传递性、长期不可预测性和伪随机性, 使得混沌密码系统分析成为研究热点 [1−5]. 其中, 一种重要的设计思路是通过对混沌系统产生的混沌序列进行判决或量化后, 得到伪随机序列 (密钥流) 直接用于掩盖明文, 这种方法即为传统的混沌流密码方式, 应用广泛.

利用混沌系统产生混沌密钥流的方法有很多种, 如: 阈值函数方法, 通过判断混沌系统数值与阈值的关系, 产生密钥流 [6]; 二进制化方法, 直接将混沌转换成二进制序列 [7]; 部分二进制化法, 抽取混沌轨道的部分或全部二进制比特 [8]; 如区间划分法, 将混沌系统的定义区间划分为 m 个不相交的区域, 并为每个区域标识惟一的数字 0—$(m-1)$, 通过判断混沌轨道进入哪个区间来生成伪随机数 [9,10]. 罗松江等 [11] 对混沌序列的复杂度和稳定性做出了一些分析, 认为评判这些方法产生的密钥流好坏的一个关键指标是随机性, 特别是独立、均匀分布特性, 而现有的混沌密钥流随机性判断大部分源于实验模拟结果, 理论证明相对匮乏.

混沌系统帐篷映射 (Tent Map) 被证明具有良好的独立、均匀分布特性 [12,13], 能够满足密钥流使用的要求. 但 Tent Map 为线性混沌系统, 在某些参数下, 由于计算机的精度有限, 数值模拟结果快速收敛于零 [14], 随机性得到破坏, 产生更多的独立同分布密钥流非线性系统, 是增强密钥流生产系统选择灵活性的重要解决途径.

本文利用拓扑共轭系统之间的同构特性, 分析提出 Tent Map 特定共轭系统的采样规则, 通过理论证明和数值模拟, 验证此类 Tent Map 共轭混沌系统产生的密钥流独立、均匀分布, 并通过 FIPS PUB 140-2[15] 和 NIST SP800-22 随机数检测 [16]. 本文提出的此类系统提供了更多的独立同分布密钥流生成系统的选择, 在继承 Tent Map 独立同分布特性的同时, 摆脱 Tent Map 在某些参数下快速收敛于零的约束.

2 独立同分布混沌密钥流生成定理

定义 1[3] 对于定义在 I 的映射 (1), 和定义在

* 国家自然科学基金 (批准号: 60573058) 资助的课题.

† 通讯作者. E-mail: qingtiantq@hotmail.com

J 的映射 (2)

$$x_{k+1} = f(x_k) \quad (x \in I), \tag{1}$$

$$y_{k+1} = g(y_k) \quad (y \in J). \tag{2}$$

当存在一个连续、可逆的函数 h, 使得 $h^{-1} \circ f \circ h(x_k) = g(x_k)$, 则称映射 f 与 g 关于 h 拓扑同构.

引理 1[3] 如果映射 f 和 g 关于 h 拓扑同构, 则 f^n 和 g^n 关于 h 拓扑同构.

引理 2[3] 如果映射 f 和 g 关于 h 拓扑同构, ρ_g 是映射 g 的概率密度函数, 那么映射 f 的概率密度函数

$$\rho_f(x) = \rho_g(h^{-1}(x)) \left| \frac{\mathrm{d}h^{-1}(x)}{\mathrm{d}x} \right|.$$

定理 1 对于 Tent Map,

$$g(x) = \begin{cases} 2x & (0 \leqslant x \leqslant 1/2) \\ 2-2x & (1/2 \leqslant x \leqslant 1) \end{cases}, \tag{3}$$

当 $ma = -2$ 时,

$$f(x) = mx^2 + a \quad x \in [-|a|, |a|], \tag{4}$$

与 $g(x)$ 关于 $h(x) = -a\cos(\pi x)$ 共轭, 且通过下面的采样规则可以产生独立同分布的混沌密钥流:

(1) 如果 $a > 0$, 将 $[-a, a]$ 划分成 $N = 2^n$ 个子区间 τ_i, $\tau_i = [t_i, t_{i+1})$, 其中 $t_i = h(i/N)$, $i = 0, 1, \cdots, N-1$, $t_N = h(N/N) = a$;

(2) 如果 $a < 0$, 将 $[a, -a]$ 划分成 $N = 2^n$ 个子区间 τ_i, $\tau_i = [t_i, t_{i+1})$, 其中 $t_i = h((N-i)/N)$, $i = 0, 1, \cdots, N-1$, $t_N = h((N-N)/N) = -a$;

(3) 定义混沌密钥流 $\{s_i\}_0^\infty$ 如下:

如果 $x_k \in \tau_i$, 那么 $s_k = i$, 并设定采样步长为 n, 即 $x_{k+1} = f^n(x_k)$.

证明

1) $f(x)$ 的满射性

当 $ma = 2$ 时, $f(x) = -\dfrac{2}{a}x^2 + a$;

如果 $a > 0$, 易知 $f(x) = \dfrac{-2}{a}x^2 + a$ 在 $[-a, a]$ 区间上的值域亦为 $[-a, a]$;

如果 $a < 0$, 易知 $f(x) = \dfrac{-2}{a}x^2 + a$ 在 $[a, -a]$ 区间上的值域亦为 $[a, -a]$;

即 $f(x)$ 为定义在 $[-|a|, |a|]$ 上的满射.

2) $f(x)$ 与 $g(x)$ 关于 $h(x)$ 共轭

若 f 与 g 关于 h 共轭, 根据定义 1 得 $h^{-1} \circ f \circ h(x) = g(x) \Leftrightarrow f \circ h(x) = h \circ g(x)$. 对于本定理,

$$\begin{aligned} h \circ g(x) &= \begin{cases} -a\cos(2\pi x) & (0 \leqslant x \leqslant 1/2) \\ -a\cos[\pi(2-2x)] & (1/2 \leqslant x \leqslant 1) \end{cases} \\ &= -a\cos(2\pi x) \quad (0 \leqslant x \leqslant 1) \\ &= h(2x). \end{aligned}$$

当 $ma = -2$, 对于 (4) 式

$$\begin{aligned} f \circ h(x) &= -\frac{2}{a} \cdot a^2 \cos^2 \frac{\pi x}{2} + a \\ &= -a(2\cos^2(\pi x) - 1) \\ &= -a\cos(2\pi x), \end{aligned}$$

所以 $f \circ h(x) = h \circ g(x)$, 即 $f(x)$ 与 $g(x)$ 关于 $h(x)$ 共轭.

3) $f(x)$ 是混沌的

刘新波等 [17] 给出两拓扑共轭的映射具有相同的 Lyapunov 指数, 因此 $f(x)$ 的 Lyapunov 指数与 Tent 映射相同, 为 $\ln 2$, 即 $f(x)$ 为混沌系统.

4) 混沌密钥流 $\{s_i\}_0^\infty$ 均匀分布

由引理 2 可知, $f(x)$ 的概率密度函数为 $\rho_{f(x)} = \rho_g(h^{-1}(x)) \left| \dfrac{\mathrm{d}h^{-1}(x)}{\mathrm{d}x} \right|$, 因此 f 落在 $[t_i, t_{i+1})$ 的概率为

$$\begin{aligned} &\int_{t_i}^{t_{i+1}} \frac{\mathrm{d}h^{-1}(x)}{\mathrm{d}x} \mathrm{d}x \\ &= \int_{h\left(\frac{i}{N}\right)}^{h\left(\frac{i+1}{N}\right)} \mathrm{d}h^{-1}(x) = h^{-1}(x) \Big|_{h\left(\frac{i}{N}\right)}^{h\left(\frac{i+1}{N}\right)} \\ &= h^{-1}\left(h\left(\frac{i+1}{N}\right)\right) - h^{-1}\left(h\left(\frac{i}{N}\right)\right) \\ &= \frac{i+1}{N} - \frac{i}{N} = \frac{1}{N}, \end{aligned}$$

即混沌值出现在每个区域中的概率是相同的, 所以伪随机序列具有均匀分布的特性.

5) 独立性分析

对于 $a > 0$ 和 $a < 0$, 证明方式相同, 本文中证明过程取 $a > 0$ 为例. 若定义 $x_k = h(\theta) = -a\cos(\pi\theta)$, 则当 $0 \leqslant \theta \leqslant 1$ 时, x_k 关于 θ 递增, 并一一对应.

当 $x_k \in \tau_i^j$, 即 $\theta \in \left[\dfrac{1}{N}\left(i + \dfrac{j}{N}\right), \dfrac{1}{N}\left(i + \dfrac{j+1}{N}\right)\right]$, 则

$$\begin{aligned} x_{k+1} &= f^n(x_k) = f^n(h(\theta)) = f^{n-1}(h(2\theta)) \\ &= \cdots = h(2^n\theta) \\ &\in \left[h\left(\frac{2^n}{N}\left(i + \frac{j}{N}\right)\right), h\left(\frac{2^n}{N}\left(i + \frac{j+1}{N}\right)\right)\right] \end{aligned}$$

$$=\left[h\left(i+\frac{j}{N}\right),h\left(i+\frac{j+1}{N}\right)\right].$$

又因为 $h(x)$ 周期为 2, 若 i 为偶数,

$$x_{k+1}\in\left[h\left(i+\frac{j}{N}\right),h\left(i+\frac{j+1}{N}\right)\right)$$
$$=\left[h\left(\frac{j}{N}\right),h\left(\frac{j+1}{N}\right)\right),$$

根据取样规则 3), $S_{k+1}=j$.

若 i 为奇数,

$$x_{k+1}\in\left[h\left(i+\frac{j+1}{N}\right),h\left(i+\frac{j}{N}\right)\right]$$
$$=\left[h\left(i+1-1+\frac{j+1}{N}\right),h\left(i+1-1+\frac{j}{N}\right)\right]$$
$$=\left[h\left(\frac{-N+j+1}{N}\right),h\left(\frac{-N+j}{N}\right)\right].$$

又因为 h 是偶函数, $x_{k+1}\in\left[h\left(\frac{N-j-1}{N}\right),h\left(\frac{N-j}{N}\right)\right]$, 根据取样规则 3), $S_{k+1}=N-j-1$. 即当 $s_k=i$ 时 $s_{k+1}=\begin{cases}j & (i\text{ 为偶数})\\ N-j-1 & (i\text{ 为奇数})\end{cases}$, 可以看出, 根据定理提出的采样规则 3), n 次区间运算使得序列当前元素以等概率转移到其他元素. 所以,

$$\begin{aligned}&\mathrm{Prob}(s_{k+1}=j,s_k=i)\\ =&\mathrm{Prob}(s_{k+1}=j|s_k=i)\mathrm{Prob}\,(s_k=i)\\ =&\mathrm{Prob}(s_{k+1}=j)\mathrm{Prob}(s_k=i),\end{aligned}$$

即由定理得到的序列中各元素相互独立.

综合 1)—5), 可以证明定理给出了一类与混沌系统 Tent Map 拓扑同构的混沌系统, 按照定理中规定的采样规则可以产生独立、均匀分布的密钥流.

3 数值模拟及测试结果

3.1 实例一

对于定理 1, 当取 $m=-2, a=1$ 时, 我们得到

$$f(x)=1-2x^2\quad(x\in[-1,1]),\tag{5}$$
$$h(x)=-\cos(\pi x)\quad(x\in[0,1]),\tag{6}$$

可以看出, $f(x)$ 和 $h(x)$ 分别为文献 [1] 中所提的 Logistic 映射和对应的变换. 当采用定理 1 中提出的采样规则 3), 可以生产与文献 [1] 相同的混沌密钥流, 并能通过 χ^2 检验, 得到独立同分布的混沌密钥流. 因此可以说, 本文的结论推广了文献 [1] 的结论.

文献 [1] 中提到由 $h(x)$ 直接计算 τ_i 的运行时间与 N 呈线性关系, 时间复杂度为 $O(N)$, 利用本文提出的定理, 通过快速判断 $\theta_k=h^{-1}(x_k)=\frac{1}{\pi}\arccos\left(\frac{x_k}{-a}\right)$ 所在区间来选取 S_k, 同样可以实现文献 [1] 中提到的快速算法.

3.2 实例二

1) 混沌系统及其性质

我们取 $m=-2/3, a=3$, 得到另一类混沌系统及其共轭的变换函数:

$$f(x)=-2/3x^2+3\quad(x\in[-3,3]),\tag{7}$$
$$h(x)=-3\cos(\pi x).\tag{8}$$

当选取步长 $n=8$ 时, 图 1 表明, 通过 $h(x)$ 划分的采样区间为定义域对称的非均匀区域.

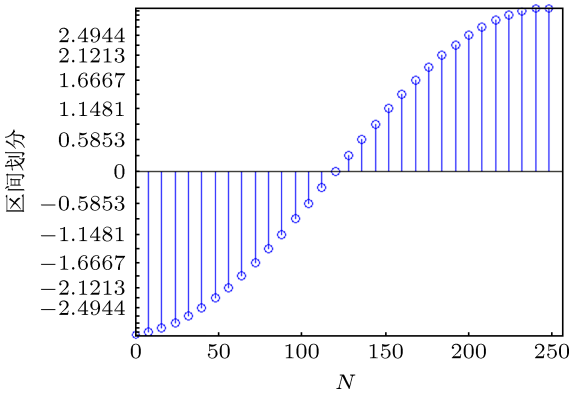

图 1 混沌区间的划分, $m=-2/3, a=3, n=8$

我们取初值 $x_0=0.2323$, 迭代公式 (7)1000 次的结果如图 2. 从图中可以看出迭代值布满整个区间, 说明系统 (7) 具有伪随机、有界性等混沌特性.

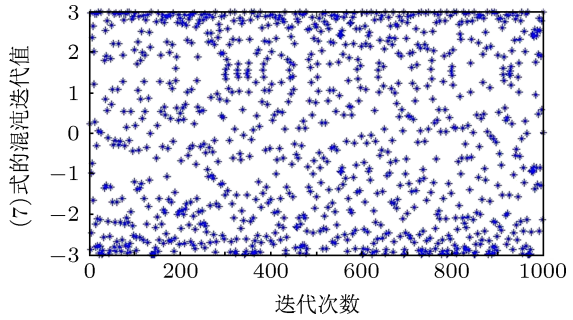

图 2 混沌迭代结果, $m=-2/3, a=3, x_0=0.2323$

然而对于 Tent Map (3) 式, 由于计算机精度的影响使得任何初始值开始的迭代值都快速收敛于

0[14], 显然, 其随机性无法得到保证. 图 3 为选取初值 $x_0 = 0.2323$ 的迭代结果, 另外的数值模拟结果也验证了 Tent Map (3) 式无法通过下文提到的 χ^2 检验以及 FIPS PUB 140-2 和 NIST SP 800-22 随机数检测.

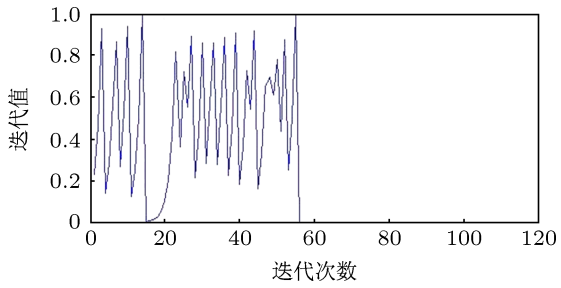

图 3 Tent Map 迭代结果

2) 测试结果

本文对混沌系统 (7) 式进行了 χ^2 检验、近似熵分析、FIPS PUB 140-2 和 NIST SP 800-22 检测以验证由定理生成的混沌系统的均匀性、复杂性和随机性.

① χ^2 检验

对于本文构造的混沌系统 (7) 式, 设定步长 $n = 8$, 选取 10 组不同的初始值, 在舍去前 100 次的迭代值后, 对 100000 个混沌密钥流序列 $\{s_k\}_0^{99999}$ 进行 χ^2 检验, 验证密钥流序列在 0—2^8 (即 0—255) 出现频率的均匀性, 结果如表 1 所示. 其中, 我们选取 χ^2 检验的显著性水平 $\alpha = 0.05$, 当序列长度 M 于 100000 时, χ^2 检验的阈值统一选取为 293.2478.

表 1 $\{s_k\}_0^{99999}$ 的 χ^2 检验结果

初值 x_0	序列长度 M	χ^2 值	阈值	结果
−2.9999	100000	252.7232	293.2478	通过
0.1270		233.4003		通过
0.2323		248.5862		通过
0.3432		278.7738		通过
0.4132		256.0870		通过
0.5632		231.3267		通过
0.6324		241.5770		通过
1.3421		277.9955		通过
2.6421		266.2042		通过
2.9999		252.7232		通过

从实验结果可以看出, 本文提出的例子满足均匀同分布的统计特性, 验证了定理的有效性和可行性.

②近似熵 (ApEn) 分析

选取初值 $x_0 = 0.2323$, 设定步长 $n = 8$, 对混沌系统 (7) 式产生的不同长度 M 的密钥流序列 $\{s_k\}_0^{M-1}$ 进行近似熵分析和比较, 结果如表 2 所示. 其中, 根据文献 [18] 中提到的近似熵计算方法, 选取比对游程长度 $l_{\rm cr} = 2$, 过滤水平 $r = 0.25$SD, SD 为 $\{s_k\}_0^{M-1}$ 的标准偏差.

表 2 近似熵分析

$l_{\rm cr}$	r	x_0	序列长度 M	近似熵
2	0.25 SD	0.2323	3000	2.0094
			4000	2.0196
			5000	2.0127
			6000	2.0114
			7000	2.0030
			8000	1.9965
			9000	1.9976

选取序列长度 $M = 4000$, 随机选用 100 组初始值, 计算近似熵, 结果如图 4 所示, 平均值为 2.0178.

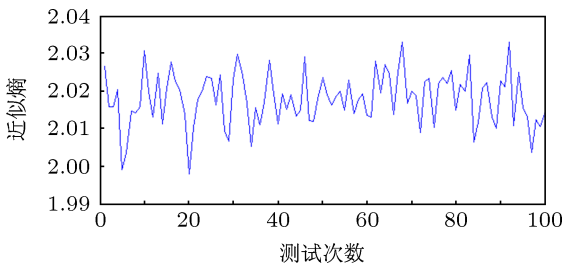

图 4 100 组近似熵结果

两种测试结果表明, 由本文定理构造的非线性混沌系统复杂性较线性 Tent Map 大大提高, 克服由于计算机精度的影响使得 Tent Map (3) 式快速收敛于 0[14] 而无法提供密钥流的问题.

③ FIPS140-2 随机数检测 [15]

对于本文构造的混沌系统 (7) 式, 设定步长 $n = 8$, 选取 100 个不同的初始值, 在舍去前 100 次的迭代值后, 选取 2500 个 8 位混沌序列值, 并转换产生 20000 个二进制序列. 对这 20000 个二进制序列进行 FIPS140-2 检测的结果如表 3 所示, 其中的各种检测结果的最大值、最小值和平均值均位于测试区间内, 表明 100 组测试均满足 FIPS 140-2 的随机性要求.

表 3 FIPS140-2 检验结果

测试项		最小值	最大值	平均值	合理区间	结果
频数测试		9879	10190	10037	9725—10225	通过
扑克测试		4.7616	31.5136	16.1160	2.16—46.17	通过
0 游程测试	游程 1	2389	2658	2512	2315—2685	通过
	游程 2	1179	1328	1261	1114—1386	通过
	游程 3	576	683	627	527—723	通过
	游程 4	263	355	315	240—384	通过
	游程 5	127	182	156	103—209	通过
	游程 6+	119	173	148	103—209	通过
1 游程测试	游程 1	2409	2644	2515	2315—2685	通过
	游程 2	1161	1355	1249	1114—1386	通过
	游程 3	574	696	628	527—723	通过
	游程 4	268	349	313	240—384	通过
	游程 5	123	185	157	103—209	通过
	游程 6+	134	183	157	103—209	通过
0 长游程测试		9	14	11.49	< 26	通过
1 长游程测试		10	21	13.89	< 26	通过

表 4 SP800-22 检验结果

测试项目	p 值	结果
频率检测	0.076395	随机
块内频数检验	0.618742	随机
游程检验	0.194155	随机
块内最长游程检验	0.955037	随机
二元矩阵秩检验	0.443138	随机
离散傅里叶匹配检验	0.147084	随机
非重叠模块匹配检验	0.473773 (平均)	随机
重叠模块匹配检验	0.968055	随机
Maurer 的通用统计检验	0.512594	随机
线性复杂度检验	0.663813	随机
序列检验	0.847994 (平均)	随机
近似熵检验	0.311063	随机
累计和检验	0.110778 (平均)	随机
随机游动检验	0.349118 (平均)	随机
随机游动状态频数检验	0.449118 (平均)	随机

④ NIST SP800-22 随机数检测 [16]

对于本文构造的混沌系统 (7) 式, 设定步长 $n = 8$, 选取初值 $x_0 = 0.2323$, 在舍去前 100 次的迭代值后, 选取 12500 个混沌序列值, 转换为 100000 个二进制序列, 进行 NIST SP800-22 的 15 项指标测试, 每项的测试结果均转换为 p 值进行判断 [18]. 表 4 测试结果中, p 值均大于显著性水平 $\alpha = 0.05$, 表明 100 组测试均满足 SP800-22 的随机性要求.

4 结 论

本文构造了一类与 Tent Map 拓扑共轭的混沌系统, 并根据同构关系, 提出了一种产生独立同分布密钥流的方法, 通过理论的证明、结论的推广和密钥流的随机性检测, 表明本文结论可为产生独立同分布密钥流提供更多的非线性系统选择, 解决 Tent Map 在某些参数下快速收敛于零而无法提供密钥流的问题. 希望我们的结论可应用于密码学、数值模拟等众多领域.

[1] Hu H P, Liu S H, Wang Z X, Wu X G 2004 *Chin. J. Comput.* **27** 408 (in Chinese) [胡汉平, 刘双红, 王祖喜, 吴晓刚 2004 计算机学报 **27** 408]

[2] Xiang F, Qiu S S 2008 *Acta Phys. Sin.* **57** 6132 (in Chinese) [向菲, 丘水生 2008 物理学报 **57** 6132]

[3] Hao B L 1995 *Starting with Parabola: An Introduction to Chaotic Dynamics* (Shanghai: Shanghai Scientific and Technological Education Publishing House) pp12–15 (in Chinese) [郝柏林 1995 从抛物线谈起 —— 混沌动力学引论 (上海: 上海科技教育出版社) 第 12—15 页]

[4] Alvarez G, Li S 2006 *Int. J. Bifurcat. Chaos* **16** 2129

[5] Lian S G, Sun J S, Wang J W, Wang Z Q 2007 *Chaos, Solitons and Fractals* **34** 851

[6] Phatak S, Rao S 1995 *Phys. Rev.* E **51** 3670

[7] Kanso A, Smaoui N 2009 *Chaos, Solitons and Fractals* **40** 2557

[8] Kocarev L, Jakimoski G 2003 *IEEE Trans. CAS*-I **50** 123

[9] Li J B, Zeng Y C, Chen S B, Chen J S 2011 *Acta Phys. Sin.* **60** 060508

(in Chinese) [李家标, 曾以成, 陈仕必, 陈家胜 2011 物理学报 **60** 060508]

[10] Sun F Y, Lü Z W 2011 *Acta Phys. Sin.* **60** 040503 (in Chinese) [孙福艳, 吕宗旺 2011 物理学报 **60** 040503]

[11] Luo S J, Qiu S S, Luo K Q 2003 *Acta Phys. Sin.* **52** 1871 (in Chinese) [罗松江, 丘水生, 骆开庆 2003 物理学报 **52** 1871]

[12] Luca A, Vlad A 2005 *In Proc. IEEE Int. Symposium on Signals, Circuits and Systems* (ISSCS 2005) Iasi, Romania, July 14–15, 2005 p227

[13] Luca A, Vlad A, Badea B, Frunzete M 2009 *In Proc. IEEE Int. Symposium on Signals, Circuits and Systems* (ISSCS 2009) Iasi, Romania, July 9–10, 2009 p1

[14] Luca A, Ilyas A, Vlad A 2011 *In Proc. IEEE Int. Symposium on Signals, Circuits and Systems* (ISSCS 2011) Bucharest, Romania, June 30–July 1, 2001 p1

[15] NIST http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf [2002]

[16] NIST http://csrc.nist.gov/publications/nistpubs/800-22-revla/SP800-22revla.pdf [2010]

[17] Liu X B, Zhao D A, Zhu Z Y 2006 *J. Jiangsu Univ. Sci. Technol.* (Natural Science Edition) **20** 4 (in Chinese) [刘新波, 赵德安, 朱志宇 2006 江苏科技大学学报 (自然科学版) **20** 4]

[18] Pincus S M 1991 *In Proc. of the National Academy of Sciences of the United States of America* **88** 2297

A class of topologically conjugated chaotic maps of tent map to generate independently and uniformly distributed chaotic key stream*

Xu Zheng-Guang[1)] Tian Qing[1)†] Tian Li[2)]

1) (*School of Automation, University of Science and Technology Beijing, Beijing* 100083*, China*)

2) (*School of Astronautics, Beijing University of Aeronautics and Astronautics, Beijing* 100091*, China*)

(Received 13 January 2013; revised manuscript received 16 February 2013)

Abstract

In this paper, a class of topologically conjugated maps of tent map is established, and the sampling rule is proved to generate the independently and uniformly distributed key streams. One example is given to show that the established chaotic system does not converge into zero in each parameter due to its nonlinear characteristic. Another example with different initial values and lengths of sequence is illustrated, in which the chaotic key stream generated by the proposed theorem is independently and uniformly distributed chaotic system and can successfully satisfy the randomness requirements in Federal Information Processing Standard 140-2(FIPS PUB 140-2) and National Institute of Standards and Technology Special Publication 800-22 (NIST SP800-22) test. The result in this paper can provide the theoretical foundation and more selections of systems to generate independently and uniformly distributed chaotic key stream.

Keywords: independent and identically distributed, chaotic system, tent map, topologically conjugate

PACS: 05.45.Ac, 05.45.Pq, 05.45.Vx **DOI:** 10.7498/aps.62.120501

* Project supported by the National Natural Science Foundation of China (Grant No. 60573058).

† Corresponding author. E-mail: qingtiantq@hotmail.com