第 57 卷 第 7 期 2008 年 7 月
1000-3290/2008/57(07)/4014-07

物 理 学 报
ACTA PHYSICA SINICA

Vol.57, No.7, July, 2008

基于单向耦合映象格子生成伪随机位序列的两种新方法*

傅志坚[1)] 曾以成[1)†] 徐茂林[2)]

1)(湘潭大学材料与光电物理学院,湘潭 411105)

2)(北京信息工程学院,应用数学研究室,北京 100101)

(2007 年 10 月 13 日收到;2007 年 11 月 14 日收到修改稿)

基于时空混沌单向耦合映象格子模型,提出生成伪随机位序列的两种新方法.利用耦合映象格子状态的不变分布特性,选取合适基准对系统中格点状态序列进行判决,生成伪随机位序列;以及基于方向相的思想,通过比较一个格点相邻时间的两个状态值来生成伪随机位序列.对生成序列的性能进行了详细分析,数值实验结果表明,它们具有理想的平衡性、相关性和游程特性,可以应用于信息安全、密码学和数字通信等领域.

关键词:伪随机位序列,单向耦合映象格子,不变分布,方向相

PACC:0545,0250

1. 引 言

伪随机位序列(pseudorandom-bit sequences,PRBS)广泛应用于信息安全[1]、密码学[2]和数字通信[3—5]等领域.快速生成相关性、平衡性和游程特性都很好的 PRBS 是这些应用的关键.

混沌系统具有初值敏感性、参数敏感性、长期不可预测性和各态历经等特性,混沌信号有伪随机性、宽带白谱和不变分布等性质[6].时空混沌单向耦合映象格子(one way coupled map lattices,OCML)是高维混沌系统,时间上、空间上均具有混沌行为,具有更高的随机性和复杂性.因而,利用时空混沌系统生成混沌 PRBS 引起了研究人员的极大兴趣[7—12].目前,生成 PRBS 的方法主要有两类:第一类,量化时空混沌系统状态值的方法[7,8].序列状态值用二进制数表示,再按一定规则从中抽取一些位,依次排列组成二值 PRBS,这种方法每迭代一步可以生成多位符号,但是可能会改变系统的混沌特性.第二类,采用判决方法[9—12].取一个合适的基准(一般取格子状态的数学期望),格点状态值大于它取 1,否则为 -1(或者 0),再依次组成序列,这种方法不改变系统的混沌本质,但是最优的基准很难确定.因此,本文基于 OCML 的不变分布特性和方向相的概念,从改善 PRBS 的平衡性和生成方式出发,提出利用 OCML 模型状态相空间的不变分布特性,选取合适的基准对系统状态序列进行判决生成 PRBS,以及基于方向相的思想生成 PRBS 等两种新方法,数值实验表明均是可行的.

2. 模 型

2.1. 单向耦合映象格子模型

在各种时空混沌模型中,OCML 由于数值计算的高效率、计算过程并行度很好等优点,在时空混沌研究中得到了广泛应用[13].格子数为 L,格点间耦合强度为 $\xi(0<\xi<1)$的系统可表示如下:

$$x_i(n+1)=(1-\xi)f[x_i(n)]+\xi f[x_{i-1}(n)],\quad i=1,2,\cdots,L, \tag{1}$$

式中 n 为离散时间坐标,i 为离散空间坐标,$x_i(n)$ 表示第 i 个格点在时刻 n 的状态值,$f(\cdot)$为格点动

* 国家自然科学基金(批准号:60772015),湘潭大学基金(批准号:KL1054/Z10054)资助的课题.

† E-mail:yichengz@xtu.edu.cn

力学函数 $f(x)=ax(1-x)$，a 是参数.

2.2. 单向耦合映象格子模型的不变分布特性

OCML 系统的时空行为可以分为五种模式，当(1)式中 ξ 和 a 在一定的范围之内时，系统处于完全发展湍流模式[13]，即完全混沌态.这时，当 OCML 系统开始运行后，经过一个短暂的瞬态过程，系统的状态就会达到一种不变分布[14].这种分布受参数 L，ξ，a 的影响，我们可用统计直方图表示.固定这三个参数中的两个，另外一个取不同的值，作相应的不变分布概率曲线，如图 1、图 2 和图 3 所示，从图中可以看出，不变分布受 a 的影响最显著，当 $\xi=0.90$，$a=3.6$ 和 $\xi=0.90$，$a=3.4$ 时，系统的状态集中在两个小的范围中，状态不具有遍历性，系统不处于完全发展湍流模式.数值实验表明，当 a 接近于最大值 4.0 时，具有遍历性.因此，在下面的数值实验中，参数 a 取 4.0.

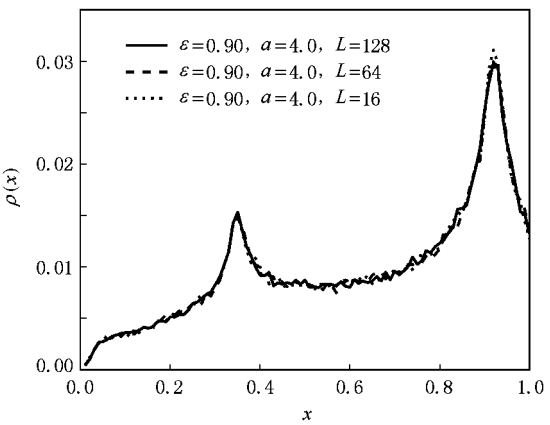

图 1　单向耦合映象格子的格点状态概率分布，L 不同，$\xi=0.90$，$a=4.0$

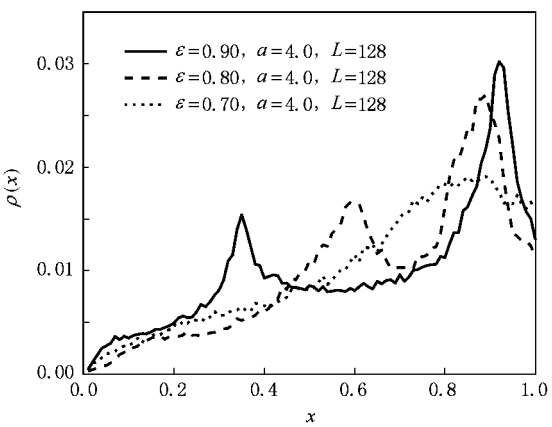

图 2　单向耦合映象格子的格点状态概率分布，ξ 不同，$a=4$，$L=128$

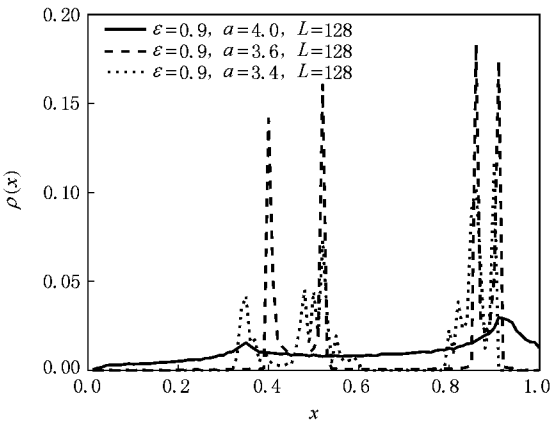

图 3　单向耦合映象格子的格点状态概率分布，a 不同，$\xi=0.90$，$L=128$

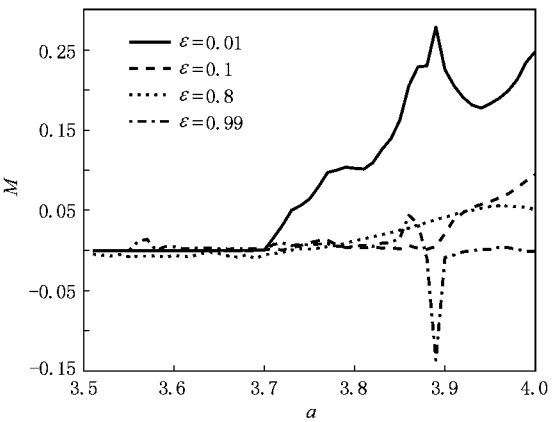

图 4　不同 ξ 下，方向相 M 与格点动力系统非线性参数 a 的关系

2.3. 单向耦合映象格子的方向相

方向相是通过比较格点 $i(1\leqslant i\leqslant L)$ 的相邻时间的状态值 $x_i(n)$，$x_i(n+1)$ 的大小来确定[15].OCML 系统的方向相定义如下：

$$M=(T^{-1}\times L^{-1})\sum_{n=1}^{T}\sum_{i=1}^{L}S_i(n),\qquad(2)$$

式中 T 表示系统迭代的次数，L 表示系统的格点数，当 $x_i(n+1)>x_i(n)$ 时，$s_i(n)=1$，当 $x_i(n+1)<x_i(n)$ 时，$s_i(n)=-1$.OCML 系统的格点状态值在迭代的过程中，有时增大，方向向上；有时减小，方向向下.在整个 OCML 系统中，当 $s_i(n)=1$ 的个数多于 $s_i(n)=-1$ 的个数时，M 大于 0；当 $s_i(n)=1$ 的个数小于 $S_i(n)=-1$ 的个数时，M 小于 0，当 $s_i(n)=1$ 的个数等于 $S_i(n)=-1$ 的个数时，M 等于 0.方向相主要受参数 ξ 和 a 的影响，作出 a 是变量，ξ 取不同值的方向相曲线，如图 4 所示，可见，随

着耦合强度的增大，M 突变的点的 a 值在增大. $\xi = 0.99$ 时，M 值接近于 0，也就是说系统的方向相接近 0.

3. 生成时空混沌伪随机位序列的新方法

OCML 系统产生的时空混沌序列是状态连续的模拟序列，应用时必须对其进行二值符号化. 本文提出基于上述模型性质的两种符号化生成时空混沌 PRBS 的新方法.

方法 1 利用混沌映射不变分布特性选取合适基准对系统状态序列进行判决生成 PRBS，用 $s_k^i, i = 1,2,\cdots,L; k = 1,2,\cdots,N$ 表示生成的序列，定义如下：

$$s_k^i = \mathrm{sgn}\{x_i(n) - x_p\}, \tag{3}$$

式中 x_p 是判决基准. 例如，图 5 所示曲线是某 OCML 系统格子状态的概率曲线，x_p 是概率分布函数等于 0.5 时对应的 x 值，这样大于基准和小于基准的状态各占一半，生成的序列中 -1 和 1 的个数相等. 在确定的 ξ 和 a 下，OCML 系统的不变分布是固定的，且可以预先确定，这样点 x_p 也可以预先求得，作为一个常数. OCML 系统运动后，每迭代一次，用每个格点的状态值和 x_p 比较，大于取 1，小于取 -1，然后组成相应的符号序列.

方法 2 基于方向相的思想来生成 PRBS. 用 $s_k^i, i = 1,2,\cdots,L; k = 1,2,\cdots,N$ 表示 PRBS. 我们可以通过下面的方法对格子的连续状态序列符号化：

$$s_k^i = \begin{cases} 1, x_i(n+1) > x_i(n), \\ -1, x_i(n+1) < x_i(n), \end{cases} \tag{4}$$

式中，当 ξ 和 a 在一定的范围内，OCML 系统处于完全发展湍流模式，方向相接近于 0，因此 $S_i(n) = -1$ 和 $S_i(n) = 1$ 的个数接近相等，即 $s_k^i = 1$ 和 $s_k^i = -1$ 的个数接近相等，PRBS 具有很好的平衡性. 但是，当系统处于完全发展湍流模式时，由于耦合强度参数的作用，在某些耦合强度参数下，各个格点会出现同时增大或者同时减小，达到同步[14]，从而生成的 PRBS 都相同，必须避免这种同步现象，由于不能进行完全的解析分析，对参数空间的数值实验表明，限定耦合强度参数处于区间(0,0.1]或[0.9,1)比较好.

采用这两种方法生成 PRBS 的速度快，具有较高的效率. 第一种方法，寄存 x_p，然后用比较器将格点状态值与之比较即可获得相应符号；第二种方法，在系统迭代过程中，只需要使用寄存器，寄存格点前一次的状态值，再利用比较器与当前值比较即可以生成 PRBS，且这个方法不需要对 OCML 系统有先验知识，如数学期望，可以避免由于求这些值而产生的误差. 虽然对状态值量化的方法每迭代一次可以生成多位符号，但是量化过程数字电路实现相对复杂，会降低速度.

L 个格点的 OCML 系统，由(1)式和(3)式或由(1)式和(4)式可以同时产生 L 个时空混沌符号序列. 如把每个格子作为一个 PRBS 发生器，如图 6 所示，则可同时生成 L 路 PRBS，极大提高生成 PRBS 的效率和实时性.

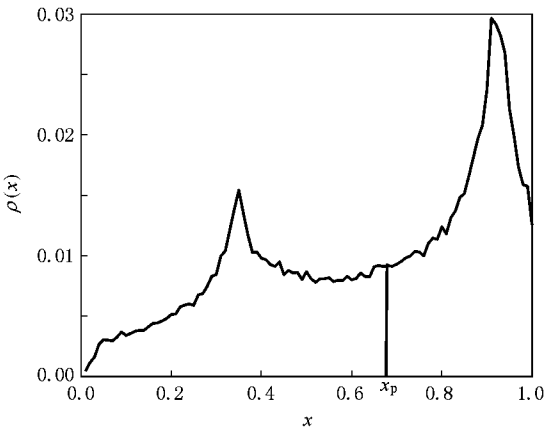

图 5 OCML 系统一个格点状态统计分布

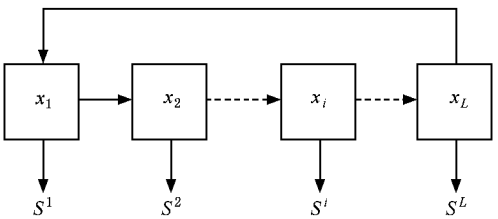

图 6 时空混沌 PRBS 发生器框图

4. 时空混沌伪随机位序列的性能分析

本节对二进制数表示生成的序列 OCML-PRBS1、数学期望作为基准的方法生成的序列 OCML-PRBS2 和本文提出的基于不变分布选取基准的方法生成的序列 OCML-PRBS3 以及利用方向相生成的序列 OCML-PRBS4 的性能进行比较分析. PRBS 用于信息安全、密码学和数字通信等领域时，主要考虑相关性、游程特性和平衡性三个方面的性能[16]. 伪随机序列的这些性能目前还不能做出解析式的分析，我们在 Matlab 平台上，通过 Monte Carlo 仿真了

1000 次，对数据进行了处理，仿真结果列在表 1、表 2 和表 3 之中.

4.1. 相关特性

相关特性是混沌 PRBS 的一个很重要的性能. 理想的 PRBS 其自相关为 δ 函数，互相关函数恒等于 0，序列之间相互正交，这样可以保证安全性和通信中多用户环境中互不干扰等. 对两个二值序列 $S^i(N)$ 和 $S^j(N)$，其相关定义如下：

$$C_{ij}(\tau) = \frac{\sum_{l=1}^{N} S^i(l) S^j(l+\tau)}{\sum_{l=1}^{N} [S^i(l)]^2}. \qquad (5)$$

当 $i = j$ 时表示自相关，$i \neq j$ 时表示互相关. 在数值实验中，对上述四种方法生成的 PRBS 分别求长度为 128，512，1024 和 4096 时的自相关和互相关，得到不同序列的自相关旁瓣最大值，自相关均值，互相关最大值和互相关均值，如表 1 所示，可以看出所有序列多具有较好的相关性能. 图 7(a) 是 OCML-PRBS3 的自相关，接近 δ 函数. 图 7(b) 是 OCML-PRBS3 的互相关函数接近 0. 图 7(c) 是 OCML-PRBS4 自相关，通过观察发现，当 $\tau = \pm 1$，序列的自相关值比较大，但是当 τ 是其他值时，序列的自相关值很小，接近于 0. 图 7(d) 是 OCML-PRBS4 互相关，它也是接近于 0 的. 因此，这两种方法生成的序列能够满足各种应用对 OCML-PRBS 相关性能的要求.

表 1　不同序列的相关性能

序列长度	序列名称	自相关旁瓣最大值	自相关均值	最大互相关	互相关均值
128	OCML-PRBS1	0.1992	0.0472	0.2192	0.0468
	OCML-PRBS2	0.2179	0.0492	0.2120	0.0482
	OCML-PRBS3	0.1990	0.0471	0.2018	0.0468
	OCML-PRBS4	0.3345	0.0540	0.2189	0.0518
512	OCML-PRBS1	0.1548	0.0235	0.1273	0.0233
	OCML-PRBS2	0.1562	0.0248	0.1327	0.0243
	OCML-PRBS3	0.1190	0.0235	0.1196	0.0234
	OCML-PRBS4	0.3337	0.0266	0.1308	0.0258
1024	OCML-PRBS1	0.0905	0.0166	0.0958	0.0165
	OCML-PRBS2	0.1481	0.0177	0.1059	0.0174
	OCML-PRBS3	0.0904	0.0166	0.0912	0.0165
	OCML-PRBS4	0.3340	0.0187	0.0997	0.0182
4096	OCML-PRBS1	0.0511	0.0083	0.0533	0.0082
	OCML-PRBS2	0.1473	0.0096	0.0708	0.0095
	OCML-PRBS3	0.0510	0.0083	0.0526	0.0082
	OCML-PRBS4	0.3342	0.0093	0.0576	0.0091

4.2. 游程特性

把随机序列中连续出现 0 或 1 的子序列称为游程. 连续的 0 或者 1 的个数称为游程长度. 随机序列中长度为 1 的游程约占游程总数的 1/2，长度为 2 的游程约占游程总数的 $1/2^2$，…. 一般说来，长度为 m 的游程约占 $1/2^m$，且任意长度 0 的游程个数和 1 的游程个数约各占一半[17]. 表 2 是上述四种方法生成的 PRBS 的游程长度为 1，2，3，4，5 游程数占游程总数的比值. 可以看出 OCML-PRBS1 和 OCML-PRBS3 具有很好的游程特性. OCML-PRBS2 和 OCML-PRBS4 的游程特性稍差.

4.3. 平衡性

平衡性是指 PRBS 中 -1 和 1 的个数接近相等. 表 3 中的数据由 $|k_{-1} - k_1|/N$ 计算得到，k_{-1} 表示符号 -1 的个数，k_1 表示符号 1 的个数，N 表示符号的总个数. 使用 x_p 作为基准来生成扩频序列，实际上就是基于序列的平衡性能，因此序列的平衡性能自然比较理想. 从表 3 中可以看出所有序列中，符号 -1，1 的个数相都差不大，其中 OCML-PRBS3 的平衡性最好，而使用数学期望作为基准生成的 OCML-PRBS2 的平衡性最差.

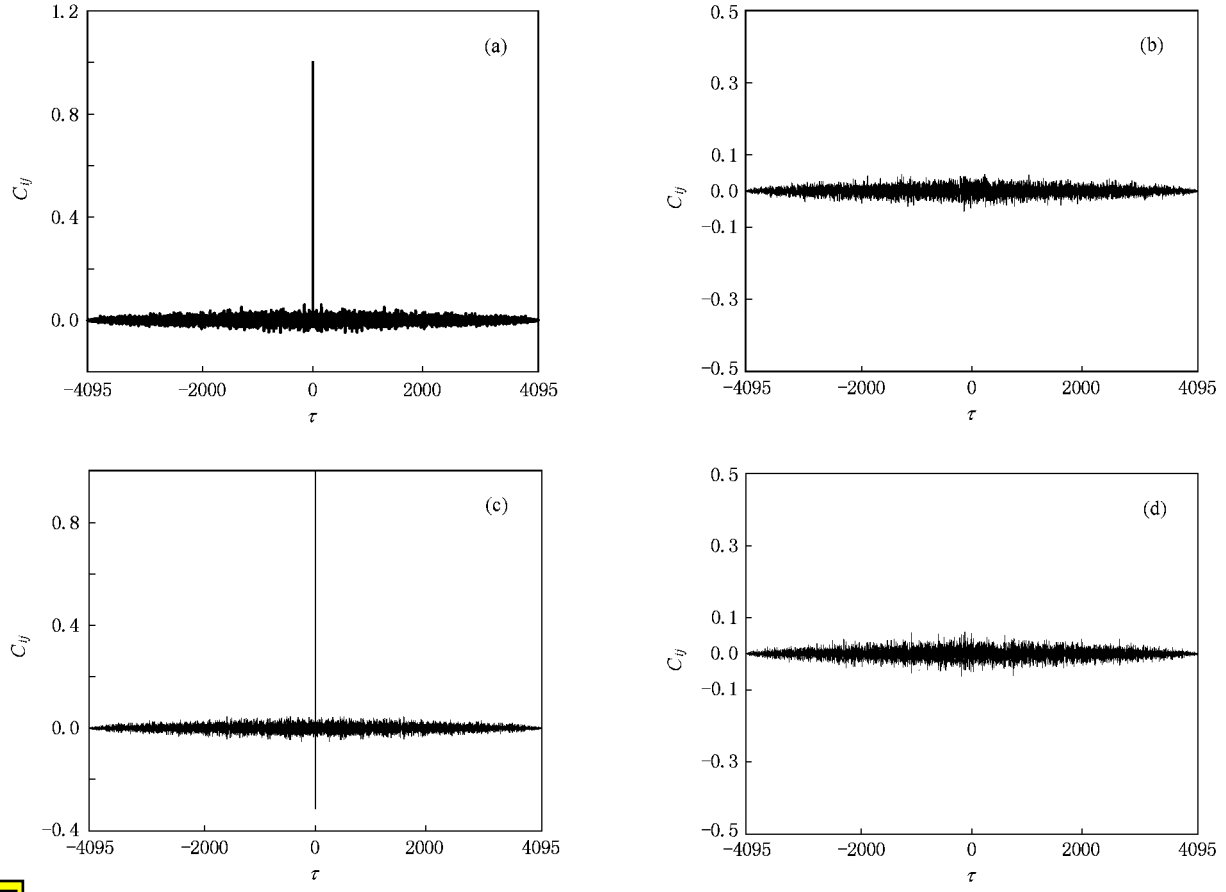

图 7 (a) OCML-PRBS3 **序列的自相关**($N = 100000, L = 128, \xi = 0.90$);(b) OCML-PRBS3 **序列的互相关**($N = 100000, L = 128, \xi = 0.90$);(c) OCML-PRBS4 **序列的自相关**($N = 100000, L = 128, \xi = 0.99$);(d) OCML-PRBS4 **序列的互相关**($N = 100000, L = 128, \xi = 0.99$)

表 2 不同长度游程占总游程数的比值

游程长度	1	2	3	4	5
OCML-PRBS1	0.5038	0.2494	0.1248	0.0617	0.0303
OCML-PRBS2	0.5040	0.2497	0.1239	0.0615	0.0306
OCML-PRBS3	0.5043	0.2501	0.1238	0.0614	0.0305
OCML-PRBS4	0.6292	0.2729	0.0776	0.0168	0.0030

表 3 1 与 −1 个数之差与符号总个数比值

序列长度	128	512	1024	4096
OCML-PRBS1	0.2293×10^{-3}	0.45487×10^{-3}	0.0786×10^{-3}	0.0259×10^{-3}
OCML-PRBS2	0.0328	0.0327	0.0325	0.0325
OCML-PRBS3	0.8093×10^{-4}	0.6879×10^{-4}	0.6496×10^{-4}	0.1015×10^{-4}
OCML-PRBS4	0.0069	0.0067	0.0067	0.0067

5. 结论与讨论

本文基于 OCML 的不变分布和方向相思想,给出了两种生成时空混沌 PRBS 的新方法,并对序列性能进行了详细分析.结果表明,新方法生成的时空混沌 PRBS 具有很好的相关性、游程特性和平衡性.此外,由于时空混沌系统在时间上和空间上都具有混沌性,以及混沌系统的初值敏感性和参数敏感性,保密性高,且在合适的耦合强度参数 ξ 和格点动力

学函数的非线性参数 a 的范围内，ξ 和 a 的微小变动都会产生完全不同的 PRBS，而这些序列的性能不会改变，这样可以生成数量众多的可用序列，ξ 和 a 还可以作为密匙. 所以，基于 OCML 系统，可以生成性能优良、数量众多，保密性好，适合应用在信息安全、密码学和数字通信等领域的 PRBS.

[1] Deng H, Hua Y, Ni W 1999 *J. of China Institute of Comm.* **20**(4) 29

[2] Su S, Lin A, Yen J C 2000 *Proc. APCCAS* 335

[3] Zhang Q, Zheng J 2000 *Proc. APCCAS* 642

[4] Xiao J H, Hu G, Qu Z L 1996 *Phys. Rev. Lett.* **77** 4162

[5] Zhang X, Shen K 2002 *Acta. Phys. Sina.* **51** 2701 (in Chinese) [张　旭、沈　科 2002 物理学报 **51** 2701]

[6] Abel A, Schwarz W 2002 *Proceedings of the IEEE* **90** 691

[7] Li P, Li Z, Halang W A, Chen G R 2006 *Phys. Lett.* A **349** 467

[8] Wang X G, Zhan M, Gang X F, Lai C H, Lai Y C 2005 *Phys. Lett.* A **334** 30

[9] Xia Y X, Shan X M, Ren Y, Yin X H, Liu F 2001 *Phys. Rev.* E **64** 067201

[10] Li N, Shan X M, Ren Y, Xia Y X, Yin X H 2002 *Systems Engineering and Elcetronics* **24**(11) 60 (in Chinese) [李　宁、山秀明、任　勇、夏永祥、尹逊和 2002 系统工程于电子技术 **24**(11) 60]

[11] Tang Q L, Yao H T, Qin T F 2002 *Journal of Guangxi University* **27**(1) 87 (in Chinese) [唐秋玲、姚海涛、覃团发 2002 广西大学学报 **27**(1) 87]

[12] Peng J, Li X M 2005 *Computer Science* **32** 196 (in Chinese) [彭　军、李学明 2005 计算机科学 **32** 196]

[13] Yang W M 1994 *Advanced Series in Nonlinear Science Spatiotemporal Chaos and Coupled Map Lattices* (Shanghai: Shanghai Scientific and Technological Education) p17 (in Chinese) [杨维明 1994 时空混沌和耦合映象格子(上海科技教育出版社)第 17 页]

[14] Zeng Y C, Tong Q Y 2003 *Acta. Phys. Sina.* **52** 285 (in Chinese) [曾以成、童勤业 2003 物理学报 **52** 285]

[15] Wang W, Liu Z H, Hu Bambi 2000 *Phys. Rev. Lett.* **84** 2610

[16] Golomb S W 1976 *Shift Register Sequence* Holden-Day

[17] Zeng Y F, Li H 2005 *The Principle of Spread Spectrum Communication* (Beijing: China Machine Press) (in Chinese) [曾一凡、李　晖 2005 扩频通信原理(北京 机械工业出版社)]

Two novel methods for generating spatiotemporal chaotic pseudorandom-bit sequences based on one way coupled map lattices*

Fu Zhi-Jian[1] Zeng Yi-Cheng[1)†] Xu Mao-Lin[2)]

1)(*Faculty of Materials, Optoelectronics and Physics, Xiangtan University, Xiangtan* 411105, *China*)

2)(*Group of Applid Mathematics, Beijing Information Technology Institute, Beijing* 100101, *China*)

(Received 13 October 2007; revised manuscript received 14 November 2007)

Abstract

Two novel methods for generating spatiotemporal chaotic pseudorandom-bit sequences (PRBS) based on the one way coupled map lattices (OCML) model are proposed. In the first one, the symbolic sequences are generated by a partition, which is based on the statistic property of the state of the one way coupled map lattice. And in the other, the sequences are obtained by comparing the two consecutive state values of a single lattice of the OCML. We compareed the performance of these two types of sequences with the conventional ones. The numerical experiments demonstrated that the sequences have ideal randomicity, excellent correlation and run-length distribution, and they are good candidates for information security, cryptography and spread-spectrum communications.

Keywords: pseudorandom-bit sequences, one way coupled map lattices, statistic distribution, direction phase

PACC: 0545, 0250

* Project supported by the National Natural Science Foundation of China (Grant No. 60772015) and the Science Foundation of Xiangtan University, China (Grant No. KL1054/Z10054).

† E-mail: yichengz@xtu.edu.cn