基于耦合映像格子模型的时空混沌二值序列及其性能分析*)

彭 军[1,2] 李学明[2] 张 伟[3] 廖晓峰[2] Eiji Okamoto[4]

(重庆工业高等专科学校计算机系 重庆400050)[1] (重庆大学计算机科学与工程学院 重庆400044)[2]

(重庆教育学院计算机与现代教育技术系 重庆400067)[3]

(筑波大学系统与情报工学研究科 筑波305-8573 日本)[4]

摘 要 基于耦合映像格子模型,给出了一种时空混沌二值序列的产生方法,并对其性能进行了详细分析。结果表明,该种时空混沌二值序列具有十分理想的随机性和相关性。此外,混沌序列容易产生和控制,具有线性复杂度高、对参数敏感等特性,因此特别适合于在保密通信和密码学等诸多领域中应用。

关键词 耦合映像格子,时空混沌,二值序列,保密通信

A Spatiotemporal Chaotic Binary Sequence Based on Coupled Map Lattices Model and its Performance Analysis

PENG Jun[1,2] LI Xue-Ming[2] ZHANG Wei[3] LIAO Xiao-Feng[2] Eiji Okamoto[4]

(Department of Computer Science, Chongqing Polytechnic College, Chongqing 400050)[1]

(Department of Computer Science and Engineering, Chongqing University, Chongqing 400044)[2]

(Dept. of Computer & Modern Education Technology, Chongqing Education College, Chongqing 400067)[3]

(Graduate School of Systems and Information Engineering, University of Tsukuba, Tsukuba 305-8573, Japan)[4]

Abstract In this paper, a technique of generating spatiotemporal chaotic binary sequences based on coupled map lattices model is proposed and the performances of binary sequences are analyzed in detail. The results indicate that this kind of spatiotemporal chaotic binary sequence has very ideal randomicity and excellent correlation. Moreover, chaotic sequences can be easily generated and controlled, and possess properties of higher linear complexity and sensitivity with respect to the system parameters, so they are very suitable to application in secure communication and cryptology.

Keywords Coupled map lattices, Spatiotemporal chaos, Binary sequences, Secure communication

1 引言

我们知道,传统密码学中常用的两种加密方法是分组密码和序列密码[1]。大多数分组密码如 DES, GOST, Lucifer, FEAL 等都是基于 Feistel 网络结构的,并精心设计了 S-盒或 P-盒,以提高密码系统的强度,此类密码的安全性依赖于密钥的安全。而序列密码采用的方法比较简单,由一个伪随机序列发生器(多数是围绕 LFSR 而设计的)产生一串伪随机序列,再与明文进行异或得到密文,序列密码的安全性依赖于伪随机序列的随机性和不可预测性,也就是说其核心问题是伪随机序列发生器的设计。目前广泛采用的序列如 m-序列,由于线性复杂度低,当采用高效的 Berlekamp-Massey 算法[18,19]时,仅需检测序列的 $2n$ 个输出位后就能够重构 LFSR,从而破译该系统[1]。因此如何借助新的手段来产生复杂度高的随机序列成为密码学界普遍关注的问题。

由于混沌序列具有类噪声、宽频谱、复杂度高、难以预测和对参数敏感等许多符合密码学要求的特性,因此正逐渐受到人们的重视[2~6]。但是采用单一的低维混沌系统存在被攻破的潜在危险,如文[7]使用的非线性动力学预测或回归映射方法,以及文[8]使用的神经网络方法等都可以成功地重构混沌系统,从而使基于混沌的保密通信系统失效。于是人们开始尝试使用超混沌系统[9]、带时延的混沌系统[10]或时空混沌系统[11~14],以期提高系统的安全性能。

本文将基于耦合映像格子模型[12],研究时空混沌序列的二值化方法,并对二值序列进行了详细的性能分析。结果表明,本文给出的时空混沌二值序列具有多项优良特性,可广泛应用于保密通信和密码学等领域。

2 耦合映像格子模型

采用文[12]中的一维耦合映像格子模型(CML, one-dimensional coupled map lattices)。

$$x_{n+1}^i=(1-\gamma_1-\gamma_2)f(x_n^i)+\gamma_1 f(x_n^{i-1})+\gamma_2 f(x_n^{i+1}) \quad (1)$$

式中 x_n^i 表示第 i 个格子在 n 时刻的状态,f 为格子的局部状态演化方程,一般取混沌映射。γ_1 和 γ_2 为耦合系数,$\gamma_1>\gamma_2\geqslant 0$,如果 $\gamma_2=0$ 则模型(1)简化为如下形式的单向耦合映像格子模型:

$$x_{n+1}^i=(1-\gamma_1)f(x_n^i)+\gamma_1 f(x_n^{i-1}) \quad (2)$$

对于一个开流系统,边界条件对系统的动力学特性影响很大[14]。本文假设系统(1)具有如下形式周期边界条件:

$$x_n^{L+i}=x_n^i,\forall\ n\in Z \quad (3)$$

其中 L 为系统规模即格子的数量。函数 f 取为 Logistic 映射:

$$f(x_n)=1-\alpha x_n^2,\ -1\leqslant x_n\leqslant 1 \quad (4)$$

*)基金项目: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项目基金(7370);重庆工业高等专科学校科研基金。彭 军 副教授,博士,研究方向为网络安全,混沌保密通信。张 伟 副教授,博士,研究方向为网络安全,计算智能。李学明 副教授,博士,研究方向为网络安全,数据挖掘。廖晓峰 教授,博士后,博士生导师,研究方向为神经网络,信号处理,混沌保密处理。

当控制参数 $a=2$时，每个格子都处于混沌状态。图1为格子数 $L=100$时系统(1)的时空演化图(演化了300步)。

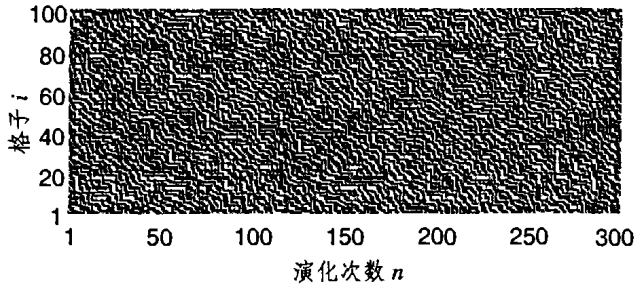

图1 L=100时系统(1)的时空演化图

文[14]研究了系统(1)的同步问题，当用一个混沌信号作为初始驱动序列，耦合系数 γ_1 和 γ_2 取适当值时可实现两个系统(驱动系统和响应系统)的时空混沌同步，进而可实现保密通信。为此我们使用 Chebyshev 映射产生混沌驱动序列，见式(5)，控制参数 $w=2$。驱动序列也可以由分段线性映射、Chua 电路或 Lorenz 系统产生。

$$x_{n+1}=\cos(2^w\arccos(x_n)),w\in Z^+,-1\leqslant x_n\leqslant 1 \qquad (5)$$

下面我们主要研究由系统(1)生成的时空混沌序列的二值化问题，并对二值化序列进行性能分析。

3 时空混沌二值序列

如果系统(1)具有 L 个格子，则可产生 L 个时空混沌序列，这些序列都是连续的实值序列，需要将其二值化后才能用于如扩频通信、数字图像加密等场合。在实验中，耦合系数 $\gamma_1=0.8,\gamma_2=0.01$，式(5)的初值 $x_0=0.6$，我们发现由(1)产生的混沌序列的随机性不是很好，当 $L=100$时，用式(5)生成的序列作为系统(1)的驱动序列并演化1000步，任取一个格子序列考察其密度分布，均具有类似图(2)的分布形态。从图中可看出分布不是关于0点对称的，序列值更多地分布在0～1之间，若用阈值0来符号化该序列将得到一个平衡性不理想的二值序列，因此需要采用另外的二值化方法来克服这个问题。

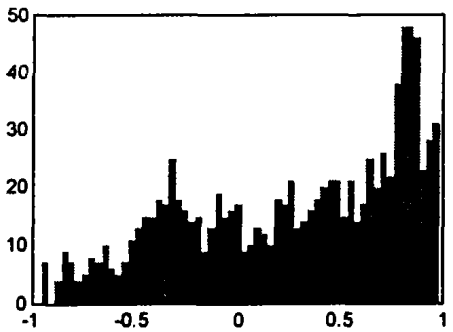

图2 时空混沌序列的密度分布图

文[15]给出了一种比较可行的方法。先将某个格子序列取反，再与另一个格子序列相加，这样得到的序列其分布基本上是关于0点对称的，然后用阈值0对其进行符号二值化操作。例如对格子序列 x_n^3 和 x_n^4，按上述思想处理后可得到如下两个新的序列 $\tilde{x}_n^3$ 和 $\tilde{x}_n^4$

$$\tilde{x}_n^3=(x_n^3-x_n^{10})/2,\tilde{x}_n^4=(x_n^4-x_n^{11})/2$$

它们的分布密度见图3和图4。从处理的结果看，新序列关于0点的对称性得到了很大的改善，这一点对获得性能优良的二值化序列是很关键的。

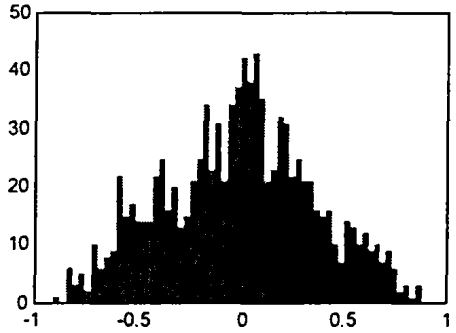

图3 序列 $\tilde{x}_n^3$ 的密度分布图

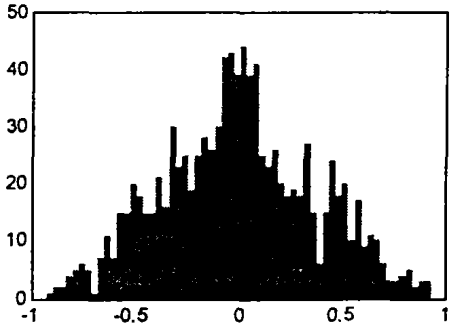

图4 序列 $\tilde{x}_n^4$ 的密度分布图

4 二值序列性能分析

本节我们将对时空混沌二值序列的多项性能进行分析，包括序列的01平衡性、独立均匀分布特性(序列检验)、游程特性、相关特性、线性复杂度、周期和参数敏感性。如果不特别说明，实验中格子数均为40，序列长度则根据需要进行指定。

4.1 平衡性检验

平衡性是指序列中的"1"与"0"的数目应该相等。为检验平衡性，我们构造如下 χ^2 统计量：

$$\chi^2=\frac{(n_0-n_1)^2}{N} \qquad (6)$$

式中 n_i 表示序列取值 i 的个数，N 为序列长度。当显著性水平取为5%时，对应的 χ^2 值为3.841。如果该统计量的值小于3.841，则该序列通过检验。对不同序列长度的混沌二值序列进行实验，结果见表1。从该表中 χ^2 项的数值看，实验中每种长度的序列都通过了检验，表明二值序列具有很好的平衡性。

表1 时空混沌二值序列平衡性检验

项目	序列长度 N				
	500	2000	5000	10000	50000
0的个数	256	987	2542	5031	24863
1的个数	244	1013	2458	4969	25137
χ^2	0.2880	0.3380	1.4112	0.3844	1.5015

4.2 序列检验

序列检验用来判定转移概率是否合理，即出现相同和不相同相邻元素的概率大致相等。令 n_{00} 表示00的个数，n_{11} 表示11的个数，n_{10} 表示10的个数，n_{01} 表示01的个数。记 $n_0=n_{00}+n_{10}$，$n_1=n_{01}+n_{11}$，则可以证明如下统计量[16]

$$\chi^2=\frac{4}{n-1}\sum_{i=0}^{1}\sum_{j=0}^{1}(n_{ij})^2-\frac{2}{n}\sum_{i=0}^{1}(n_i)^2+1 \qquad (7)$$

近似服从自由度为2的 χ^2 分布，当显著性水平取为5%时，对应的 χ^2 值为5.991。

驱动序列取不同初值(可由随机数产生),对200组长度均为20000的混沌时空序列进行了序列检验,结果通过率为97.5%。

4.3 游程特性

S. W. Golomb[17]在其提出的序列随机性公设第2条中指出,在一个长度为 T 的周期内,1游程的个数占游程总数的1/2,2游程的个数占游程总数的$1/2^2$,…,d 游程的个数占游程总数的$1/2^d$,而任意长度的0的游程个数与1的游程个数相同。

取序列长度分别为128、256、512、1024和2048,表2为每个长度下100组时空混沌序列各个游程的平均值,我们只给出了前面5个游程的实验数据。从表2中的数据可看出,时空混沌序列能很好地满足 Golomb 提出的对随机序列的游程特性要求。

表2 时空混沌二值序列游程特性

项目	序列长度 N				
	128	256	512	1024	2048
1游程	0.5050	0.4961	0.4985	0.5005	0.4994
2游程	0.2568	0.2481	0.2535	0.2544	0.2541
3游程	0.1279	0.1225	0.1273	0.1289	0.1285
4游程	0.0627	0.0603	0.0638	0.0656	0.0656
5游程	0.0309	0.0300	0.0321	0.0335	0.0332

4.4 相关特性

相关特性是混沌序列应用于扩频通信和密码学的一个很重要性质。我们期望混沌序列的自相关函数类似于函数 δ,而互相关函数接近于零。设 $a^{(1)}$,$a^{(2)}$代表长度为 N 的两个不同的序列,根据相关性定义,序列 $a^{(1)}$和 $a^{(2)}$的非周期互相关函数为:

$$C_{a^{(1)},a^{(2)}}(m)=\begin{cases}\dfrac{1}{N}\sum_{i=0}^{N-1-m}a_i^{(1)}(a_{i+m}^{(2)})^*, & 0\leqslant m<N\\ \dfrac{1}{N}\sum_{i=0}^{N-1+m}a_{i-m}^{(1)}(a_i^{(2)})^*, & 1-N\leqslant m<0\\ 0, & |m|\geqslant N\end{cases}\tag{8}$$

当 $a^{(1)}=a^{(2)}$时,式(8)即为序列的非周期自相关函数。实验中我们随机地抽取了两个时空混沌序列,如第3节中的 $\tilde{x}_n^3$和 $\tilde{x}_n^4$,计算了 $\tilde{x}_n^3$ 的自相关函数以及 $\tilde{x}_n^3$ 与 $\tilde{x}_n^4$ 的互相关函数,我们截取相关间隔为−500～500,并进行归一化处理,对应的结果如图5和图6所示。理想的自相关特性是当 $N\to\infty$时有 $C(0)\to0.5$和 $C(m)\to0(m\neq0)$,而互相关函数处处为零。但由于受计算精度的影响,序列的长度不能无限长,导致自相关旁瓣和互相关函数不是恒为零。即使这样,从测试结果看,我们给出的时空混沌序列的自相关特性和互相关特性还是比较理想的。

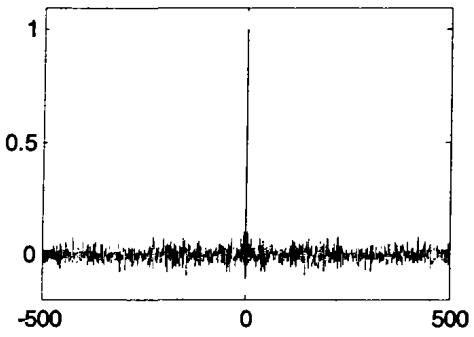

图5 序列 $\tilde{x}_n^3$ 的自相关函数

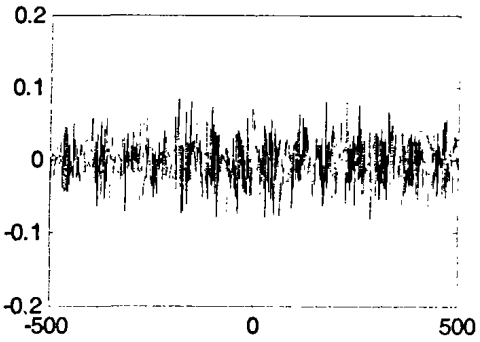

图6 序列 $\tilde{x}_n^3$ 与 $\tilde{x}_n^4$ 的互相关函数

4.5 线性复杂度

线性复杂度在密码学中的重要意义在于:对于一个线性复杂度为 n 的序列,只要知道$2n$ 个任意连续码元,就可以给出该序列的等效线性反馈逻辑,从而复制出该序列[1]。因此序列的线性复杂度越高,其被破译的可能性就越低。

Berlekamp-Massey 算法[18,19]可在多项式时间 nL 内计算出线性复杂度为 L 的 n 长序列的线性复杂度。表3给出了用 B-M 算法计算的时空混沌序列的线性复杂度。由文[19,20]知,对于一个长为 N 的独立等概率同分布二进制随机序列,其线性复杂度应逼近于 $N/2$,并且不论序列有多长,其线性复杂度的方差都逼近于一个常数86/81。从表3中的计算结果得知,时空混沌二值序列具有十分理想的线性复杂度,即 $LC\approx N/2$。

表3 时空混沌二值序列的线性复杂度

项目	序列长度 N				
	256	512	1024	2048	4096
线性复杂度 LC	127	255	511	1024	2047

4.6 周期性

理论上混沌实值序列的周期应该是无限长的,然而在二值化时,由于计算机的有限字长效应,使得混沌二值序列的周期缩短。本文给出的时空混沌二值序列也存在同样问题。

为了有效克服混沌系统因有限精度效应而产生的短周期行为,我们可以采用更高计算精度的计算机,或者用伪随机发生器(PRNG)产生的伪随机数去扰动混沌轨道,以改善离散轨道的遍历性,也可以采用 m-序列与混沌序列相结合的方式[21,22]。例如周红等[21]利用 m-序列与有限精度下的混沌二值序列进行异或得到新的二值序列,同时将其延时一个时间单位后反馈给混沌系统,以产生下一个有限精度混沌二值序列。此方法能保证得到的新的混沌二值序列的周期是 m-序列周期的整数倍。因此我们可以采用类似的方法,以满足工程应用中对时空混沌二值序列长周期的需求。

4.7 参数敏感性

混沌序列对系统参数和初值的极端敏感依赖性是混沌系统固有的特性。这主要是由于系统的 Lyapunov 指数大于零,导致从相似初始值出发的两条轨道随着时间的演化将以指数速率相分离。对时空混沌二值序列的参数敏感性进行实验,驱动系统(5)取不同初值和不同控制参数,实验结果见表4。现举例说明:如第1列数据,驱动序列初值分别取0.300000和0.299999(仅相差10^{-6}),控制参数 w 取相同值2,时空混沌序列长度为1000,这样就可以得到两组混沌二值序列,每组都有

(下转第232页)

合图像，保留了不同聚焦点图像中的清晰区域及其各种特征信息，融合效果优于其它几种融合方法。而且，将本文的方法应用于医学图像融合，效果也较理想。

融合算法中，保留低频部分的比例参数 R 和区域局部能量计算选择的窗口大小参数 W 的选择，根据不同的图像有所不同，使用的时候可以根据情况通过经验和实验的方法选取。此外，对于小波分解层数的选取，本文中是直接选择了一层小波分解，使用时根据图像的不同，也可以选择多层小波分解，这样，可以保留更多的高频分量参与局部能量的判定分析，提高融合效果。

参 考 文 献

1 Aggarwal J K. Multisensor Fusion for Computer Vision [M]. Berlin Heidelberg, Springer-Verlag, 1993

2 朱述龙，张占睦. 遥感图像获取与分析[M]. 北京：科学出版社，2000

3 Pohl C, Van Genderen J L. Multi-sensor image fusion in remote sensing: concepts, methods, and applications [J]. IntJ Remote Sensing, 1998, 19(5): 823～854

4 Varshney P K. Multi-sensor data fusion [J]. Electron & Commun Eng J, 1997, 9(6): 245～253

5 Yocky D A. Image merging and data fusion by means of the discrete two dimensional wavelet transform [J]. J. Opt Soc Am A, 1995, 12(9): 1834～1841

6 焦李成，保铮. 小波理论与应用：进展与展望[J]. 北京：电子学报，1993, 21(7): 91～96

7 Daubechies I. Orthogonal bases of compactly supported wavelets [J]. Com. Pure Appl. Math., 1988, 41(2): 909～996

8 徐飞，施晓红著. MATLAB 应用图像处理[M]. 西安：西安电子科技大学出版社，2002. 5

（上接第198页）

40个序列（格子数为40）。计算每个格子对应的两个序列的位变化率，然后对40个格子序列的计算结果求平均值，得到表4中的位变化率50.53%。其他列的数据均按此方法产生。

表4 时空混沌二值序列的参数敏感性

项目	序列长度 N			
	1000	2000	5000	10000
测试条件	x0=0.300000	x0=0.300000	x0=0.300000	x0=0.300001
（x0为驱动系统初值，w 为	x0=0.299999	x0=0.300000	w=2	w=2
驱动系统控制参数）	w=2	w=2	w=3	w=3
位变化率(%)	50.53	49.77	50.14	49.93

表4中的实验结果表明，时空混沌二值序列对驱动系统的初值和参数非常敏感，不同初值和控制参数下得到的二值序列都有接近50%的位变化率，因此对参数进行猜测都将导致对序列破译的失败。

结论 本文基于一维耦合映像格子模型，用 Chebyshev 混沌映射作为驱动序列，给出了时空混沌二值序列的产生方法，并对二值序列的性能进行了详细分析。分析结果表明，本文讨论的时空混沌二值序列具有十分理想的随机性和相关性。由于混沌序列的产生非常方便，只需修改驱动系统的初值和控制参数，就可以产生数量众多性能优良的二值序列，并且序列的线性复杂度高、难以破译，可广泛应用于保密通信、密码学等诸多领域。如用时空混沌二值序列替代 m-序列或 Gold 序列，以满足 CDMA 通信对大容量的需求。

由于耦合映像格子模型可以一次同时产生多个随机序列（与格子的规模有关），因此可利用该模型来设计多路通信系统，以满足如数字图像等大数据对象的多路保密通信需求。本文的进一步工作可研究这种多路保密通信系统，我们将在后续的文章中报道。

参 考 文 献

1 Schneier B. Applied Cryptography: Protocols, algorithm and source code in C(Second Edition). Wiley, New York, 1996

2 Kohda T, Tsuneda A. Pseudonoise sequences by chaotic nonlinear maps and their correlation properties. IEICE Trans. Commun., 1993, E76-B: 855～862

3 Werter M J, An Improved Chaotic Digital Encoder. IEEE Trans. on CAS-II, 1998, 45(2): 227～229

4 Stojanovski T, Kocarev L. Chaos based random number generators Part I: Analysis [cryptography]. IEEE Trans. on CAS-I, 2001, 43(3): 281～288

5 Stojanovski T, Pihl J, Kocarev L. Chaos based random number generators Part II: Practical realization. IEEE Trans. on CAS-I, 2001, 43(3): 382～385

6 Kocarev L, Jakimoski G. Pseudorandom bits generated by chaotic maps. IEEE Trans. on CAS-I, 2003, 50(1): 123～126

7 Pérez G, Cerdeira H A. Extracting messages masked by chaos. Phys. Rev. Lett., 1995, 74(11): 1970～1973

8 Yang T, Lin B Y, Chun M Y. Application of neural networks to unmasking chaotic secure communication. Physica D, 1998, 124(1-3): 248～257

9 Tsay S C, Huang C K, Chiang C T. Design the hyperchaotic cryptosystems via the Gerschgorin theorem. Chaos, Solitons and Fractals, 2004, 19(4): 935～948

10 彭军，廖晓峰，吴中福，等. 一个时延混沌系统的耦合同步及其在保密通信中的应用. 计算机研究与发展，2003, 40(2): 263～268

11 Guptea N, Sharmaa A, Pradhan G R. Dynamical and statistical behaviour of coupled map lattices. Physica A, 2003, 318 (1-2): 85～91

12 Aranson I, Golomb D, Sompolinsky H. Spatial coherence and temporal chaos in macroscopic with asymmetrical couplings. Physical Review E, 1992, 68(24): 3495～3498

13 Xiao J H, Hu G, Qu Z L. Synchronization of spatiotemporal chaos and its application to multichannel spread-spectrum communication. Physical Review E, 1996, 77(20): 4162～4165

14 Jiang Y, Parmananda P. Synchronization of spatiotemporal chaos in asymmetrically coupled map lattices. Physical Review E, 1998, 57(4): 4135～4139

15 李宁，山秀明，任勇，等. 一种实用的时空混沌二值化方法. 系统工程与电子技术，2002, 24(11): 60～63

16 邓浩，华一满，倪皖荪. 混沌伪随机序列和数字语音保密通信. 通信学报，1999, 20(4): 29～35

17 Golomb S W. Shift Register Sequences. Holden-Day, San Francisco, 1967

18 Massey J L. Shift-register synthesis and BCH decoding. IEEE Trans. on IT, 1969, IT-15(1): 122～127

19 Janson B. The shortest feedback shift register, that can generate a given sequence. Advances in Cryptology, EURO CRYPTO'89 (LNCS 435), 1990. 90～99

20 Rueppel R A. Linear complexity and random sequences. Advances in Cryptology, EURO CRYPT'85 (LNCS 219), 1986. 167～188

21 周红. 有限精度混沌系统的 m 序列扰动实现. 电子学报，1997, 25(7): 95～97

22 李一兵，楼喆，李彬. 一种新的复合混沌扩频序列. 哈尔滨工业大学学报，2001, 22(3): 75～79