一种基于混沌控制 m 序列的密钥序列生成方案

詹 明 张翠芳
(西南师范大学电子与信息工程学院 重庆 400715)

摘 要 该文在 Shannon 关于混乱理论的指导下，在混沌吸引子的多维空间中，利用混沌运动的初值敏感性和长期不可预测性，提出了一种生成密钥序列的新方案，详细地论述了密钥序列的生成过程；计算了密钥空间的大小；对所生成的密钥序列作了局部随机性检验和复杂度分析。结果表明，所生成的密钥序列适合数据加密。

关键词 保密通信，混沌，m 序列，密钥序列
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2006)12-2351-04

A Scheme for Generating Key Sequences Based on Chaotic Control of m Sequence

Zhan Ming Zhang Cui-fang
(*School of Electronics and Information Engineering*, *Southwest Normal University*, *Chongqing* 400715, *China*)

Abstract Directed by Shannon's disorder theory, this paper present a scheme for generating key sequences by using the sensitivity to initial values and the long time unpredictability of chaos motion. The generating scheme and process of the key sequence are described in detail. The size of the key space, randomness testing and linear complexity testing are carefully studied by computer simulation. The results indicate that the key sequences satisfy the requirements of data encrypting.

Key words Secure communications, Chaos, *m* sequence, Key sequence

1 引言

混沌信号由于其一系列突出的特点，在保密通信领域中的应用引起了广泛的关注。数字混沌保密通信方案不仅易于控制，保密性强，而且非常容易与现有数字通信系统兼容，近期实用可能性也最大[1,2]。基于混沌的数字保密通信研究，目前主要采用对混沌信号进行处理或借助混沌信号加扰的方法来获取数字混沌序列。根据Shannon在"保密系统的通信理论"中所提出的混乱思想，本文利用吸引子中混沌运动轨迹点在吸引子相空间中位置的初值敏感性和长期不可预测性，与m序列相结合，输出新的密钥序列。

2 生成密钥序列的方案

Shannon提出了混乱和散布这两种影响密码计算量和密文统计特性的理论，使密文与相应密钥之间形成复杂的关系，即使要破译一小段密文，也要同时找出整个密钥，这比采用统计方法确定密钥要困难得多[3]。混沌系统有高度的初值敏感性，微小的初值差异将被迅速扩散。利用混沌运动，依据如下 3 个步骤，将多个不同周期的m序列段交错置乱[4]，既不破坏序列的随机性，又可以扩展序列的周期，达到获得较高加密强度之目的。

(1)在多维混沌系统 A 的吸引子上选择一定数目的点(本文选用蝴蝶吸引子)，以其为中心，设置范数大小依据混沌运动规律而变化的控制空间，各个空间互不重叠；每一个控制空间上，再选择一个本原多项式，并确定其初始状态；

(2)选取另外一个初值不同的相同混沌系统 A，让它做混沌运动。当运动的轨迹点经过某一控制空间时，利用此空间上的本原多项式，输出长度按混沌规律变化的 m 序列段。之后脱离控制空间继续运动，直到进入下一个控制空间。选择控制空间时，保证相邻的两个控制空间是互异的；

(3)线性反馈移位寄存器每启动一定次数或者每生成一定比特数的序列后，计数器发出触发脉冲，改变控制空间本原多项式、初始状态或控制空间数量、中心位置以及范数。如此循环，输出的 m 序列小段构造出整个密钥序列。

3 密钥序列的生成

选取(也可选择其他方程)lorenz 映射，henon 映射，logistic 映射，lozi 映射，帐篷映射，β 映射，chebyshev 映射，作为生成混沌运动的系统。图 1 为生成密钥序列的具体框图。

(1)Chebyshev 映射，为自身和其他混沌方程确定迭代次数，$\lfloor\ \rfloor$表示向下取整。

$$x(n+1)=\cos(k\arccos(x(n))),$$
$$k=3,\quad \text{xche}(n)=\lfloor 1000x(n)\rfloor,\quad x(n)\geq 0.03 \tag{1}$$

(2)Lorenz 方程，根据初始值不同区分为 lorenz(1)和 lorenz(2)。lorenz(1)确定球体控制空间的中心坐标，lorenz(2)确定具体用于生成序列的控制空间。

2005-03-31 收到，2005-12-20 改回
西南师范大学青年基金(swnuq2004025)资助课题

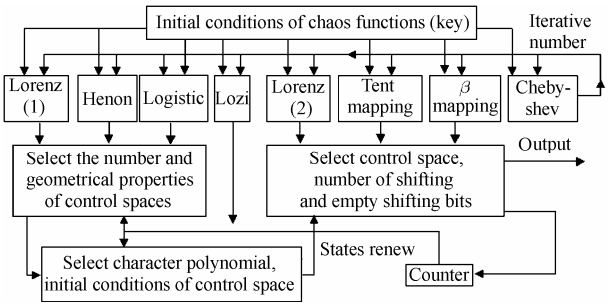

图 1 生成密钥序列的方案

Fig.1 Scheme for generating key sequences

$$\left.\begin{aligned} \mathrm{d}x/\mathrm{d}t &= a(y-x), \quad a=10 \\ \mathrm{d}y/\mathrm{d}t &= bx-y-xz, \quad b=28 \\ \mathrm{d}z/\mathrm{d}t &= xy-cz, \quad c=8/3 \end{aligned}\right\} \tag{2}$$

(3)Logistic 映射的作用是在生成序列之前，确定将要被用于选择的控制空间数目。

$$\left.\begin{aligned} x(n+1) &= ux(n)(1-x(n)), \quad u=0.4 \\ x\log(n) &= \lfloor 40x(n) \rfloor, \quad 0.2 \le x(n) < 1 \end{aligned}\right\} \tag{3}$$

(4)Henon 映射在初始值的作用下，为各个控制空间选取半径。

$$\left.\begin{aligned} x(n+1) &= A - x^2(n) + By(n), \quad A=1.4, \quad B=0.3 \\ y(n+1) &= x(n), \quad x\mathrm{hen}(n) = x(n), \quad 0.1 \le x(n) \le 0.6 \end{aligned}\right\} \tag{4}$$

(5)Lozi 映射有两个变量，分别用于选取控制空间的本原多项式和移位寄存器的初始状态。

$$\left.\begin{aligned} x(n+1) &= 1 + y(n) - A\,|x(n)|, \quad x\mathrm{loz}(n) = \lfloor 40x(n) \rfloor \\ y(n) &= Bx(n), \quad y\mathrm{loz}(n) = \left\lfloor 2^{x\mathrm{loz}(n)-1} y(n) \right\rfloor \\ A &= 1.5, \quad B = 0.4 \end{aligned}\right\} \tag{5}$$

(6)帐篷映射。作用是确定移位寄存器每次移位的长度，消除移位长度规律性。

$$\left.\begin{aligned} x(n+1) &= 2hx(n), \quad 0 < x(n) < 0.5 \\ x(n+1) &= 2h(1-x(n)), \quad 0.5 \le x(n) < 1 \\ h &= 0.89, \quad x\mathrm{zha}(n) = \left\lfloor \frac{4}{3} x\mathrm{loz}(n) x(n) \right\rfloor \end{aligned}\right\} \tag{6}$$

(7) β 映射。确定移位寄存器只移位而不输出的序列长度，消除同一伪随机序列相邻比特段之间的联系。

$$\left.\begin{aligned} x(n+1) &= 2\beta x(n), \quad 0 \le x(n) < 0.5 \\ x(n+1) &= 2\beta(x(n)-0.5), \quad 0.5 \le x(n) \le 1 \\ h &= 0.99, \quad x\beta(n) = \lfloor 50x(n) \rfloor \end{aligned}\right\} \tag{7}$$

输入系统参数，任意地选取初始条件，迭代一定次数后，方程变量再按式(1)–式(7)做相应转化，为密钥序列的生成作初始化准备。

初始化以及随后的状态更新，继承了混沌系统的初值敏感性，微小的初值差异将造成控制空间和本原多项式分配的完全不同。取表 1 中数据，初始化后控制空间的中心位置、半径见图 2(a)，分别将 *x*lor1(1)，*x*hen(1)和 *x*log(1)减小 0.001，控制空间中心位置、半径大小以及数目将有巨大变化，依次见图 2(b)，图 2(c)和图 2(d)。

表 1 混沌方程参数与初始条件

Tab.1 Initial conditions and parameters of chaos functions

混沌方程	lorenz(1)	henon	logistic	lozi
初始条件	*x*1=3.137 *y*1=5.761 *z*1=0.975	*x*(1)=0.374 *y*(1)=0.852	*x* (1)=0.461	*x* (1)=0.157 *y* (1)=0.734
混沌方程	lorenz(2)	帐篷映射	β 映射	chebyshev
初始条件	*x*2=4.381 *y*2=1.095 *z*2=3.278	*x*(1)=0.597	*x* (1)=0.413	*x* (1)=0.628, 初始迭代次数 *N*=10

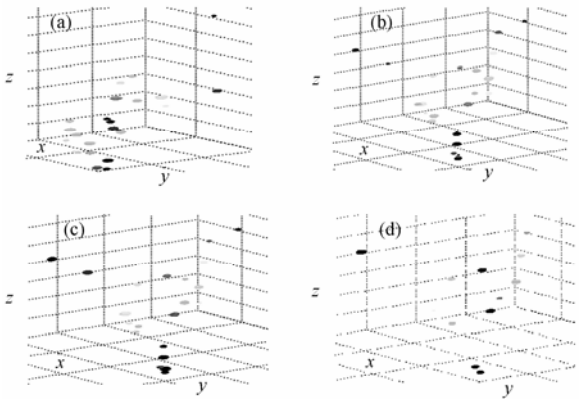

图 2 控制空间几何属性初始化初值敏感性仿真示意图

(a) 取表 1 中数据初始化结果 (b) *x*lor1 减小 0.001

(c) *x*hen(1)减小 0.001 (d) *x*log(1)减小 0.001

Fig.2 Initial conditions' geometrical sensitivity of control spaces

(a) Results of using data of table 1 (b) *x*lor(1) decreases by 0.001

(c) *x*hen(1) decreases by 0.001 (d) *x*log(1) decreases by 0.001

改变其他的初值，将获得类似结果。初始化过程结束后，随着混沌运动的规律，图 1 中各个环节相互配合、相互制约，输出密钥序列。

4 密钥序列的性能分析

仿真中假设发送的是数字化后的正弦波 $x(k)=\sin k\pi/20$ $(k=0,1,2,\cdots)$。加密时，各方程依表 1 取初值。在码组计数器的触发下，每 100 组序列段，更新控制空间的本原多项式和初始状态；每 500 组序列段，更新控制空间数目、中心位置、半径。

4.1 初值敏感性分析

法定收信者由于使用了相同的初始条件，将正确地解密出正弦信息。而非法接收者，所截获的信息将是一堆杂乱无章的数据。

在解密过程的仿真中，假定 8 个混沌方程的 14 个密钥参数中只有一个参数减小了 0.001，考察恢复出来的信息与原始信息之间的对应关系。取前 50 个字的数据，原始信息与错误解密结果波形比较图如下(“·”表示传递的原始信息，“*”表示解密出的信息)。

图 3 表明，密钥序列结构具有高度的敏感性，微小的密钥差异将不能正确恢复出原始信息。对其他密钥参数进行仿真，结果是类似的。

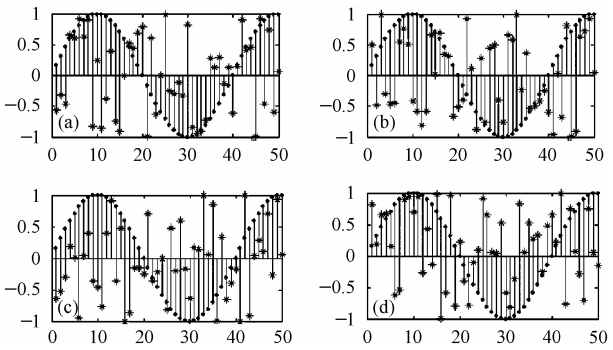

图 3　原始信息与错误解密信息波形比较图

(a) *x*lor2(1)减小 0.001　(b) *x*log(1)减小 0.001

(c) *x*che(1)减小 0.001　(d) *x*loz(1)减小 0.001

Fig.3 Comparative figure of original information and error information

(a) *x*lor2(1) decreases by 0.001　(b) *x*log(1) decreases by 0.001

(c) *x*che(1) decreases by 0.001　(d) *x*loz(1) decreases by 0.001

4.2　保密性分析

注意到以上仿真结论是在 14 个密钥参数中，除 N 之外的 13 个参数只有一个有千分之一差异情况下进行的。对于非法的接收者，要完全猜中 12 个参数，且第 13 个数值猜测精度超过千分之一，实际上是不可能的。

假设 14 个参数中，N (Chebyshev 映射初始迭代次数)的变化范围是 1~20，其它 13 个参数只在 0~1 内取初值，破译者若能精确到千分之一，就算破译密钥。N 有 20 种取值可能，其它 13 个参数每个有 10^3 种取值可能，密钥空间 K 为

$$K=\overbrace{10^3\times10^3\times\cdots\times10^3}^{13个}\times20=2\times10^{40}$$

从计算速度和存储空间上，目前计算机远达不到破解目的。而 14 个密钥参数的取值大多超过了所假设的范围，图 3 表明，即便精确到了千分之一，离破解密钥还有相当差距。

4.3　局部随机性分析

实际中，截获者所截取的密文，可以肯定地认为是整个密文序列的一小段，因此必须对密钥序列的各个段落进行统计检验，所做的检验称为局部随机性检验，一般情况下要求给定序列的检验值落在 95%的真随机序列范围内，称之为显著性水平[2]。以下是局部随机性检验的数据仿真结果。

(1) 频率检验仿真测试如表 2 所示。

(2) 序列检验仿真测试如表 3 所示。

(3) 扑克检验仿真测试检验结果如表 4 所示。取分组长度为 8，被检测序列长度均是 8 的倍数。

(4)自相关检验仿真测试，取长度 80000bit 的数据，根据不同移位，检验结果如 5 所示。

(5)游程检验仿真测试，取长度为 2^{18}bit的数据，检验结果如 6 所示。

4.4　复杂度分析

在设计密钥序列以及衡量其性能时，复杂度是一个非常重要的刻画指标[5,6]。从所生成的密钥序列中，取出长度不同、互不重叠的序列段，根据Massey算法进行局部线性复杂度分析。

对于任何一个有限长的序列，线性复杂度太小或者接近序列的长度都是不安全的。线性复杂度为序列长度一半附近的密钥序列，具有较好的保密性和安全随机性[6]。表 7 的测试结果显示，密钥序列具有相当理想的复杂度。

表 2　频率检验测试结果

Tab.2 Results of frequency testing

序列长度	5000	10000	20000	30000	40000	50000	60000
频率检验值	1.548	0.025	0.039	0.041	0.01	0.269	1.856
检验水平	5%显著水平：3.84						

表 3　序列检验测试结果

Tab.3 Results of sequence testing

序列长度	5000	10000	20000	30000	40000	50000	60000
序列检验值	3.776	2.114	1.595	1.515	2.674	2.053	2.923
检验水平	5%显著水平：5.99						

表 4　扑克检验测试结果

Tab.4 Results of poker testing

序列长度	10240	20480	30720	40960	51200	61440	71680
扑克检验值	259.6	247	243.6	258.6	234.4	229.3	259.9
检验水平	5%显著水平：279.2						

表 5　自相关检验测试结果

Tab.5 Results of self-correlation testing

移位值	10000	20000	30000	40000	50000	60000	70000
自相关值	17735	15202	12663	10116	7601	5034	2458
期望值 μ	17736	15224	12669	10135	7654	5067	2533

表 6 游程检验测试结果

Tab.6 Results of run-length testing

游程长	1	2	3	4	5	6	7	8	9
间隔数	33015	16247	8265	4012	1985	1037	508	243	145
块组数	32824	16323	8241	4050	2061	1002	544	248	138
合 计	65839	32570	16506	8062	4046	2039	1052	491	283

表 7 复杂度测试结果

Tab.7 Results of complexity testing

序列段长度	50	100	500	1000	2000	3000
复杂度	26	51	250	497	1001	1502
序列段长度	4000	5000	6000	7000	8000	9000
复杂度	2000	2501	2999	3501	4000	4500

除表 1 之外，对其他多组密钥参数均进行了同样的研究，仿真图形和数据测试结果都是类似的，表明生成的密钥序列具有较强的抗计算分析和抗统计分析能力。

5 结束语

本文在 Shannon 关于混乱理论的指导下，利用混沌运动轨迹点空间位置的特性，与 m 序列相结合，提出了一种密钥序列生成方案，详细论述了密钥序列的生成，研究了这种密钥序列的抗破译性能。结果表明这种密钥序列的密钥空间大，具有计算上的保密性；通过了 5%显著水平的局部随机性检验，具有比较理想的随机性；它的线性复杂度相当理想；密钥序列可用于数字信息的加密。

参 考 文 献

[1] 赵耿, 方锦清. 混沌通信分类及其保密通信的研究. 自然杂志, 2003, 25(1): 21−30.

[2] Frey D R. Chaotic digital encoding: An approach to secure communication. *IEEE Trans. on Circuits Systems* II, 1993, 40(10): 660−666.

[3] 张凤仙, 郑玉洁. 通信保密技术. 北京: 国防工业出版社, 2003, 36−40.

[4] Macwillams F J, Sloane N J. A. Pseudo-random sequences and arrays. *Proc. IEEE*, 1976, 64(12): 1715−1729.

[5] 王宏霞. 混沌技术在现代保密通信中的应用研究. [博士论文], 成都：电子科技大学, 2002.

[6] 许春香, 魏仕民, 肖国镇. 关于周期序列的线性复杂度. 西安电子科技大学学报, 2001, 28(4): 434−437.

詹 明： 男，1975 年生，讲师，研究方向为数字信号处理、保密通信技术.

张翠芳： 女，1960 年生，教授，博士，研究领域为神经网络、信号处理、控制理论和虚拟仪器.