新的基于 Legendre 扰动的混沌序列

王 冰[1,2],赵 耿[2]
WANG Bing[1,2],ZHAO Geng[2]

1.西安电子科技大学 通信工程学院,西安 710071
2.北京电子科技学院,北京 100070
1.Department of Communication Engineering,Xidian University,Xi'an 710071,China
2.Beijing Electronic Science and Technology Institute,Beijing 100070,China
E-mail:buddy0112@163.com

WANG Bing,ZHAO Geng.New chaotic sequence based on Legendre sequence.Computer Engineering and Applications, 2009,45(32):98-100.

Abstract: Chaotic systems are sensitive to initial conditions and chaotic paramenters,and chaotic sequences are non-periodic and pseudo-random.These properties of chaotic systems are suitable for sequence encryption.A sequence encryption method based on chaos is proposed.Meanwhile,a Legendre sequences is uesd as the parameter sequence and the perturbation sequence.In order to avoid a limitation of the number of Legendre sequences,a prime number table is applied.The computer simulation results show that the chaotic sequence has good cryptography properties.Therefor,this method is fairly good in security and can be implemented easily in software.

Key words: chaos-map;Legendre-sequence;a prime number

摘 要:由于混沌系统对初始条件和混沌参数非常敏感以及生成的混沌序列具有非周期和伪随机性的特征,近年来混沌系统在密码学研究领域得到了较多的研究。提出一种基于混沌的序列密码生成方法,该方法通过引入扰动序列使得输出的混沌序列具有良好的均匀分布和随机统计特性,同时为了克服扰动序列数量的有限性,设计了一个素数表用来不定时更新扰动序列的输入。理论研究和模拟结果表明,该混沌序列具有较好的保密性而且便于软件实现。

关键词:混沌映射;Legendre 序列;素数
DOI:10.3778/j.issn.1002-8331.2009.32.031 **文章编号**:1002-8331(2009)32-0098-03 **文献标识码**:A **中图分类号**:TN918

1 引言

自 1989 年 Robert A.J.Matthews 首次将混沌用于密码学研究,并提出了一种基于 Logistic 映射的混沌流密码方案以来,混沌密码学便作为密码学的一个分支开始得到了广泛的应用。混沌系统作为一种高度复杂的非线性动态系统,具有宽频谱、类随机特性、对结构参数及初始状态的极端敏感等一系列性质,近年来被大量地应用于通信保密领域[1-2]。

混沌映射由于其固有的伪随机性和遍历性,选择用它作为伪随机数发生器是目前一大发展趋势。但是,由于实际中的密码运算基本上是在有限域上实现的,当连续域上的混沌映射数字化以后,其性能将下降,使原来没有周期的混沌序列将出现短周期的重复,且周期长度随机[3]。当前,对混沌序列周期长度的分析尚没有理论结果(数值模拟表明周期长度和计算精度与初值选取有关)。但是学者们还是提出了一些工程改进方法,比如提高计算精度,将多个混沌系统串联起来,以及基于扰动的算法等。

提出了一种基于 Legendre 序列随机扰动的 Logistic 混沌序列,并对这种方法进行了初步的研究和实现。仿真模拟表明利用 Legendre 序列良好的伪随机性、自相关性和较高的线性复杂度等特性对混沌序列进行扰动,提高了混沌序列的随机性、复杂性,改善了有限精度所带来的不足,并使得输出序列的周期增大。理论分析和计算机模拟结果表明,该方法可以产生具有良好统计特性的密钥流,而且便于软件实现。

2 Logistic 映射和 Legendre 序列

2.1 Logistic

Logistic 映射又被称为虫口问题,是一个描述生物种群系统演化的数学模型。其映射形式为:

$$x_{n+1}=\mu x_n(1-x_n),0<x_n<1 \quad (1)$$

其中,$1\leqslant\mu\leqslant4$,$\mu\in(0,4]$称为分形参数。当 $0<\mu\leqslant3$ 时,迭代后的值为稳定不动点,μ 逐渐增大,出现倍周期分岔现象,当 $3.569\ 945\ 972\cdots<\mu\leqslant4$ 时,系统工作于混沌状态。此时所产生的

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No.60773120)。
作者简介:王冰(1983-),女,研究生,主要研究方向:密码通信、基于混沌的序列密码的研究与分析;赵耿(1964-),男,博士,教授,主要研究方向:密码通信与计算机技术。
收稿日期:2008-06-27 **修回日期**:2008-10-08

序列$\{x_n, n=0,1,2,\cdots\}$具有非周期、非收敛以及对初始值十分敏感等特性，序列的均值为 0.5，遍历特性等同于均值为 0.5 的白噪声[2]。

从理论上讲，混沌序列应该是周期无限长、随机性好、具有理想自相关和互相关特性的序列。但是在实际应用中，由于精度的限制和量化等问题的存在，伪随机序列不可避免地将会产生短周期，乃至性能下降。因而有必要寻找一种方法，对混沌生成的序列进行适当的变化，使得在有限精度的条件下，混沌伪随机序列的性能能得到相应的改善。由此，在二值量化的基础上，给出了具有较好独立性与相关性的一种新的基于 Legendre 序列置乱的扰动方案，在第 3 章、第 4 章会给出具体方法和性能分析。

2.2 Legendre 序列

Legendre 序列是良好的 0 均值伪随机序列。

定义 取定 p 是一个奇素数，称序列 $z=z_1 z_2 z_3\cdots$为一个Legendre 序列，如果：

(1)当 j 是 p 的倍数时，$z_j=0$；

(2)当 j 不是 p 的倍数(即 j 与 p 互素)，且 j 是(mod p)平方剩余时，$z_j=1$；

(3)当 j 不是 p 的倍数(即 j 与 p 互素)，且 j 是(mod p)非平方剩余时，$z_j=0$。

$$z_j=\frac{1}{2}(1+(\frac{j}{p}))$$

由以上方法产生的 Legendre 序列具有很好的可利用的性质。

性质 1　Legendre 序列的最小周期是 p。

性质 2　Legendre 序列中 0 出现的次数比 1 出现的次数多 1，即可认为在一个最小周期段内序列是均衡的。

性质 3　设素数 p 充分大。取定 $\boldsymbol{s}$ 为任意一个固定的 l 维布尔向量，随机地选取 Legendre 序列的 l 长的一段 $A=z_t z_{t+1} z_{t+2}\cdots z_{t+l+1}$ 则有以下概率 $P(A=\boldsymbol{s})=2^{-l}+O(p^{-\varepsilon})$。其中 $0<\varepsilon<1$，ε 只依赖于 l。

Legendre 序列在严格最小周期段内有一个符号差错时，序列的线性复杂度保持稳定，不会急剧衰退，性质稳定，所以对生成新序列的随机性也有了较严格的保证(性质 2)。另外，二值 Legendre 序列的自相关性能也非常好(峰值为 $p=1$，其余为 -1)。这些都使得选取 Legendre 序列做扰动在线性复杂度、稳定性、自相关性等方面不会逊色于 m 序列。

但是不得不注意的是，虽然 Legendre 序列产生简单，可其序列的数量有限，限制了扰动序列的容量。为了克服上述缺点，同时增大序列的周期，设计中引入一个大素数表。设该表有 N 个单元，表中的素数尽可能取大，并在初始状态时充分将其混乱，当系统真正运行时就不定期从表中索取大素数，产生新的 Legendre 序列，实现多种不同 Legendre 序列对混沌序列进行扰动。为了增强性能，在初始化后还可以定期用混沌序列对素数表进行更新。这样一来 Legendre 序列的选择性变得更加复杂和难于预测，从另一个角度讲，也相对改善了序列选取的有限问题和混沌序列的短周期现象。

3　Legendre 序列扰动下的混沌序列

首先，选择 256 个大素数作成一个 16×16 的素数表。

(1)选取 Logistic 混沌映射生成一个类随机实值序列；

(2)对实值序列根据公式 $x_n=\mathrm{sgn}(x_n)=\begin{cases}0, 0<x_k<0.5\\ 1, 0.5<x_k<1\end{cases}$ 进行二进制 0/1 值转化，得到一个 GF(2)上的类随机序列 X_n；同时，根据实值序列做另外一种二进制转换，即把实数值序列转化为一定长度的浮点数形式得到：

$|x_k|=0.b_1(x_k)b_2(x_k)\cdots b_i(x_k)\cdots b_L(x_k)$，其中 $b_i(x_k)\in GF(2)$ 是 x_k 的第 i 位

此处选择 $L=8$，则每次迭代取小数点后 8 比特数，即 $b_0 b_1 b_2\cdots b_6 b_7$，再将其转化为对应的十进制作为对大素数表的位选取序号；

(3)用 Logistic 混沌序列初始化大素数表。因为混沌序列初始值随机性并不是很好，所以一般初始的迭代值会被舍去，那么这里利用前面的这些迭代值对大素数表进行初始化：

设 i，j 为表格序号，$i=0$–255，$j=H(b_0 b_1 b_2\cdots b_6 b_7)$，每迭代一次将序号为 i 和 j 的单元内容对(见图 1)，实际中会迭代300 次，这样就先完成了对素数表的初始化；

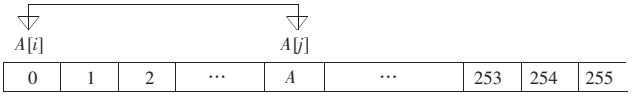

图 1　素数表初始化

(4)P 的选择过程：

```
if(flag<=300)   flag 作为初始迭代次数的标志
  Do  P=2;      //大素数初始化过程
    A[i]↔A[j];
    Flag++;
Else  p=A[i];   //开始进入序列生成，当一个 Legendre 序列生成后，返回素数表接着取下一个素数作为新序的输入
    i++;
```

(5)在经过混沌序列的初始迭代和素数表的初始化过程后，按如下(图 2)过程用选取的素数作为 P，产生 Legendre 序列 Y_m，并对混沌二值序列进行扰动最终产生一个新型的序列。

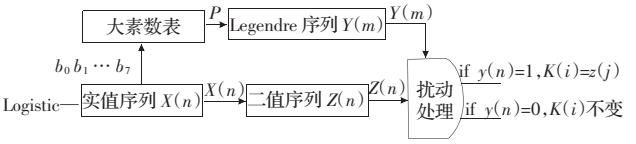

图 2　设计原理图

为了更好地利用素数表，还可以对其表进行不定期的变换，比如当 K 输出 20 000 位后，重新对素数表进行初始化将其打乱，从而再次增加了混沌序列的周期。

4　新的混沌伪随机序列性能检验

4.1　平衡性

保证序列中 0 和 1 的个数大致相等，这也是二值序列具有随机性的最基本保证。设 1 的个数为 N_1，0 的个数为 N_0。这里取 20 000 个二进制位做测试，计算 $\chi^2=(N_0-N_1)^2/N^2$，与 1 自由度的 χ^2 分布比较，对应 5%的显著水平，只要 χ^2 的值不大于 3.84[4]，则认为序列具有较好的随机性。即说明该方法产生的伪随机序列 K 中“0”和“1”的个数大致相同，结果如表 1：

表 1　平衡性

参数名	参数值				
初值 x	0.875 698	0.475 267	0.235 798	0.974 311 1	0.398 575 462 51
N_1	9 981	10 035	10 043	10 060	9 988
N_0	10 019	9 965	9 957	9 940	10 012
χ^2	1.4×10^{-5}	1.2×10^{-5}	1.849×10^{-5}	3.6×10^{-5}	1.4×10^{-5}

实验表明序列 0/1 分布符合要求。

4.2 Poker 测试

将所产生的二进制序列{K}取 20 000 个值,分成大小为 5 000 个段,每段由 4 个二进制位组成。每段所表示的十进制是 0~15。对于一个真正随机的位流,0~15 的个数也应该是随机分布的。假设 n_i 是数字 i 的个数,即 n_i 是 0001 段的个数,n_8 是 1 000 段的个数。将这些值代入下式:$X=\frac{16}{5\,000}\sum_{i=0}^{15}n_i^2-5\,000$,如果 1.03<$X$<57.4,测试通过[5]。经计算 X=15.507 200 符合测试范围。

4.3 连串测试

连串就是指 1 或 0 连续的序列。在真正的随机位流中,连串的长度应是随机分布的。FIPS 140-1 中对于 20 000 个检测位,如果连串数在以下范围[5]内则通过测试(见表 2):

表 2 连串测试

参数名	参数值				
连串长度	1	2	3	4	5
范围	2 267~2 733	1 079~1 421	502~748	223~402	90~223
测试值	2 575	1 121	656	267	135

由表 2 可见,随机选取初始值,得到的连串数值在有效检测范围内,连串的随机性符合要求。

4.4 初值敏感性

混沌序列应该具备对初始条件的敏感性,这是所有混沌系统的内在性质。在检验新序列过程中对混沌初始条件进行微小变化,通过统计得到的二值序列中相应位置上 0 和 1 值的变化情况(见表 3),位变化率越接近 50%[4],说明该系统对于初始条件越敏感。

表 3 初值敏感性

参数名	参数值			
序列长度	20 000			
Legendre 参数 p	2 203	2 203	2 203	44 497
混沌系统参数	0.600 000	0.650…0(15 位)	0.897 40…02(15 位)	0.650…0(15 位)
变化参数	0.600 000 1	0.650…1(15 位)	0.897 4…03(15 位)	0.650…1(15 位)
位变化率/(%)	49.130	49.985	49.845	49.880

5 结论

用 Legendre 序列来对混沌序列进行扰动的研究还很少,这里对这种想法做了初步的分析与实现。统计结果与理论分析表明,采用该文提出的方法产生的混沌序列能通过随机性检验,具有优良的位随机性能及相关特性,且软件实现简单。该文方法提高了原混沌序列的复杂性、随机性,改善了短周期现象,也改善了由于计算机精度问题所带来的缺陷。特别是大素数表的引入,为 Legendre 序列在密码加密的应用提供了新的思路。

参考文献:

[1] Frey D R.Chaotic digital encoding:An approach to secure communication[J].IEEE Trans Circuit and Systems,1993,40(10):660-666.

[2] Dedieu H,Kennedy M P,Hasler M.Chaos shift keying:Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits[J].IEEE Trans Circuit and Systems,1993,40(10):634-642.

[3] 王相生,甘骏人.一种基于混沌的序列密码生成方法[J].计算机学报,2002,25(4).

[4] 高飞.广义混沌二值序列生成方法[J].计算机工程,2007,33(14):130-132.

[5] Spillman R.经典密码学与现代密码学[M].叶阮健,曹英,张长富,译.北京:清华大学出版社,2005:97-101.

[6] 王亥,胡健栋.Logistic-map 混沌扩频序列[J].电子学报,1997,25(1):20-23.

[7] 周红,凌燮亭.有限精度混沌系统的 m 序列扰动实现[J].电子学报,1997,25(7):95-97.

[8] 李树钧.数字化混沌密码的分析与设计[D].西安:西安交通大学,2004.

(上接 97 页)

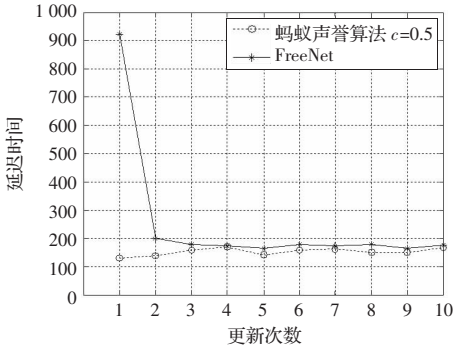

图 3 比较延迟时间

明,与现有算法相比,该算法具有更好的网络搜索能力。基于声誉的信任管理是个有前景的研究方向,今后还将做进一步研究。

参考文献:

[1] Corncllli F,Damiani E,Capitani S D.Choosing reputable servents in a P2P network[C]//Proceedings of the Eleventh International World Wide Web Conference,2002:441-449.

[2] kamvar S D,schosser M T.EigenRep:Reputation Management in P2P Network[C]//Proceedings of the Twelfth International World Wide Web Conference,2003:123-134.

[3] Damiani E.A reputation-based approach for choosing reliable resources in P2P networks[C]//Proceedings of the Ninth ACM Conference on Computer and Communications Security,2002:207-216.

[4] Dorigo M,Maniezzo V,Colorni A.The ant system:Optimization by a colony of cooperating agents[J].IEEE Transactions on Systems,Man and Cybernetics,1996,26(1):29-41.

[5] Kamvar S D,Schlosser M T,Garcia-Molina H.The eigentrust algorithm for reputation management in P2P network[C]//Proceedings of the Twelfth International Conference on World Wide Web,2003:640-651.

[6] Wang W,Zeng G S,Yuan L L.A reputation multi-agent system in semantic web[C]//Proceedings of the Ninth Pacific Rim International Workshop on Multi-Agents,2006:211-219.

[7] Jiang T,Baras J S.Ant-based adaptive reputation evidence distribution in MANET[C]//Proceedings of the Twenty-fourth International Conference on Distributed Computing Systems Workshops,2004:588-593.

[8] Kaelbling L P,Littman M L,Moore A W.Reinforcement learning:A survey[J].Journal of Artificial Intelligence Research,1996,4(1):237-285.

[9] Subramanian D,Druschel P,Chen J.Ants and reinforcement learning:A case study in routing in dynamic networks[C]//Proceedings of IJCAI-97 International Joint Conference on Artificial Intelligence,Morgan Kaufmann,1997:832-838.

[10] Clarke I,Sandberg O,Wiley B.Freenet:A distributed anonymous information storage and retrieval system[C]//Proceedings of the ICSI Workshop on Design Issues in Anonymity and Unobservability,2000:311-322.