基于扰动的混沌序列密码算法设计与研究

胡治孝
(杭州电子科技大学 计算机学院,浙江 杭州 310018)

摘要:有限精度效应(FPE)在很大程度上削弱了混沌密码系统的密码学特性,是近年来制约混沌密码学发展的瓶颈问题。针对 FPE 问题,分析了线性反馈移位寄存器(LFSR)与一维 Logistic 映射的混沌动力学特性,提出了一种基于二者的混沌序列密码算法。该算法采用伪随机序列扰动与密码反馈相结合的方法来改善加密效果。系统由软、硬件均可实现,在模拟实验中以软件为例,采用 C ++语言编写代码。实验结果表明,密文流在有限精度下具有良好的数学特性。密码系统较好地解决了 FPE 问题,具有实用价值。

关键词:混沌;序列密码;有限精度效应;扰动;反馈
中图分类号:TP309.7 **文献标识码**:A **文章编号**:1001 - 4551(2010)03 - 0063 - 04

Design and research of a chaotic stream cipher based on perturbation

HU Zhi-xiao
(Department of Computer, Hangzhou Dianzi University, Hangzhou 310018, China)

Abstract: One major issue in digital chaotic cryptography is the numerical implementation, because of finite precision effect(FPE). Aiming at FPE, linear feedback shift register (LFSR) and one-dimensional logistic map were analyzed first. Then a hybrid encryption algorithm based them was proposed, both pseudo-random sequences and cipher feedback were used to improve the algorithm. This system can be easily implemented by both software and hardware, software was taken for example. The simulation result shows that the cipher stream has a good mathematic character. The cipher system could solve FPE effectively and has a good practical value.

Key words: chaos; stream cipher; finite precision effect(FPE); perturbation; feedback

0 引 言

混沌是确定性系统中的一种貌似随机的运动。混沌系统具有如下基本特性:确定性、有界性、对初始条件的敏感性、拓扑传递性和混合性、宽带性、快速衰减的自相关性、长期不可预测性和伪随机性[1-3],混沌系统所具有的这些基本特性恰好能够满足保密通信及密码学的基本要求。Shannon 证明了“一次一密”密码体制是不可破的[4]。若能以一种方式产生一随机序列,这一序列由密钥所确定,则利用这样的序列就可以进行加密。这样的密码体制称为序列密码体制,又称为流密码。

Robert A. J. Matthews 于 1989 年发表了文章《On the derivation of a“chaotic”encryption》[5],第一次提出把混沌用于密码学,并提出了一种基于变形 Logistic 映射的混沌流密码方案。从而数字化混沌密码系统和基于混沌同步的保密通信系统的研究引起了相关学者的高度关注[6],数字混沌密码学得到了长足的发展。但在近几年,有限精度效应(finite precision effect, FPE)成为了制约本学科发展的瓶颈问题,由于混沌序列的生成器总是在有限精度的条件下实现的,其精确程度取决于计算机的精度,这使得任何混沌序列最终都是周期性的,且其周期最大为 2^{n-1}(其中 n 为计算机系统的精度),因此在有限精度的条件下混沌是不存在的[7]。

伪随机序列扰动被证明是一种简便而有效的解决 FPE 问题的方法。其基本策略可以表述如下:运行一个在相应的离散空间上满足均匀分布的简单伪随机数发生器(PRNo),产生一个伪随机的扰动信号,它以异

收稿日期:2009 - 07 - 22
作者简介:胡治孝(1984 -),男,浙江杭州人,主要从事密码学、网络安全等方面的研究. E-mail: huzx_1984@ yahoo. com. cn

或或者其他扰动函数叠加(扰动)到当前的混沌轨道上去,以此来影响混沌系统的输出特性。m - 序列正是一种优质的伪随机数发生器,它能够简单有效地产生伪随机序列,完全符合用作扰动的要求[8]。

本研究在分析相关理论的基础上,提出一种基于 Logistic 映射以及线性反馈移位寄存器(linear feedback shift register,LFSR)的混合伪随机序列扰动密码算法。该算法采用 LFSR 产生 m - 序列,对混沌系统输出进行扰动,并在此基础上定时更新输入状态、接收来自密文的反馈。

1 系统的部件组成

1.1 线性反馈移位寄存器与 m - 序列

线性反馈移位寄存器(LFSR)是指这样一类反馈移位寄存器,它的反馈函数是 $a_1, a_2, \cdots, a_n$ 的线性函数,其表达式 $f(a_1, a_2, \cdots, a_n) = c_n a_1 \oplus c_{n-1} a_2 \oplus \cdots \oplus c_1 a_n$,其中 $c_i \in \{0,1\}$,$c_n = 1$,其结构如图 1 所示。n 级 LFSR 对应于零输入的输出是周期性的,其周期 $r \leqslant 2^{n-1}$,当其输出序列 $\{a_i\}$ 周期达到最大(2^{n-1}),称 $\{a_i\}$ 为 m 序列,即当且仅当 LFSR 的特征多项式 $p(x) = 1 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} + c_n x^n$ 为本原多项式。LFSR 被广泛应用于密钥流产生器中,其主要优点有:硬件实现方便;其产生的 m - 序列周期很大,且具有良好的统计特性[9]。

LFSR 因其结构特点而易于使用代数工具进行分析,这在带来操作方便的同时也带来了不安全的因素,因而在其反馈过程中加入密文的影响。密文反馈的基本特性在于把密文反馈给系统,影响后面的加密过程,从而给密码分析造成密文统计上的难度。基于 LFSR 的密码反馈最简单的形式就是将加密完成后的密文流作为下一轮循环的输入。本算法的具体反馈过程将在后文详细介绍。

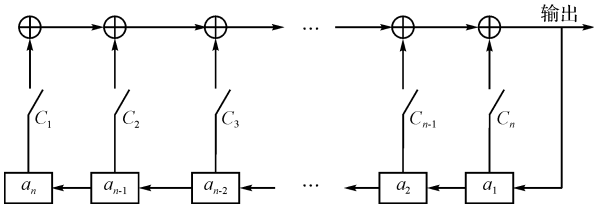

图 1 LFSR 的结构

1.2 Logistic 映射

Logistic 映射是一个典型非线性混沌方程,它虽然简单却体现出混沌运动的基本性质[10]。Logistic 映射如下式:

$$X_{n+1} = bX_n(1 - X_n) \quad X_n \in [0,1] \tag{1}$$

式中 b—控制参量,$b \in [0,4]$。

b 值确定后,由任意初值 $X_0 \in [0,1]$,可迭代出一个确定的序列 $X_1, X_2, \cdots, X_n$,对于不同的 b 值,系统(1)将呈现不同的特性。在开区间(0,1)中随机选一个数作为迭代初值 X_0,丢弃前 100 次的迭代数据,再开始绘制 X_i 的轨迹,当 $b \in [2.5,4]$ 时,绘制出来的图形如图 2 所示。由图可以看到,在 $b = 3$ 时,单线开始一分为二,这表明出现了 2 个周期点。当 b 从 3 变到 $1 + \sqrt{6}$ 的过程,是 2 周期窗口。在 $b = 1 + \sqrt{6}$ 处,开始出现了 4 周期。在此之后,大量的倍周期分支出现在越来越窄的 b 的间隔里,经过 n 次分支,周期长度为 2^n,这种周期倍化的过程是没有限制的,不过相应的 b 却有一个极限值:3.569 945 672…。当 $b > 3.569\ 945\ 672\cdots$ 时,便进入了混沌区。当 $b = 4$ 时由系统(1)产生的序列 $\{X_i\}$ 在运动形式上具有下列典型的混沌特征:

(1) 随机性。当 $b = 4$ 时,Logistic 映射在有限迭代内不稳定运动,随后其长时间的动态行为将显示随机性质。

(2) 规律性。尽管 $\{X_i\}$ 体现出随机性质,但它是由确定性方程(1)导出的,初值 X_0 确定后 X_i 便已确定,即其随机性是内在的,这就是混沌运动的规律性。

(3) 遍历性。混沌运动的遍历性是指混沌变量能在一定范围内按其自身规律不重复地遍历所有状态。

(4) 对初值的敏感性。初值 X_0 的微小变化将导致序列 $\{X_i\}$ 远期行为的巨大差异。

(5) 具有分形的性质。混沌的奇异吸引子在微小尺度上具有与整体自相似的几何结构。

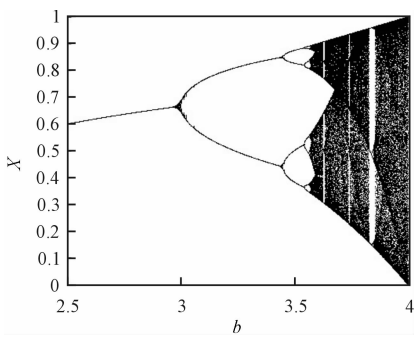

图 2 Logistic 映射分支图

2 密码算法的设计

2.1 密码系统初始化

密码系统的主要部件为 2 个 LFSR 与 1 个 Logistic 映射,其结构如图 3 所示。本研究取 Logistic 映射表达式中的 $b = 4$。LFSR1 被用来生成扰动 m - 序列,定时

更新 Logistic map 的状态，并接受来自密文的反馈。LFSR2 则用于产生 Logistic 映射的初值。假定系统的精度为 32 位，LFSR1 的特征多项式 $P_1(x)=1+x^3+x^{11}+x^{13}+x^{29}+x^{32}$，LFSR2 的特征多项式 $P_2(x)=1+x^5+x^7+x^{23}+x^{31}+x^{32}$。系统所使用的会话密钥为 8 位字符输入，其中初始状态的产生由以下算法给出：设输入的会话密钥为 computer，则选择字符串的第 1、3、5、7 位 cmue，按 ASCII 码解码，其码值为 0x636D7565，作为 LFSR1 的初始状态 L_0；选择字符串的第 2、4、6、8 位 optr，其码值为 0x6F707472，作为 LFSR2 的初始状态 L'_0，迭代产生 16 位二值序列，然后除以 2^{16} 得到(0,1)上的小数，作为 Logistic 映射的初值 X_0。

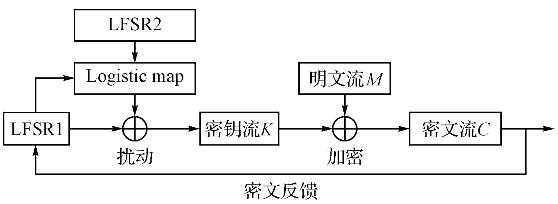

图 3　密码系统的结构

2.2　算法描述

（1）输入会话密钥 K_0，得到 L_0 与 X_0；

（2）LFSR1 移位，产生序列 $\{l_i\}$；

（3）Logistic 映射迭代，产生序列 $\{x_i\}$；

（4）产生密钥流 $k_i=l_i\oplus x_i$；

（5）加密得密文流 $c_i=m_i\oplus k_i$；

（6）密文反馈，将当前 32 位密文依次推入 LFSR1 的参数 a_i 队列；

（7）n_i 次迭代后，将 LFSR1 的当前状态转化为 [0,1] 上的小数，作为下一轮 Logistic 映射的初值 X_i；

（8）输出密文流 $\{c_i\}$。

其中，L_0 与 X_0 由 2.1 节提到的密钥初始化方法得到。LFSR1 由其反馈函数生成扰动序列 $\{l_i\}$，要求扰动幅度（连续参与扰动的位数）n_r 满足一定的条件，具体情况参阅文献[11]。

扰动算法的关键在于伪随机序列对于密钥流的影响。在此目标下，本研究执行如下操作：当一轮 n_r 位扰动完成后，进行密文反馈，将当前开始输出的第 1 个密文比特位推入如图 1 所示的 LFSR1 参数队列中的寄存器 a_1 继续迭代，按此过程重复进行 32 次，直至 LFSR1 所有 32 位参数均由密文流替代，完成其状态更新；与此同时，由时钟控制产生一个随机时间 t，将此时 LFSR1 的 32 位参数当前状态按照 2.1 节提到的 Logistic 映射初始化的方法转化成 [0,1] 上的小数并赋予 X_n，同时记录迭代次数 n_0，此后每隔时间 t 进行相同操作，保存迭代次数序列 $\{n_i\}$。

为了优化系统性能以对抗密钥分析，本研究在将 Logistic 映射每次的迭代结果 X_i 转化为 0－1 序列 $\{x_i\}$ 时，引入不可逆转换函数 $T(X)$，其定义如下式所示：

$$x_i=T(X_i)=\begin{cases}0, X_i\in\bigcup_{d=0}^{2^{n-1}-1}I_{2d}^n\\1, X_i\in\bigcup_{d=0}^{2^{n-1}-1}I_{2d+1}^n\end{cases}\qquad(2)$$

式中　n—任意正整数，$n>0$；$I_0^n,I_1^n,I_2^n,\cdots$—[0,1] 区间的 $2n$ 个连续的等分区间，这里取 $n=16$。

由于混沌序列信号 X_i 具有良好的随机统计特性，这样生成的 $\{x_i\}$ 在理论上具有均衡的 0－1 比和 δ-like 的自相关等优良的统计特性。本算法属于对称密码算法，故解密过程与加密完全相同，只需在第 n_i 次迭代时进行相应的输入更新，在连续 n_r 位后进行密文反馈即可[12-13]。

3　模拟实验及性能分析

文献[12]分析了在类似的 m－序列扰动下输出混合序列的周期性，其结论是混合序列的周期 T，应为 m－序列的周期 P 与混沌系统周期 Q 的最小公倍数，即 $T=[P,Q]$。由于前面已取 Logistic 映射的输出为 16 位精度，因此 $1\leqslant Q\leqslant 2^{16}-1$，又 $P=2^{32}-1$，因此从理论上来说 T 是一个足够大的数字，其最佳状况是“当 P 与 Q 互素时”。当然，这还是针对没有考虑密文反馈的情况。

本算法用 C++ 代码实现，其实验结果输出如下：设明文为“Chaos-based cryptography (sometimes called ‘chaotic’ cryptography) has been around for more than a decade by now. During this time of foundation and development, it came to mean different things, mostly depending on the implementation.”，会话密钥为 security，加密后的文本如图 4 所示。

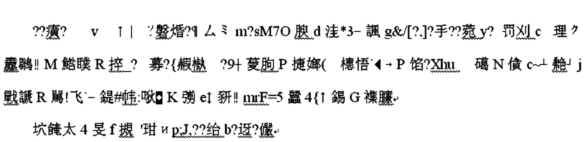

图 4　加密后的文本

首先检验密文字符的统计学特性。明、密文字符串长度均为 235，分别统计其中的 0、1 个数，结果明文 1 的个数 873，明文 0 的个数 1 007，密文 1 的个数 947，密文 0 的个数 933。密文序列体现了良好的 0－1 统计特性。

密文分布是密码系统一个非常重要的特征,为了更好地表现这一特性,本研究通过二维图形来进行展示。明文分布和密文分布分别如图 5、图 6 所示,其中横坐标表示明、密文字符序列的序号,纵坐标为字符的 ASCII 码值。从中可以看到,明文字符的码值相对较为集中在某些码值区间,而密文字符的码值分布十分均匀,扩散到整个码值区间(0 ~ 255),并且不带有明文字符序列的任何统计信息,大大增加了密码分析的难度,达到了理想的效果。

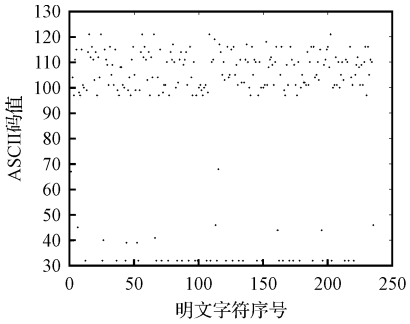

图 5 明文分布

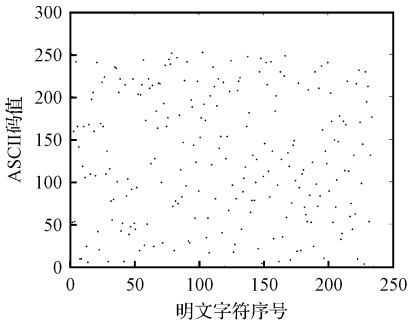

图 6 密文分布

本研究最后进行解密实验。在解密时,输入会话密钥 security,所得结果如图 7 所示。为了测试密文对密钥的敏感程度,将输入的会话密钥改为 securitx,即在会话密钥二值化后 64 位中的最后一位由 1 改为 0,其余 63 位不变,所得的解密文本如图 8 所示,结果与明文完全不同,没有丝毫可循之处,充分体现了密码系统对密钥的敏感性。

Chaos-based cryptography (sometimes called 'chaotic' cryptography) has been around for more than a decade by now. During this time of foundation and development, it came to mean different things, mostly depending on the implementation.

图 7 正确解密恢复的明文

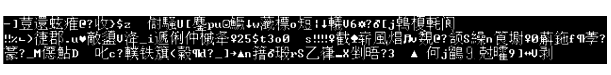

图 8 密钥微小差别时恢复的明文

4 结束语

实现扰动策略的关键是如何选取优良的伪随机序列产生器与混沌系统。据此,本研究以 LFSR 与 Logistic 映射为例,将混沌密码学与传统密码学相结合,提出一种 m - 序列扰动的混沌反馈密码算法。对加密算法产生的密文序列进行统计学特性测试,结果表明所得结果均比较符合密码学理论要求。算法在以软件实现时运算速度受到一定影响,这个问题在硬件实现的情况下不存在,因此系统的硬件实现将有一定的实用价值。展望未来,对更高性能的混沌系统与伪随机序列产生器的研究将会更充分地提高加密解密的效率,更好地促进数字混沌序列密码学的发展。

参考文献(References):

[1] KOCAREV L, JAKIMOSKI G, STOJANOVSKI T, et al. From chaotic maps to encryption schemes[J]. **Pro. IEEE Int. Sym. CAS**,1998(4):514 - 517.

[2] 刘长江. 混沌算法在成型机节能中的应用[J]. 机电工程技术,2008,37(12):82 - 84.

[3] 王 巍,侯利民. 基于混沌优化 PID 控制的渗碳炉温控制系统的研究[J]. 2008,37(3):22 - 23.

[4] SHANNON C E. Communication theory of secrecy system [J]. **The Bell System Technical Journal**, 1949, 28(4): 656 - 715.

[5] MATTHEWS R. On the derivation of a "chaotic" encryption algorithm[J]. **Cryptologia**,1989,XIII(1):29 - 41.

[6] KOCAREV L. Chaos-based cryptography: a brief overview [J]. **IEEE Circuits and Systems**,2001,1(3):6 - 21.

[7] AMIGÓ J M, KOCAREV L, SZCZEPANSKI J. Theory and practice of chaotic cryptography[J]. **Physics Letters A**, 2007,366(3):211 - 216.

[8] 周 红,罗 杰. 有限精度混沌系统的序列扰动方法[J]. 电子学报,1997,25(7):95 - 97.

[9] 卢开澄. 计算机密码学—计算机网络中的数据保密与安全[M]. 3 版. 北京:清华大学出版社,2003.

[10] 邓绍江,李传东. 基于 Logistic 映射混沌加密算法的设计与实现[J]. 重庆大学学报:自然科学版,2004,27(4):61 - 63.

[11] 王相生,甘骏人. 一种基于混沌的序列密码算法[J]. 计算机学报,2002,25(4):351 - 356.

[12] 韦鹏程. 混沌序列密码设计与实现研究[D]. 重庆:重庆大学计算机学院,2004.

[13] 胡志刚,王来云,胡树根,等. 单亲遗传算法在二维不规则件排样中的应用[J]. 轻工机械,2009,27(1):46 - 49.

[**编辑**:李 辉]