第 59 卷 第 4 期 2010 年 4 月
1000-3290/2010/59(04)/2289-09

物 理 学 报
ACTA PHYSICA SINICA

Vol. 59, No. 4, April, 2010

基于线性反馈移位寄存器和混沌系统的伪随机序列生成方法*

张雪锋† 范九伦

(西安邮电学院信息与控制系,西安 710061)

(2009 年 7 月 15 日收到;2009 年 8 月 4 日收到修改稿)

结合线性反馈移位寄存器(LFSR)和混沌理论各自的优点,采用循环迭代结构,给出一种将 LFSR 和混沌理论相结合的伪随机序列生成方法. 首先根据 LFSR 的计算结果产生相应的选择函数,通过选择函数确定当前迭代计算使用的混沌系统,应用选择的混沌系统进行迭代计算产生相应的混沌序列;然后把生成的混沌序列进行数制转换,在将得到的二进制序列作为产生的伪随机序列输出的同时将其作为反馈值与 LFSR 的反馈值进行相应的运算,运算结果作为 LFSR 的最终反馈值,实现对 LFSR 生成序列的随机扰动. 该方法既可生成二值伪随机序列,也可生成实值伪随机序列. 通过实验对生成的伪随机序列进行了分析,结果表明,产生的序列具有良好的随机性和安全性.

关键词: 线性反馈移位寄存器, 混沌系统, 伪随机序列, 随机性

PACC: 0545

1. 引 言

流密码技术是密码学中一类主流加密技术,已被广泛应用于信息加密、分布式计算、码分多址(CDMA)系统等领域. 流密码技术的核心是构造高性能的密钥流,密钥流是通过伪随机数发生器(pseudo-random number generator, PRNG)生成的,设计性能良好的密钥流生成器是流密码领域的一个研究热点[1—3].

线性反馈移位寄存器(linear feedback shift register, LFSR)是一种基本的密钥流生成器,由于采用逻辑运算,具有原理简单、计算速度块、便于硬件实现等优点,成为构造密钥流生成器的重要部件之一. 目前基于 LFSR 的伪随机序列生成技术主要分为两类:一类是 LFSR 和非线性 Boolean 函数相结合产生伪随机序列,如非线性组合流密码、前馈流密码等方法[4,5];另一类是用一个 LFSR 去控制另一个 LFSR,如钟控型生成器和缩减型生成器等[6,7]. 上述方法在生成伪随机序列的过程中需要进行大量的位运算,通常每次计算只能产生 1 bit 的输出. 而现代处理器的每个时钟可以处理多达 64 bit 的操作,相比之下,这种传统的基于 LFSR 的伪随机序列生成技术的软件实现效率很低,安全性较差[8,9]. 为此,研究者着手考虑结合 LFSR 的优点并融入其他技术,来获得性能更好的密钥流生成器. 其中,结合 LFSR 和混沌理论各自的优点来设计性能优良、安全性高的伪随机序列生成器是目前的一个发展方向.

混沌具有良好的伪随机性、初值敏感性和遍历性等特点,同时具有确定可再生的性质,基于混沌理论的伪随机序列生成技术研究引起了广泛的关注[10—12]. 混沌系统良好的密码学特性保证了产生的伪随机序列的安全性,但是,由于大多数混沌系统形式复杂,浮点运算的计算过程繁琐,导致这类方法的硬件实现困难. 目前,在将 LFSR 和混沌理论相结合来生成伪随机序列方面,已取得了一些研究成果. 文献[13]提出了一种基于 LFSR 和 logistic 混沌系统的扩频序列生成方法,该方法对两组不同初始条件的 LFSR 和 logistic 映射计算结果进行异或运算,然后通过判决过程确定最终生成序列的取值. 但该方法每次运算只产生 1 bit 的序列值,生成效率较低. 文献[14]给出了一种结合分段线性混沌映射和 LFSR 的流密码设计方案,加密过程采用自同步加密结构,应用分段线性混沌映射产生的序列与

* 陕西省自然科学基金(批准号:SJ08F24)资助的课题.

† E-mail: zhangxuefeng3@163.com

LFSR 产生的 m 序列进行简单的异或运算,将所得结果应用于流密码,该方法的不足是 LFSR 的短周期问题依然存在. 文献[15]设计了一种基于混沌控制 m 序列的密钥序列生成方案,其中需要用到 7 个不同的混沌系统作为反馈移位寄存器本原多项式的选择函数,计算过程复杂,不便于硬件实现.

本文给出一种新的 LFSR 和混沌系统相结合的伪随机序列生成方法,该方法采用 LFSR 产生选择函数来确定混沌系统,通过循环迭代结构生成相应的伪随机序列. 鉴于 LFSR 和混沌系统相结合具有较大的密钥空间,采用 LFSR 产生选择函数来确定混沌系统的方式增加了密码分析攻击的难度. 在我们的设计中,通过将 LFSR 的反馈值和生成的二进制序列反馈值进行异或运算的方式实现了对 LFSR 的随机扰动,使得生成序列具有良好的安全性和随机性. 本方案的一个优点是可以根据加密算法的需要一次计算产生多比特的序列值,保证了计算过程具有更高的效率. 本文不仅实现了二值伪随机序列的生成,而且实现了实值伪随机序列的生成. 这两种伪随机序列产生过程通过对多个简单的混沌系统进行统一的循环迭代计算来实现,降低了计算过程的复杂性,也便于硬件实现.

2. LFSR 与混沌系统

2.1. 线性反馈移位寄存器(LFSR)

反馈移位寄存器,特别是线性反馈移位寄存器,是许多密钥流生成器的基本器件. 一个反馈移位寄存器由两部分组成:移位寄存器和反馈函数. 移位寄存器是一个位序列,它的长度用位表示,如果移位寄存器的长度是 n 位,则称为 n -位移位寄存器. 每次运算的结果实际只改变序列中的一个值,其中移位寄存器中除最右端的位以外,其余所有位向右移一位,新的最左端位的值根据寄存器中其他位的值计算得到. 反馈移位寄存器的基本结构如图 1 所示,其中 $f(a_1,a_2,\cdots,a_n)$ 为反馈函数,当反馈函数为线性函数时,相应的反馈移位寄存器被称为线性反馈移位寄存器.

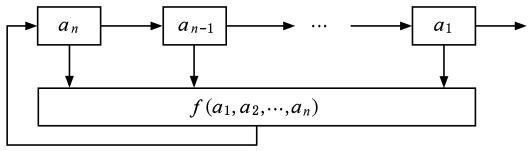

图 1 反馈移位寄存器基本结构

定义 1 一个长度为 L 的线性反馈移位寄存器(LFSR)由 $0,1,\cdots,L-1$ 共 L 个级(或延迟单元)和一个时钟构成,每个级都有 1 bit 的输入和 1 bit 的输出,并且可以存储 1 bit 字符,时钟用于控制数据的移动. 每个时间单位内执行下述操作:

1)输出 0 级所存储的字符,作为输出序列的一部分;

2)对每个 $i(1 \leqslant i \leqslant L-1)$,将第 i 级的存储内容移入第 $i-1$ 级;

3)第 $L-1$ 级中存储的新元素称为反馈比特 s_j,它由 $0,1,\cdots,L-1$ 级中一个固定的子集合的内容进行模 2 相加而得到.

LFSR 的基本结构如图 2 所示. 其中每个 c_i 取值为 0 或 1,图中闭合的半圆表示“与”运算,反馈比特 s_j 由那些 i 级的内容进行模 2 求和运算而得到,这里 $0 \leqslant i \leqslant L-1$ 且 $c_{L-i}=1$. 例如 4 阶线性反馈移位寄存器的反馈函数为:$f(D)=1+D+D^3$,则相应的线性反馈移位寄存器基本结构如图 3 所示.

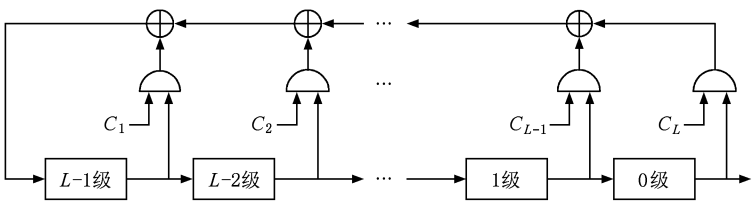

图 2 长度为 L 的 LFSR 基本结构

当图 3 所示的 LFSR 初始状态为[0,0,0,0]时,相应的输出序列为 0 序列. 当初始状态为[0,1,1,0]时,每一个时刻 t 相应的 D_3,D_2,D_1,D_0 各级存储的二进制数见表 1.

线性反馈移位寄存器 LFSR 的输出序列为:$s=0,1,1,0,0,1,0,0,0,1,1,1,1,0,1,\cdots$, 结果表明,

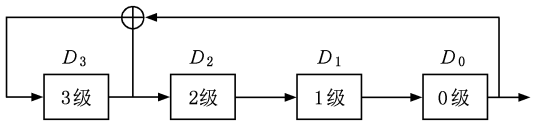

图 3　对应 $f(D) = 1 + D + D^3$ 的 LFSR 基本结构

该 LFSR 的输出序列周期仅为 15，这样的序列直接应用于加密算法无法保证必要的安全性. 要使得应用 LFSR 产生的二值序列具有更大的周期和良好的随机性，可以采用增大反馈函数阶数的方式，也可以通过对生成序列进行相应的扰动来实现. 但这些方法的缺点是计算速度较慢，只能增大生成序列的周期，并没有完全解决反馈移位寄存器具有周期性和周期较小的问题.

表 1　LFSR $< 4, 1 + D + D^4 >$ 对应的存储器状态

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
D_3	0	0	1	0	0	0	1	1	1	1	0	1	0	1	1	0
D_2	1	0	0	1	0	0	0	1	1	1	1	0	1	0	1	1
D_1	1	1	0	0	1	0	0	0	1	1	1	1	0	1	0	1
D_0	0	1	1	0	0	1	0	0	0	1	1	1	1	0	1	0

2.2. 混沌系统

本文所给算法中选用了两种常用的混沌映射——logistic 混沌映射和立方映射，这两种映射计算简单，被广泛应用于加密算法、混沌优化等方面[16,17]. Logistic 映射定义如下

$$g(x_n) = 1 - \mu x_n^2, \tag{1}$$

其中 $x_0 \in (-1,1)$，当 $1.401155 < H \leqslant 2$ 时，系统进入混沌状态. 无限精度计算条件下，logistic 映射产生序列的概率密度函数为

$$p(x) = \frac{1}{\pi \sqrt{1 - x^2}} \quad (x \in (-1,1)). \tag{2}$$

根据 $p(x)$ 可知，应用 logistic 映射生成序列 $\{x_i, i = 1,2,\cdots,N\}$ 的数学期望、自相关函数、互相关函数等相关统计特性的计算结果如下.

序列 $\{x_i, i = 1,2,\cdots,N\}$ 的数学期望 $\bar{x}$ 为

$$\bar{x} = \lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} x_i = \int_{-1}^{1} x p(x)\,\mathrm{d}x = 0. \tag{3}$$

序列 $\{x_i, i = 1,2,\cdots,N\}$ 的自相关系数 $R(\tau)$ 为

$$\begin{aligned} R(\tau) &= \lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} (x_i - \bar{x})(x_{i+\tau} - \bar{x}) \\ &= \int_{-1}^{1} x f^{\tau}(x) p(x)\,\mathrm{d}x - \bar{x}^2 \\ &= \begin{cases} 0.5 & (\tau = 0) \\ 0 & (\tau \neq 0) \end{cases}. \end{aligned} \tag{4}$$

序列 $\{x_{i1}, i = 1,2,\cdots,N\}$ 和 $\{x_{i2}, i = 1,2,\cdots,N\}$ 的互相关系数 $B(\tau)$ 为

$$\begin{aligned} B(\tau) &= \lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} (x_{i1} - \bar{x})(x_{(i+\tau)2} - \bar{x}) \\ &= \int_{-1}^{1}\int_{-1}^{1} x_1 f^{\tau}(x_2) p(x_1) p(x_2)\,\mathrm{d}x_1\,\mathrm{d}x_2 - \bar{x}^2 \\ &= 0. \end{aligned} \tag{5}$$

立方映射定义为

$$h(x_n) = 3x_n - 4x_n^3, \tag{6}$$

其中 $x_0 \in (-1,1)$. Logistic 映射和立方映射的函数曲线如图 4 所示.

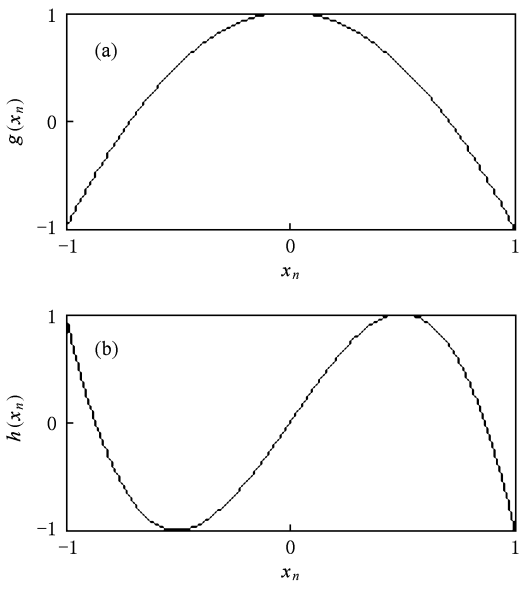

图 4　混沌映射函数曲线　(a) logistic 映射 ($\mu = 2$)，(b) 立方映射

当 $\mu = 2$ 时，这两种映射产生的混沌序列取值区间均为 $(-1,1)$，该性质能够保证在以上两种混沌系统之间进行混合迭代计算时，运算结果具有封闭性.

3. 伪随机序列生成的基本原理

本文将给出二种伪随机序列生成方法,一种是生成二值伪随机序列,另一种是生成实值伪随机序列.其实现过程采用 LFSR 与混沌系统相结合的方式和循环迭代结构,具体流程图见图 5 和图 6.

3.1. 二值伪随机序列生成方法

二值序列生成的基本流程图如图 5 所示.

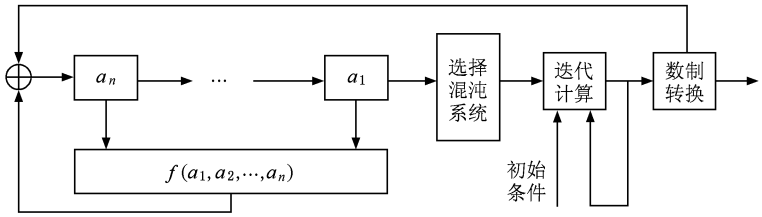

图 5 二值序列生成流程

生成二值伪随机序列的具体过程如下:

1)首先根据 LFSR 的计算结果产生相应的选择函数,通过选择函数确定当前迭代计算使用的混沌系统,依据选择的混沌系统进行迭代计算,产生相应的伪随机序列;

2)将生成的伪随机序列根据加密算法的需要进行相应的数制转换,得到的二进制值作为最终产生的伪随机序列输出;

3)在将生成的二值序列输出的同时,将其作为反馈值与 LFSR 的反馈值进行异或运算,运算结果作为 LFSR 的最终反馈值,该过程实现了对 LFSR 生成序列的随机扰动.

计算流程中的数制转换过程采用多电平量化法,该方法首先将生成的混沌序列中的值 x 归一化到区间[0,1]上记为 x', 然后将 x' 表示成二进制形式:

$$x' = \sum_{i=0}^{\infty} a_i \cdot 2^{-(i+1)},\ a_i = 0 \text{ 或 } 1. \tag{7}$$

舍弃 x' 的前 M 位,取其随后的 L 位,则有:

$$x'' = \sum_{i=M}^{L+M-1} a_i \cdot 2^{-(i+1)} = 2^{-(L+M)} \sum_{i=0}^{L-1} a_i \cdot 2^{L-1-i}, \tag{8}$$

令

$$X = \sum_{i=0}^{L-1} a_i \cdot 2^{(L-1)-i}. \tag{9}$$

则公式(9)表示一个由 L 位二进制表示的整数 $X \in \{0,1,2,\cdots,2^L-1\}$,且它与 x 存在一一对应关系.每次迭代计算可产生一个 L 比特的二进制序列.该序列作为生成序列输出的同时,还作为反馈值与 LFSR 的反馈值进行相应的运算.

采用以上方法生成二值伪随机序列具有以下优点:

1)通过 LFSR 产生选择函数来确定混沌系统的方式增加了密码分析攻击的难度,使得生成的伪随机序列具有良好的安全性;

2)采用混沌系统进行迭代计算能够保证该方法具有较大的密钥空间;

3)计算过程可以根据实际加密过程的需要,在数制转换环节经过一次迭代计算产生多位二进制序列值,能够有效保证产生伪随机序列的速度;

4)计算过程中可以应用多个简单混沌系统进行统一的循环迭代计算,降低了计算过程的复杂性.

3.2. 实值伪随机序列生成方法

实值伪随机序列在优化计算、数据加密等方面有着广泛的应用.鉴于此,在二值伪随机序列生成方法的基础上,我们进一步给出一种 LFSR 和混沌系统相结合的实值伪随机序列生成方法.实值伪随机序列生成的基本流程如图 6 所示.

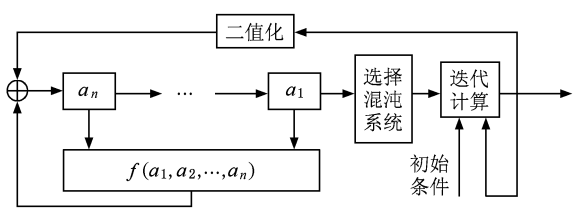

图 6 实值序列生成流程

生成实值伪随机序列的具体过程如下:

1)根据 LFSR 的计算结果产生相应的选择函数,通过选择函数确定当前迭代计算使用的混沌系统;

2)应用选择的混沌系统进行迭代计算产生相应的伪随机序列,将其作为实值伪随机序列输出;

3)将生成的伪随机序列进行数制转换,生成的二值序列与 LFSR 的反馈值进行异或运算,运算结果作为 LFSR 的最终反馈值,该过程实现对 LFSR 生成序列的随机扰动.

以上迭代计算过程中,反馈机制二值化过程可以采用二值量化法来实现. 对于混沌序列 $x_i, i = 1, 2, \cdots, N$. 定义二值化结果为:

$$y_i = \begin{cases} 0 & x_i \leqslant t \\ 1 & x_i > t \end{cases}, \tag{10}$$

其中 t 为二值量化的阈值,一般情况下, $t = \bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$.

图 5 和图 6 的迭代计算过程可以通过多个不同的简单混沌系统实现. 需要强调的是,迭代计算过程中选择的混沌系统必须具有相同的象空间,这样才能保证应用选择机制实现在不同混沌系统之间进行迭代计算时运算过程的封闭性.

4. 生成序列的性能分析

本节我们以 $f(D) = 1 + D + D^3$ 为反馈函数的 4 阶 LFSR 来产生相应的选择函数,以 logistic 映射和立方映射混沌系统作为循环迭代计算的混沌系统,对本文提出的二种伪随机序列生成方式进行验证,其性能分析包括相关性分析、初值敏感性分析等.

4.1. 二值序列性能分析

4.1.1. 相关性分析

二值序列的一个重要应用领域是扩频通信. 在扩频通信中,扩频码的自相关特性决定了扩频系统的捕捉、跟踪、多址和抗干扰的能力,扩频码的互相关函数特性决定了扩频系统的抗多址干扰的能力,因此,扩频码的相关特性的好坏对扩频系统的工作性能影响极大.

设伪随机序列 b_n 的长度为 N, 则该序列的自相关系数定义为[18]:

$$ac(m) = \frac{1}{N}\sum_{i=1}^{N-m} b_i b_{i+m} \tag{11}$$

其中 m 为步长参数. 自相关系数的值与步长 m 有关,当步长变化时,如果自相关系数变化越小,说明对应序列的随机性越好.

假设不同的两个二值序列 b_{1n} 和 b_{2n} 的长度均为 N, 则相应的互相关函数定义为:

$$cc(m) = \begin{cases} \frac{1}{N}\sum_{i=1}^{N-m} b_{1i} b_{2(i+m)} & (0 \leqslant m \leqslant N) \\ \frac{1}{N}\sum_{i=1}^{N-m} b_{1(i+m)} b_{2i} & (-N \leqslant m < 0) \end{cases}. \tag{12}$$

互相关函数取值越接近 0,说明两个序列越互不相关,差异程度越大. 自相关系数和互相关系数分析的实验结果如图 7 所示.

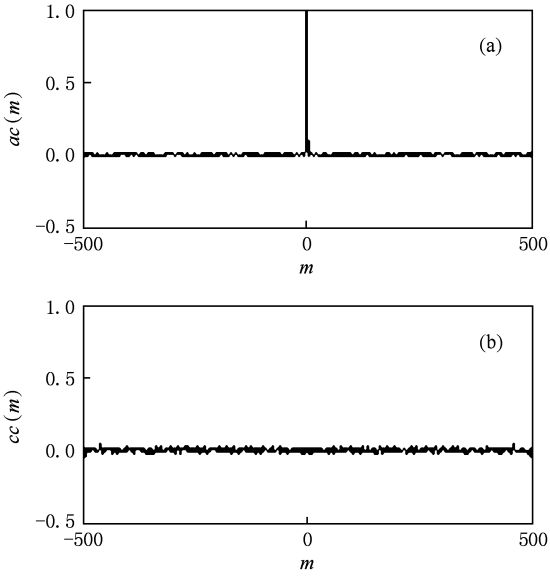

图 7　相关性分析　(a)自相关系数,(b)互相关系数

本文通过选择不同初值进行了大量的实验. 结果表明,初值对产生的二值序列的相关性没有显著影响,几乎任意初值产生的伪随机序列均具有良好的相关性. 这表明本文方法生成序列的随机性能良好.

4.1.2. 平衡度分析

在 CDMA 通信中,扩频码序列的平衡性与多址通信系统载波抑制有密切的关系,扩频码序列的平衡性不好,则系统的载波泄露大,因此在多址通信中,均要求选取平衡性能良好的扩频序列. 设扩频序列的长度为 N,序列中 1 与 −1 的个数分别为 P 和 Q, 则该扩频序列的平衡度定义为[18]

$$E(N) = \frac{|P - Q|}{N}. \tag{13}$$

平衡度的值越小,说明序列中 −1与 1 的个数越接近,随机性越好. 图 8 给出本文方法生成序列的平

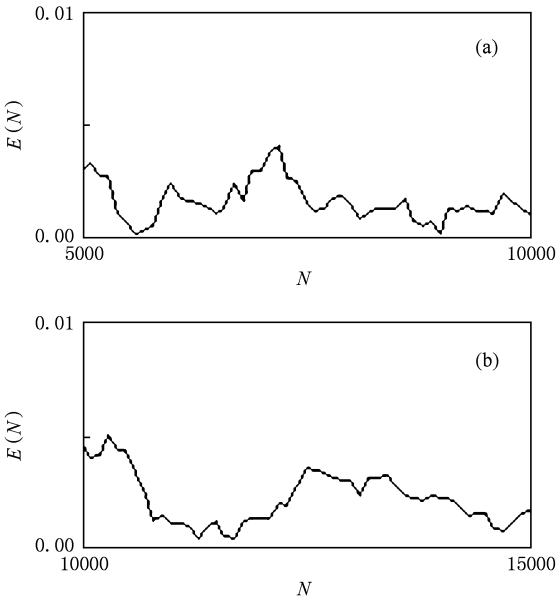

图 8 平衡度分析 (a)序列长度从 5000 到 10000 的平衡度,(b)序列长度从 10000 到 15000 的平衡度

衡度随序列长度 N 变化的实验结果,其中图 8(a)生成的伪随机序列长度从 5000 增加到 10000,图 8(b)生成的伪随机序列长度从 10000 增加到 15000.

实验结果表明,应用本文方法产生的伪随机序列的平衡度随着序列长度 N 的增加而逐步减小,具有良好的平衡度.

4.1.3. *初值敏感性分析*

初值敏感性分析过程中,我们对系统的初始条件进行微小变化,通过计算得到的两个伪随机序列的位变化率来评价系统的初值敏感性,位变化率越接近 50%,说明该系统对于初始条件越敏感.

设初值不同的两个二值序列 b_{1n} 和 b_{2n} 的长度均为 N,则相应的位变化率定义为:

$$bt(N) = \frac{\sum_{i=1}^{N} |b_{1i} - b_{2i}|}{N} \times 100\%. \qquad (14)$$

以下实验中的序列长度均为 $N = 100000$. 表 2 分别给出当反馈移位寄存器的初始状态和混沌系统的初始条件分别发生微小变化时,产生的二值序列位变化率. 结果表明本文方法对 LFSR 的初始状态和混沌系统的初始条件均具有良好的敏感性,因为当初始值发生微小的变化时,所生成的伪随机序列中均有约 50% 的位的取值发生了变化,很接近理想状态下对初始条件的敏感性要求. 这里 S 表示反馈移位寄存器的初始状态,X_0 表示混沌系统的初始条件.

表 2 初值敏感性分析

	初始值	变化后初始值	位变化率/%
S	9	9	49.83
X_0	0.314	0.3140000001	
S	9	9	50.20
X_0	0.314	0.314	
S	9	10	50.12
X_0	0.314	0.3140000001	

表 2 的实验结果表明,当 LFSR 的初始条件 S 或者混沌系统的初始条件 X_0 发生微小改变时,生成序列的位变化率均非常接近理想状态的 50%. 图 9 的实验结果表明,随着生成的序列长度的增加,相应的位变化率也随着生成序列的长度产生变化,但位变化率总体趋于 50%. 说明应用本文所给方法生成的序列具有良好的初值敏感性.

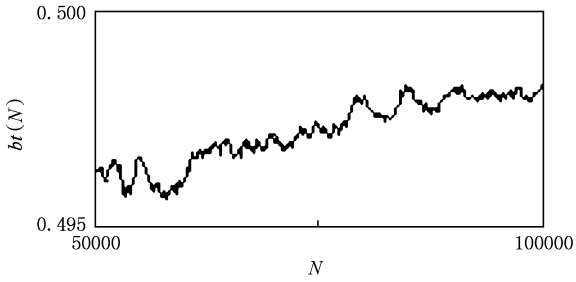

图 9 初值敏感性分析

4.2. 实值序列性能分析

4.2.1. *相关性分析*

应用公式(11)和(12)计算产生的实值伪随机序列的自相关系数和互相关系数,相应的实验结果如图 10 所示.

通过对 LFSR 和混沌系统选择不同初值进行大量的实验,我们发现几乎任意初值产生的序列均具有良好的相关性,取值接近混沌系统在无限精度状态下实现的理想状态,说明生成序列的随机性能良好.

4.2.2. *功率谱分析*

谱分析法是识别混沌的一个重要的手段. 根据 Fourier 分析理论,任何一个周期振和一系列谐振的叠加,各谐振的振幅与频率的关系为离散谱;而对于任何一个非周期运动,我们不能把它展开成 Fourier 级数,而只能展开成 Fourier 积分,即非周期运动的频谱是连续的. 若某动力学系统的频谱定长

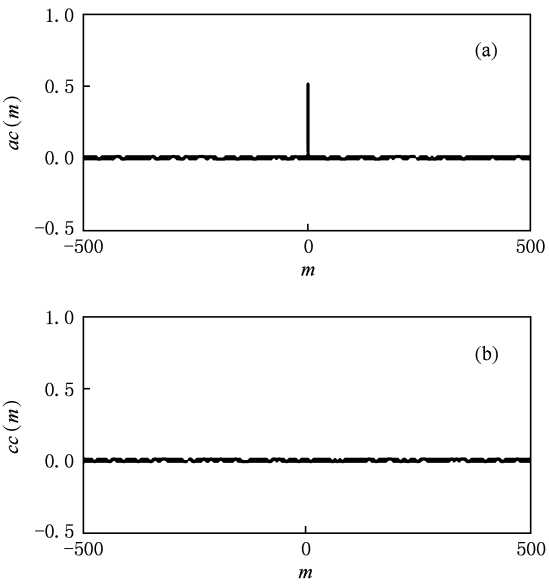

图 10　相关性分析　(a)自相关系数,(b)互相关系数

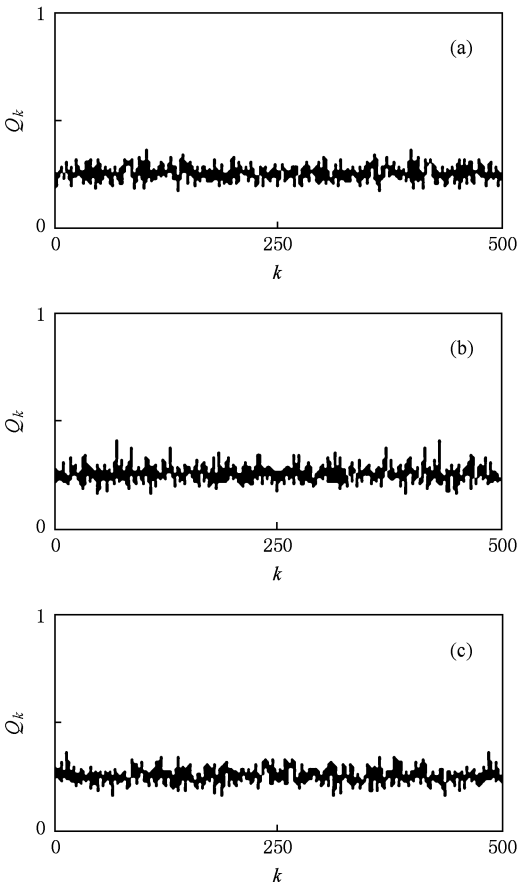

图 11　功率谱分析　(a) logistic 映射,(b)立方映射,(c)本文方法

且连续可重现,则可确定该系统是混沌的.

一个信号的时域描述和频域描述是一一对应的,功率谱分析能够提供信号的域信息. 对遍历随机过程的一个样本序列,它只是无穷多个可能的随机序列中的一个. 因此,这个序列实际上不能真正代表一个随机过程. 但是,不管取哪个序列,通过该序列计算的自相关函数总是相同的. 一个信号的时间序列看上去是不规则的,但其功率谱却可能呈现出规律性.

对时间序列 $x_i, i = 1,2,\cdots,N$, 其功率谱可通过以下方式计算[19]:

1)首先根据(11)式计算其自相关系数 $ac(m)$;

2)然后对 $ac(m)$ 进行离散 Fourier 变换,得到 Fourier 系数为

$$P_k = \sum_{j=1}^{N} ac(j)\mathrm{e}^{\mathrm{i}\frac{2\pi}{N}kj}. \tag{15}$$

记 $\alpha_k = \mathrm{Re}(P_k), \beta_k = \mathrm{Im}(P_k)$,则有 $Q_k = \alpha_k^2 + \beta_k^2$. Q_k 被称为序列 x_i 的功率谱或者功率谱函数. 当功率谱具有单峰(或者几个峰),则对应周期(或者拟周期)序列;当功率谱无明显的峰值或者峰值连成一片,则对应混沌序列(见图 11).

实验结果表明,应用本文方法产生的实值伪随机序列的功率谱没有明显的峰值,功率谱分析的实验结果与应用混沌映射生成序列的功率谱分析结果相似,说明本文方法产生的实值伪随机序列的性能良好.

4.2.3. *初值敏感性分析*

以下我们分析本文方法产生的实值序列与应用混沌映射产生的实值序列的分叉情况. 其中图 5 中的混沌系统采用 logistic 映射和立方映射. 相应的实验结果如图 12 和图 13 所示. 其中图 12 中的实线表示 logistic 映射和立方映射生成序列分布情况,虚线表示本文方法生成序列分布情况.

图 12 的实验结果表明,当初始条件相同时,本文方法生成序列相比于应用混沌映射所生成的序列出现了明显的分叉,说明两种方法产生的序列并不相同. 图 13 的实验结果表明,当初始条件发生微小变化时,应用本文的方法生成序列都将导致计算结果很快出现明显的分叉,说明本文所给方法对初值具有良好的敏感性,保证了生成序列的安全性.

5. 结　　论

本文在 LFSR 和混沌理论的基础上,给出了一

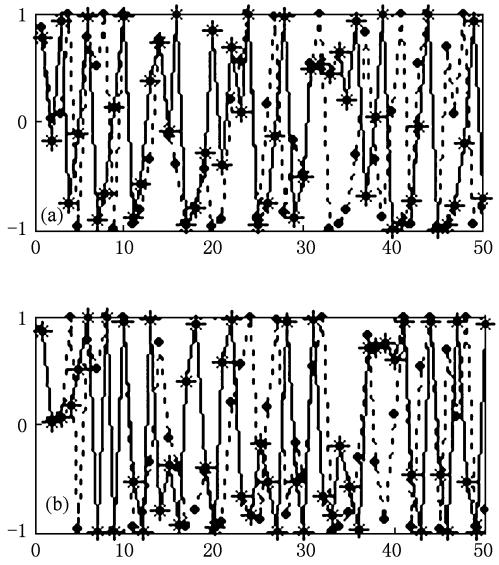

图 12 不同系统分叉情况 (a)本文方法(虚线)与 logistic 映射(实线),(b)本文方法(虚线)与立方映射(实线)

种 LFSR 和混沌系统相结合的伪随机序列生成方法. 该方法采用选择机制,通过循环迭代结构生成相应的伪随机序列,仿真结果表明,应用本文方法产生的序列具有良好的性能. 本文方法的优点是:采用选择机制,将低阶的 LFSR 和简单的混沌系统相结合使得算法具有较大的密钥空间;通过生成的二进制序列反馈值对 LFSR 进行随机扰动,使得生成序列具有良好的安全性和随机性;计算过程通过对多个简单的混沌系统进行统一的循环迭代计算,降低了计算过程的复杂性,也便于硬件实现. 下一步我们将考虑本文方法硬件实现的设计问题,为实际应用奠定基础.

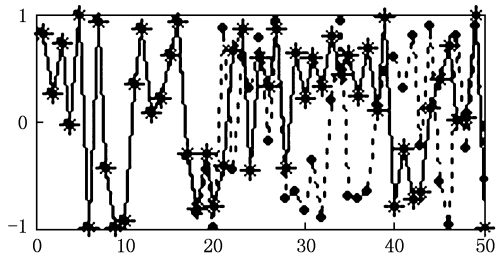

图 13 本文方法的初值敏感性分析

[1] Li N, Qi W F 2006 *IEEE Trans. Inf. Theor.* **52** 2271

[2] Wang K, Pei W J, Xia H S, Cheung Y M 2008 *Phys. Lett.* A **372** 4388

[3] Gao J T, Dong L H, Hu Y P 2006 *Chin. J. Comput.* **29** 936 (in Chinese) [高军涛、董丽华、胡予濮 2006 计算机学报 **29** 936]

[4] Xiao H, Xiao G Z, Wang X M 2008 *J. Xidian Univ.* (*Nat. Sci.*) **35** 76 (in Chinese) [肖 鸿、肖国镇、王新梅 2008 西安电子科技大学学报(自然科学版) **35** 76]

[5] Zeng G, He K C, Han W B 2007 *Sci. Chin. Ser.* E **37** 209 (in Chinese) [曾 光、何开成、韩文报 2007 中国科学 E 辑(信息科学) **37** 209]

[6] Xiao H, Zhang C R, Xiao G Z, Wang X M 2008 *J. Commun.* **29** 210 (in Chinese) [肖 鸿、张串绒、肖国镇、王新梅 2008 通信学报 **29** 210]

[7] Huang X L, Wu C K 2008 *J. Software* **19** 1256 (in Chinese) [黄小莉、武传坤 2008 软件学报 **19** 1256]

[8] Jin C H, Shi J H, Deng H 2008 *J. Electron. Inf. Tech.* **30** 665 (in Chinese) [金晨辉、史建红、邓 辉 2008 电子与信息学报 **30** 665]

[9] Zhang B, Feng D G 2006 *Sci. Chin. Ser.* E **36** 357 (in Chinese) [张 斌、冯登国 2006 中国科学 E 辑(信息科学) **36** 357]

[10] Narendra S, Aloka S 2009 *Opt. Commun.* **282** 1104

[11] Ausloos M, Dirickx M 2006 *The Logistic Map and the Route to Chaos* (Berlin: Springer-Verlag) p36

[10] Yu Z B, Feng J C 2008 *Acta Phys. Sin.* **57** 1409 (in Chinese) [余振标、冯久超 2008 物理学报 **57** 1409]

[11] Zhang Q C, Tian R L, Wang W 2008 *Acta Phys. Sin.* **57** 2799 (in Chinese) [张琪昌、田瑞兰、王 炜 2008 物理学报 **57** 2799]

[12] Wang Y F, Shen H B, Yan X L 2006 *J. Zhejiang Univ.* (*Engng. Sci.*) **40** 1972 (in Chinese) [王云峰、沈海斌、严晓浪 2006 浙江大学学报(工学版) **40** 1972]

[13] Zhan M, Zhang C F 2006 *J. Electron. Info. Tech.* **28** 2351 (in Chinese) [詹 明、张翠芳 2006 电子与信息学报 **28** 2351]

[14] Behnia S, Akhshani A, Mahmodi H, Akhavan A 2008 *Chaos Soliton. Fract.* **35** 408

[15] Pareek N K, Patidar V, Sud K K 2006 *Image Vision Comput.* **24** 926

[16] Wang X Y, Wang M J 2008 *Acta Phys. Sin.* **57** 731 (in Chinese) [王兴元、王明军 2008 物理学报 **57** 731]

[17] Yang R, Zhang B 2006 *Acta Phys. Sin.* **55** 5667 (in Chinese) [杨 汝、张 波 2006 物理学报 **55** 5667]

Pseudo-random sequence generating method based on LFSR and chaotic system*

Zhang Xue-Feng†　Fan Jiu-Lun

(*Department of Information and Control, Xi'an Institute of Posts and Telecommunications, Xi'an* 710061, *China*)

(Received 15 July 2009; revised manuscript received 4 August 2009)

Abstract

A cyclic iteration structure pseudo-random sequence generating method based on combined LFSR and chaotic systems is presented. Firstly, a choice function is chosen based on LFSR's computing result, and the selected chaotic function is used for generating the corresponding chaotic sequence by using iterative computation. The chaotic sequence is processed by binary system transformation, and the generated binary sequence is output as the end pseudo-random sequence. At the same time, the generated binary sequence is used as feedback value and operates with the LFSR's feedback value, the corresponding result is taken as the final feedback of LFSR. This process can achieve random perturbation of LFSR. And a real number pseudo-random sequence generating method is also presented. Performance of pseudo-random sequence generated by using our method is also analyzed by experiment, and simulation results show that the generated sequences have qualities of randomicity and security.

Keywords: linear feedback shift register, chaotic system, pseudo-random sequence, randomicity

PACC: 0545

* Project supported by the Natural Science Foundation of Shaanxi Province, China (Grant No. SJ08F24)

† E-mail: zhangxuefeng3@163.com