

基于 Logistic 映射的混沌随机数发生器研究

许 栋¹, 崔小欣¹, 王 田¹, 徐晓倩¹, 于敦山¹, 崔小乐², 程玉芳³

(1 北京大学 微纳电子研究院, 北京 100871; 2 北京大学 深圳研究生院, 广东 深圳 518055;
3 国民技术股份有限公司, 广东 深圳 518057)

摘 要: 分析了 Logistic 映射的混沌特性以及有限精度实现导致的特性退化问题, 采用线性反馈移位寄存器 LFSR 生成 m 序列对混沌映射施加扰动的方法设计实现了混沌伪随机数发生器, 针对不同实现精度分析硬件资源消耗情况, 并对产生的序列采用美国国家标准与技术研究院 (NIST) 所颁布的 SP800-22 标准进行测试并分析了随机性能. 结果表明, 产生序列具有良好的随机特性, 并且扰动间隔和扰动幅度的变化对有效克服有限精度效应影响显著.

关键词: Logistic 映射; 混沌; 伪随机数发生器; m 序列; 扰动

中图分类号: TN4

文献标识码: A

文章编号: 1000-7180(2016)02-0001-06

Research on Chaotic Pseudo Random Bit Generator Based on Logistic Map

XU Dong¹, CUI Xiao-xin, WANG Tian¹, XU Xiao-qian¹,
YU Dun-shan¹, CUI Xiao-le², CHENG Yu-fang³

(1 Institute of Microelectronics, Peking University, Beijing 100871, China;
2 Shenzhen Graduate School, Peking University, Shenzhen 518055, China;
3 Nationz Technologies Inc, Shenzhen 518057, China)

Abstract: In this paper, the chaotic characteristics of Logistic map and problem of its property degeneration due to finite precision implementation are analyzed. Method of perturbing the chaotic map with m -sequence generated by Linear Feedback Shift Register is used to implement chaotic Pseudo Random Bit Generator (PRBG). The consumption of hardware resources is researched for various hardware quantization wordlength. The generated sequences are tested under SP800-22 standard launched by National Institute of Standards and Technology (NIST) and their random properties are analyzed. Experimental results indicate that through adjusting perturbing interval and range, the chaotic characteristics degeneration due to the finite precision effects could be overcome effectively, and the output sequences have favorable random property.

Key words: Logistic map; chaos; PRBG; m -sequence; perturbation

1 引言

伪随机序列 (Pseudo Random Bit Sequence) 在信息安全领域具有巨大的应用和研究价值. 特别在流密码设计中, 如何实现能产生优良二进制随机序列的密钥流发生器是整个密码系统的核心与关键. m 序列及其改进序列由于具有类随机的一些特性并且

算法简单易于软硬件实现, 被传统的伪随机数发生器所广泛采用. 然而 m 序列线性复杂度较低, 对于一个 L 级线性反馈移位寄存器 (Linear Feedback Shift Register) 生成的 m 序列, 只要取得其中任意连续的 $2L$ 位就可以确定整个序列以及产生该序列的特征多项式, 对于安全可靠要求较高的场合 m 序列不能满足性能要求^[1].

收稿日期: 2015-03-27; 修回日期: 2015-05-19

基金项目: 深圳市基础研究项目 (JCYJ20140417144423194, JCYJ20140417144423198); 深圳市战略新兴产业发展专项资金创新环境建设计划项目 (ZDSY20130402095348589)

混沌是确定的非线性系统中出现的内在随机性现象,它具有如下特点:对系统初始条件高度敏感、正的 Lyapunov 指数、运动的遍历性、有界性、分形与分维性、自相似性、连续功率谱以及类噪声性等^[2-3]. 利用混沌算法产生的序列具有非周期性和伪随机性,且敏感依赖于系统初始参数,两个混沌系统即使仅有初始条件存在微小差别,迭代轨迹也会自重合逐渐远离,直至最终完全不同,其长期行为不可预测,因此该算法非常适合实现伪随机数发生器.

本文采用混沌 Logistic 映射构建的数字混沌迭代系统,设计实现了一种混沌随机数发生器.

2 算法介绍

2.1 混沌 Logistic 映射

Logistic 映射是简单非线性的一维离散迭代映射,易于硬件实现,已成为数字混沌系统中使用最为广泛的混沌映射之一. 其迭代方程如式(1)所示^[3].

$$\begin{aligned} x_{n+1} &= \mu x_n (1 - x_n), \\ \mu &\in (0, 4], x_n \in (0, 1) \end{aligned} \quad (1)$$

式中, μ 是控制参数, x_n 是迭代状态值, x_0 是迭代初始值, $n = 0, 1, 2, \dots, x_n$ 定义在连续的实数域 0 到 1 之间,随着控制参数 μ 改变,Logistic 映射的迭代行为会发生显著的变化.

图 1(b) 展示了初始值 $x_0 = 0.45$ 时 Logistic 映射的分岔图,它描述了映射迭代值随参数 μ 变化时的分布情况. 其中横坐标为参数 μ , 纵坐标为迭代状态值 x_n . 由图 1(b) 可见,随着 μ 的增大,映射迭代运动可能呈现多种状态,包括恒定为 0、单态平衡、双态平衡、倍周期分岔至四平衡态. 当 $3.569\ 945\ 672 < \mu \leq 4$ 时,迭代值不局限于几个平衡态,而是散布在一定的区间内,没有稳定的周期平衡点,迭代映射进入混沌状态,同时该状态下 Logistic 映射的 Lyapunov 指数为正数. 对于一维映射, Lyapunov 指数定义为

$$\lambda = \lim_{n \rightarrow \infty} \lambda_n = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)| \quad (2)$$

该指数用于表征系统的稳定性,其值可能大于、小于或等于 0. 当 λ 为正数时,运动轨道在每个局部都不稳定,可以作为系统进入混沌状态的判据; λ 为负数表明运动轨道在局部稳定,即周期运动. Logistic 映射的 Lyapunov 指数如图 1(a) 所示. 同图 1(b) 结合可见,随 μ 增大,不同指数值 λ 分别对应映射迭代值分布的不同状态^[2].

为了验证混沌映射对初始条件的高度敏感性,

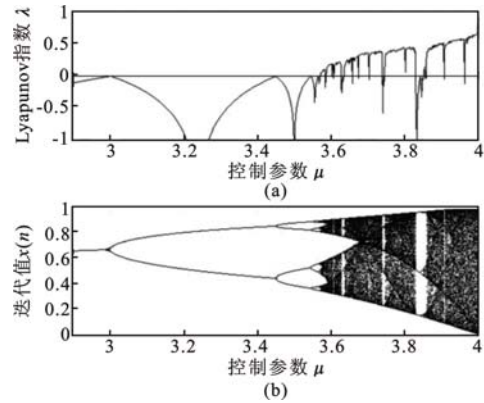


图 1 Logistic 映射倍周期分岔及其相应 Lyapunov 指数图

针对不同的初始值 $x_0 = 0.45$ 和 $x_0 = 0.450\ 001$, 在 μ 均为 4 的条件下分别迭代 60 次, 迭代轨迹如图 2 所示. 可见混沌系统对初始条件极端敏感, 两个迭代系统仅初始状态值 x_0 存在微小差别, 随着迭代次数增加, 误差被迅速放大, 轨迹由重合逐渐分离至互不相关, 迭代序列最终完全不同. 这一特性使得破解混沌加密系统初始参数的难度极大.

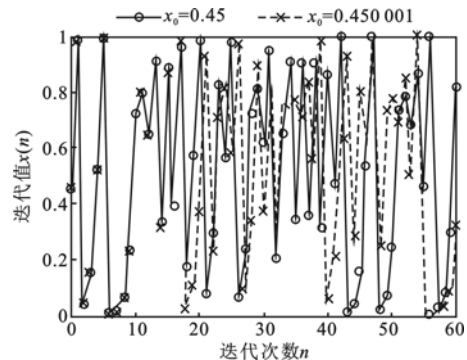


图 2 Logistic 映射不同初始值的迭代情况

2.2 利用 m 序列对 Logistic 映射施加扰动

理想的 Logistic 混沌映射定义在连续的实数域, 给定初始迭代值 x_0 和区间 $[3.569\ 945\ 672, 4]$ 内的控制参数 μ , 即可产生不可预测的非周期迭代序列. 但是由于数字系统的有限量化精度导致系统产生量化误差, 随机性能将发生退化. 假定计算精度为 L 位, Logistic 映射的迭代值只能在 2^L 个状态值中循环, 理想非周期的迭代序列退化为最大 2^L 的周期序列. 由于数字化的有限精度效应, 数字混沌映射存在短周期、分布特性和自相关性退化等问题, 致使简单利用混沌迭代算法实现的伪随机序列发生器性能无法满足加密的要求.

目前, 克服有限精度效应主要有三种思路: (1) 提高计算精度, 这是克服此问题最为有效的方

法^[4].但随着精度的提高,运算量成几何级增长,大大影响运算速度,硬件实现也会消耗极大的资源;(2)对混沌系统施加随机扰动,提高系统的复杂性,增大序列周期^[5]; (3)采用混沌多系统叠加或级联^[6].以上方法都能在一定程度上克服有限精度效应造成的混沌特性损失,对于安全性、实现难度以及资源消耗等要求不同的应用场合,可以综合考虑选择合适的方案实现混沌伪随机数发生器.

综合考虑随机码性能要求和硬件复杂度,我们选择利用线性反馈移位寄存器(LFSR)生成的 m 序列对 Logistic 映射迭代循环施加扰动的方法,设计实现混沌伪随机数发生器.系统的结构框图如图3所示.该方案中,混沌映射和 LFSR 相互独立,混沌迭代的结果 x_{n+1} 经过量化得到二进制比特序列,再与 LFSR 输出的 m 序列进行异或,实现扰动,并将扰动结果返回至混沌迭代系统的输入端,进行下一轮迭代运算.

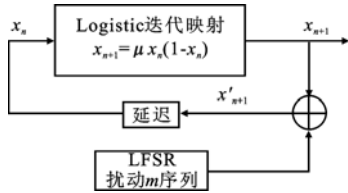


图3 m 序列扰动 Logistic 映射的混沌发生器结构框图

迭代输出结果采用二值量化算法生成伪随机码流,定义一个阈值 μ^* ,将迭代序列 $\{x_n\}$ 量化得到二进制序列 $\{y_n\}$,量化函数为

$$y = \begin{cases} 1, & x_i \geq \mu^* \\ 0, & x_i < \mu^* \end{cases} \quad (3)$$

为了达到最好的量化效果,根据 Logistic 映射迭代值分布特性,这里 μ^* 取 0.5,即将迭代值的二进制小数最高位输出.

针对混沌迭代循环,每迭代 Δ 次进行一次 m 序列的扰动,每次扰动用当前迭代值二进制形式的最低若干位,分别与 LFSR 的相应位进行异或,扰动的位数称为扰动幅度 p ,实现结构如图4所示.如果生成 m 序列的 LFSR 为 N 级,则 m 序列的周期为 $2^N - 1$,那么相比原数字混沌映射,经过扰动的混沌序列的周期就至少扩大了 $\Delta(2^N - 1)$ 倍^[7].

3 硬件实现

3.1 硬件的数据格式

Logistic 映射硬件结构中包括加法器和乘法器.从硬件速度和实现复杂度考虑,采用定点小数运算,其定点小数的数据格式为

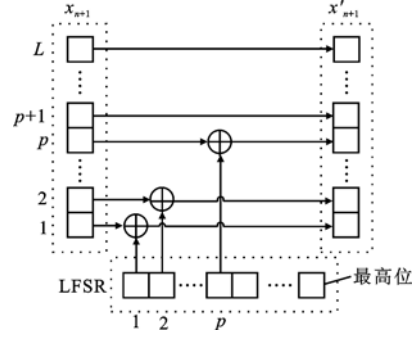


图4 m 序列扰动结构

$$x_n = 0.b_1b_2b_3b_4b_5 \cdots b_{L-1}b_L \quad (4)$$

硬件实现中,采用宽度为 L 的寄存器存储一个迭代值,而对于控制参数 μ ,因其取值范围为 $[3.569\ 945\ 672, 4]$,无法用上述定点小数形式实现,我们对原 Logistic 方程加以变形:

$$\begin{aligned} x_{n+1} &= \mu x_n (1 - x_n) \\ &= (4 - d)x_n (1 - x_n) \\ &= 4x_n (1 - x_n) - dx_n (1 - x_n) \end{aligned} \quad (5)$$

令 $\mu = 4 - d$ 则 $d = 4 - \mu \in [0, 0.430\ 054\ 328]$, d 替代 μ 作为系统初始输入参数,这样所有数据全部可以用定点小数形式实现,且控制参数可以作为密钥的一部分^[8].

3.2 混沌伪随机数发生器的硬件结构

基于 Logistic 映射的伪随机数发生器的硬件结构如图5所示.系统的实现精度为 L 位,使用 2 个 $L \times L$ 位乘法器,在每个乘法器的输出结果的 $2L$ 位中截取高 L 位作为下一级的输入,不同的是在第一个乘法器中截取输出的 $[2L-3:L-2]$ 位,实现宽度为 L 位的 $4x_n(1-x_n)$ 结果.减法器的输出结果经过量化器二值量化产生二进制随机序列,由于阈值选取 0.5,只需将 $(x_{n+1})_L$ 的最高位输出即可.每隔 Δ 次迭代,将 $(x_{n+1})_L$ 的最低 p 位(即扰动幅度)同 LFSR 输出的 m 序列最低 p 位异或得到 $(x'_{n+1})_L$,待下一时钟送入混沌迭代模块进行下一轮迭代.

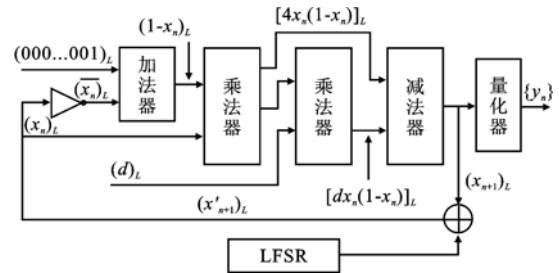


图5 基于 Logistic 映射的伪随机数发生器结构图

为了研究硬件计算精度与随机数性能之间的关

实现精度	24		32		36		40		48		64	
	P_T	Prop	P_T	Prop	P_T	Prop	P_T	Prop	P_T	Prop	P_T	Prop
SP800-22												
频率测试	F	P	P	P	P	P	P	P	P	P	P	P
子序列频率测试	F	P	P	P	P	P	P	P	P	P	P	P
游程测试	F	P	P	P	P	P	P	P	P	P	P	P
最大游程测试	F	P	P	P	P	P	P	P	P	P	P	P
二元矩阵秩测试	F	F	P	P	P	P	P	P	P	P	P	P
离散傅里叶变化测试	F	F	P	P	P	P	P	P	P	P	P	P
非重叠模型匹配测试	F	F	P	F	P	P	P	P	P	P	P	P
重叠模型匹配测试	F	F	P	P	P	P	P	P	P	P	P	P
Universal Statistical	F	P	P	P	P	P	P	P	P	P	P	P
线性复杂度测试	F	F	P	P	P	P	P	P	P	P	P	P
连续性测试	F	F	F	F	P	P	P	P	P	P	P	P
渐近熵测试	F	F	F	F	P	P	P	P	P	P	P	P
累积和测试	F	F	P	P	P	P	P	P	P	P	P	P
随机偏移测试	F	F	P	P	P	P	P	P	P	P	P	P
随机偏移衍生测试	F	F	P	P	P	P	P	P	P	P	P	P

表 2 改变扰动间隔对测试结果的影响

扰动间隔 Δ	25	50	75	100	300	500	1 000	3 000
32 位精度	23	13	11	7	9	14	46	122
36 位精度	15	3	0	0	6	3	7	10

表 3 改变扰动幅度对测试结果的影响

扰动幅度 p	3	7	10	15	22	25	27	29	30
32 位精度	6	6	6	6	5	8	9	14	21
36 位精度	4	2	2	2	0	0	1	4	19

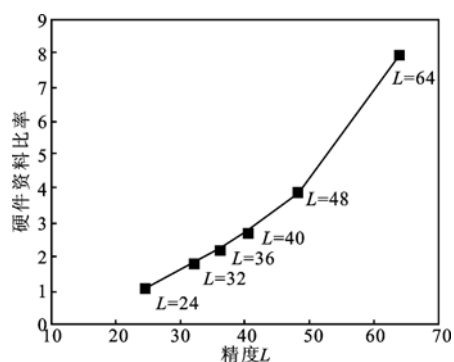


图 7 硬件资源消耗随精度增大变化趋势

表 4 精度为 36 位的 Logistic 伪随机数发生器综合结果

资源	消耗量	片内资源利用率/%
Slices	171	12
Slice Flip Flops	97	3
4 input LUTs	293	10
MULT18X18s	8	66
GCLKs	1	6

综合考虑输出序列的随机特性和硬件开销,我们选取精度 $L=36$, 基于 Xilinx Virtex-II Pro XC2VP2

FPGA 器件,设计实现了一款带 m 序列扰动的 Logistic 伪随机数发生器. 该随机发生器在满足 NIST 测试标准的前提下,硬件资源相对最优,具体硬件参数如表 4 所示.

4.3 密钥空间分析

基于 Logistic 映射的带 m 序列扰动伪随机数发生器的密钥由三部分组成,初始状态值 x_0 ,控制参数 μ 的变型 d ,以及 LFSR 的初始状态. 实验结果表明当精度为 36 位以上时,所生成的序列通过了所有的测试项目. 由于 Logistic 映射的参数 μ 越接近 4 系统的混沌特性越好,因此其变型 d 的取值空间有所缩小,假定其最高 10 位都置为 0,即 μ 最小取 3.999,此时的取值空间为 $36 + 26 + 36 = 98$,密钥空间为 2^{98} ,用穷举攻击几乎不可能破解密钥.

5 结束语

本文研究并实现了带 m 序列扰动的 Logistic 混沌伪随机数发生器,对其所产生的二进制序列采用 NIST 的 SP800-22 标准进行测试分析性能,实验表明,Logistic 映射算法简单而混沌特性复杂,易于硬件实现,通过 m 序列扰动可有效克服有限精度效应,提高运算精度能够显著改善序列的随机特性. 当采用 36 级 LFSR 产生 m 序列扰动,实现精度达到 36 位,扰动间隔 $\Delta = 100$,扰动幅度 $p = 22$ 时,产生的序列即可通过标准的全部测试项目,并且序列随机性能随着扰动间隔 Δ 和扰动幅度 p 的增大均呈先提高再降低的趋势,随着实现精度的提高,硬件资源的消耗近似呈指数增长.

参考文献:

- [1] 王相生. 序列密码设计与实现的研究[D]. 上海:中国科学院上海冶金研究所,2001.
- [2] 禹思敏. 混沌系统与混沌电路:原理、设计及其在通信中的应用[M]. 西安:西安电子科技大学出版社,2011:2-73.
- [3] 张天蓉. 蝴蝶效应之谜:走近分形与混沌[M]. 北京:清华大学出版社,2013.
- [4] 刘嘉辉,张宏莉. 基于可扩展精度的 Logistic 混沌随机序列的并行计算方法[J]. 中国科学技术大学学报,2011,41(9):837-846.
- [5] 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.
- [6] Pareek N, Patidar V, Sud K. Cryptography using multiple one-dimensional chaotic maps[J]. Communications in Nonlinear Science and Numerical Simulation, 2005, 10(7): 715-723.
- [7] Sang T, Wang R, Yan Y. Perturbance-based algorithm to expand cycle length of chaotic key stream[J]. Electronics Letters, 1998, 34(9): 873-874.
- [8] 樊昌信,曹丽娜. 通信原理[M]. 6 版. 北京:国防工业出版社,2006.

作者简介:

许 栋 男,(1989-),硕士研究生. 研究方向为数字集成电路设计.

崔小欣(通讯作者) 女,(1979-),博士,副教授. 研究方向为低功耗数字系统设计、信息安全硬件设计、SOC 及 NOC 设计等. E-mail:cuixx@pku.edu.cn

崔小乐 男,(1975-),博士,副教授. 研究方向为 VLSI 测试与可测性设计、电子系统可靠性等.

程玉芳 女,(1985-),硕士,工程师. 研究方向为密码学.