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 Dong[1], CUI Xiao-xin, WANG Tian[1], XU Xiao-qian[1],
YU Dun-shan[1], CUI Xiao-le[2], CHENG Yu-fang[3]
(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

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.