文章编号:1671 - 6833(2008)01 - 0044 - 04

一种混沌伪随机序列发生器的 FPGA 实现

盛利元[1], 刘 念[1], 曹莉凌[2]

(1. 中南大学 物理科学与技术学院,湖南 长沙 410083; 2. 上海水产大学 工程学院,上海 200090)

摘 要: 随着混沌理论应用于产生伪随机序列的发展,用现场可编程逻辑门阵列实现了基于 TD - ERCS 混沌的伪随机序列发生器. 为了便于硬件实现并减少硬件占用资源,对原算法(即基于 TD - ERCS 构造伪随机序列发生器的算法)进行了适当改进,密钥空间缩减到 2^{160}. 设计采用双精度浮点运算,选用 Cyclone 系列的 EP1C20F400 芯片,完成了 CPRSG 的系统仿真实验. 系统的硬件电路占用 17716 个逻辑单元,占芯片资源 88%,工作频率 50 MHz,CPRS 产生速率 10 Mbps.

关键词: 混沌;切延迟椭圆反射腔映射混沌系统;混沌伪随机序列发生器;现场可编程门阵列;统计特性

中图分类号: TN 431.2; TN 918.2 **文献标识码**: A

0 引言

高度安全的伪随机序列发生器是信息加密的核心算法,几乎各类加密算法都需要. 近几年来,随着混沌密码理论的深入研究,现场可编程门阵列(Field Programmable Gate Array, FPGA)实现混沌伪随机序列发生器(Chaotic Pseudo - Random Sequences Generator, CPRSG)引起了人们的极大兴趣. 寻找一种性能优良的 CPRSG 并且完成其硬件实现意义重大,是理论研究与工程应用研究的新挑战.

有关 PRSG 的传统算法都是基于整数理论的,如线性移位寄存器及其改进的 Gold 序列、非线性同余发生器、细胞自动机序列、RC4、SEAL(IBM)等,适合 FPGA 实现,速度快、占用资源小,但用于加密算法安全性不够[1]. BBS (Blum, Blum and Shub) 算法是一种基于大数分解的算法,被认为安全性高,在 133 MHz 时钟频率下速率仅为 225 bps[2],也不适合用作流密码.

混沌系统对初始条件极为敏感,具有貌似随机的动力学行为,因而具备构造 PRSG 的基本条件,但用 FPGA 实现存在理论上和技术上的困难.

本文的动机是要用 FPGA 实现一个高度安全的 CPRSG. 与文献[3 - 5]不同,首次采用 64 - bit 浮点运算, CPRSG 算法[6],是一种基于 TD - ERCS (Tangent - Delay Ellipse Reflecting Cavity map System)[7]的算法. 与其它混沌系统相比,TD - ERCS 具有全域混沌、全域零相关特性,巨大的参数和初值空间,不存在稳定的短周期,是差分分析免疫的[8],实验显示它还具有极强的抗退化能力,因此,由 TD - ERCS 构造的 CPRSG 的安全性是可以信赖的. 实验采用由华清远见公司提供的高级 FPGA 教学实验平台,芯片选用逻辑资源为 50 万门的 Cyclone EP1C20F400,采用 VHDL (VHSIC Hardware Description Language)完成各功能模块设计. CPRSG 硬件电路共占用 17 716 个逻辑单元,占芯片资源 88%,工作频率为 50 MHz,CPRS 产生速率为 10 Mbps.

1 基于 TD - ERCS 混沌系统的 PRSG

文献[6]给出了该 CPRSG 算法,为了便于硬件实现和减少硬件资源,对原算法作如下改进:①仅用一个 TD - ERCS 产生伪随机序列,密钥空间缩减为 2^{160};②缩小切延迟参数的取值范围,$m = 2,4,5,6,\cdots,17,18$,占用 1 字节存储单元;③用户通过上位机软件直接给 x_0、$\mathrm{tg}\alpha$、μ 及 m 赋值,通过串口发送给硬件系统(下位机)运算,简化了硬件实现过程;④采用一种硬件快速实现方法[9]归一化处理迭代产生的 x 和 k 值.

收稿日期:2007 - 10 - 27;修订日期:2008 - 01 - 12

基金项目:国家自然科学基金资助项目(60672041)

作者简介:盛利元(1956 -),男,湖南益阳人,中南大学教授,硕士,主要从事混沌理论、混沌密码理论和汉语语音信息处理方面的研究,E - mail:itpo@ mail. su. edu. cn.

2　CPRSG 的 FPGA 实现

整体结构为上位机与下位机两部分，上位机由用户控制实现与下位机之间数据交换，下位机是 CPRSG 的 FPGA 硬件系统. 笔者仅讨论下位机的实现原理.

2.1　下位机系统的整体结构

下位机系统的整体结构如图 1 所示，主要包括通用异步收发(Universal Asynchronous Receiver / Transmitter，UART)控制器、初始值缓存分配器、结果序列缓存转换器以及 TD - ERCS 算法实现单元 4 个模块. 4 个模块中，TD - ERCS 算法实现单元中的浮点运算器是核心，关系到 CPRSG 的随机特性，是实现的重点. 为了降低系统实现成本，设计了特定功能状态机与数据选择器，实现分时复用各浮点运算器，兼顾了硬件系统实现时资源与速度的平衡.

2.2　各功能模块设计

2.2.1　UART 控制器

UART 控制器辅助 PRSG 硬件系统与串行设备(本文特指计算机)进行串口通信. 为了充分利用 EP1C20F400 中富余的硬件资源，在 FPGA 内部实现 UART 功能. UART 波特率为 9 600 bit/s，收发一次的数据包括 1 位起始位、8 位字符数据位、1 位停止位，不含奇偶校验位，共 10 位. 图 2 为 UART 整体设计图，主要由接收检测器、波特率发生器、移位寄存器、计数器和收发控制器组成.

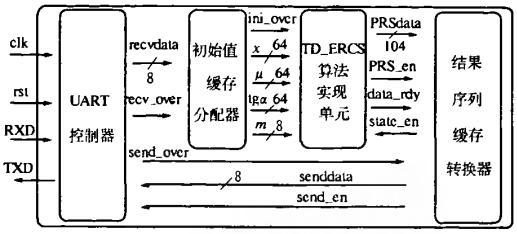


图 1　系统整体框架图

Fig. 1　The frame diagram of CPRSG

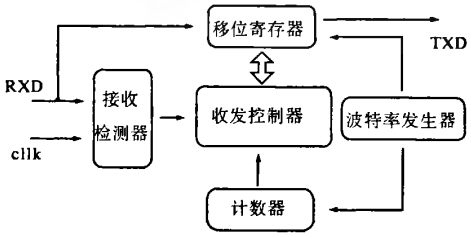


图 2　UART 整体框架图

Fig. 2　The frame diagram of UART

2.2.2　初始值缓存分配器

初始值缓存分配器获取 UART 控制器接收到的 20 字节的串行数据，分配给 TD - ERCS 系统作为初始值及参数，并触发 TD - ERCS 算法实现单元开始进行迭代运算，通过编写 VHDL 行为级代码，综合得到的寄存器传输级(RTL)电路如图 3 所示.

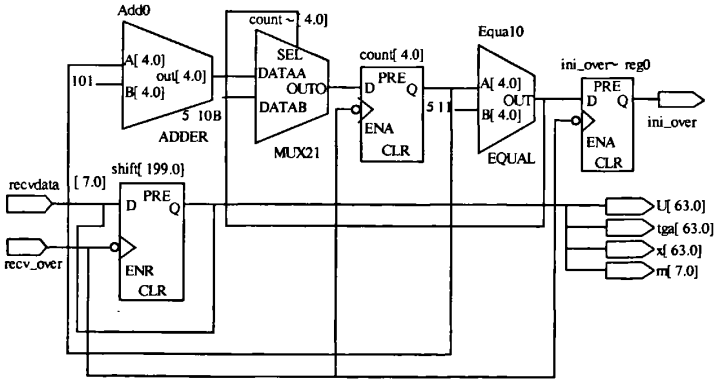


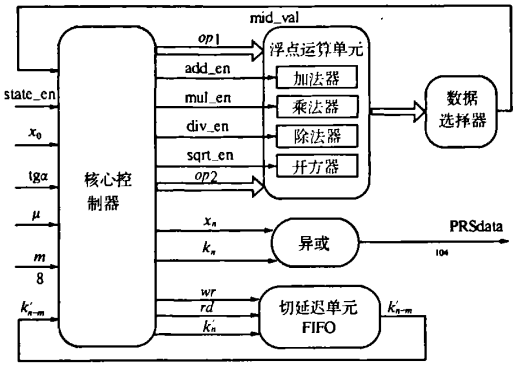
图 3　初始值缓存分配器 RTL 电路图

Fig. 3　The RTL circuit diagram of initializers

2.2.3　TD - ERCS 算法实现单元

TD - ERCS 算法实现单元是关键部分，其功能为：获取初始值，进行 TD - ERCS 迭代运算，产生结果序列 CPRS，其结构如图 4 所示. 该单元由 5 个子模块组成：①核心控制器，根据 TD - ERCS 算法定义状态，产生浮点运算及读写 FIFO 控制信号；②浮点运算单元，执行 IEEE754 标准双精度浮点加、乘、除及开方运算，其中加法采用 LOP 算法，乘法采用 Wallace 树结构与修正的 Booth 编码相结合实现，除法与开方运算采用基为 2 的 SRT 算法实现；③先入先出存储器 FIFO，保存 TD - ERCS 产生的部分 k_n 值；④数据选择器，选择正确的运算结

果;⑤异或门,对 *TD - ERCS* 算法产生的实数 x_n 和 k_n 的尾数进行异或操作生成最终的 CPRS.



(注:图中未标识的数据总线宽度均为64bit)

图4 TD - ERCS 算法实现单元结构框图

Fig.4 The frame diagram of TD - ERCS

2.2.4 结果序列缓存转换器

结果序列缓存转换器的功能是保存 CPRS,并依据 UART 控制器的设计规范,对 CPRS 数据总线宽度进行转换,经 UART 发送至串行设备. UART 数据总线宽度为 8 位,而 TD - ERCS 算法单元每一轮迭代产生的结果序列数据总线宽度为 104 位,数据格式不匹配,系统无法在一个节拍内通过 UART 将数据发送至串行设备,需设置缓存器转换数据格式,通过 13 个节拍发送一轮 CPRS 数据. 该模块信号连接图如图 5 所示.

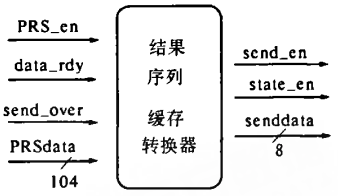


图5 结果序列缓存转换器模块的框图

Fig.5 The frame diagram of result convertor

3 功能模块与系统仿真

采用 Altera 公司的仿真及逻辑综合工具 Quartus II,先后分别将设计好的各功能模块以及系统综合后下载到 EP1C20F400 中. 表 1 给出了各主要功能模块的编译结果,全系统综合后占用17 716个逻辑单元,逻辑资源利用率为 88%,最大时钟频率为 3.17 MHz. 通过上位机输入初始值 $x_0 = 0.25$、$tg\alpha = 0.75$、$\mu = 0.5$ 及 $m = 2$,data104 为最终产生的伪随机序列,仿真结果如图 6 所示,所得 CPRS 上传至上位机显示并保存为文本文件供测试.

表1 系统的各主要功能模块的编译结果

Tab.1 The synthesis results of function modules

功能模块		占用逻辑单元(LE)/资源占用率	最大时钟频率/MHz	最差传输延时/ns	最差建立时间 t_{pd}/ns	最差时钟输出时间 t_{co}/ns	最差保持时间 t_h/ns
UART		162 个/(<1%)	116.63	8.574	8.127	13.335	-1.030
初始值缓存分配器		211 个/(1%)	155.50	6.431	6.210	10.906	-2.583
TD - ERCS 单元	FIFO	21 个/(<1%)	290.87	3.438	4.788	11.669	-1.869
	浮点加法器	1429 个/(7%)	83.31	12.004	24.980	9.842	-1.567
	浮点乘法器	3576 个/(18%)	73.50	13.606	23.878	9.217	-2.128
	浮点除法器	6953 个/(34%)	2.49	401.767	8.360	31.679	-2.606
	浮点开方器	3116 个/(16%)	320.10	3.124	5.609	9.379	-3.310
	核心控制器	1853 个/(9%)	149.08	6.708	6.118	10.653	0.036
	异或	52 个/(<1%)	—	—	—	—	—
	数据选择器	216 个/(1%)	500.00	2.000	6.158	14.190	5.303
结果序列缓存转换器		127 个/(<1%)	191.86	5.212	7.450	10.517	-0.572

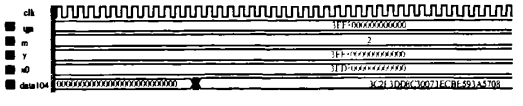


图6 伪随机序列发生器的仿真波形

Fig.6 The simulation of CPRSG

4 结论与展望

由于混沌系统定义在实数域上,混沌密码算法在数字机上实现时,为了最大限度减少混沌退化引起的安全性隐患,不仅是软件,而且硬件也都应采用双精度浮点运算,这种方案也有利于混沌密码算法标准化制定和安全性分析. 虽然采用双精度浮点运算占用较多的系统资源,运行速度也受到影响,但是,就密码算法而言,安全性是第一位的,而系统资源以及运算速度会随着芯片制造技术的进步逐渐弱化. 所以从长远来说,采用双精度浮点运算实现混沌密码算法是混沌密码走向实用的必然过程. 如果混沌系统是安全的,算法速度

快,一定程度上也能弥补采用双精度浮点运算的缺陷.

采用双精度浮点算法用 FPGA 实现一个混沌的流密码,它能够最大限度地保留混沌系统在理论分析和数字实验中呈现的安全特性,因此,本文由 FPGA 实现的 CPRSG 的安全性可以得到充分保障. 运算速度上,本系统产生流密码速率达到 10 Mbps,远优于其它混沌系统. 笔者给出的 CPRSG 的硬件实现是探索性的,作为第一款采用双精度运算的混沌密码实验芯片,在安全性能够得到保障的前提下以算法和程序走通为首要目标,应该说,在算法改进、程序结构优化方面还有效大的压缩空间,也没有考虑到能耗问题.

参考文献:

[1] MENEZES A J, VAN OORSCHOT P C, VANSTONE S A. Handbook of Applied Cryptography[M]. 5th edition. New York: CRC Press, 2001.

[2] TSOI K H, LEUNG K H, LEONG P H W. Compact FPGA - based true and pseudo random number generators[C]//In FCCM 2003 IEEE Computer Society. Washington DC: IEEE computer Society, 2003: 51 - 61.

[3] MUNAKATA T, SINHA S, DITTO W L. Chaos computing: implementation of fundamental logical gates by chaotic elements[J]. IEEE Trans: CAS - I, 2002, 49(11): 1629 - 1633.

[4] MAO Y B, CAO L, LIU W B. Design and FPGA implementation of a pseudo - random bit sequence generator using spatiotemporal chaos[J]. ICCCAS, 2006, (3): 2114 - 2118.

[5] 高金峰,徐惠芳. 模拟电感与集成化混沌信号发生器实现研究[J]. 郑州大学学报:工学版,2005,54(3):102 - 105.

[6] 盛利元,曹莉凌,孙克辉,等. 基于 TD - ERCS 混沌系统的威随机数发生器及其统计特性分析[J]. 物理学报,2005,54(9):4031 - 4033.

[7] 盛利元,孙克辉,李传兵. 基于切延迟的椭圆反射腔离散混沌系统及其性能研究[J]. 物理学报,2004,53(9):2871 - 2976.

[8] 盛利元,闻姜,曹莉凌. TD - ERCS 混沌系统的差分分析[J]. 物理学报,2007,56 (1):78 - 83.

[9] SHENG L Y, XIAO Y Y, SHENG Z. A universally valid algorithm on transforming chaotic sequences into uniform pseudo - random sequences[J]. Acta Phys Sin, 2007, 56(12): 20 - 25.

FPGA Implementation of a Chaotic Pseudo - Random Sequence Generator

SHENG Li - yuan[1], LIU Nian[1], CAO Li - ling[2]

(1. School of Physics Science and Technology, Central South University, Changsha 410083, China; 2. College of Engineering Science & Technology, Shanghai Fisheries University, Shanghai 200090, China)

Abstract: With the development of chaos theory based pseudo - random number generator (PRNG), in this paper, a FPGA (Field Programmable Gate Array) based implementations of a chaotic pseudo - random sequence generator (CPRSG) is presented. It is a bit serial implementation of a pseudo - random number generator based on TD - ERCS which is appropriately improved and the key space of CPRSG is reduced to 2^{160} in order to facilitate the realization of hardware and reduce hardware resources occupied. An effort of synthesizing the improved algorithm into a Cyclone EP1C20F400 FPGA is also reported. The design is with double - precision floating - point operations and the system hardware circuit occupies 17,716 logical elements, accounting for 88% chip resources. Elementary hardware simulation results show that the throughput of the CPRSG chip reaches up to 10 Mbps under a running condition of 50 MHz clock frequency.

Key words: chaos; TD - ERCS; CPRSG; FPGA; statistic characteristics