

一种基于 PCIE 的 FPGA 密码芯片验证测试系统

刘学光,李树国

(清华大学 微电子所,北京 100084)

摘 要: 搭建了一种基于 PCIE 通信的用于密码芯片的 FPGA 验证与测试系统. 该系统针对 SM234 密码芯片的验证测试,提出了一种芯片流片前后验证测试的方法. 在芯片流片前利用 FPGA 实现密码芯片逻辑,以验证密码芯片的功能,降低芯片的流片风险. 同时,为密码芯片后期测试提供一种可行的测试方案,以缩短密码芯片的后期测试时间. 鉴于密码芯片三种密码算法的高速数据传输要求,系统选择 PCIE 作为板卡的数据传输总线来提高验证测试系统的效率.

关键词: PCIE; 密码芯片; FPGA 验证; 测试

中图分类号: TN49

文献标识码: A

文章编号: 1000-7180(2014)11-0079-04

A FPGA Verification and Test System for Cryptographic Chip Based on PCIE

LIU Xue-guang, LI Shu-guo

(Institute of Microelectronics, Tsinghua University, Beijing 10084, China)

Abstract: This paper builds a FPGA verification and test system for cryptographic chip based on PCIE communication. The system provides the method of FPGA verification before tapeout and test after tapeout for SM234 cryptographic chip. Using FPGA implements logic of the cryptographic chip to verify the chip function and reduce the risk of tapeout. Meanwhile, the system provides a feasible chip test scheme for the post test to cut down the test time. Given the requirement of high-speed data transmission, the system selects the PCIE bus to complete the data transmission between card and computer, improves the efficiency of SM234 cryptographic chip verification and test plan.

Key words: PCIE; Cryptographic chip; FPGA verification; test

1 引言

本系统所使用的密码芯片为我们课题组开发的 SM234 密码芯片,该芯片支持 SM2、SM3、SM4 三种密码算法多种模式的运算. SM2/SM3/SM4 是国家密码管理局公开的密码算法. SM2 是一种非对称密码算法,可实现签名、验证、加密、解密等功能; SM3 是一种消息摘要算法; SM4 是一种对称加密算法,可实现加密、解密等功能.

密码芯片的设计复杂,实现成本高,所以有必要在密码芯片流片前对其进行 FPGA 验证,以减小芯

片的流片风险. 同时,密码芯片流片后需要使用大量测试向量及高速的数据传输,这给密码芯片的测试板卡设计带来一定的难度.

PCIE 是一种通用总线和接口标准,采用了点对点串行连接,每个设备都有自己的专用连接,不需要向整个总线请求带宽,可以达到 PCI 以及更早期的计算机总线所不能提供的高带宽.

2 系统硬件设计

2.1 PCIE 总线的层次结构

PCIE 总线采用全双工串行传输模式,并使用

收稿日期: 2014-02-01; **修回日期:** 2014-03-27

基金项目: 国家“八六三”计划项目(2012AA012402);国家自然科学基金项目(61073173);清华大学自主研发计划项目(2011Z05116)

数据包进行数据传输,其层次结构分为物理层、数据链路层和事务层,如图 1 所示.在 PCIE 体系结构中,数据报文首先在设备的核心层(Device Core)中产生,然后再经过事务层(Transaction Layer)、数据链路层(Data Link Layer)和物理层(Physical Layer),最终发送出去,而接收端也需要通过物理层、数据链路层和事务层,并最终到达核心层^[1].

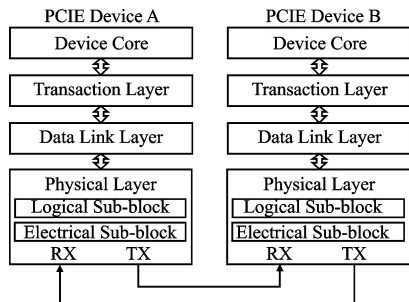


图 1 PCIE 总线层次结构

事务层主要用于完成 TLP(Transaction Layer Package)的装配和拆解,TLP 是被用来传输事务的数据包,比如存储器读或者存储器写,配置读或配置写或者其他特定类型的事务.数据链路层是事务层和物理层之间的连接,负责两层之间的沟通.物理层将来自数据链路层的并行数据信息转变为合适的串行数据发送给链路另一边的设备.

2.2 验证板卡架构

板卡 PCIE 接口基于 Xilinx 的 PCIE 的 IP 硬核实现,其符合 PCIE V1.1 协议要求,PCIE 总线工作在 1.25 GHz,单通道传输带宽为 2.5 GT/s.该 PCIE 硬核只提供 PCIE 接口的物理层和数据链路层,用户需要根据实际需求设计事务层^[2].

板卡需完成密码芯片流片前的 FPGA 验证和流片后的测试.基本思路是在一块验证板上使两个 FPGA 互连,同时为密码芯片预留焊盘,其中一个 FPGA 完成密码芯片原型实现,另一个 FPGA 完成 PCIE 总线传输和密码芯片的控制.在芯片流片前,利用其中一块 FPGA 实现密码芯片逻辑 FPGA 验证与测试设计;在芯片流片后,将密码芯片焊接至预留焊盘,完成密码芯片的测试.验证板卡的整体设计如图 2 所示.

板卡主要包括 FPGAI、FPGAII、SM234 芯片以及其他必要的外围电路.FPGAI 选用 Xilinx 公司的 XC5VF30T,完成 PCIE 通信逻辑、数据的临时储存和密码芯片的控制逻辑.FPGAII 选用 Xilinx 公司的 XC3S1000,实现密码芯片原型.

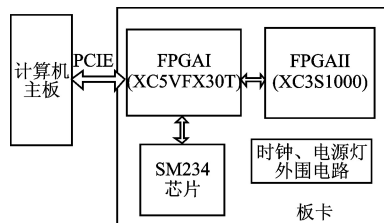


图 2 验证系统整体设计框图

2.3 板卡的通信逻辑与芯片控制逻辑

板卡的通信逻辑与芯片控制逻辑由 FPGAI 来实现,主要包括 PCIE 总线逻辑,密码芯片控制逻辑以及双口 SRAM,具体结构如图 3 所示.

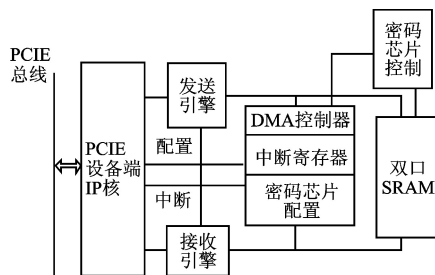


图 3 通信逻辑与芯片控制逻辑结构

板卡工作时通过 PCIE 总线将计算机内存中的数据传输到 FPGAI 的双口 SRAM^[3],然后启动密码芯片进行处理,并将处理后数据存放至双口 SRAM 当中,最后通过 PCIE 总线将处理后数据传输至计算机内存.

PCIE 接口的事务层主要包括三个模块:DMA 控制器、发送引擎和接收引擎.发送引擎完成 TLP 的组装,接收引擎完成 TLP 的拆解,DMA 控制器负责控制 PCIE 总线进行 DMA 数据传输^[4].

2.3.1 发送引擎和接收引擎逻辑实现

发送引擎和接收引擎分别完成 TLP 的组装和拆解.当发送 TLP 时,先由 TLP 头生成逻辑产生 TLP 头存储于 FIFO 当中,然后发送引擎状态机将 TLP 头和相应数据组装成完整的 TLP,发送给 PCIE 硬核.当接收到 TLP 时,先由接收引擎状态机将 TLP 内信息提取出来,分别将数据和数据信息存放在 FIFO 当中,然后由数据存储状态机根据数据信息将数据存放在响应存储单元当中.

2.3.2 密码芯片控制逻辑实现

密码芯片内 SM2 采用寄存器来临时存放待处理数据和处理后数据,故控制逻辑需将不同地址的寄存器写入待处理数据,然后通过配置 SM2 控制寄存器启动芯片进行运算,待运算结束后将处理后数据读出;SM3 采用 FIFO 临时存放待处理数据,采用寄存器存放处理后数据,当 FIFO 不为空的时候

即开始运算,不需要额外的启动信号,故控制逻辑当 FIFO 不满的时候将芯片内传输数据,利用 Last_Byte 信号标志待处理数据传输完成,当运算结束后,读取寄存器内的处理后数据;SM4 采用两个 FIFO 临时存放待处理数据和处理后数据,采用同时写入待处理数据和读取处理后数据的传输方式,故控制逻辑同时进行写入操作和读出操作.三种算法的输入输出控制逻辑的流程图如图 4 所示.

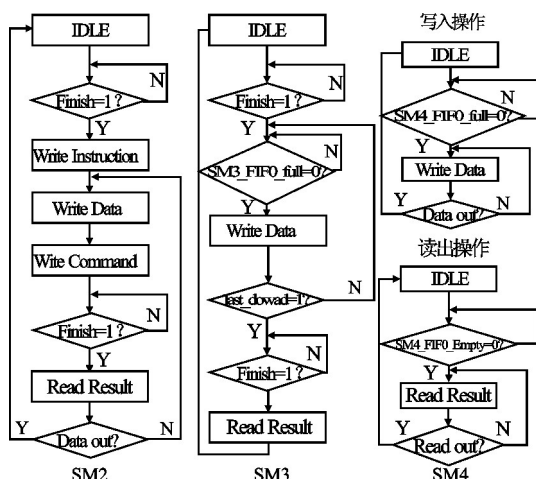


图 4 芯片控制逻辑流程图

2.4 板卡的硬件实现

板卡实物如图 5 所示,主要包括 FPGA1, FPGAII,为密码芯片预留的焊盘以及其他电源转换、FPGA 配置等外围电路. FPGA1 与密码芯片焊盘之间的连线运用蛇形走线使得信号线的长度差距在 100mil 以内,保证了板卡可以在比较高的时钟频率下工作.

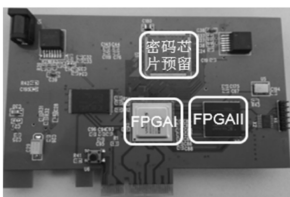


图 5 板卡实物图

3 系统驱动程序设计

3.1 WDF 框架驱动程序

WDF(Windows Driver Foundation)驱动程序框架是微软基于 WDM(Windows Driver Model)驱动程序框架提出的新一代的驱动程序框架.

WDF 提供了 KMDF(Kernel-mode Windows Driver Foundation)和 UMDF(User-mode Windows Driver Foundation)两个框架,该系统的驱动程序采

用 KMDF^[5].

驱动程序的入口程序为 DriverEntry,当在计算机上加载驱动程序后,DriverEntry 创建 WDFdriver 对象并注册添加新设备的回调函数.在插入设备后,调用 EvtDeviceAdd 来初始化驱动程序,主要包括获取设备内存空间,初始化 IO 队列,初始化中断服务,初始化 DMA 传输服务.本文的驱动程序主要实现三个功能,分别是 PIO 数据传输,DMA 数据传输和设备发起的中断处理.图 6 所示为驱动程序的总体流程.

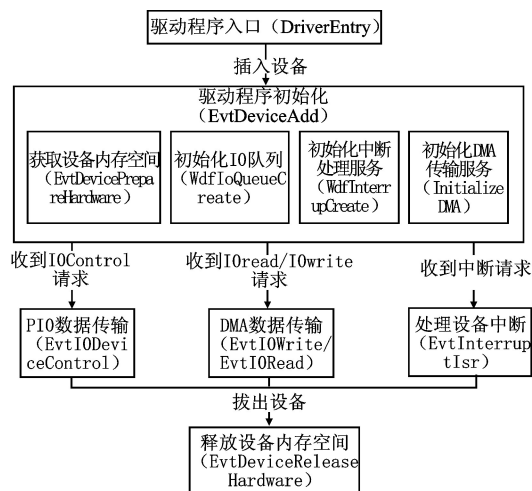


图 6 驱动程序的总体流程

3.2 PIO 数据传输

当板卡插入到 PCIE 插槽中时,驱动程序为板卡的分配内存地址空间,板卡采用 128 Byte 的内存地址空间,由 32 个 32 bit 寄存器组成的寄存器堆实现.对于驱动程序来说,处理器与寄存器堆的通信相当于处理器与内存之间的通信.

PIO 数据传输的主要功能包括 DMA 配置,密码芯片配置、中断寄存器的读写以及其他相关信息的读写.

3.3 DMA 数据传输

PIO 的传输速度非常有限,且需要占用处理器资源,故只适用于少量信息的读写.密码芯片的待处理数据和处理后数据的传输由 DMA(Direct Memory Access)传输完成. DMA 传输将数据直接在计算机内存和板卡之间进行传输,传输过程由板卡进行控制,不需要处理器的介入,不但传输速率高,而且节省了处理器运算资源. DMA 传输过程如下:

(1)在驱动程序初始化的时候建立 DMA 适配器对象,同时申请两段物理地址连续的内存作为 DMA 读和 DMA 写的公用缓冲区,同时获取两段公

用缓冲区的物理首地址;

(2)将缓冲区的物理首地址通过 PIO 的方式写入板卡的 DMA 操作寄存器;

(3)当有数据 DMA 传输 IO 请求时,在 EvtIoRead 或 EvtIoWrite 例程中,用 WdfDmaTransaction Initialize 函数初始化 DMA 传输;调用 WdfDma TransactionExecute 函数,启动 DMA 传输;

(4)由 EvtProgramReadDma 或 EvtProgramWrite Dma 函数对板卡的 DMA 操作寄存器进行配置;

(5)启动 DMA 传输后,板卡的 DMA 控制器完成计算机内存和板卡内双口 SRAM 之间的数据传输.当传输完成后,板卡发起中断;

(6)当驱动程序接收到板卡发起的中断时,在 EvtInterruptDpc 例程中测试 DMA 传输是否结束,若没有则调用 WdfDmaTransactionExecute 函数,继续启动 DMA 传输;若传输结束,则完成 IO 请求.

4 SM234 密码芯片 FPGA 验证

SM234 芯片接口逻辑电路的 FPGA 验证步骤如下:

(1)密码芯片接口逻辑在 FPGAII 中的实现

将密码芯片内 PLL 的 IP 核去除,内部时钟由 IO 直接提供;将密码芯片所使用的 FIFO 的 IP 核更换为 FPGA 的 IP 核;将 SM2/SM3/SM4 算法核心逻辑电路更换为对待处理数据逐位取反后直接输出;最终将修改后的密码芯片逻辑使用 FPGA 进行实现,烧入 FPGAII.

(2)通信逻辑与密码芯片控制逻辑在 FPGAI 中的实现

将通信逻辑和密码芯片控制逻辑烧入 FPGAI. FPGAI 内的数据临时存储在双口 SRAM 中. FPGAI 有两个时钟域,分别是 PCIE 通信逻辑时钟域和密码芯片控制逻辑时钟域,通过双口 SRAM 进行连接.

(3)利用 ChipScope 进行验证

通过 DMA 方式将待处理数据由计算机内存传输至 FPGAI 内双口 SRAM,启动密码芯片进行计算,通过 ChipScope 观察密码芯片接口信号波形,验证接口逻辑是否正确.将处理后数据由 FPGAI 内双口 SRAM 传输至计算机内存,对比处理后数据与标准结果数据.

5 SM234 密码芯片的测试设计

由于可利用 FPGAII 实现密码芯片的接口逻

辑,所以流片之前已经可以开展密码芯片的测试设计工作.芯片测试的数据流如图 7 所示.

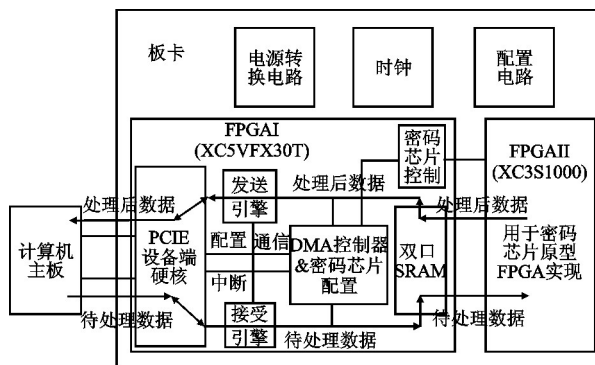


图 7 芯片测试时的数据流向

芯片测试目的为测试芯片对 SM2、SM3、SM4 三种算法的正确性、最高工作频率以及吞吐率,基本思想是逐步提高芯片算法逻辑电路工作频率,得到芯片能够正常工作的最大时钟频率,然后测试在该频率下密码芯片各算法的吞吐率.具体测试步骤如下所示.

(1)FPGA 实现

同 4 节中的步骤 1 和 2,将芯片接口逻辑烧入 FPGAII,将通信逻辑和芯片控制逻辑烧入 FPGAI.密码芯片的算法逻辑电路采用较低的时钟频率.

(2)密码芯片配置

通过 PIO 的方式配置密码芯片的工作模式.

(3)密码芯片的测试与计时

通过 DMA 将一定量的待处理数据传输至 FPGAI 的双口 SRAM 当中,启动密码芯片对待处理数据运算,同时计数芯片控制逻辑的时钟数;当密码芯片运算结束时,停止计数;将处理后数据由 FPGAI 的双口 SRAM 传输至计算机内存,对比处理后数据与标准结果.重复以上过程足够多次.

(4)如果步骤 3 结果正确,提高密码芯片算法逻辑电路的工作频率,回到步骤 2.如果结果错误,进入步骤 5.

(5)采用最后一次能够使密码芯片正常工作的时钟频率,重复步骤 2 和 3,将记录下的时钟数读出,算出密码芯片的净工作时间,结合处理的数据量得到密码芯片的吞吐率.

6 结束语

本文设计了一个使用 PCIE 接口通信的密码芯片 FPGA 验证测试系统.该验证系统提供了高速数

(下转第 87 页)

时间.为此抓取了模型和硬件实际的运算周期数(如表5所示),由上表格可以看出,两者的运算周期数完全相同.



图4 乒乓运算示意图

表5 大点数纯运算周期数

点数	SystemC IDE 仿真周期数	FPGA 仿真周期数
512k	3 490 304	3 490 304
1024k	5 717 818	5 717 818

4 结束语

针对在 Soc 设计中实现软硬件协同的要求,本文提出了一种可配置的周期精确的 FFT 模型.通过与硬件测试结果的比对,模型实现了小点数周期精确,达到了完善硬件设计、验证各项性能指标、缩短硬件研发时间的目的.

参考文献:

- [1] Ali Ahmadinia, Balal Ahmad, Ahmet Erdogan, et al. System C-based reconfigurable IP modelling for system-on-chip design[C]// IEEE NASA/ESA Conference on Adaptive Hardware and Systems. Piscataway, NJ: Adaptive Hardware and Systems, 2008:362-367.
- [2] 何卫强,杨靓,卢强.基于 SystemC 的周期精确级 DSP

处理器建模[J].微电子学与计算机,2012,29(4):107-110.

- [3] SystemC Version 2.0 User' Guide [EB/OL]. [2012-01-13]. Inc. <http://www.systemc.org>.
- [4] Bidet E, Castelain D, Joanblanc C, et al. A fast single-chip implementation of 8192 complex point FFT[J]. IEEE Journal of Solid-State Circuits, 1995, 30(3): 300-304.
- [5] Hongjiang He, Hui Gu. The realization of FFT algorithm based on FPGA Co-Processor[C]// Second International Symposium on Intelligent Information Technology Application, Beijing, 2008: 239-243
- [6] Lihong Jia, Yonghong Gao, Hannu Tenhunen. Efficient VLSI implementation of radix-8 FFT algorithm [C]// IEEE Pacific Rim Conference on Communications. Piscataway, NJ: Computers and Signal Processing, 1999: 468-471.
- [7] 邓波,戎蒙恬,汤晓峰.可配置高速高精度 FFT 的硬件实现[J].计算机工程,2006(17):254-256.
- [8] Lu Shyuekung, Yeh Chienhung, Lin Hanwen. Efficient built-in self-test techniques for memory-based FFT processors [C]// Proceedings of the 10th IEEE Pacific Rim International Symposium on Dependable Computing. Piscataway, NJ: Computer and Signal Processing, 2004: 468-471.

作者简介:

樊恩辰 男,(1990-),硕士研究生.研究方向为 ASIC 设计、多核处理器.

(上接第 82 页)

据传输接口、多功能的芯片控制逻辑和易于修改的驱动程序,可以满足 SM234 密码芯片的 FPGA 验证与测试要求.本系统降低密码芯片的流片风险,提高了芯片测试效率,减少了密码芯片的开发时间和开发成本.

参考文献:

- [1] 王齐. PCI Express 体系结构导读 [M]. 北京:机械工业出版社,2010.
- [2] Xilinx. LogiCore IP endpoint block plus V1.9 for PCIeExpress [s]. USA:California:Xilinx Corp., 2008.

[3] 何妍,李树国.一种具有双 PCI 接口的 ASIC 验证系统[J].微电子学,2006(4):36-38.

- [4] Xilinx. Virtex-5 FPGA integrated endpoint block for PCI express designs [s]. USA: California: Xilinx Corp., 2008.
- [5] 武安河. Windows 设备驱动程序 WDF 开发 [M]. 北京:电子工业出版社,2009.

作者简介:

刘学光 男,(1989-),硕士研究生.研究方向为信息安全.
李树国 男,(1963-),教授,博士生导师.研究方向为信息安全算法及其大规模集成电路设计与实现