第 42 卷 第 3 期 计 算 机 工 程 2016 年 3 月
Vol. 42 No. 3 Computer Engineering March 2016

·开发研究与工程应用· 文章编号：1000-3428(2016)03-0289-06 文献标识码：A 中图分类号：TN919.5

高速串行数据处理模块的设计与实现

徐 健，侯振龙，龚东磊，方 明

（中国电子科技集团公司第三十二研究所，上海 200233）

摘 要： 为提高现有密码模块中数据加解密算法的多样性和安全性，设计并实现一种基于双现场可编程门阵列（FPGA）与数字信号处理器（DSP）架构的数据处理模块。2 片 FPGA 分别与 DSP 通过外部存储器接口（EMIF）总线进行互联。FPGA 1#利用 PCIe，EMIF 总线实现其与上位机和 DSP 的通信，并结合分散-收集型直接内存存取模块最大化 PCIe 链路带宽。FPGA 2#使用 AURORA 协议与 FPGA 1#进行串行通信，实现多个加解密算法的并行工作，同时支持算法的全局和局部重构。DSP 负责数据加解密算法的参数配置、密钥生成与安全管理。在中标麒麟操作系统下的板级功能与性能验证结果表明，该模块与主机的通信速率可达 11.36 Gb/s，同时具有密码安全性高和算法可重构的特点，适用于高速数据协同处理领域。

关键词： 直接内存存取；数字信号处理器；PCIe 总线；现场可编程门阵列；中标麒麟操作系统

中文引用格式： 徐 健，侯振龙，龚东磊，等. 高速串行数据处理模块的设计与实现[J]. 计算机工程，2016，42(3)：289-294.

英文引用格式： Xu Jian，Hou Zhenlong，Gong Donglei，et al. Design and Implementation of High-speed Serial Data Processing Module[J]. Computer Engineering，2016，42(3)：289-294.

Design and Implementation of High-speed Serial Data Processing Module

XU Jian，HOU Zhenlong，GONG Donglei，FANG Ming

（The 32nd Research Institute of China Electronics Technology Group Corporation，Shanghai 200233，China）

【Abstract】 In order to improve the diversity and safety of data encryption and decryption algorithms in cryptographic modules，this paper designs and implements a data processing module based on dual Field Programmable Gate Array（FPGA） and Digital Signal Processor（DSP） architecture. Two pieces of FPGA are interconnected with a DSP by External Memory Interface（EMIF） bus. FPGA 1# communicates with PC and DSP by PCIe and EMIF bus，and Scatter-gather Direct Memory Access（SG-DMA） is used for high-speed data transferring application. FPGA 2# realizes serial communication with FPGA 1# by AURORA protocol，makes multiple algorithms work in parallel，and supports global and partial reconfiguration of the algorithm. DSP realizes parameter configuration as well as key generation and management for data encryption and decryption algorithms. The driver and application software are designed on NeoKylin operating system to test the module's function and performance. Results show that the rate of communication between the module and the host is up to 11.36 Gb/s，and the module has the characteristics of high safety and reconfiguration suitable for high-speed data co-processing field.

【Key words】 Direct Memory Access（DMA）；Digital Signal Processor（DSP）；PCIe bus；Field Programmable Gate Array（FPGA）；NeoKylin operating system

DOI： 10.3969/j.issn.1000-3428.2016.03.052

1 概述

随着密码系统的发展，数据的存储安全成为信息安全领域的研究热点。信息的加密存储、传输、身份认证、密钥管理等都对密码平台的功能及性能提出了更高要求。数据处理模块作为平台对用户数据进行加解密和信息安全处理，可以起到数据安全存储的作用。在数据处理模块的设计初期，保障算法多样性和算法安全性便是设计的重要目标。本文设计了一种高速串行数据处理模块，可用于解决现有密码模块中数据加解密算法的多样性和安全性两方面的问题。在算法多样性方面：支持多算法并行工作模式，该硬件基于双现场可编程门阵列（Field Programmable Gate Array，FPGA）+数字信号处理器（Digital Signal

作者简介：徐 健（1963－），男，高级工程师，主研方向为计算机体系结构；侯振龙，工程师；龚东磊、方 明，高级工程师。

收稿日期：2015-07-13 修回日期：2015-09-26 E-mail：xuj@ecict.com.cn

Processor,DSP)架构,其中的一片 FPGA 专门处理算法,DSP 通过配置不同的配置文件来达到算法的多样性。在算法安全性方面:上电时处理算法的 FPGA 内部没有配置逻辑,DSP 也只有引导程序,它们如何工作均取决于主机下载的配置文件;FPGA 负责算法并行工作,DSP 负责密钥随机生成与安全管理。

2 数据处理模块架构设计

2.1 传统硬件架构设计

传统的数据加解密模块系统架构通常采用单 FPGA、单 DSP 或 FPGA + DSP 架构,如文献[1-3]提出的 3 种典型架构。前两者将总线接口逻辑、加解密算法以及密钥管理整合在一起,增加了 FPGA 或 DSP 代码层次架构的复杂性,同时对 FPGA 器件的逻辑资源或 DSP 定浮点处理能力要求较高,导致设计成本和开发周期的增加。而 FPGA + DSP 架构通常将 FPGA 作为与上位机通信的接口,DSP 实现特定数据加解密算法以及密钥的产生与管理。很明显,以上 3 种架构都无法实现算法、密钥以及对外通信接口的安全隔离以及各功能维护升级的独立性。

2.2 改进型硬件架构设计

基于以上硬件架构分析,本文提出采用双 FPGA + DSP 协同处理的架构,如图 1 所示,2 片 FPGA 分别与 DSP 通过外部存储器接口(External Memory Interface,EMIF)总线互联。

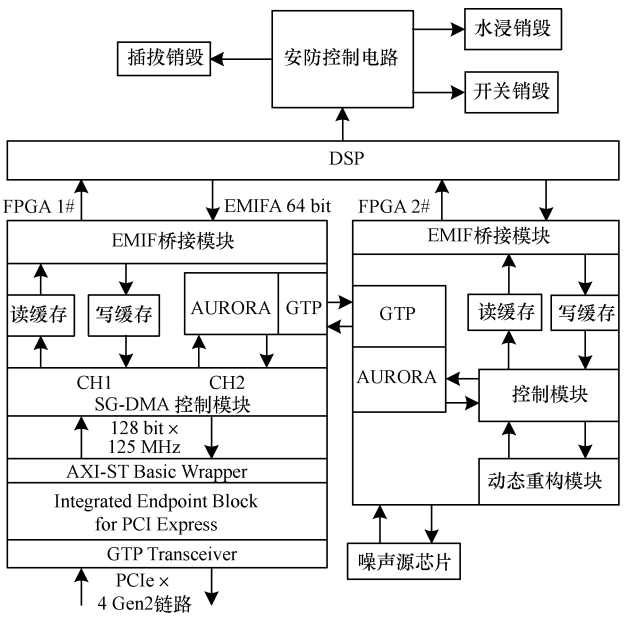

图 1 数据处理模块架构

在图 1 中,FPGA 1#实现通过外部高速总线 PCIe 接口与上位机通信以及通过 DSP EMIF 总线实现与 DSP 之间的通信;FPGA 2#负责具体实现特定需求的加解密算法;DSP 选用 TI 公司的 TMS320C6416T,实现对 FPGA 2#的算法参数配置、密钥生成与管理以及基于特定通信协议的 2 片 FPGA 之间数据包转发、封包、解包。

在整个硬件架构中,通过 FPGA 1#,FPGA 2#,DSP 三者之间的有机结合实现了对外接口、算法以及密钥之间的安全隔离,同时也充分体现了 FPGA 的并行逻辑处理能力以及 DSP 的定点运算能力。

3 功能设计

整个模块的功能设计包括高速串行接口、加解密算法动态重构、密钥随机生成与安全管理三大部分,其中,密钥随机生成与安全管理主要有 DSP 实现,本文不做详述。

3.1 高速串行接口设计

整个模块中接口的传输速率是设计的核心部分。为满足 10 Gb/s 高吞吐率的明文或密文传输速率,需要解决与上位机通信接口[4]速率以及算法 FPGA 2#与接口 FPGA 1#之间的通信速率瓶颈问题。因此,设计采用高可靠的高速串行链路来满足设计要求,即采用 PCIe2.0 串行总线结合分散-收集型直接内存存取(Scatter-gather Direct Memory Access,SG-DMA)来实现与上位机通信,2 片 FPGA 通过 AURORA 串行总线设计机制来满足通信速率瓶颈问题。

3.1.1 PCIe 逻辑设计

在本文设计中,使用 7 系列 PCIe 2.0 硬核[5]实现物理转 TLP(Transaction Layer Packet)层,使设计能够以最低的时延发挥高性能 PCIe 端点的功能。PCIe 端点在物理层、数据链路层和事务处理层中有大量复杂的协议需要处理[6-7],Xilinx 将 PCIe 硬核实现在器件的架构中,用于处理全部的 PCIe 操作,便于集中设计 SG-DMA 操作本身的功能。图 2 显示了 PCIe 硬核的顶层功能模块和接口[8-9]。本文使用 Vivado 集成环境来配置和生成 PCIe 端点 IP。

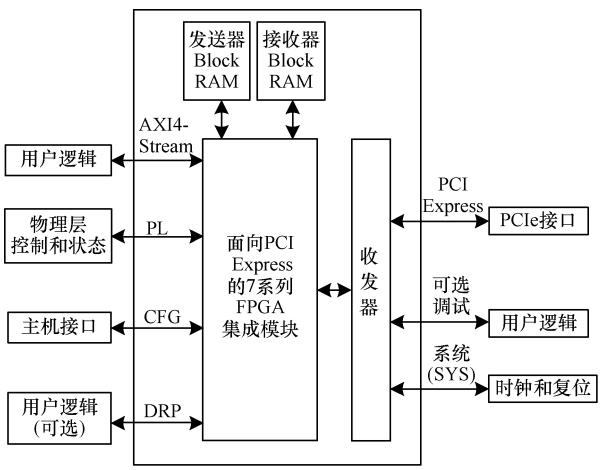

图 2 PCIe 硬核顶层的功能模块与接口设计

3.1.2 AXI4-Stream 总线设计

AXI4-Stream 总线[10]是高带宽、低延迟的片内互联

总线,面向高速数据流传输。总线采用握手机制实现数据收发,没有地址通道和读写使能,数据由主接口向从接口的单向传输。同时,允许无限制的数据突发传输规模,可以显著降低信号路由速率。本文设计中,2 片 FPGA 内部模块间的互联均采用 AXI4-Stream 总线。

3.1.3　SG-DMA 逻辑设计

传统 Block DMA 在实际应用中很难申请到一大片连续的物理空间,每次传输时对寄存器设置和中断响应的操作会导致系统开销和时延增加。SG-DMA 则很好地解决了这个问题。

本文设计该模块的目的是充分利用 PCIe 的带宽,达到板间传输数据速率大于 10 Gb/s 的指标。由于 DMA 的实现方式没有统一的标准,因此根据不同的应用,可以设计出不同的 DMA 架构。经过大量研究,本文设计一种面向 PCIe2.0 应用的 SG-DMA,SG-DMA 模块的功能框图如图 3 所示。

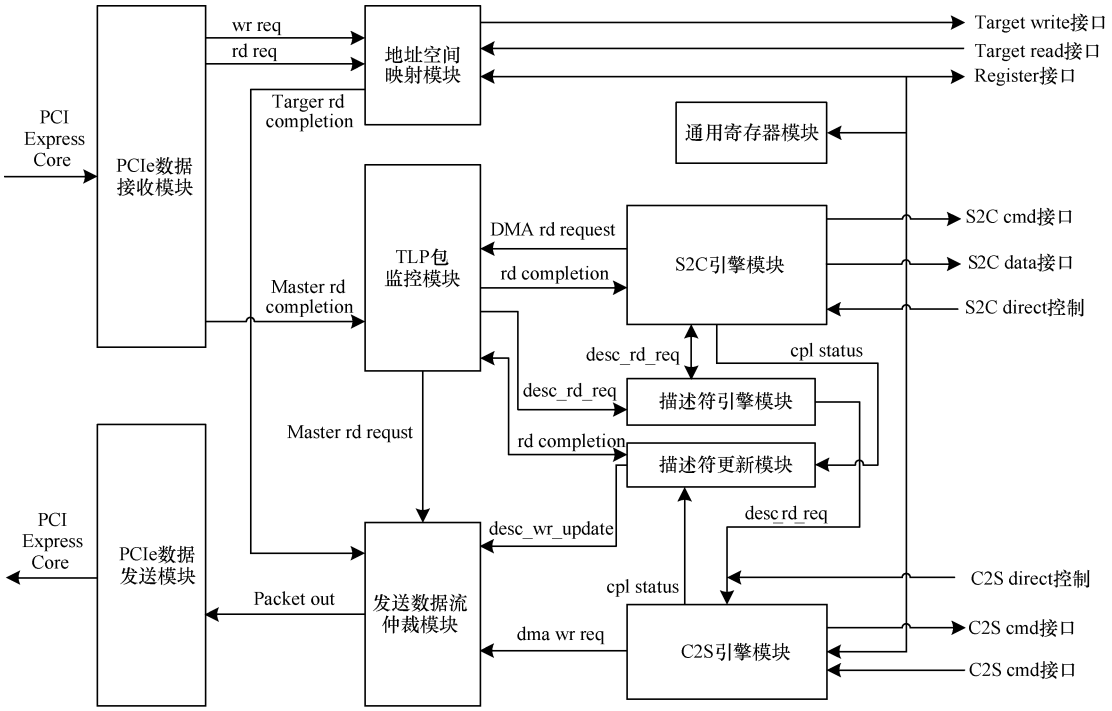

图 3　SG-DMA 模块功能框图

SG-DMA 的主要功能是处理来自主机的 TLP 数据包并做出响应。SG-DMA 用作对主机存储器的 PCIe 主控访问,在主机和本地存储器之间传输数据。主机向 DMA 控制器发送命令,控制 DMA 访问。该命令代码嵌入在特定的主机 TLP 寄存器写操作的数据中。SG-DMA 控制器初始化 SG-DMA 写请求,响应主机的读取命令,将数据从本地存储器迁移到主机存储器。同样,对于主机的写入命令,SG-DMA 控制器初始化 DMA 请求,将数据从主机存储器迁移到本地存储器中。

本文设计中定义的描述符由 4 个双字组成,PCIe 硬核应用层的宽度为 128 bit,即:单时钟周期可以接收全部描述符信息,优化 SG-DMA 内部架构,减少内部时延。描述符分为主机至板卡方向和板卡至主机方向,其具体结构如图 4、图 5 所示。可以看出,描述符分为控制区和状态区两部分,其中,控制区的寄存器是在描述符发送到 SG-DMA 引擎之前,由软件指定工作方式与流程;状态区的寄存器是在完成一次 SG-DMA 之后,由 SG-DMA 引擎完成对数据搬运状态的标注。

S2C状态寄存器	保留	S2C剩余字节数
S2C控制寄存器	保留	描述符的大小
主机内存的起始地址		
下一描述符的地址指针		5'b00000

图 4　S2C 描述符结构

C2S状态寄存器	保留	描述符的大小
C2S控制寄存器	保留	C2S剩余字节数
主机内存的起始地址		
下一描述符的地址指针		5'b00000

图 5　C2S 描述符结构

3.2　算法重构

为满足数据加解密算法的安全性(算法不驻留板卡,即算法掉电销毁)以及算法的动态配置和加载,在设计 FPGA 2#时,采用无片外 Flash 器件的设计方式,应用通过 DSP 的 EMIF 总线以及 GPIO 模拟 FPGA 配置 SelectMap(×16)的方式实现,即算法 FPGA 2#的配置

文件由上位机通过 PCIe 总线传递给FPGA 1#,FPGA 1# 通过 DSP 的 EMIF 总线传递给 DSP,DSP 再从 EMIF 总线上读取并以 SelectMap (×16)方式配置算法 FPGA 2#。由于 FPGA 基于 SRAM,因此掉电情况下可以起到较好的加解密算法保护作用。

3.2.1 EMIF 桥接模块设计

FPGA 连接 DSP 的 EMIFA,该部分的逻辑设计如图 1 所示,由 3 个子模块组成:Read FIFO Buffer, Write FIFO Buffer 和 EMIF Bridge,完成 DSP 与 FPGA 之间的数据交换,支持 DSP 的 EDMA/QDMA 操作。设计该模块的目的是达到板上 FPGA 与 DSP 的通信速率大于 1 Gb/s 的指标,并支持 DSP 的 EDMA/QDMA 操作。

EMIF[11]是连接外部存储器与 DSP 芯片内其他单元的接口。DSP 可通过 EMIF 接口的控制对外部存储器和外设进行访问。它具有较强的接口能力及较高的数据读写访问速度,数据宽度为 64 bit。EMIF 桥接模块如图 6 所示。

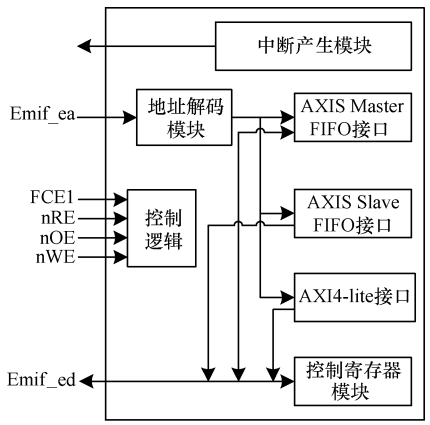

图 6 EMIF 桥接模块功能框图

在实际工作中,DSP 对 EMIF 总线的写时序为 Setup time:1,Strobe time:1,Hold time:1;DSP 对 EMIF 总线的读时序为 Setup time:1,Strobe time:2,Hold time:1。在设计过程中,要求对 PCB 走线和 FPGA 内部逻辑进行严格设计才能达到以上的时序要求。

3.2.2 可重构设计

该模块设计的目的是提高系统灵活性,FPGA 2#内部有多个算法同时工作,增加了部分可重构的特性,Xilinx 的部分重构技术使 FPGA 的灵活性得到很大的提高,可以在不影响逻辑正常运行的前提下,动态更新某一算法。文献[12-14]从不同应用角度分析了重构的一般设计方法。重构流程主要分为 3 步:(1)主机发送配置命令给 DSP,DSP 收到后分析主机即将发送的配置文件,是全局重构还是局部重构。如是全局重构,则配置文件存放在外部 Flash 中。如是局部重构,则文件存放在 SDRAM 中,分析完成后返回响应命令包。(2)接收主机发送的配置文件,根据命令包内容选择存储方式。接收完成直接配置 FPGA 2#,硬件配置电路使用 SelectMap (×16)配置方式。该配置方式为并行配置,在大幅缩短全局配置时间的同时,还支持局部重构配置。(3)当 DSP 检测到 FPGA 2#配置完成信号有效后,发送配置完成包给主机,主机接收到信号后结束本次配置流程。

3.2.3 驱动设计

为顺应国产化的发展趋势,将本文设计的高速串行数据处理模块运行在国产化平台上,操作系统选用中标麒麟[15](内核版本 2.6.32),驱动架构如图 7所示。

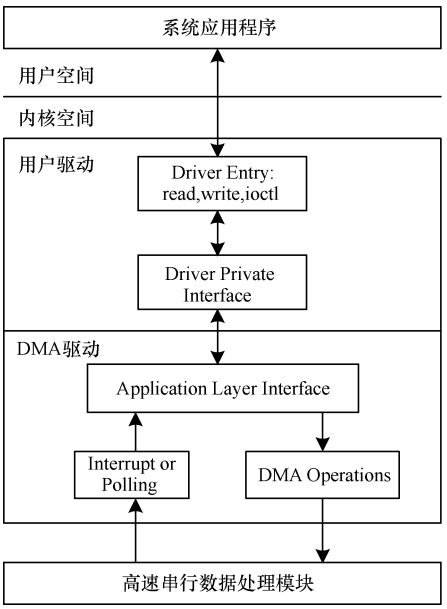

图 7 驱动架构

该驱动设计利用一些结构体来传递应用程序和驱动程序之间的信息。PCI 设备驱动操作的 2 个关键的结构体如下:

```
static struct pci_driver DmaDriver = {
        .name       = "Pcie_DMA",
        .id_table   = DmaDriverpci_tbl,
        .probe      = DmaDriverAdd,
        .remove     = __devexit_p(DmaDriverRemove),
        };
static struct file_operations procfs_fops = {
        .open       = procfs_open,
        .read       = seq_read,
        .write      = procfs_write,
        .llseek     = seq_lseek,
        .release    = single_release,
        }
```

4 测试方法与验证结果

在中标麒麟操作系统下,驱动安装完成后,分别

设计 3 个系统应用对模块功能做进一步验证。

4.1　板间互联速率测试

本文测试的板间速率是指主板与模块通过 PCIe 总线互联,在无差错传输的前提下所能达到的最大速率。测试模型如图 8 所示,可以看出,在 FPGA 1# 内部将 SGDMA 模块后端数据收发接口互联为一个回环,测试数据速率。

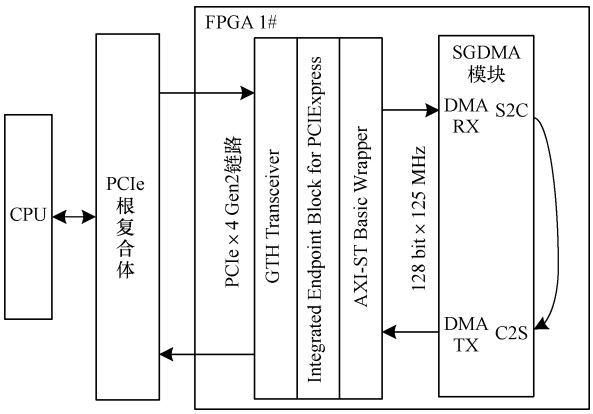

图 8　板间互联速率测试模型

主机侧发送的 4 GB 数据采用轮间方式测试 SGDMA 的性能。为配合测试,本文设计了基于 Linux 的应用程序,在驱动安装完成后,在终端中键入./NKdriverFileDh运行测试程序,如图 9 所示,可以看出经过收发平均速度为 11.36 Gb/s(1.420 GB/s)。

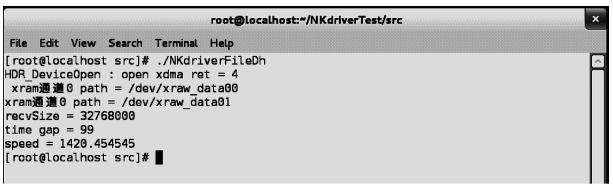

图 9　板间互联速率测试界面

4.2　DSP 接口速率测试

DSP 接口速率的测试模型如图 10 所示。数据从主机发送至 DSP 后,DSP 将数据暂存在 SDRAM 中,存储完成后再写进 FPGA。SGDMA 模块将数据写进主机内存的相应地址中并产生 MSI 中断,通知主机接收数据。

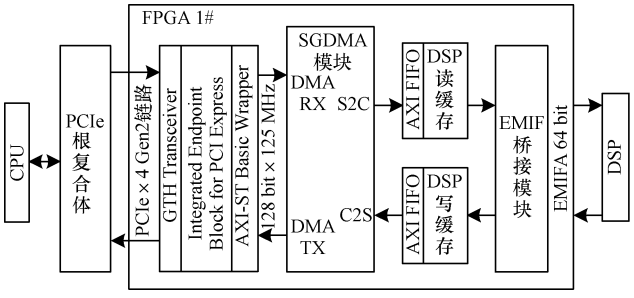

图 10　DSP 接口速率测试模型

为配合测试,设计基于 Qt 开发环境的图形化界面,如图 11 所示。从测试结果可以看出,数据传输时间是 17 989 ms,传输数据长度是 1 187 687 731 Byte,得到的传输速度是 63.019 5 MB/s(504.156 Mb/s)。因为测试结果显示的是数据的双向速率,所以 DSP 与 FPGA 之间的单向读写平均速率为 1 008.312 Mb/s,大于 1 Gb/s。

图 11　DSP 接口速率测试界面

4.3　FPGA 重构功能测试

板卡支持的重构功能主要是指重构 FPGA 2#,这片 FPGA 可以作为专用密码处理和数据加解密处理应用,支持多算法核的局部重构功能。FPGA 重构测试模型如图 12 所示。

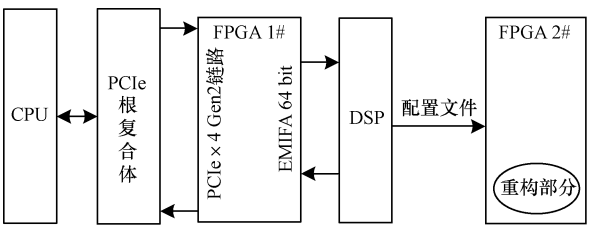

图 12　FPGA 重构功能测试模型

FPGA 重构功能基于 Qt 开发环境,配置完成后的界面如图 13 所示,简单直观,同时支持配置 DSP。

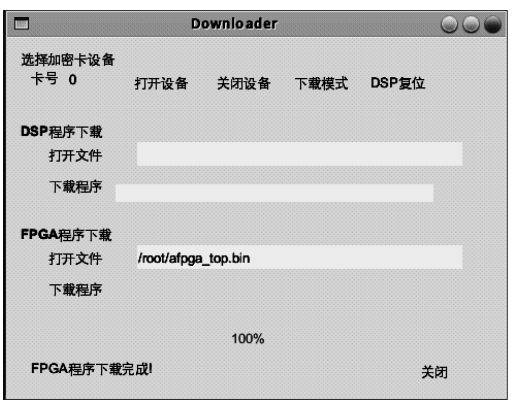

图 13　FPGA 重构功能测试软件界面

该主机将全局重构配置文件或者局部重构配置文件(bin 文件)发送给 DSP,DSP 将配置文件放入

其外部 Flash 中,由于发送配置文件前,DSP 会收到主机发送的配置命令帧并区别全局配置指令和局部配置指令,因此 DSP 在收到配置文件后,直接通过 SelectMap(×16)的方式配置 FPGA 2#。

5 结束语

本文设计的基于双 FPGA + 单 DSP 架构的安全高速串行数据处理模块具有 FPGA 灵活性、并行逻辑处理能力、可重构特性以及 DSP 定浮点处理能力,并且保障了算法的安全性和灵活性,较传统的 PCI 总线接口获得了更高的传输速率。该模块在高速数据协同处理和复杂算法处理方面,具有良好的用户体验和广阔的应用前景。因此,将该数据处理模块应用于视频编解码领域是下一步研究的主要内容。

参考文献

[1] 杨 斐,彭 鹏. 基于 AES 的可重构加密系统的 FPGA 设计[J]. 微型机与应用,2014,33(24):2-4.

[2] 顾兆丹. 基于 DSP 下视频流的对称密码算法性能测试[J]. 机电一体化,2015,(6): 69-72.

[3] 韩天峰. PCI 密码设备 FPGA + DSP 设计方案[J]. IT 技术,2008,(12): 92-93.

[4] Xilinx. High-Speed Serial I/O Made Simple[EB/OL]. [2015-06-10]. http://www. xilinx. com.

[5] 马鸣锦,朱剑冰,何红旗,等. PCI、PCI-X 和 PCI Express 的原理及体系结构[M]. 北京:清华大学出版社,2007.

[6] Budruk R, Anderson D, Shanley T. PCI Express System Architecture[M]. Littleton, USA: Mindshare, Inc. ,2008.

[7] PCI Express Base Specification Revision 2. 0[EB/OL]. [2015-06-10]. http://www. pcisig. com.

[8] Xilinx. 7 Series Integrated Block for PCIe[EB/OL]. [2015-06-10]. http://www. xilinx. com.

[9] Wilen A H, Schade J P, Thornburg R. Introduction to PCI Express——A Hardware and Software Developer's Guide[Z]. 2003.

[10] ARM. AMBA4 AXI4-Stream Protocol Version: 1. 0[EB/OL]. [2015-06-10]. http://www. arm. com.

[11] TI. TMS320C6000 EMIF to External FIFO Interface[EB/OL]. [2015-06-10]. http://www. ti. com.

[12] 陆振林,赵元富,兰立东,等. 基于可重构技术的 DSP 任务动态加载方法研究[J]. 电子技术应用,2015,41(10):24-26.

[13] 周盛雨. 基于 FPGA 的动态部分重构系统实现[D]. 北京:中国科学院大学,2007.

[14] 杜 林,邹孝付. 基于 FPGA 的动态重构技术研究与实现[J]. 自动化与仪器仪表,2015,(7):103-106.

[15] IBM. Linux 下 PCI 设备驱动程序开发[EB/OL]. [2015-06-10]. http://www. ibm. com/.

编辑 陆燕菲

(上接第 288 页)

[10] He Lin, Yu Zhuliang, Gu Zhenghui, et al. Bhattacharyya Bound Based Channel Selection for Classification of Motor Imageries in EEG Signals[C]//2009 中国控制与决策会议论文集 2. 北京:[出版者不详],2009: 2353-2356. [11] Kołodziej M, Majkowski A, Rak R. Implementation of Genetic Algorithms to Feature Selection for the Use of Brain-computer Interface [J]. Przeglad Elektrotechniczny,2011,87(5):71-73.

[12] Jolli I T. Principal Component Analysis[J]. SpringerBriefs in Optimization,2013,16(11):576-595.

[13] 唐肖芳,周金治. 基于散度分析的脑电信号特征选择[J]. 计算机工程,2015,41(5):290-294.

[14] Harrag A, Saigaa D, Harrag N. Linear Discriminant Analysis, Principipal Component Analysis and Sequential Forward Search for Speaker Feature Extraction: A Comparative Study[J]. International Journal of Engineering Intelligent Systems for Electrical Engineering & Communications,2011,19(4):207-212.

[15] 崔自峰,吉小华. 基于线性判别分析的特征选择[J]. 计算机应用,2009,29(10):2781-2785.

[16] Babatunde O, Armstrong L, Leng J, et al. A Genetic Algorithm-based Feature Selection[J]. British Journal of Mathematics & Computer Science,2014,(5):889-905.

[17] 刘 冲,颜世玉,赵海滨,等. 多类运动想象任务脑电信号的 KNN 分类研究[J]. 仪器仪表学报,2012,33(1): 1714-1720.

[18] Blankertz B, Mller K R, Curio G, et al. The BCI Competition[J]. IEEE Transactions on Neural System and Rehabilitation Engineering,2004,51(6):1044-1051.

[19] 巩笑晓. 运动想象脑电信号的特征提取算法研究[D]. 合肥:安徽大学,2014.

[20] Chang Chih-chung, Lin Chih-jen. LIBSVM: A Library for Support Vector Machines[J]. ACM Transactions on Intelligent Systems and Technology, 2007, 2(3): 389-396.

编辑 索书志