基于 FPGA 的 SATA 硬盘加解密控制器设计

刘文国，李广军，林水生

（电子科技大学通信与信息工程学院，成都 610051）

摘　要：随着信息时代的到来，数据存储和保护的需求与日俱增，如何有效实现对硬盘数据的加密保护成为一个重要的课题。文章首先分析了目前常用的硬盘数据加密方法，并在比较各种加密方案的基础上给出了基于 FPGA 的 SATA 硬盘加解密控制器设计方案。基于 SATA2.0 接口的广泛应用性，文章接着介绍了 SATA 的体系结构，并由此给出了系统的总体设计构架和详细设计方案。本控制器采用Synopsys 公司的SATA VIP辅助验证，测试平台为Xilinx ML505开发板，并采用Xilinx公司的Virtex-5 FPGA 作为最终实现，测试结果表明能够正确有效地实现硬盘数据的加解密工作。在 SATA 加解密控制器设计与实现方面的研究成果，具有通用性、可移植性，有一定的理论及经济价值。

关键词：SATA；加解密控制器；FPGA；Verilog HDL

中图分类号：TN702　　文献标识码：A　　文章编号：1681-1070（2009）06-0025-04

Design of SATA Hard Disk Encryption/decryption Controller based on FPGA

LIU Wen-guo, LI Guang-jun, LIN Shui-sheng

（*University of Electronic Science and Technology, School of Communication and Information Engineering, Chengdu* 610051,*China*）

Abstract: With the advent of the information era, the need for data storage and data protection has been becoming more and more urgent, so how to protect the hard disk data become an important task. This paper firstly analyzes several common ways of hard disk data protection, and then presents the design scheme of SATA hard disk encryption/decryption controller based on FPGA after comparison. Because of the common use of SATA2.0 interface, this paper then introduces the system structure of SATA2.0 protocol and presents the general architecture and detailed scheme. The controller adopts SATA VIP as assistant verification, Xilinx ML505 as test platform and Virtex-5 FPGA of Xilinx as the final implementation. The test shows that it can efficiently encrypt/decrypt the Hard Disk data. The design method of this paper is of theoretic and economical value and can be applied to many purposes.

Key words:SATA; encryption/decryption controller; FPGA; verilog HDL

1　引言

SATA2.0 接口是传输速率达到 3Gbps 的串行接口，由于采用了吉比特以太网结构和 8b/10b 编码技术，同时还支持NCQ（本地命令队列）、端口复用器、交错启动、热插拔等功能，在硬盘领域被广泛采用。目前，实现硬盘数据加密的方法有如下几类：

（1）基于密码的硬盘锁

密码硬盘锁是 ATA 硬盘的标准功能。用户可使

用一个特殊命令来设置一个用来访问硬盘的密码。了解 BIOS 功能的用户可以设置密码，每次系统启动时，都必须输入正确密码才能访问硬盘。该方法看似有效，但若有人能确定密码，将能访问硬盘的所有数据。

（2）软件加密方法

软件加密方法比较常见的有修改硬盘主引导程序、修改主分区表、编写硬盘驱动程序实现加密功能。操作比较简单，但对于经验丰富的程序员可进行相应的修复，实现硬盘数据的解密。

（3）硬件加密方法

硬件加密卡一般由加解密芯片和密钥存储芯片构成。加密卡使用时连接在主板和 ATA 硬盘之间，能自动对写入硬盘的所有用户数据进行加密，并在读取时解密。加密和解密的速度与接口的传输速度大致相同，不会导致硬盘性能下降。

其中，硬件加密方法明显优于其他加密方法：

●硬件加密方法不依赖于具体的操作系统，只和硬盘接口协议有关。

●硬件加密方法使用硬件电路实现加解密算法和接口协议的控制电路，不占用系统资源。

●硬件加密方法具有安全可靠的密钥存储方式。

本设计采用 FPGA 并用 Verilog HDL 语言用硬件加密的方法实现了 SATA 硬盘加解密控制器。并对代码用仿真工具 MODELSIM 进行了仿真与验证测试，能够实现主机硬盘间数据的可靠传输。

2 SATA 2.0 协议的体系结构

SATA 2.0 协议分为四层架构：物理层、链路层、传输层和应用层。应用层负责所有 ATA 命令的执行和控制命令块寄存器的访问。传输层负责把控制信息和数据放入在主机和设备之间传输的包或者帧里面，这种帧被称为帧信息结构（Frame Information Structure，FIS）。链路层负责从帧里面取出数据，使用 8b/10b 编码或者解码每个字节，并且插入控制字符使得 10b 的数据流能够被正确解码。物理层负责通过串行数据流的方式发送和接受已经被加密的信息。体系结构如图 1 所示。

3 SATA控制器总体架构

根据 SATA 2.0 协议规定，主机硬盘间所传数据按类型可以分为：从主机到设备传输的原语、配置帧、非加密帧和需要加密的帧；从设备到主机传输的原语、非解密帧和需要解密的帧。对不同类型数据需要采用不同的处理方式。系统的总体结构如图 2 所示。

其中，控制器包括虚拟设备与虚拟主机。应用在支持 SATA2.0 接口的主机和硬盘之间，根据在主机和硬盘间传输帧的类型对其进行相应的处理，实现在传输中对数据加解密的功能。靠主机方是一个虚拟设备，相当于一个设备控制器与主机完成交互，而靠设备方是一个虚拟主机，相当于一个主机控制器与设备完成交互。通过本系统协调主机和设备的传输，并且把主机和设备之间传输的数据经过加解密处理，完成硬件层上的加解密操作。

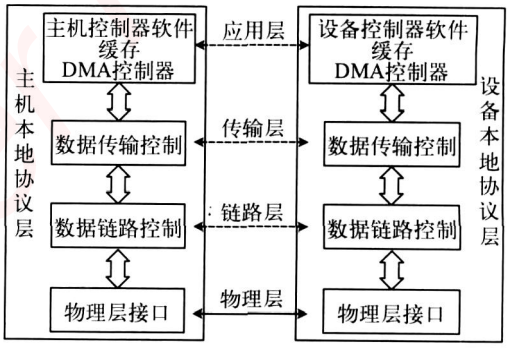


图 1 SATA 2.0 体系结构

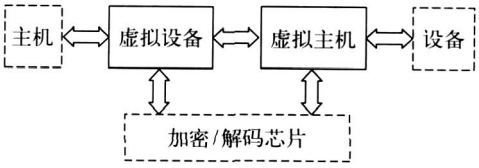


图 2 SATA 控制器总体架构

4 系统详细设计方案

SATA 数据传输分为两个方向：主机到硬盘和硬盘到主机。其中两个方向发送的数据除了个别帧只有主机发往设备外基本类型相同，因此系统在结构上呈总体对称性。控制器详细实现结构如图 3 所示。

其中，虚线框内表示的为系统辅助设计环境。包括 FPGA 里面自带的物理收发器（MGT）和一个外置的加解密芯片。物理接口使用了 XILINX Virtex-4 Rocket IO MGT，MGT 经配置后可以支持 SATA 2.0 协议，串行传输速度可以达到协议标准 3Gbps，实现协议规定的物理层功能，起到 PHY 芯片的作用，支持主板 PHY 芯片和 SATA 硬盘 PHY 芯片与本系统的

互联和通信。外置的加解密芯片可以通过接口与本控制器实现连接，将需要加密的数据送入该芯片然后送往设备端或将需要解密的数据送入芯片解密后送往主机端。该系统包含两个PHY PACKET模块，分别与主机和硬盘对接。

PHY 接口单元（PIU）负责把 MGT 接口转为本设计核心逻辑使用的接口，把核心逻辑接口和 MGT 接口隔离开来，降低设计的耦合度。设计该模块最主要的原因是为了在改变 PHY 的时候只需要在该模块里面做一些相关的改变就可以了，不需要改变核心逻辑。该系统中包含两个 PHY 接口单元，分别用于与主机和硬盘对接。

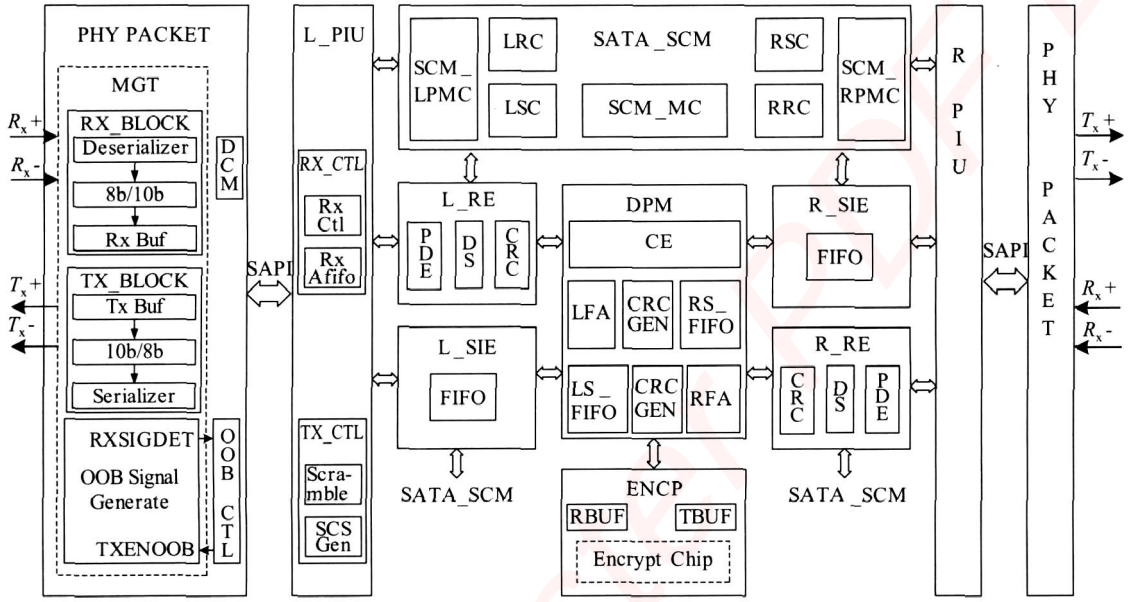


图 3 系统详细结构

接收判断模块（RE）用于分析接收到的数据类型，将原语和数据区分开来，对数据进行解扰和CRC校验。从一帧里去掉 SOF、EOF 和帧内原语，提取出数据信息交给后面的数据处理模块处理。该系统中包含两个接收判断模块，分别用于接收主机和硬盘发送的数据。

发送控制模块（SCM）是本系统的核心模块，它根据接收到的来自于接收判断模块的信息，分别进行功率管理，接收和发送帧，控制两端的发送接口引擎发送合适的原语或者数据，使主机和硬盘协调工作。所有接收和发送的控制操作都由该模块完成。该模块主要包括 7 个子模块，其中包括一个主控制器模块（SCM_MC），左边上电和功率管理控制模块（SCM_LPMC），右边上电和功率管理控制模块（SCM_RPMC），左边接收帧控制模块（SCM_LRC），右边发送帧控制模块（SCM_RSC），左边发送帧控制模块（SCM_LSC），右边接收帧控制模块（SCM_RRC）。主控制器模块负责帧外原语的发送和接收，以及为进入帧接收和发送模块做准备，左边上电和功率管理控制模块负责和主机相连的链路的上电过程和进入相应的功率管理状态，右边上电和功率管理控制模块负责和硬盘相连的链路的上电过程和进入相应的功率管理状态，左边接收帧控制模块和右边发送帧控制模块一起完成从主机到硬盘的数据传输过程，右边接收帧控制模块和左边发送帧控制模块一起完成从硬盘到主机的数据传输过程。

数据处理模块（DPM）用于分析接收到的帧的内容，提取出相应的命令放在命令寄存器中。如果接收到的是数据帧，会通过分析命令寄存器中的内容判断该数据帧是否需要加密或者是解密。对处理之后的数据生成 CRC，然后把其放在发送 FIFO 中，在发送接口状态机的控制下把数据发送到发送接口引擎。数据处理模块中数据的通路有三种不同情况，对于不需要加密或者解密的数据帧直接生成 CRC，然后发送到发送 FIFO 中等待发送出去；对于需要加密或者解密的数据帧如果加解密芯片配置成功，那么就送到加解密芯片中进行相应的加密或者解密操作；如果加解密芯片没有配置成功，那么对所有的数据取反。

发送接口引擎（SIE）主要有两个作用：一是接收数据处理模块处理之后的数据，把其缓存起来，然后通知发送控制模块数据准备好可以发送；二是在发送控制模块的控制下，发送数据到 PHY，经过

PHY 串行化之后发送到 SATA 线上。该系统中包含两个发送接口引擎，分别发送数据给主机和硬盘。

5 验证与测试

验证与测试主要分为三个阶段：第一个阶段为模块级仿真，由 RTL 设计人员验证模块功能，保证基本功能正确；第二个阶段为 EDA 系统的验证，由负责系统验证的人员进行，RTL 设计人员辅助系统验证；第三个阶段为 FPGA 测试，由软件设计人员和 RTL 设计人员共同完成，系统验证人员提供支持。模块级仿真是采用 Mentor 公司的 modelsim 对 Verilog 代码进行功能仿真。其中需要加密的帧传输时序图如图 4 所示。EDA 系统验证采用 SYNOPSYS 的 SATA Device VIP 作为硬盘模型，并且使用行为级方式实现了主机行为模型。测试环境如图 5 所示。

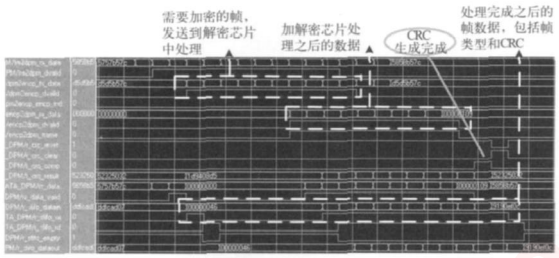


图 4 需要加密的帧传输时序图

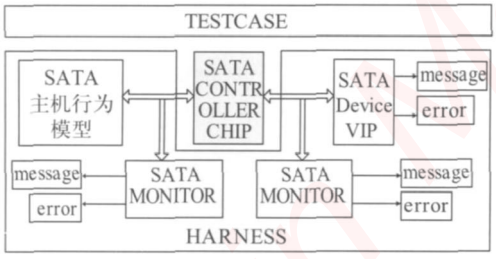


图 5 系统验证环境

其中，SATA CONTROLLER CHIP 为被测试的控制器模块。SATA 主机行为模型是使用行为级描述方式写出的用于验证的主机行为模型，用于模拟主机的操作。SATA MONITOR 模块接口信号为标准 synopsys SATA VIP MONITOR 接口信号。MONITOR 模块监视整个 SATA 总线的时序。SATA Device VIP 是能够响应 SATA 事务处理的总线功能模型。这个模型能够被用来验证 SATA 主机控制器。message 是采样 SATA MONITOR 和 SATA Device VIP 在运行期间发出的 MESSAGE 事件的小模块。error 是监测 SATA MONITOR 和 SATA Device VIP 在运行期间发出的 ERROR 事件。

FPGA 测试使用 Xilinx ML505 开发板为测试平台，主芯片为 Virtex-5 FPGA，最大可使用四对 MGT，在实际测试的时候使用了两个，一个连在电脑的 SATA 接口上，一个与硬盘相连。需要分别对其进行环路测试、单向连接测试及传输测试。其中环路测试结果如图 6 所示。

图 6 环路测试结果

6 结论

本文在分析各种硬盘加密技术的基础上，给出了基于 FPGA 的 SATA 2.0 硬盘加解密控制器硬件设计方案，并在 Xilinx ML505 开发板和 Virtex-5 FPGA 上得到了验证，能够正确地实现数据的加解密功能。该设计方法适用于对各种 SATA 2.0 接口硬盘的加解密保护。

参考文献：

[1] 叶顶胜.基于 FPGA 的 Serial ATA 1.0a 设备 IP CORE 设计[D].成都：西南石油大学，2006.

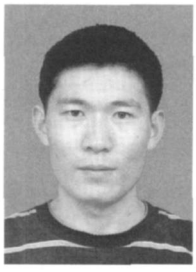
[2] APT Technologies Inc, Dell Computer Corporation, Intel Corporation, et al. Serial ATA: High Speed AT Attachment Revision 1.0a[OL]. http://www.sata-io.org,2003,7.

[3] Dell Computer Corporation, Hewlett Packard Corporation, Intel Corporation, et al. Serial ATA: High Speed AT Attachment Revision 2.5[OL]. http://www.sata-io.org, 2005,10.

[4] 李星.基于 ATA 总线的硬盘加密卡的设计与实现[D].南京：东南大学，2006.

[5] 张开来.基于 DES 算法的硬盘加密设计与实现[D].西安：西北工业大学，2003.

[6] 张彦敏.基于 IDE 硬盘的数据采集存储系统研究[D].哈尔滨：哈尔滨工程大学，2005.



作者简介：

刘文国（1982-），男，山东泰安人，在读硕士研究生，研究方向为通信与信息 ASIC 设计方向。

嵌入式资源免费下载

总线协议：

1. 基于 PCIe 驱动程序的数据传输卡 DMA 传输
2. 基于 PCIe 总线协议的设备驱动开发
3. CANopen 协议介绍
4. 基于 PXI 总线 RS422 数据通信卡 WDM 驱动程序设计
5. FPGA 实现 PCIe 总线 DMA 设计
6. PCI Express 协议实现与验证
7. VPX 总线技术及其实现
8. 基于 Xilinx FPGA 的 PCIE 接口实现
9. 基于 PCI 总线的 GPS 授时卡设计
10. 基于 CPCI 标准的 6U 信号处理平台的设计
11. USB30 电路保护
12. USB30 协议分析与框架设计
13. USB 30 中的 CRC 校验原理及实现
14. 基于 CPLD 的 UART 设计
15. IPMI 在 VPX 系统中的应用与设计
16. 基于 CPCI 总线的 PMC 载板设计
17. 基于 VPX 总线的工件台运动控制系统研究与开发
18. PCI Express 流控机制的研究与实现
19. UART16C554 的设计
20. 基于 VPX 的高性能计算机设计
21. 基于 CAN 总线技术的嵌入式网关设计
22. Visual C 串行通讯控件使用方法与技巧的研究
23. IEEE1588 精密时钟同步关键技术研究
24. GPS 信号发生器射频模块的一种实现方案
25. 基于 CPCI 接口的视频采集卡的设计
26. 基于 VPX 的 3U 信号处理平台的设计
27. 基于 PCI Express 总线 1394b 网络传输系统 WDM 驱动设计
28. AT89C52 单片机与 ARINC429 航空总线接口设计
29. 基于 CPCI 总线多 DSP 系统的高速主机接口设计
30. 总线协议中的 CRC 及其在 SATA 通信技术中的应用

VxWorks：

1. 基于 VxWorks 的多任务程序设计
2. 基于 VxWorks 的数据采集存储装置设计
3. Flash 文件系统分析及其在 VxWorks 中的实现
4. VxWorks 多任务编程中的异常研究
5. VxWorks 应用技巧两例
6. 一种基于 VxWorks 的飞行仿真实时管理系统
7. 在 VxWorks 系统中使用 TrueType 字库
8. 基于 FreeType 的 VxWorks 中文显示方案
9. 基于 Tilcon 的 VxWorks 简单动画开发
10. 基于 Tilcon 的某武器显控系统界面设计
11. 基于 Tilcon 的综合导航信息处理装置界面设计
12. VxWorks 的内存配置和管理
13. 基于 VxWorks 系统的 PCI 配置与应用
14. 基于 MPC8270 的 VxWorks BSP 的移植
15. Bootrom 功能改进经验谈
16. 基于 VxWorks 嵌入式系统的中文平台研究与实现
17. VxBus 的 A429 接口驱动
18. 基于 VxBus 和 MPC8569E 千兆网驱动开发和实现
19. 一种基于 vxBus 的 PPC 与 FPGA 高速互联的驱动设计方法
20. 基于 VxBus 的设备驱动开发
21. 基于 VxBus 的驱动程序架构分析
22. 基于 VxBus 的高速数据采集卡驱动程序开发

Linux：

1. Linux 程序设计第三版及源代码
2. NAND FLASH 文件系统的设计与实现
3. 多通道串行通信设备的 Linux 驱动程序实现
4. Zsh 开发指南-数组
5. 常用 GDB 命令中文速览
6. 嵌入式 C 进阶之道
7. Linux 串口编程实例
8. 基于 Yocto Project 的嵌入式应用设计
9. Android 应用的反编译
10. 基于 Android 行为的加密应用系统研究
11. 嵌入式 Linux 系统移植步步通
12. 嵌入式 CC++语言精华文章集锦
13. 基于 Linux 的高性能服务器端的设计与研究

14. S3C6410 移植 Android 内核
15. Android 开发指南中文版
16. 图解 Linux 操作系统架构设计与实现原理（第二版）
17. 如何在 Ubuntu 和 Linux Mint 下轻松升级 Linux 内核
18. Android 简单 mp3 播放器源码
19. 嵌入式 Linux 系统实时性的研究
20. Android 嵌入式系统架构及内核浅析
21. 基于嵌入式 Linux 操作系统内核实时性的改进方法研究
22. Linux TCP IP 协议详解
23. Linux 桌面环境下内存去重技术的研究与实现

Windows CE：

1. Windows CE.NET 下 YAFFS 文件系统 NAND Flash 驱动程序设计
2. Windows CE 的 CAN 总线驱动程序设计
3. 基于 Windows CE.NET 的 ADC 驱动程序实现与应用的研究
4. 基于 Windows CE.NET 平台的串行通信实现
5. 基于 Windows CE.NET 下的 GPRS 模块的研究与开发
6. win2k 下 NTFS 分区用 ntldr 加载进 dos 源代码
7. Windows 下的 USB 设备驱动程序开发
8. WinCE 的大容量程控数据传输解决方案设计
9. WinCE6.0 安装开发详解
10. DOS 下仿 Windows 的自带计算器程序 C 源码
11. G726 局域网语音通话程序和源代码
12. WinCE 主板加载第三方驱动程序的方法
13. WinCE 下的注册表编辑程序和源代码
14. WinCE 串口通信源代码
15. WINCE 的 SD 卡程序[可实现读写的源码]
16. 基于 WinCE 的 BootLoader 研究

PowerPC：

1. Freescale MPC8536 开发板原理图
2. 基于 MPC8548E 的固件设计
3. 基于 MPC8548E 的嵌入式数据处理系统设计
4. 基于 PowerPC 嵌入式网络通信平台的实现

5. PowerPC 在车辆显控系统中的应用
6. 基于 PowerPC 的单板计算机的设计
7. 用 PowerPC860 实现 FPGA 配置
8. 基于 MPC8247 嵌入式电力交换系统的设计与实现
9. 基于设备树的 MPC8247 嵌入式 Linux 系统开发
10. 基于 MPC8313E 嵌入式系统 UBoot 的移植
11. 基于 PowerPC 处理器 SMP 系统的 UBoot 移植

ARM：

1. 基于 DiskOnChip 2000 的驱动程序设计及应用
2. 基于 ARM 体系的 PC-104 总线设计
3. 基于 ARM 的嵌入式系统中断处理机制研究
4. 设计 ARM 的中断处理
5. 基于 ARM 的数据采集系统并行总线的驱动设计
6. S3C2410 下的 TFT LCD 驱动源码
7. STM32 SD 卡移植 FATFS 文件系统源码
8. STM32 ADC 多通道源码
9. ARM Linux 在 EP7312 上的移植
10. ARM 经典 300 问
11. 基于 S5PV210 的频谱监测设备嵌入式系统设计与实现
12. Uboot 中 start.S 源码的指令级的详尽解析
13. 基于 ARM9 的嵌入式 Zigbee 网关设计与实现
14. 基于 S3C6410 处理器的嵌入式 Linux 系统移植
15. CortexA8 平台的μC-OSⅡ及 LwIP 协议栈的移植与实现

Hardware：

1. DSP 电源的典型设计
2. 高频脉冲电源设计
3. 电源的综合保护设计
4. 任意波形电源的设计
5. 高速 PCB 信号完整性分析及应用
6. DM642 高速图像采集系统的电磁干扰设计
7. 使用 COMExpress Nano 工控板实现 IP 调度设备
8. 基于 COM Express 架构的数据记录仪的设计与实现

9. 基于 COM Express 的信号系统逻辑运算单元设计
10. 基于 COM Express 的回波预处理模块设计
11. 基于 X86 平台的简单多任务内核的分析与实现
12. 基于 UEFI Shell 的 PreOS Application 的开发与研究
13. 基于 UEFI 固件的恶意代码防范技术研究