

自动配速的 SATA 硬盘加密桥的设计与实现

万晨庚, 李树国

(清华大学微电子所, 北京 100084)

摘 要: 硬盘加密是大容量安全存储的核心问题. 基于 SATA 接口, 提出一种桥接方式实现的硬盘加密桥设计. 该设计实现了加密算法可配置, 可实现对称加密的 SM4 和 AES 等算法, 并能够自动检测并匹配 SATA1.0 与 SATA2.0 两种速度. 重点介绍了 SM4 算法的实现. FPGA 验证表明, 计算机可以通过硬盘加密桥识别及读写硬盘. 用 WIN7 系统的 CrystalDiskMark 硬盘测速软件对硬盘读写进行测速, 结果表明加入硬盘桥后读速率在 242 MB/s 以上, 写速率约为 160 MB/s.

关键词: SATA 硬盘加密桥; 自动配速; SM4; AES; FPGA

中图分类号: TN79.1

文献标识码: A

文章编号: 1000-7180(2014)09-0024-04

Disk-Encrypt Design Based on SATA Interface With Automatic Speed-Configuration

WAN Chen-geng, LI Shu-guo

(Institute of Microelectronics, Tsinghua University, Beijing 100084, China)

Abstract: Disk encryption is the core problem of large capacity safety storage. Based on SATA Interface, the paper proposes a design by building a SATA interface bridge. The design has configurable encryption-core which supports SM4 and AES. The paper mainly introduces the implement of SM4. The bridge supports SATA1.0 and SATA2.0 with automatic speed-configuration. FPGA testifies that, disk can be correctly recognized with the bridge. Speed test done by using the software CrystalDiskMark shows that read speed is above 242 MB/s with the bridge in the WIN7 system.

Key words: SATA Disk-Encrypt Bridge; Automatic Speed-Configuration; SM4; AES; FPGA

1 引言

随着硬盘容量的不断扩大、传输速度的不断提高, 硬盘安全存储越来越重要. 传统软件加密的速率低、CPU 资源占有率高、安全性差的问题逐渐凸显. SATA (Serial Advanced Technology Attachment, 串行高级技术附件) 接口是硬盘存储的通用接口, 并正在向传输速度快、便携性好、兼容性强的方向发展^[1]. 使用 SATA 硬件接口为数据加密, 以其速率高、密钥管理灵活的优点成为解决硬盘安全存储问题的首选方案.

硬件加密方案有两种, 一种是硬盘厂商生产的

自加密硬盘, 另一种是第三方厂商生产的加密桥. 考虑到 SATA 串行通用接口的高速率, 所以采用对称加密算法对数据进行加解密. 而对称加密算法通常为并行输入, 因此在保证加密速度, 同时不变更现有设备的情况下, 加密桥的方案拥有通用性高, 安全性高, 灵活性强的优势. 本文提出了一种桥接方式实现的、通过 SATA 接口提取并行数据, 并可利用多种对称加密算法进行加解密操作的方案.

2 SATA 接口结构

SATA 接口包含主机端和设备端两部分, 根据不同的作用又分为物理层、链路层、传输层和应用层

收稿日期: 2013-11-20; 修回日期: 2014-01-13

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

四个层级^[2]. 物理层负责接收和发送编码后的串行数据流. 链路层负责从组建好的帧中提取数据,进行 8B/10B 编解码,并嵌入控制位保证 10 bit 数据流正确解码. 传输层负责存放控制信息和数据,并以帧(Frame Information Structure, FIS)的形式在主机与设备间传输. 应用层负责所有的 ATA 命令执行^[3].

3 SATA 接口加密桥系统设计

为了从主机与硬盘的通信中提取数据实现加解密, SATA 接口加密桥系统首先需要同主机和硬盘两端均建立稳定连接,并将串行数据转化为并行;其次从并行数据中解析出协议所规定的原语,根据协议对其做出响应,维持原语交互稳定性;最后从交互的原语中提取数据,并将其送入加解密引擎.

根据以上设计思想, SATA 接口加密桥系统由物理层、自动配速模块、链路层、加解密控制模块、密钥管理模块组成,系统结构如图 1 所示. 虚拟设备物理层使用 OOB(Out Of Band)信号与主机建立连接,并将高速串行数据转化为并行与虚拟设备链路层进行传输,虚拟设备链路层对并行数据解析成原语,并按照协议完成原语响应. 虚拟主机物理层、链路层结构功能与虚拟设备相同,但在数据传输时保证设备优先.

物理层建立通信的过程中,由于主机和硬盘所支持的最高速率可能不同,而且有 4 种不同的情况. 为解决速度匹配问题,系统中加入了自动配速模块. 该模块通过 OOB 信号检测,识别主机和硬盘两端所共同支持的最大传输速率,并自动配置加密桥两端物理层以此速率建立连接.

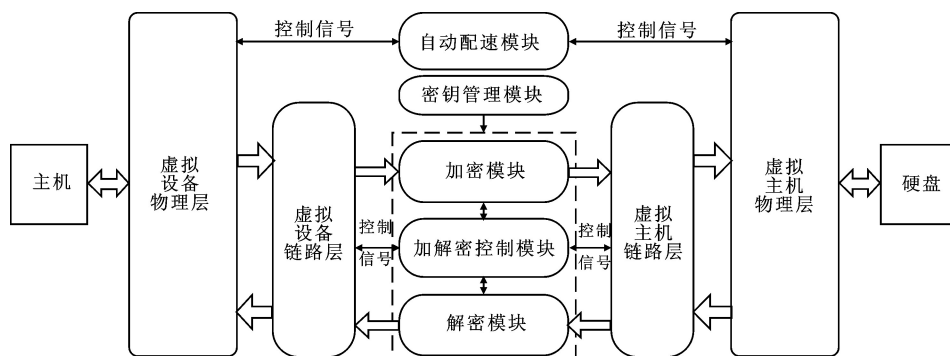


图1 SATA 接口加密桥系统

物理层建立连接以后,将串行数据转化为并行,与链路层进行交互. 链路层功能分为接收和发送两个部分. 接收部分将物理层传来的并行数据进行原语解码,虚拟设备将主机发送的寄存器帧进行命令解析,识别不同类型数据帧,并对读写数据进行解扰,送入加解密模块. 发送部分检测到加解密模块处理完毕的数据时,链路层状态机控制原语产生,对数据进行 CRC 校验和加扰,添加帧头和帧尾,发送给物理层.

与两端链路层连接的是加解密模块. 当加解密模块对数据进行处理时,不同的对称加密算法会对数据通路造成不同程度的延时. 国密算法 SM4 分组长度为 128 bit,密钥长度也为 128 bit,加密算法与密钥扩展算法都采用 32 轮非线性迭代结构. AES 支持 128 bit、192 bit、256 bit 三种密钥长度的对称加密算法. 对于不同的密钥长度, AES 加密的轮次也不同,分别为 10、12 和 14 轮. SM4 算法流程如图 2 所示.

设计中考虑了对以上两种主流对称加密算法的

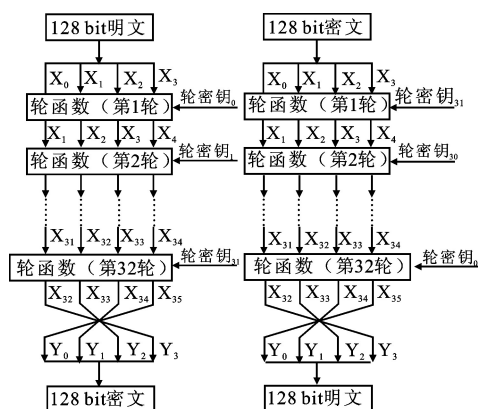


图2 SM4 算法加解密流程

兼容性,密钥管理模块向加解密模块提供 128 bit、192 bit、256 bit 三种密钥长度. 链路层向加解密模块输入 128 位数据. 加解密控制模块在链路层与加解密模块之间起到协调作用:一方面通过外部配置选择加密模式,见表 1,从链路层获取数据信号来控制加解密的开始、暂停与结束;另一方面通过检测加解密模块的工作状态控制链路层的原语交互,保证

加解密过程中传输保持稳定. 这些原语交互包括数据加解密进行中 HOLD、HOLDA 及 DMAT 的处理, 和数据加解密完毕后负责打包数据的 SOF 和 EOF 的解析与发送.

表 1 加密模式配置情况

配置接口(2 bit)	00	01	10	11
加密模式	不加密	SM4	AES	保留

为满足 SATA 二代 3.0 Gb/s 的通信速率, 加解密模块吞吐量需要大于 3.0 Gb/s, 否则会成为数据通信速率的瓶颈, 降低加密桥的传输速率. 为提高时钟频率, 增加单模块吞吐量, 设计了独立的加密模块与解密模块, 均由加解密控制模块控制.

4 SATA 接口加密桥系统的 FPGA 实现

SATA 加密桥的实现, 使用 XILINX 公司的 XUPV5 开发板, FPGA 型号为 Virtex5-lx110t. 板内提供两个通用 SATA 接口, 内置高速串行收发器 RocketIO GTP. GTP 收发器支持多种串行通信协议, 内置 8B/10B 编码器、串行 COMMA 码对齐、时钟校正等模块, 支持 100 Mb/s~3.75 Gb/s 的传输速率^[2], 满足 SATA1.0(1.5Gbps)和 SATA2.0(3 Gb/s)^[4].

加密桥分为三部分进行实现: SATA 接口部分、加解密核部分、密钥管理部分.

SATA 接口部分中, 加密桥物理层使用 GTP 收发器, 产生和检测 OOB 信号来与主机和硬盘建立连接, 将串行数据转换成并行, 并完成 10B/8B 解码后与链路层相接. 自动配速模块通过检测 OOB 信号控制 GTP 模块收发速度, 根据物理层协议完成速度的自动匹配. 链路层分为接收器、发送器和顶层控制模块三部分来实现. 接收器负责将物理层解码后的并行数据转换成 32 位, 并按照协议规定的 18 种原语及其特性进行原语的解扰^[5]. 发送器负责发送相应的原语和数据, 对接收到的原语进行响应, 或发送加解密后的数据. 顶层控制模块负责对接收到的 FIS 进行解析, 判断 FIS 的类型, 储存寄存器帧所对应的命令, 并发送给加解密控制模块.

链路层与加解密模块的连接采用 FIFO 缓存的方式. 链路层将读写命令所对应的数据帧提取出来, 写入 FIFO, 当加解密模块准备就绪时从 FIFO 中读取所需数据. 同样的, 加解密模块处理完的数据之后先写入 FIFO, 在链路层顶层模块所指示状态就绪时, 读取 FIFO 中数据, 添加帧头、CRC 校验值和帧尾, 发送给物理层.

加解密核部分由可配置的对称加密算法构成. 为保证吞吐率, AES 和 SM4 均采用 ECB 模式. 考虑到输入到输出延时的限制, 加密模块每个时钟周期仅实现一轮迭代, 这样对于不同长度的密钥, 加密模块会表现出不同的性能. AES 算法中, 128 bit 密钥最快, 256 bit 密钥最慢^[6]. 经过 FPGA 布局布线, AES 一轮迭代的延时最小为 8.2 ns, 其中线延时约为 88%, 这是因为运算数据位宽过大导致布局布线困难. 根据 FPGA 优化后的最小延时, 使用 FPGA 内部锁相环提供 120 MHz 时钟, 计算 AES 模块在 128 bit、192 bit、256 bit 密钥模式下能够达到的吞吐率分别为 174.6 MB/s、147.8 MB/s 和 128.1 MB/s, 在 SATA-2 代接口中会成为瓶颈. 所以本设计最终采用双引擎 AES 设计, 使实际吞吐率能够达到 SATA-2 代接口要求.

SM4 算法由输入明文到输出密文需要 32 轮迭代, 每轮迭代包括轮密钥的生成和轮函数的计算. 经过算法优化, 提前生成轮密钥, 降低每轮迭代延时, 并使用查表法实现轮函数. 在 FPGA 中完成布局布线, 其最小延时为 7.9 ns, 满足加解密模块提供的 120 MHz 要求. 但由于迭代次数较多, 吞吐率仅为 480 Mb/s. 如果采用多引擎, 一方面会增加多核调度控制的复杂度, 并有可能导致延时增加, 另一方面会增加面积, 造成很大程度上的资源浪费. 所以本设计采用八级流水方式实现 SM4 设计, 如图 3 所示, 每四轮迭代的数据存储在同一个寄存器中, 共添加八个段间寄存器.

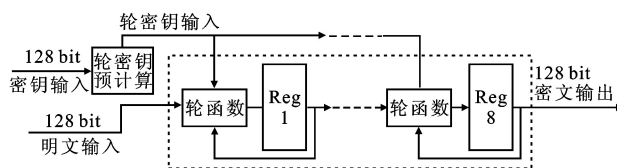


图 3 SM4 流水线结构图

用此方案在 FPGA 上实现, 占用 slice 资源是原来的 2.3 倍, 其中寄存器资源是原来的 1.7 倍, LUT 资源是原来的 3.8 倍, 如表 2 所示. 而理论吞吐率是原来的 8 倍, 能够达到 3.84 Gb/s, 满足传输要求.

表 2 SM4 非流水线与八级流水资源占用对比

	Slice Registers	Slice LUTs	Occupied Slice
非流水	1 422	1 290	691
八级流水	2 369	4 924	1 601

密钥管理部分独立于数据传输通路, 主要完成密钥输入的功能. 这要求密钥管理模块既能够更新

用户密钥,又能够将用户密钥在数据传输之前输入加解密模块。本设计选用开发板内置的 EEPROM (STMicroelectronics M24C08),通过 IIC 总线与加解密模块相连。用户首先将标识有个人信息的密钥通过 IIC 总线写入 EEPROM 中,在加密桥启动时按照不同加密引擎和不同模式对密钥的需求,将相应长度的密钥输入。用户可以通过开发板查看或更改 EEPROM 中的密钥。

5 验证与测试

为保证高速数据传输的精确性,使用 ModelSim SE 6.6f 对 CRC 校验模块、加解扰模块、AES 和 SM4 模块的正确性进行验证,模拟可能遇到的不同情况对原语响应逻辑、数据提取逻辑、密钥管理模块和自动配速模块。

在完成对整个系统不同模块的仿真验证后,搭建实体测试平台,进行 FPGA 综合、验证与测试。使用 ISE Project Navigator 对设计进行综合,FPGA 资源占用情况见表 3。

表 3 本设计 FPGA 资源占用情况

	使用数	使用率
Slice Registers	10 642 个	15%
Slice LUTs	22 731 个	32%
Occupied Slices	8 365 个	48%
Bonded IOBs	32 个	5%
Block RAM/FIFO	72 kB	1%

主机端使用 DELL Inc. 集成主板,设备端使用 SUMSUNG-SSD(64G),主机和设备均通过通用 SATA 接口与 FPGA 开发板相连。通过加密模式配置,分别在不加密、AES 加密(密钥长度 128 bit)、SM4 加密、保留(将数据取反)的情况下对硬盘识别和读写进行测试。在 WIN7 环境下,均能够通过加密桥对 SSD 硬盘进行正确的设备识别、格式化和读写操作。使用 CrystalDiskMark 硬盘测速软件,在上述不同情况下进行测速。测试结果表明,读速率在 242 MB/s 以上,受限于 SSD 硬盘最大写入速率,写速率在 160 MB/s 左右。表 3 中列出了本设计与 X Wall Mx 对比数据。

表 4 本设计读写速率与 Xwall MX 对比

算法 测试项	不加密 读/写	SM4 读/写	AES 读/写	取反 读/写
本设计/(Mb/s)	251/160	242/159	247/158	248/160
Xwall MX/(Mb/s)	150/150	150/150	150/150	150/150

6 结束语

本文介绍了通过桥接方式,实现提取输入输出硬盘数据并加解密的设计。该设计拥有可配置的加解密核,不仅支持国密算法 SM4,而且支持国际标准 AES。其中 SM4 使用流水线形式实现以满足吞吐率要求。SM4 与 AES 均支持 ECB 模式。加密桥同时兼容 SATA-1 代和 SATA-2 代速率并实现自动匹配,使用相同的设计思想,在更高级的 FPGA (如 Virtex-7)中可以实现 SATA-2 与 SATA-3 的同时兼容和自动匹配。加密桥提供数据位宽为 128 位、密钥长度可配置的加解密接口,可嵌入和配置 SM4 和 AES 等不同对称加密引擎,并实现了可靠的密钥管理。加入硬盘桥后在不同加密模式下测速,读速率均在 242 MB/s 以上,写速率约为 160 MB/s。

参考文献:

- [1] SATA-IO. SATA express specification from SATA-IO in ratification [EB/OL]. [2013-01-03]. <http://www.sata-io.org/index.asp>.
- [2] Xilinx. Virtex5 FPGA GTP transceiver user guide[s]. San Jose,CA USA:Inc. XILINX,2009.
- [3] Working Draft Project. American national standard. ATA/ATAPI command Set - 2 [s]. New York,USA, 2009.
- [3] SATA-IO. Serial ATA revision 3.0 specification[s]. Beaverton,Oregon USA:SATA-IO Administration,2009.
- [4] Don Anderson, MindShare. SATA storage technology [M]. London UK:MindShare Press, 2007.
- [5] 谭帆,李树国. 可配置加密算法的 SATA 接桥器的设计与实现[J]. 微电子学与计算机, 2013, 30(12): 22-26.

作者简介:



万晨庚 男,(1989-),硕士研究生。研究方向为 SATA 接口与硬盘加密设计。

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。