

可配置加密算法的 SATA 桥接器的设计与实现

谭 帆, 李树国

(清华大学 微电子所, 北京 100084)

摘 要: 针对大容量数据在存储过程中出现的安全问题, 提出了一种可配置加密算法的 SATA 加密桥接器, 在不更换现有设备的情况下, 对硬盘中的数据进行加密. 首先分析了当前硬盘加密技术的现状, 然后结合当前主流的 SATA 接口给出了系统的总体架构和详细的设计方案. 本设计在 Xilinx XUPV5 平台上进行了实现, 以 AES 加密算法为例, 在 ECB 模式下使用 256 bit 密钥能够达到理论值 284 MB/s 的加解密吞吐量. 测试结果表明, 该加密桥接器不仅能够实现对硬盘数据加解密的功能, 而且具有较好的兼容性.

关键词: SATA; AES; FPGA; 加密; 可配置

中图分类号: TP33

文献标识码: A

文章编号: 1000-7180(2013)12-0022-05

Design and Implementation of a SATA Bridge with Configurable Encryption Algorithm

TAN Fan, LI Shu-guo

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

Abstract: In order to deal with security issues aroused during storage of large amount of data, we present an algorithm-configurable SATA encryption bridge, which can encrypt the data in the hard drive without replacing existing equipment. This paper first analyzes the status of current hard drive encryption technology, then combine with the current mainstream SATA interface to give an overall architecture of the encryption system and details of this design. We implement the design on Xilinx XUPV5 platform with AES encryption algorithm and get a theoretical throughput of 284 MB/s in ECB mode using 256 bit key. Test results show that the encryption bridge is not only able to encrypt and decrypt data in the hard drive, but also has a good compatibility with other hardware.

Key words: SATA; AES; FPGA; encryption; configurable

1 引言

计算机技术的发展使得人们对数据存储的需求发生了爆炸式的增长. 由于网络环境复杂多变, 所以无论是企业还是个人的数据存储安全都受到了严重的威胁. 按照以往的解决方案, 通常先使用软件对数据加密后存储的方式来对数据进行保护, 然而这一方案存在着加密速度极低、系统资源占用率高等显著缺点. 因此比较好的方案是使用硬件对数据进行加密, 在保证数据安全的前提下, 提高加密速度, 降低系统复杂度. 许多国外厂商在硬件存储加密领域

推出了高性能的 SATA 加密产品, 如 Enova 公司的 X-wall MX^[1] 系列芯片, 加解密的吞吐率达到了 150MB/s, 应用于政府、军队等部门. 考虑到 SATA 接口在存储设备中的主流程度, 以安全性较高、较易实现的 AES 算法为例, 实现了一种 SATA 加密桥接器. 该桥接器不仅具有较高的加解密吞吐率和较好的兼容性, 还提供了一个标准接口来植入其他的加解密算法, 实现某些特定的应用.

2 SATA 体系结构

SATA 的全称是 Serial Advanced Technology

收稿日期: 2013-01-27; **修回日期:** 2013-03-28

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

Attachment(串行高级技术附件),是一种高速串行传输协议^[2],数据传输速率最高能够达到 6.0 Gb/s,取代了 PATA(并行 ATA)作为硬盘与 PC 机通信的标准. SATA 接口具有传输带宽大,物理结构简单,支持热插拔,检错能力强等特点,能够满足绝大多数大容量存储设备对接口功能的需求,因此当前主流的大容量存储设备都使用 SATA 接口. SATA 体系结构如图 1 所示,自底向上分别是物理层、链路层、传输层以及应用命令层. 物理层负责数据的串行化和解串、时钟恢复、OOB(带外信号)通信以及 K 码检测等工作. 链路层负责 8b/10b 编解码、加解扰、CRC 校验、FIS 的接收与发送等工作. 传输层负责组帧与解帧、FIFO 控制等工作,应用命令层负责命令的执行与寄存器信息的维护等工作.

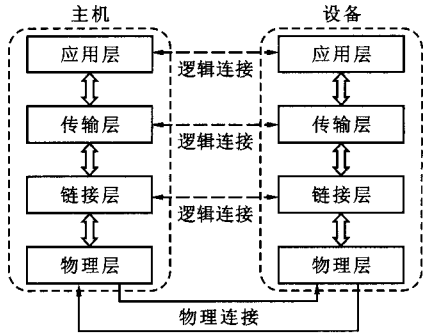


图 1 SATA 体系结构

3 AES 加密算法

AES 是美国国家标准与技术研究所(NIST)选择出的一种对称加密算法^[3]. 该算法仅使用逻辑运算操作,结构简单,数据块之间的并行性强,易于硬件实现. 由于 AES 是对称加密算法,因此明文和密文的长度是相等的,非常适合用于对存储设备中数据的加密. AES 加密算法将输入的明文数据进行密钥加运算后,根据密钥长度的不同进行 10~14 次轮操作,轮操作包括了行移位、S 盒变换、列混合以及密钥加. AES 规定了三种密钥长度,分别是 128 bit, 192 bit 和 256 bit,密钥越长,所需要的轮操作次数就越多,加密的强度也越大,安全性也越强. AES 算法加密和解密的过程如图 2 所示.

4 SATA 加密桥总体架构

加密桥需要对写入设备的数据进行加密,对从设备中读出的数据进行解密,因此需要对串行的数据流进行逐步的解析,得到写入或者读出的数据. 要得到这些数据,就必须按照 SATA 协议实现物理

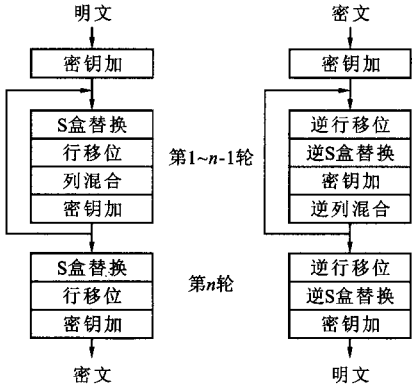


图 2 AES 算法加密和解密过程

层、链路层. 得到数据以后,将数据交给加解密模块进行处理,处理后的数据仍然按照 SATA 协议规定的方式发送出去,这样就得到了 SATA 加密桥的总体架构,如图 3 所示. 作为一种桥接设备,需要同时与主机和设备进行通信,而通信的过程都要符合 SATA 协议中的相关要求,因此与主机方通信的部分可以认为是一个虚拟 SATA 设备,与设备通信的部分可以认为是一个虚拟 SATA 主机,中间的部分协调和控制虚拟设备与虚拟主机的行为,完成协议上的交互与数据的传输.



图 3 SATA 加密桥总体架构

5 SATA 加密桥详细设计方案

SATA 加密桥的详细架构如图 4 所示,由于加密桥两端的接口都是 SATA 接口,因此架构上两端也呈现出对称的特性. 中间虚线内部是加密算法模块,通过简单的接口与控制部分连接,这个模块是可以替换的,用户可以根据应用的需要更换加解密的算法,加入特定的功能等.

SATA 接口部分主要由物理层和链路层组成,物理层调用了 Xilinx Virtex5 FPGA 中的 GTP_DUAL^[4]单元,对其进行适当的配置后构成符合 SATA 物理层协议以及电气标准的串行收发器,通过适当的动态配置,其速率可以支持 SATA 的二代速率 3 Gb/s,同时兼容 SATA 的一代速率 1.5 Gb/s. GTP 的接收通道主要实现了解串,OOB 信号检测,接收缓冲以及 8b/10b 解码的功能,发送通道主要实现了 8b/10b 编码,发送缓冲和串行化发送的功能. 此外,物理层还包括一些其他模块:时钟产生模块调用

机和设备交互的一系列数据,可能是存储体上的数据,也可能是协议中的一些配置数据,我们只对存储体上的数据进行加密和解密,因此还需要对数据帧加以区分.数据帧中的载荷内容是跟当前设备执行的命令相关的,因此筛选出了 ATA 命令集中跟存储体数据读写相关的命令,当设备在执行这些命令的时候,我们按照需求对它们交互的数据进行加解密处理.这些命令包括但不限于 READ DMA、READ SECTOR、READ MULTIPLE、READ FPDMA QUEUED、READ BUFFER、WRITE DMA、WRITE SECTOR、WRITE MULTIPLE、WRITE FPDMA QUEUED、WRITE BUFFER 等.其中和 READ 相关的命令均做解密处理,和 WRITE 相关的命令均做加密处理.

此外,Main Control 模块还要处理 FIS 的发送冲突,FIS 发送与接收的错误以及协调两边的链路层进行 FIS 收发.SATA 协议中规定,设备具有较

高的数据传输优先级.当主机和设备直接相连的时候,优先级问题很容易解决,但是在主机和设备之间加入了桥接器以后,优先级的关系被打断了,这时候我们使用的策略是,当主机正在传输数据且设备提出发送数据请求时,我们让加密桥丢弃主机发来的数据,然后向主机返回接收错误,利用 SATA 协议中的重传机制让主机重新发送,此时将设备需要发送数据的请求提交给主机端,这时候主机会优先处理设备的发送请求,自己的重发过程将在接收完设备的数据后再进行.这一过程只会发生在执行 NCQ (本地命令重排)命令时发生,被丢弃的数据因为会再次发送所以对命令的执行没有影响,故而功能是正确的.在错误处理方面,我们采用的原则是让一端发生的错误复现在另一端,这样就由真正地主机或者设备来处理错误,从而保证了对协议的忠实.Main Control 模块的状态转移图如图 7 所示.

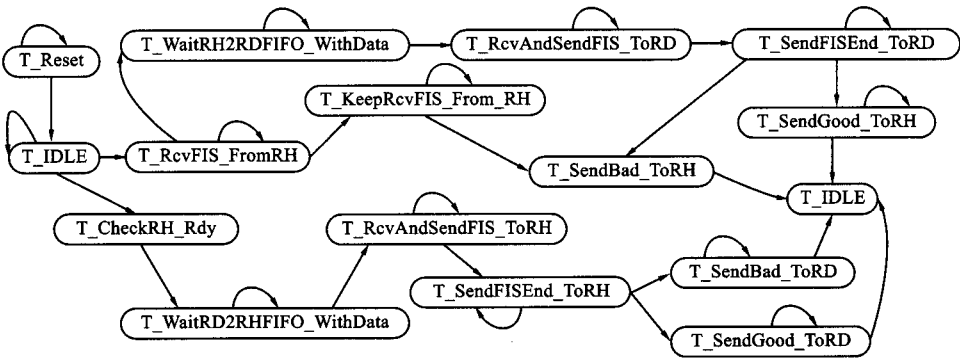


图 7 Main Control 状态转移图

CHIP CORE 中的 interface 模块协助 Main Control 模块向加解密模块提供必要的信息,同时把繁杂的 FIFO 空满标志、FIS 启始停止、数据等信号转化成较为简单的读写接口,屏蔽了多余的信号对加解密模块设计所带来的不便,这时外部读写数据就好像是在操作一个 FIFO.当数据方向是从主机到设备时,interface 模块开启加密通道,然后从相应的 FIFO 中读数据,把加密完的数据写入到相应的 FIFO 中去;当数据方向是从设备到主机时,interface 开启解密通道,然后从相应的 FIFO 中读数据,把解密完的数据写入到相应的 FIFO 中去.作为实例,我们采用了 AES 算法来实现了加解密模块,不仅保证了数据加密有足够的安全性,还满足了系统对数据处理吞吐率的要求.设计的 AES 可以使用 128 比特,192 比特或者 256 比特的密钥,来满足不同强度的加密需求.在 FPGA 上进行了实现,使用

的器件是 XC5VLX110T,整个设计占用 FPGA 资源的情况如表 1 所示.

表 1 FPGA 资源占用情况			
资源名称	使用情况	资源总数	百分比/%
Registers	3 162	69 120	4
Slice LUTs	11 637	69 120	16
Occupied Slices	3 943	17 280	22
Memory	216 kB	5 328 kB	4
IO	9	640	1
BUFG/BUFCTRLs	9	32	31
PLLs	1	6	16

6 验证与测试

在实际的验证过程中,大部分模块是可以设在

计完成之后立即被验证的,对于一些运算功能模块,例如 CRC 校验模块,加解扰模块,AES 模块等,它们所实现的功能都有标准的 C 模型,只要保证在输入相同的情况下,这些模块的输出和对应的 C 模型输出相同就可以了.对于控制模块,使用受约束的随机向量作为输入,使得状态机中的各种分支都被遍历到,然后观察状态机的输出控制信号是否和预期的一样,以此来保证控制模块的正确性.完成单独模块的初步验证后,把整个系统搭建好,成为一个 DUT(Design Under Test),然后搭建一个大的验证环境.使用了主机模型、硬盘模型作为验证环境的主要部分,把 SATA 加密桥放置在主机模型和设备模型中间,然后编写大量的测试用例,让主机模型发出各种操作命令来验证 DUT 的功能.使用 Mentor 公司的 Modelsim 对整个环境进行了仿真,其中对于物理层建立连接、速度协商、FIS 的收发等过程进行了重点的验证,模拟了协议中提到的各种可能发生的情况.

在完成了整个设计的功能验证后,我们进行了 FPGA 测试.使用的是 Xilinx XUPV5 开发平台.开发板上的两个 SATA 接口,一个接电脑主机,一个接机械硬盘或者 SSD(固态硬盘).测试平台的实物如图 8 所示.



图 8 测试平台

将进行过功能验证的设计下载到 FPGA 后,使用了 Windows XP, Windows 7 以及 Ubuntu Linux 操作系统, Intel、AMD 和 NVidia 的芯片组, Seagate、Western Digital 的机械硬盘和以及 Samsung 的固态硬盘对加密桥进行了兼容性测试.在各种操作系统、芯片组以及硬盘的组合下,均能在计算机上得到硬盘的信息,并对硬盘进行正常的读写操作.使用两款硬盘测试软件对 SSD 以及机械硬盘读写速率进行测试后得到的结果如图 9 所示.需要说明的是,使用的 SSD 的最大写速率为 160 MB/s,因此在写操作时,SSD 本身成为了瓶颈,而不是加密桥.



图 9 机械硬盘及 SSD 加解密测试结果(左为 SSD)

由于 AES 三种密钥长度下,需要的运算量是不同的,因此在三种模式下实际的吞吐率也是不同的.在连接 SSD 的情况下,对 SATA 加密桥中不同密钥长度下 AES 的最高性能进行了测试,同时与 Enova 公司的 X-Wall MX 系列芯片的性能进行了对比,结果如表 2 所示.

表 2 AES 三种密钥长度测试结果与对比

AES 密钥长度	128 bit	192 bit	256 bit
我们的设计	247.9 MB/s	245.3 MB/s	220.3 MB/s
X-wall MX 系列	150 MB/s	150 MB/s	150 MB/s

7 结束语

本文给出了可配置加密算法的 SATA 加密桥接器的设计方案,并以较小的资源代价在 Xilinx XUPV5 平台上进行了硬件实现.同时,对该方案进行了较全面的测试,测试结果表明,本设计有如下几个特点:①兼容性好,能够在各种硬件的组合下正常工作,并且支持 SATA I 与 SATA II;②加解密吞吐量大,加密桥的插入几乎不影响原本的通信速率,和业界成熟产品 X-Wall MX 系列芯片相比有较大优势;③可扩展性好,提供简单易用的加解密模块接口,因此具有较高灵活性,方便各种对称加密算法的植入.

参考文献:

- [1] Enova Technology. X-Wall MX brochure [EB/OL]. [2013-02-27]. http://www.enovatech.net/support/download/X-Wall_MX_Brochure.pdf.
- [2] Serial ATA International Organization. Serial ATA revision 3.0 gold[S]. United States: SATA-IO, 2009.
- [3] Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory. FIPS-197. Advanced encryption standard[S]. United States: FIPS, 2001.

(下转第 30 页)



图4 背景建模与检测结果

不同的更新累积掩膜对背景进行更新,利用基于边缘的相关匹配算法,来识别和提取前景目标,从而实现了视场内的遗留物或搬移物的高效检测.实验结果表明本文所提出的检测算法大大降低了计算的复杂度,使算法能满足视频监控系统实时处理的要求,检测视场内的遗留物或搬移物有较高的检测精度和鲁棒性,降低了误警率.

参考文献:

- [1] 陈颖鸣,陈树越,张显亨.智能视频监控中异常行为识别研究[J].微电子学与计算机,2011,27(11):102-105.
- [2] 夏应高,朱秀昌.用于监控视频的滞留与搬移物体的检测算法[J].视频应用与工程,2008,32(12):86-88.
- [3] Stauffer C, Grimson W E L. Adaptive background mixture models for real-time tracking[J]. IEEE Computer Vision and Pattern Recognition, 1999(2):

246-250.

- [4] 谢立,胡玲玲,吕一品,等.面向智能视频监控系统运动目标检测的轮廓提取方法[J].东南大学学报:自然科学版,2012(42):32-33.
- [5] 毕国玲,赵建,曲锋,等.一种高效的前景目标检测算法[J].仪器仪表学报,2012(8):1102-1104.
- [6] 王琛,郭继昌,冯晓敏.基于双层背景的遗弃物检测方法[J].计算机工程,2011,37(24):167-168.
- [7] Singh A, Sawan S, Hanmandlu M, et al. An abandoned object detection system based on dual background segmentation[C]// Proceedings of the 6th IEEE International Conference on Advanced Video and Signal Based Surveillance. Genova, AVSS, 2009:352-357.
- [8] 汤一平,富吉勇,陈耀宇.基于全方位计算机视觉的遗留物检测系统[J].计算机测量与控制,2010,18(3):517-519.
- [9] Porikli F. Detection of temporarily static regions by processing video at different frame rates[C]// 2007 IEEE conference on advanced video and signal based surveillance. UK:London;2007:236-241.

作者简介:

毕国玲 女,(1981—),博士研究生,助理研究员.研究方向为嵌入式技术、数字图像处理、软件设计等.

赵建 女,(1967—),研究员,硕士生导师.研究方向为数字图像处理、目标识别与跟踪、视频编解码等.

续志军 男,(1953—),研究员,博士生导师.研究方向为光电精密仪器跟踪.

孙强 男,(1971—),研究员,博士生导师.研究方向为现代红外光学仪器.

(上接第26页)

- [4] Xilinx Inc. Virtex-5 FPGA rocketIO GTP transceiver user guide[EB/OL]. [2013-02-27]. http://www.xilinx.com/support/documentation/user_guides/ug196.pdf.
- [5] Donovan Anderson, Mike Jackson, Duncan Penman. SATA storage technology [M]. United States: Mindshare Press, 2007.
- [6] 牛戴楠,李江涛,周仟.基于FPGA的SATA III控制器的实现[J].雷达与对抗,2012(9):22-25.
- [7] 陈杰.基于SATA2.0协议的高速大容量存储控制系统的设计与实现[D].成都:电子科技大学,2011.

作者简介:

谭帆 男,(1987—),硕士研究生.研究方向为信息安全芯片设计.



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.

