

移动硬盘加解密板卡的设计与实现

秦宗庆¹, 张伯泉¹, 曹海波²

(1 广东工业大学 计算机学院, 广东 广州 510006; 2 电子科技大学 通信抗干扰国家级重点实验室, 四川 成都 640051)

摘 要: 针对移动硬盘数据安全问题, 分析、优化了 AES 加密算法, 提出了 Microblaze 与轮内、轮间三级流水线 AES 加解密 IP 核结合的架构, 设计并实现了一种介于硬盘与电脑 USB 接口之间的加解密安全卡. 仅需在电脑 USB 与硬盘间串联该安全卡, 普通硬盘便可以升级为加密硬盘. 在 Spartan6-Nexys3 FPGA 开发板上实验结果表明, 该加解密系统能在 120 MHz 时钟下达到 174.08 Mb/s 的吞吐率, 系统吞吐率高、资源消耗低.

关键词: AES 算法; 流水线; Microblaze; 加密; 解密

中图分类号: TN47

文献标识码: A

文章编号: 1000-7180(2014)05-0140-04

Design and Implementation of Mobile Hard Disk Encryption and Decryption Cards

QIN Zong-qing¹, ZHANG Bo-quan¹, CAO Hai-bo²

(1 College of Computer, Guangdong University of Technology, Guangzhou 510006, China;

2 National Key Laboratory of Science and Technology on Communications,

University of Electronic Science and Technology of China, Chengdu 610051, China)

Abstract: For the security of data stored in the mobile hard disk, the AES algorithm is optimized and a pipelined encryption and decryption system which combines a Microblaze with an AES core is presented. The security card is designed to work between the USB interfaces of the computer and the mobile hard disk. A traditional mobile hard disk can be turned to a security one simply by using this card. The experimental results on Spartan6-Nexys3 FPGA show that the encryption and decryption system can achieve 174.08 Mb/s at 120 MHz clock with very low resource consumption.

Key words: AES algorithm; pipeline; Microblaze; encryption; decryption

1 引言

移动硬盘应用越来越广泛, 数据的安全性至关重要, 现有仅靠操作系统安全功能来保证硬盘数据安全性的方法过于脆弱^[1]. 因此, 很多硬盘加密方案被提出. 主流加密手段主要分为两大类: 软加密和硬加密. 软加密需要在电脑安装加密软件, 并且加密速度慢, 效率低. 硬加密通常是将加密软件固化为 ASIC 芯片, 使用专用芯片对数据加密, 从而提高加密速度.

AES^[2] 全称是 Advanced Encryption Standard, 即高级加密标准. 作为新一代数据加密标准, AES

具有安全性强、效率高、实现简单等优点.

针对硬盘数据安全问题, 本文设计了一种基于 AES-128 的硬盘高速加密板卡.

2 加解密板卡整体结构

文献[3]中, 由 ARM CPU 完成硬盘数据加解密的方案, 该方案加密速率慢, 无法适应硬盘高速加解密. 因此本文采用了 Microblaze 与 AES 加解密模块结合的方案.

如图 1 所示, 本文设计的硬盘加解密系统由数据传输部分、数据控制部分、数据加解密三部分组成. 其中, 数据传输部分主要包括 USB Core、FIFO;

数据控制部分由 Microblaze 负责;数据加密部分由 AES IP 核、控制逻辑组成。

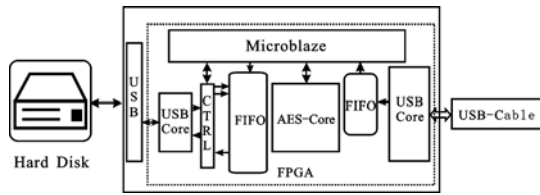


图1 加解密板卡结构

在该系统中,对数据吞吐量要求较高的部分(USB 读写, AES 加解密)用 Verilog HDL 硬件描述语言实现专用电路,经 AXI 总线挂载到 Microblaze,实现硬件加速。对吞吐量要求较低的部分(任务调度、数据打包)由 Microblaze 负责控制。该板卡数据流:USB Core 负责与 USB-Cable 通信,对 USB 令牌包、握手包分析,截取数据包后将数据包送 FIFO 缓存, Microblaze 调用 AES 核对 FIFO 中数据以 128 bit 为单位进行加密,并将加密后的数据包与初始令牌包、握手包等打包后送 FIFO, USB-Core 在控制逻辑控制下从 FIFO 读取加密后的数据经硬盘 USB 接口送硬盘存储。在系统运行过程中,只有数据包被更改。

3 AES 算法级优化与结构级优化

3.1 AES 算法分析

AES 加密算法主要由三部分构成:轮变换、轮数(Nr)和密钥扩展(KeyExpansion), AES 的解密运算是加密运算的逆运算。如图 2 所示, Add-R-Key 为密钥加, SubByte 为字节变换, Shift-Rows 为行移位, M-Columns 为列混合。AES 加密时首先使用初始密钥进行一次密钥加(Add-R-Key), 然后进行 Nr-1 次轮变换, 最后再进行一次轮变换。其中, 初始的密钥加法和每个轮变换的输入均为状态和一个轮密钥。从初始密钥导出轮密钥的过程记作密钥扩展(KeyExpansion), 初始密钥加法的输入记为 ExpandedKey[0], 第 i 轮的轮密钥记为 ExpandedKey[i]。AES 解密时子密钥的使用顺序正好与加密时相反, 本文中 Nr=10。

3.2 字节变换算法优化

字节变换(Sub Bytes):是 AES 加密算法中唯一的非线性变换,它是对矩阵中每个状态字进行独立的运算,它包含了一个作用在状态字上的 S 盒,对一个字节作有限域 GF(2⁸)上的乘法逆,并外加一个仿射变换。通常有两种方法实现字节变换:一是查找表法,二是有限域运算。查找表法是通过 S 盒对矩

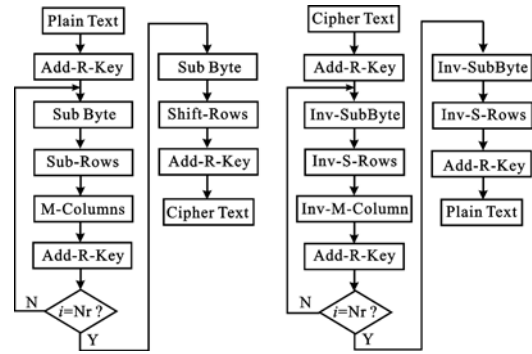


图2 AES 加解密流程

阵中的每个字节进行替换,由于需要提前将所有被替换的字节计算出来,存储在芯片中,每次实行字节变换时进行查找,并且解密操作时用到的 S 逆盒与加密操作的 S 盒是两张不同的表,所以至少需要 256 乘 8 位表, FPGA 需要消耗 256 乘 8 的 Block-RAMs。而高斯运算中字节变换和逆字节变换共享了 GF(2⁸)乘法逆,因此基于高斯运算的方法比查找表法更节约资源。基于高斯运算的优化字节变换算法如下:

若记乘法逆运算为

$$a(x) \cdot b(x) \bmod m(x) = 1, \quad (1)$$

则称 $b(x)$ 是 $a(x)$ 的逆元。其中

$$m(x) = x^8 + x^4 + x^3 + x + 1. \quad (2)$$

仿射变换定义:

$$L_{u,v}: a(x) \mapsto L_{u,v}(a(x)) =$$

$$u(x) \cdot a(x) + v(x) \bmod a(x^8 + 1), \quad (3)$$

如果记:

$$F = \begin{bmatrix} f_0 & f_1 & f_2 & f_3 & f_4 & f_5 & f_6 & f_7 \\ f_7 & f_0 & f_1 & f_2 & f_3 & f_4 & f_5 & f_6 \\ f_6 & f_7 & f_0 & f_1 & f_2 & f_3 & f_4 & f_5 \\ f_5 & f_6 & f_7 & f_0 & f_1 & f_2 & f_3 & f_4 \\ f_4 & f_5 & f_6 & f_7 & f_0 & f_1 & f_2 & f_3 \\ f_3 & f_4 & f_5 & f_6 & f_7 & f_0 & f_1 & f_2 \\ f_2 & f_3 & f_4 & f_5 & f_6 & f_7 & f_0 & f_1 \\ f_1 & f_2 & f_3 & f_4 & f_5 & f_6 & f_7 & f_0 \end{bmatrix} \quad (4)$$

$$a = \begin{bmatrix} a_7 \\ a_6 \\ a_5 \\ a_4 \\ a_3 \\ a_2 \\ a_1 \\ a_0 \end{bmatrix}, \quad v = \begin{bmatrix} v_7 \\ v_6 \\ v_5 \\ v_4 \\ v_3 \\ v_2 \\ v_1 \\ v_0 \end{bmatrix} \quad (5)$$

则仿射变换可以表示为

$$L_{u,v}(a) = F \cdot a + v \quad (6)$$

综上所述, S 盒的非线性变换表达式为

$$y = L_a \cdot x^{-1} + v \quad (7)$$

式中, L_a 为 F 矩阵, x 为 a 向量, $GF(2^8)$ 上的任意元素都可以看作 $GF(2^4)$ 子域上的一个一次多项式 $T = T_h x + T_l (T_h, T_l \in GF(2^4))$, 其乘法以 $x^2 + \lambda x + \eta (\lambda, \eta \in GF(2^4))$ 为模数.

令 $T^{-1} = (T_h x + T_l)^{-1} = \alpha x + \beta$, 可以推导出

$$\begin{aligned} (T_h x + T_l)(\alpha x + \beta) &= T_h \alpha x^2 + (T_h \beta + T_l \alpha) x + T_l \beta \\ &= T_h \alpha (\lambda x + \eta) + (T_h \beta + T_l \alpha) x + T_l \beta \quad (8) \\ &= (T_h \alpha \lambda + T_h \beta + T_l \alpha) x + (T_h \alpha \eta + T_l \beta) \\ &= 1, \end{aligned}$$

从而得到

$$\begin{cases} (T_h \lambda + T_l) \alpha + T_h \beta = 0 \\ T_h \alpha \eta + T_l \beta = 1 \end{cases} \quad (9)$$

$$\begin{cases} T_h \beta = -(T_h \lambda + T_l) \alpha \\ T_h^2 \alpha \eta + T_h \beta T_l = T_h \end{cases} \quad (10)$$

进而得到

$$(T_h^2 \eta + T_h T_l \lambda + T_l^2) \alpha = T_h, \quad (11)$$

$$\alpha = T_h (T_h^2 \eta + T_h T_l \lambda + T_l^2)^{-1} \quad (12)$$

$$\beta = (T_h \lambda + T_l) (T_h^2 \eta + T_h T_l \lambda + T_l^2)^{-1} \quad (13)$$

因此,

$$\begin{aligned} (T_h x + T_l)^{-1} &= T_h (T_h^2 \eta + T_h T_l \lambda + T_l^2)^{-1} x + \\ & (T_h \lambda + T_l) (T_h^2 \eta + T_h T_l \lambda + T_l^2)^{-1} \end{aligned} \quad (14)$$

可以看出, 该算法将 $GF(2^8)$ 上的求逆运算简化为 5 次乘法、2 次平方、3 次加法运算.

3.3 密钥扩展算法实现

记初始密钥为 $Key[0]$, 轮密钥 $ExpandedKey[i]$ 从 $ExpandedKey[i-1]$ 计算得来, $p[j] (0 \leq j \leq 3)$ 是 $ExpandedKey[i-1]$ 的第 j 列, $w[j]$ 是 $ExpandedKey[i]$ 的第 j 列, 那么 $ExpandedKey[i]$ 的计算方式如下:

$$w[0] = (RW(SW(p[3]))) \oplus rec[i] \oplus p[0]$$

$$w[1] = p[1] \oplus w[0]$$

$$w[2] = p[2] \oplus w[1]$$

$$w[3] = p[3] \oplus w[2]$$

其中, $RW()$ 的输入是 4 字节的 $[a_0, a_1, a_2, a_3]$, 输出是 4 字节的 $[a_1, a_2, a_3, a_0]$, $SW()$ 进行 4 字节的字节变换, $rec[i]$ 的值为 $[x^{i-1}, \{00\}, \{00\}, \{00\}]$, 其中 x 值为 2.

3.4 AES IP 核结构级优化

在数字系统设计中, 具体器件的工艺决定了触

发器的时钟到数据输出的延时 (T_{co})、D 触发器的建立时间 (T_{setup}), 器件选定后我们可以改变的只有组合逻辑的延时 (T_{delay}). 因此, 缩短触发器间组合逻辑的延时是提高同步电路速度的关键. 由于一般同步电路都不止一级锁存, 而要使电路稳定工作, 时钟周期不能太高, 必须满足最大延时要求, 这样就不可避免地限制了系统的最高频率. 缩短最长延时路径, 才可提高电路的工作频率. 本文针对 AES 算法特点采用了三种方法:

(1) 优化算法的硬件实现方式, 减少逻辑资源消耗;

(2) 通过对综合器添加约束, 减少走线延时;

(3) 将大的组合逻辑分解, 中间插入触发器, 即采用“流水线”(Pipelining) 技术.

图 3 为本文实现的 AES 加密算法的整体结构. 其中, A-R-K 为轮密钥加, S-Rows 为行移位, Mix-C 为列混合, 通过轮内插入 128 位寄存器 (128-Reg) 将组合逻辑拆分, 并采用牺牲面积换取速度方式进行逻辑复制, 实现轮内 3 级流水与轮间 3 级流水结合.

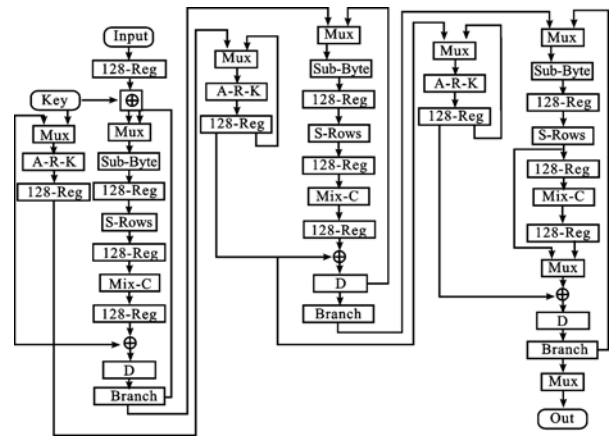


图 3 轮内、轮间三级流水线结构

4 实验平台与结果分析

本文基于 TSMC 0.18 μm 工艺库, 将设计的 AES IP 核用 Synopsys DC 进行综合, 并与其它论文实现的 AES IP 核进行了对比. 本文优化的 AES IP 核综合结果如表 1 第二列所示: 消耗了 39583 门, 最高时钟频率可以达到 170.1 MHz, 吞吐率达到 1.94 Gb/s. 从面积上看, 通过对 AES 的简化运算, 降低了代码复杂度, 节约了资源消耗, 与文献[4]未进行优化的实现方法相比, 资源节约 38%. 从系统运行最高频率上看, 由于本文对影响关键路径的组合逻辑进行拆分, 使得系统的最长路径延时缩短, 时钟可以达到 170.1 MHz. 从吞吐率方面比较, 本

文通过采用轮内、轮间三乘三级流水线技术,用面积换取吞吐量的提升,相对比文献[4],面积多消耗了125%,同时吞吐率提高了142%。从吞吐率与面积对比情况,本文实现的AES IP核吞吐率最高,资源消耗适中,适合应用于对吞吐量要求较高的场合。

表1 Synopsys DC综合AES结果比较

	本文	文献[5]	文献[4]	文献[6]
工艺/ μm	180	180	180	180
面积/Gates	39 583	58 445	17 519	173 000
最高时钟/MHz	170.1	125.0	62.5	100.0
吞吐率/(Gb/s)	1.94	1.60	0.80	1.82
吞吐率/面积(kb/G)	51.39	28.70	47.90	11.10

本项目实验平台FPGA采用Xilinx公司的xc6slx45-3csg324,开发工具为ISE,FPGA综合结果如表2所示。

表2 FPGA综合所有模块结果

Target FPGA device	Atlys-xc6slx45
Encryption thought	174.08MBs (1.36 Gb/s)
Speed grade	-3
Clock frequency	120 MHz 480 MHz
Number of Slice LUTs	5 369/27 288(19%)
Number of Slice Registers	4 120/54 576 (7%)
Block RAMS	28/116(24%)
Number ofPLL_ADVs	1/4(25%)

100 MHz经PLL倍频到120 MHz和480 MHz,120 MHz用来给AES加密IP核提供时钟,480 MHz时钟用来获取USB线上的串行信息,经串并转换后提供给USB核。在FPGA上经ISE布线后,实现的无流水线操作的AES加解密算法IP核由于组合逻辑的路径延时,最大时钟频率为80 MHz。在轮间插入128 bit寄存器,轮内3级流水后,AES核时钟频率可达到120 MHz而不会出现时序违例。在加密效率方面,AES加解密IP核在流水线满负荷工作下仅需要11个时钟周期即输出一组密文。在消耗资源方面,该系统以较小的资源消耗得到了较大的运行效率提升。综上所述,本文采用的轮内3级流水与轮间3级流水结合的方案,达到了高性能与资源节约的平衡。

在实际实验中,对硬盘的加密传输速度峰值达到了60 MB/s;对单个1GB的文件进行传输实验,加密时写平均速率20 MB/s,解密时读平均速率25 MB/s。

5 结束语

本文改进了AES加解密算法的硬件实现结构,降低了资源消耗,提高了加解密速率,实现了适用于移动硬盘的数据加密卡,实验证明了该方案的有效性。由于本文采用的是USB2.0,加解密速率受限于USB接口。今后工作是将加解密板卡升级到支持USB3.0标准,达到更高的吞吐率。

参考文献:

- [1] 董军利,宋福刚,管文强,等.基于AES&RSA混合加密策略的硬盘分区加密技术[J].微电子学与计算机,2012,29(001):135-137.
- [2] Daemen J,Rijmen V,谷大武.高级加密标准(AES)算法—Rijndael的设计[M].北京:清华大学出版社,2003.
- [3] Wang C, Wang G, Sun Y, et al. ARM Realization of storage device encryption based on chaos and AES algorithm[C]//Chaos-Fractals Theories and Applications, 2011 Fourth International Workshop on. Hangzhou:IEEE,2011:183-187.
- [4] Liang Y, Li Y. A low-power and cost-effective AES chip design for healthcare devices[C]//Biomedical and Health Informatics, 2012 IEEE-EMBS International Conference on. Hong Kong:IEEE,2012:795-798.
- [5] Srinivas Shastry P V, Kulkarni A, Sutaone M S. ASIC implementation of AES[C]//India Conference, 2012 Annual IEEE. Kochi:IEEE,2012:1255-1259.
- [6] Kuo H, Verbaughede I. Architectural optimization for a 1.82 Gbits/sec VLSI implementation of the AES Rijndael algorithm[C]//Cryptographic Hardware and Embedded Systems. Berlin Heidelberg: Springer, 2001:51-64.

作者简介:

- 秦宗庆 男,(1987—),硕士.研究方向为集成电路设计。
 张伯泉 男,(1974—),博士,副教授.研究方向为集成电路设计。
 曹海波 男,(1989—),硕士.研究方向为数字信号处理。