FPGA 的 AES 高速处理模型设计

韩津生[1]，林家骏[1]，叶建武[2]，周文锦[3]

（1. 华东理工大学 信息科学与工程学院，200237 上海，daidaidou@163.com；2. 东方通信股份有限公司，310053 杭州；
3. 天津市政府国际经济研究室，300041 天津）

摘　要： 为了提高 AES 的处理速度，提出了 AES 的全流水线设计思想. 通过对全流水线路径上相应 MEM 资源和逻辑资源的深入分析，找出制约数据块工作效率的因素，采用双通道运算模型，创建各流水线节点的高速模型，实现 AES 的全流水线设计. 实验结果表明：在 EP4CE40F29C8 的 FPGA 芯片上执行 AES 加解密运算，其吞吐量达到 7.2 Gbps. 在全流水线架构下，双通道的设计思想使得流水线上的所有数据块处于高效工作状态，系统在低成本的前提下实现了性能的大幅提高.

关键词： AES；全流水线；双通道

中图分类号： TN791　　**文献标志码：** A　　**文章编号：** 0367－6234(2012)03－0128－04

Design of AES high-speed model on FPGA

HAN Jin-sheng[1], LIN Jia-jun[1], YE Jian-wu[2], ZHOU Wen-jin[3]

(1. School of Information Science & Engineering, East China University Of Science And Technology, 200237 Shanghai, China, daidaidou@163.com; 2. Eastern Communications Company Limited, 310053 Hangzhou, China;
3. Tianjin Municipal Government, International Economic Research, 300041 Tianjin, China)

Abstract: To improve the performance of AES on FPGA, an idea of fully pipeline is proposed. After analyzing the needs of memory and logic elements deeply and finding out the factors restricting the efficiency of data blocks, the high-speed operation of the pipeline node model with dual channel mold is found to implement the AES full line. Experimental results show that the throughput of the AES encryption and decryption algorithm on FPGA of EP4CE40F29C8, can reach up to 7.2 Gbps. In the framework of fully pipeline, the idea of dual channel mold makes all the pipeline data blocks in efficient working condition. System under the premise of low-cost achieves a substantial improvement in performance.

Key words: AES; fully pipeline; dual channel

2001 年，美国国家标准技术局（NIST）发布了高级加密标准 AES[1]. AES 是一个对称分组密码算法，用来取代 DES，从而成为广泛使用的新标准. AES 的分组长度是 128 bit，密钥长度支持 3 种：128，192，256 bit，随着密钥长度的增加，执行的轮数也随之增加. AES 作为新一代的数据加密标准，其安全性、高性能、高效率、易用性和灵活性等优点被完全体现出来，AES 的设计分别考虑了软件和硬件平台的适应性，既能适应 8 bit 单片 CPU、也能适应通用的 32 bit CPU；能够作流密码、消息认证码发生器、随机数发生器、HASH 算法等. 到目前为止，还没有已知的攻击方法对 AES 有效.

AES 硬核的设计是众多应用研究的方向，考虑应用的灵活性和芯片的发展趋势[2-3]，FPGA 成为设计实现的主流硬件平台[4-5]. 2000 年，K. Gaj 等[6] 设计实现了 331.5 Mpbs 的 AES 核；2004 年，Shuenn-Shyang Wang 等[7] 将其提升到了 1.604 Gpbs；2009 年，H. Rais 等[8] 设计的 AES 核达到 3.090 Gpbs，同年，为满足 GPON 数据加密的应用需求，UT 开发小组[9] 采用二级流水线方式实现了 4.144 Gpbs 的处理能力.

收稿日期： 2011－10－15.
基金项目： 国家自然科学基金资助项目（60903186）.
作者简介： 韩津生（1963—），男，博士研究生，高工；
林家骏（1948—），男，教授，博士生导师.

1　AES 算法

图 1 显示了 AES(128 bit 密钥)的完整结构. 分组明文长度为 128 bit,经过加密路径产生 128 bit的分组密文;同理,128 bit 分组密文经过解密路径还原成 128 bit 的分组明文. 在图 1 中,加解密路径主要存在 4 个操作:轮密钥加、字节代换、行移位和列混淆. 轮密钥加是位异或运算;字节代换是面向 S 盒的置换过程;行移位是指变换路径上 128 bit 过程数据以字节为单位的有序置换操作;列混淆是指置换数据的矩阵乘法运算. 加解密路径共享密钥扩展方法,但是解密路径的密钥需要在加密路径的扩展密钥基础之上增加列混淆操作.

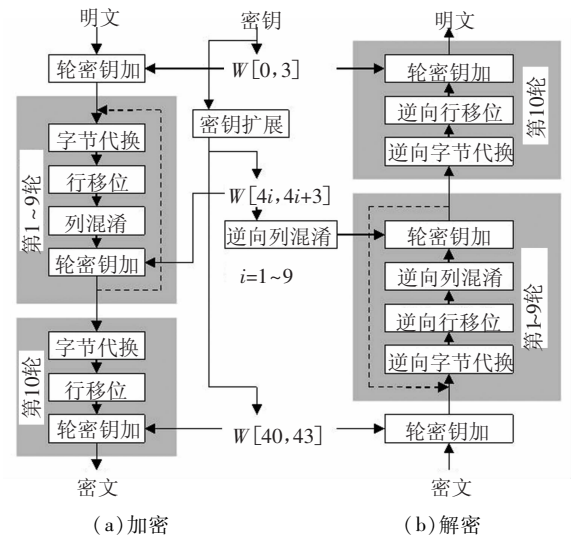

图 1　AES 的加密和解密

加解密路径的轮运算是 AES 算法的功能核心,而轮运算具备共同的结构. 考虑 FPGA 的资源消耗,通过 ROM 或 RAM 方式来组织轮运算是目前的主要设计思路之一. 在该方式下,轮运算的伪码描述为

$$T0_{n+1} = ae0[T0_n \& 0xff] \hat{} ae1[(T1_n \gg 8) \& 0xff] \hat{} ae2[(T2_n \gg 16) \& 0xff] \hat{} ae3[(T3_n \gg 24)] \hat{} rk[4n+0],$$

$$T1_{n+1} = ae0[T1_n \& 0xff] \hat{} ae1[(T2_n \gg 8) \& 0xff] \hat{} ae2[(T3_n \gg 16) \& 0xff] \hat{} ae3[(T0_n \gg 24)] \hat{} rk[4n+1],$$

$$T2_{n+1} = ae0[T2_n \& 0xff] \hat{} ae1[(T3_n \gg 8) \& 0xff] \hat{} ae2[(T0_n \gg 16) \& 0xff] \hat{} ae3[(T1_n \gg 24)] \hat{} rk[4n+2],$$

$$T3_{n+1} = ae0[T3_n \& 0xff] \hat{} ae1[(T0_n \gg 8) \& 0xff] \hat{} ae2[(T1_n \gg 16) \& 0xff] \hat{} ae3[(T2_n \gg 24)] \hat{} rk[4n+3].$$

式中: $T0_n$、$T1_n$、$T2_n$、$T3_n$ 分别为上一轮的数据输出,数据宽度为32 bit; $T0_{n+1}$、$T1_{n+1}$、$T2_{n+1}$、$T3_{n+1}$ 分别为本轮的处理结果,数据宽度为 32 bit. 数据总宽度为 128 bit, 与分组数据宽度保持一致. 而 *ae*0、*ae*1、*ae*2、*ae*3 分别为 32 bit 宽、容量为 256 的数据块,每个数据块的大小为 8 192 bit,字节代换、行移位和列混淆 3 个操作等效于 *ae*0、*ae*1、*ae*2、*ae*3 的查表;"^" 操作为异或操作,等效为位加;*rk* 为本轮处理的扩展密钥.

2　AES 全流水线模型设计

2.1　FPGA 的 MEM 结构

Altera 公司的 CYCLONE IV 为新一代高性价比 FPGA,其基本 MEM 块为 M9K 颗粒. M9K 可以按照设计要求设计成 FIFO、单端 RAM(包含 ROM)、双端口 RAM. 在 AES 的应用中,ae0、ae1、ae2、ae3 主要体现地址到数据的转换,可以通过 ROM 或双端口 RAM 来实现. 按照 M9K 的特征,ae0、ae1、ae2、ae3 的读出路径的高速等效工作模型如图 2 所示.

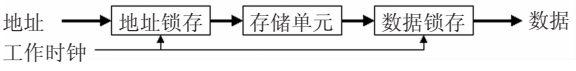

图 2　数据块工作模型

图 2 中的第 2 级锁存可以按照应用要求来选择,带锁存输出能让存储单元工作在更高的工作速度,提高存储单元的数据吞吐量. 按图 2 表示,每进行一次 *ae* 查表,需要两个工作时钟.

在高效的工作模式下,数据块地址到数据,需要两个工作时钟,为提高存储单元工作效率,需采用流水线的读取方式. 此种方式,在工作时钟的驱动下,移位后的数据依次进入地址锁存器,查表后的数据依次从数据锁存器中输出.

2.2　AES 轮运算流水线模型

按照流水线的设计思想,轮运算的基本模型如图 3 所示.

在图 3 中, *ae*0、*ae*1、*ae*2、*ae*3 在图 2 所示模型下的工作,其输入为移位后的地址,以流水线的方式进入数据块,而输出就是对应字节代换、行移位和列混淆后的数据,这些数据以流水线的方式输出. 5 异或模块以流水线的方式处理完成轮密钥加,最后形成下一轮处理的分组数据.

从该模型看出, 分组数据 $T0_n$、$T1_n$、$T2_n$、$T3_n$ 分别经过 6 个工作时钟才能完成一次轮运算,得到 $T0_{n+1}$、$T1_{n+1}$、$T2_{n+1}$、$T3_{n+1}$, 而 *ae*0、*ae*1、*ae*2、*ae*3 代表的数据块只产生了 4 个有效的输出,在流水线方式下,数据块工作效率存在 1/3 的损失.

上述 *ae* 查表操作的地址输入和查表后的数据异或处理最终等效为逻辑运算,地址输入最终

体现为 6 输入的逻辑运算,后期的异或处理为 5 输入的逻辑运算,这些逻辑运算在 FPGA 中是通过 LUT 来实现的,对于 CYCLONE IV,LUT 为 4 输入 – 输出结构,为提高逻辑运算的工作频率,前后都需要增加一级流水线. 这样,从流水线路径上,形成了深度为 8 的节点模型,其中 4 个工作时钟用于数据块的地址到数据的转换,4 个工作时钟用于逻辑运算和地址数据的输入输出消耗. 采用这种 8 工作时钟的节点模型,能有效提高节点的工作频率,但是,数据块的工作效率降为 1/2.

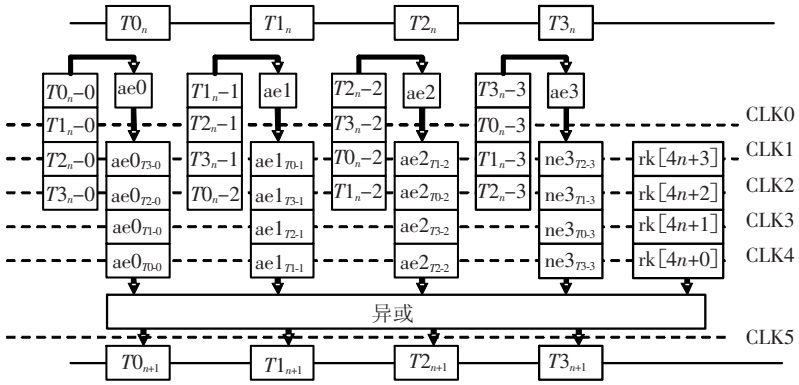

图 3 AES 轮运算的基本模型

2.3 AES 全流水线模型设计

采用双通道的思想能有效解决这一问题,实现 AES 的全流水线结构. 提取图 3 的处理流程,通过分组数据交替的方式连续穿过流水线,即当 A 通道数据工作在数据块时,B 通道数据工作在组合逻辑部分,其简化模型如图 4 所示.

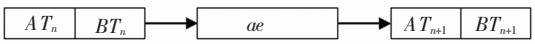

图 4 轮运算的双通道简化模型

在图 4 中,AT_n、BT_n 分别为 A、B 通道的 $T0_n$、$T1_n$、$T2_n$、$T3_n$ 数据,AT_{n+1}、BT_{n+1} 分别为经过轮处理后 A、B 通道的 $T0_{n+1}$、$T1_{n+1}$、$T2_{n+1}$、$T3_{n+1}$ 数据,ae 为 $ae0$、$ae1$、$ae2$、$ae3$ 数据块.

图 4 的 A、B 通道是对于相对独立的分组数据而言,正常的 AES 数据加解密是由若干分组数据组成,这些分组数据被依次送入 AES 加解密通道. 在流水线工作模式下,并不存在 A、B 通道的区分,只是表现为分组数据量的成倍增加,即由原来的每 8 个工作时钟送入一组分组数据变成每4 个时钟送入一组分组数据.

轮运算理论资源消耗:除 4 个 M9K 外,地址输入部分将消耗 64 个 LE 单元,其中的 64 个 LUT 全部用于逻辑运算;后期的异或处理和数据缓冲将消耗 128 个 LE,其中有 64 个 LUT 用于逻辑运算;分组数据输出将消耗 128 个 LE,其中 32 个 LUT 用于逻辑运算.

轮运算最终消耗 4 个 M9K 和 320 个 LE.

3 AES 加解密模型

在 10 轮的轮处理过程中,前 9 轮的处理方式是完全一样的,只有最后一轮的处理略有差异,并且最后一轮存在资源和流水线深度裁减的条件,这可以在设计上予以体现,但是,为保持流水线结构的相对完整,本模型并不做差异化处理.

按照图 4 的思想完成图 1 所示的 AES 硬核设计,其轮运算部分构成了一个流水线深度为 40 的全流水线结构,其电路结构图如图 5 所示.

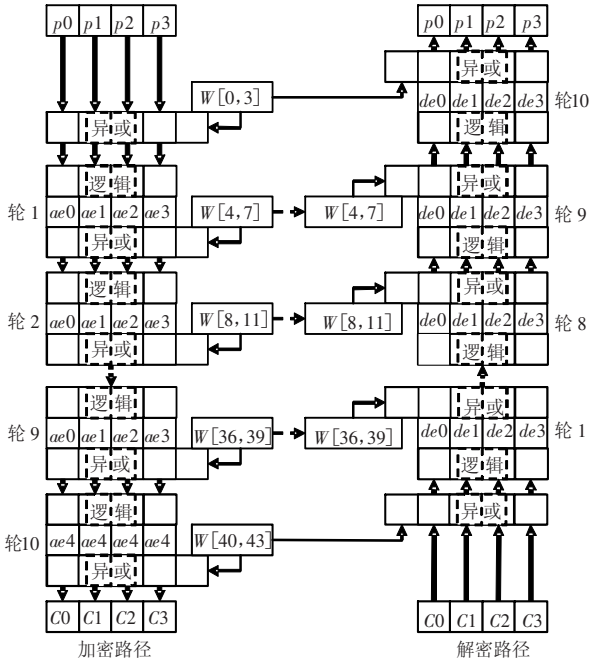

图 5 加解密电路结构图

在图 5 中,$P0$ – 3 为分组明文,$C0$ – 3 为分组密文,W、W' 分别为加、解密密钥,$ae0$ – 4、$de0$ – 4 分别为加、解密 S 盒和列混淆数据块.

轮前逻辑消耗等效为 1 个工作时钟,数据块消耗等效为 4 个工作时钟,异或操作部分消耗等效为 3 个工作时钟,10 轮操作共 80 个工作时钟.

4　实　验

EP4CE40F29C8 的 LE 总数量为 42 193 个, M9K 为 126 个. 在 EP4CE40F29C8 上,按照图 5 模型设计出 AES 核,加密部分的 10 轮轮处理实际资源消耗为 3 200 个 LE 和 40 个 M9K,解密部分亦是如此,这和理论计算完全一致.

LE 实际消耗占比为 15.2%,M9K 消耗占比为 63.5%. 从这个数据来看,FPGA 的 M9K 资源为关键资源,所以,M9K 在 FPGA 中的利用率及其工作效率是 AES 处理能力和 FPGA 对 AES 处理能力的关键所在,这一点和 AES 核的理论分析模型完全一致.

EP4CE40F29C8 中 M9K 的最高工作频率为 238 MHz,工具软件显示,本 AES 核的 F_{max} 为 238 MHz,这说明本 AES 核对流水线路径上的各节点的处理完全符合理论设计要求. 考虑实际系统的设计限制,本 AES 核选定工作频率为 225 MHz,能通过系统的全面测试,满足应用要求.

表 1　性能比较

算法	所用器件	价格/ $	处理带宽/ Mbps	性价比/ (Mbps · $^{-1}$)
文献[10]	XC3S500E	18.17	530	29.17
文献[4]	XC5VLX50	306.72	3 090	10.07
文献[5]	XC5VLX110T	1945.69	4 144	2.13
文献[11]	EP1C12Q240C8	39.05	256	6.56
本文 AES	EP4CE40F29C8	135.47	7 200	53.14

5　结　论

1) 对 AES 算法进行分析,其以字节代换为核心的算法结构特点利于在 FPGA 上实现. 采用流水线设计技术是行之有效的方法,但是,流水线的工作效率特别是 MEM 的访问效率是制约算法处理能力的因素. 在全流水线架构下,双通道的设计思想使得流水线上的所有数据块处于高效工作状态,并最终达到了 MEM 的极限工作效率.

2) 采用全流水线结构,实现了特定 FPGA 下高性能 AES 核的设计目标. 理论上,本 AES 核的数据吞吐量为 7.616 Gbps,实验最终选定 225 MHz 为 AES 核的工作频率,处理能力为 7.2 Gbps.

3) 对 AES 核的性能进行了比较,结果表明,本文所设计的 AES 核与目前已有的部分核相比,在低成本的前提下实现了性能的大幅提高,达到 53.14 Mbps/ $ 的处理能力.

参考文献:

[1] NIST. Federal Information Information Processing Standards Publication Announcing the Advanced Encryption Standard(AES)[EB/OL]. (2008-09-02)[2010-09-29]. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, 2001.

[2] OFweek 电子工程网. FPGA 创新之旅:Xilinx 深耕通信市场[EB/OL]. [2011-08-10]. http://info.ec.hc360.com/2011/08/110922478188.html.

[3] Xilinx. URL: http://china.xilinx.com/publications/prod_mktg/7-Series-Product-Brief.pdf.

[4] IYER N C, ANANDMOHAN P V, POORNAIAH D V, et al. High throughput, low cost, fully pipelined architecture for AES crypto chip[C]//2006 Annual IEEE India Conference. Washington, DC: IEEE Xplore, 2006: 1-6.

[5] HUANG Chi-wu, CHANG Chi-jeng, LIN Mao-yuan, *et al*. The FPGA implementation of 128-bits AES algorithm based on four 32-bits parallel operation[C]//Proceedings of the The First International Symposium on Data, Privacy, and E-Commerce. Washington, DC: IEEE Computer Society, 2007: 462-464.

[6] KRIS G, PAWEL C. Comparison of the Hardware Performance of the AES Candidates Using Reconfigurable Hardware[EB/OL]. [2010-08-01]. http://teal.gmu.edu/crypto/AES_gaj.PDF.

[7] WANG Shuenn-shyang, NI Wan-sheng. An efficient fpga implementation of advanced encryption standard algorithm[C]//Proceedins of the IEEE International Symposium on Circuits and Systems. Washington, DC: IEEE Computer Society, 2004: 23-26.

[8] RAIS M H, QASIM S M. A novel FPGA implementation of AES-128 using reduced residue of prime numbers based S-box[EB/OL]. [2009-01-20]. http://paper.ijcsns.org/07_book/200909/20090939.pdf.

[9] 李涛,成晓雄,王文华,等. 一种 GPON-AES 的 FPGA 优化实现[J]. 电信科学, 2009, 25(12):100-104.

[10] 黄前山, 季晓勇. 基于低成本 FPGA 的 AES 密码算法设计[J]. 通信技术, 2010, 43(9): 156-158.

[11] 王春蕾, 苏保照. 基于 FPGA 的 AES-128 加密芯片的设计与实现[J]. 青岛职业技术学院学报, 2009, 22(3): 71-74.

(编辑　张　红)