

轻量级 AES 加解密芯片设计与实现

彭 浩, 刘 恺, 张 亮, 廖 望, 戴 葵

(华中科技大学 光学与电子信息学院, 湖北 武汉 430074)

摘 要: 为满足资源受限环境下的安全加解密芯片的设计要求, 提出了一种轻量级 AES 加解密实现方法. 该方法采用 8 位串行数据通路, 模块复合结构, 并对加解密过程中的状态矩阵、列混合模块和密钥扩展模块的设计优化, 用最少的硬件资源实现加解密功能, 有效地提高硬件利用率. 仿真及实验证明, 该设计具有芯片面积小、功耗低的优点, 可以满足无线移动网络以及其他资源受限环境.

关键词: AES 算法; 轻量级; 嵌入式系统; 复合结构

中图分类号: TP302.2

文献标识码: A

文章编号: 1000-7180(2014)08-0094-04

The Light-Weight AES Encryption and Decryption Chip Design and Implementation

PENG Hao, LIU Kai, ZHANG Liang, LIAO Wang, DAI Kui

(School of Optical and Electronic Information, Huazhong University of Science & Technology, Wuhan 430074, China)

Abstract: In order to meet the design requirement of security chip with the functions of encryption and decryption under resource-constrained condition, this paper puts forward a light-weight AES encryption and decryption method. With 8-bit serial data path and modular composite structure, this method optimizes state matrix, mixcolumns module and key expansion module in the process of encryption and decryption. It is able to achieve the functions of encryption and decryption with minimal hardware resources and thus effectively improves the hardware utilization. According to simulation and experiment, the design has the advantages of small chip area and low power consumption, being available in wireless mobile network and other resource-constrained environments.

Key words: AES; light-weight; embedded system; modular composite structure

1 引言

近年来,随着信息产业的不断发展,以 RFID、Zigbee 技术为代表的低功耗低速的嵌入式系统得到广泛的应用,但其面临的安全问题日益严峻. 通过采用轻量级加密技术来满足资源受限的嵌入式系统的安全需求已成为主流发展趋势. AES 是当今世界著名的加密标准算法^[1],它具有安全、适应领域广、实现方便等特点^[2]. 近年来随着 AES 的逐渐应用普及,国内外很多公司和研究机构都在对 AES 算法进行深入研究,并提出了一些优化方法^[3-4]. 采用流水线的优化手段^[4-6]来加快 AES 算法的速度;通过增

加算法中数据处理的并行度,以提高数据吞吐率,但这些方案使用了很多重复的硬件结构,因此需要消耗较多的硬件资源.

采用循环迭代结构^[7-8],以尽量缩小芯片面积,达到低成本、低功耗的设计目标,但该方法仅实现了加密功能,未实现解密功能. 本文针对资源受限的嵌入式加解密应用,提出一种采用复合结构的轻量级 AES 加解密芯片的硬件设计方法,以满足低功耗低成本的加解密芯片设计需求.

2 AES 算法概述

AES 是一种迭代型对称区块加解密算法,该算

收稿日期: 2013-10-27; 修回日期: 2013-12-11

基金项目: 湖北省自然科学基金(ZRZ0051)

3.2 加解密流程控制

在加密过程中,明文以 8 位为单位输入状态矩阵,先将明文与输入的密钥进行异或运算,运算结果进行 SubBytes 变换,然后将变换结果存到状态矩阵中,完成初始密钥加和第一次轮变换的 SubBytes 变换。

接下来进行 9 次常规轮变换。由于该状态矩阵的每个寄存器单元分别存储 1 个字节数据,因此仅需对图 4 中的每行寄存器进行相应的数据移位更新,即可完成 ShiftRows 操作。然后将 S00, S10, S20, S30 这 4 个寄存器组成了 32 位数据作为 MixColumns 模块的输入数据,将 MixColumns 模块输出的 32 位数据作为 S03, S13, S23, S33 的输入,水平移位 3 个字节,完成 MixColumns 变换。再将状态矩阵中的每一个单元进行一次 AddRoundKey 操作,就完成了 AES 的一次常规轮变换。

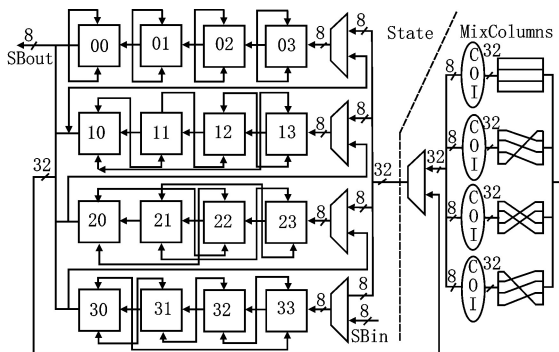


图 4 状态矩阵和列混合模块数据流图

由于最后一次轮变换比常规变换少一次 MixColumns 操作,因此,不再是使用 MixColumns 模块的输出作为状态寄存器输入,而是通过在状态寄存器与 MixColumns 模块之间设置一个 32 位选择器,将 MixColumns 模块的输入作为选择器输出,从而完成该轮变换。通过这样的设计,最后一次轮变换与常规轮变换可以使用同一个 LFSR 控制,不需要额外的控制电路。

最后,将 state 矩阵的 S00 与 key 矩阵的 K00 的异或结果作为输出,完成密文的输出。此过程可与最后一次轮变换并行进行,以提高芯片运行效率。

解密是加密的逆向过程,本文涉及的解密流程不再赘述。

3.3 轮密钥生成优化

虽然在流程上,解密是加密的逆过程,但解密过程中所使用的轮密钥却与加密不同。加密时是先使用 key_0 ,然后再使用 $key_1, key_2, \dots, key_{10}$ 。而解密就要先使用 key_{10} ,然后由 key_{10} 反推 key_9 ,以此类推。

为最大程度减小芯片面积,需要尽可能减少寄存器数量。因此,在原加密过程中的密钥矩阵上做一定结构改进,使之兼容解密过程的轮密钥变换。为此,需要先了解轮密钥的产生过程。

假设 key_i 是加密过程中的第 i 个轮密钥, key_{i+1} 则是第 $i+1$ 个轮密钥, key_i 的密钥矩阵如图 5 所示, key_{i+1} 的密钥矩阵如图 6 所示。

$$\begin{bmatrix} W_{00} & W_{01} & W_{02} & W_{03} \\ W_{10} & W_{11} & W_{12} & W_{13} \\ W_{20} & W_{21} & W_{22} & W_{23} \\ W_{30} & W_{31} & W_{32} & W_{33} \end{bmatrix} \quad \begin{bmatrix} M_{00} & M_{01} & M_{02} & M_{03} \\ M_{10} & M_{11} & M_{12} & M_{13} \\ M_{20} & M_{21} & M_{22} & M_{23} \\ M_{30} & M_{31} & M_{32} & M_{33} \end{bmatrix}$$

图 5 key_i 的密钥矩阵 图 6 key_{i+1} 的密钥矩阵

以第一行为例,两个密钥矩阵之间关系如下:

$$M_{00} = W_{00} \oplus \text{SUBWORD}$$

$$M_{01} = W_{01} \oplus M_{00}$$

$$M_{02} = W_{02} \oplus M_{01}$$

$$M_{03} = W_{03} \oplus M_{02}$$

由此可以推导出如下关系式:

$$W_{00} = \text{SUBWORD} \oplus M_{00}$$

$$M_{00} \oplus M_{01} = W_{01}$$

$$M_{02} \oplus W_{01} = W_{02} \oplus M_{00}$$

$$M_{03} \oplus (W_{02} \oplus M_{00}) = W_{03} \oplus W_{01}$$

因此,可以将密钥矩阵设计为图 7 所示结构。

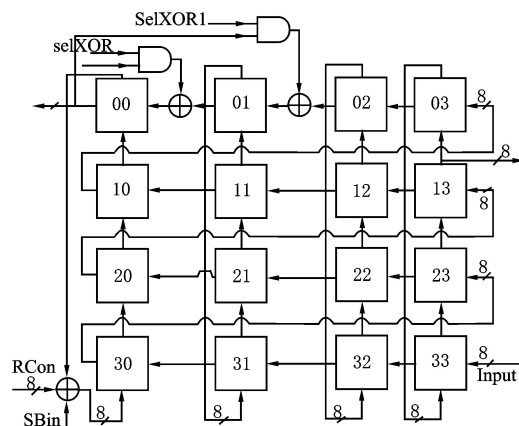


图 7 密钥矩阵数据流图

在解密过程中,假设原密钥矩阵存的是 key_{i+1} ,仍以第一行为例,将其以水平的方式移位 16 个周期,每 4 个周期将 selXOR 置为 8'h0,得到的新密钥矩阵第一行如下:

$$[M_{00} \quad W_{01} \quad W_{02} \oplus M_{00} \quad W_{03} \oplus M_{01}]$$

然后继续水平方式移位 16 个周期,每两个周期将 selXOR1 置为 8'h0,从而得到如下结果:

$$[M_{00} \quad W_{01} \quad W_{02} \quad W_{03}]$$

最后,套用加密时密钥矩阵的变换方式,用 W_{03}

生成 SUBWORD 与 M_{00} 异或,就可以得到 W_{00} ,从而生成 key_i ,得到解密过程所需的轮密钥。

4 验证与测试结果

本文用 Verilog 实现了该加密算法,采用 ModelSim 软件对整个芯片进行功能和时序仿真,并在 Altera 公司的 Cyclone II EP2C20 上进行适配,在工作频率为 10 MHz 的条件下,输入明文 6b c1 be e2 2e 40 9f 96 e9 3d 7e 11 73 93 17 2a,密钥 2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c,仿真后得到的密文为 3a d7 7b b4 0d 7a 36 60 a8 9e ca f3 24 66 ef 97,结果正确。当输入与上述仿真过程相同的密文和密钥后,也可得到相同的明文,验证了整个加解密算法的正确性。同时进行了 DC 综合,在工作频率为 10 Hz、0.18 μm 工艺下,芯片面积为 0.036 mm^2 。

目前已有一些针对 AES 算法的优化方案,如比较知名的 Amir Moradi^[10]、Akashi Satoh^[11]、P. Hamalainen^[12]等,下面主要从芯片功能、工艺、等效门数(面积)、时钟周期、工作频率(速度)、功耗等方面对本文提出的设计方案与上述方案进行比较,结果如表 1 所示。

表 1 不同 AES 算法优化方案的硬件性能比较

采用方案	功能加/解密	采用工艺/ μm	等效门数/GE	加/解密周期/时钟	时钟频率/kHz	功耗/ μW
传统 AES	加/解密	0.18	7 236	160/240	100	15/14.3
Amir. M	加密	0.18	2 421	210	100	6.66/无
P. Ham	加密	0.18	3 100	160	100	3.8/无
Akashi. S	加/解密	0.11	5 398	54/42	100	12.3/11
本文方案	加/解密	0.18	3 840	226/880	100	7.3/5.1

从表中数据可以看出,虽然 Amir Moradi 方案芯片面积最小,P. Hamalainen 方案功耗最低,但这两个方案仅支持加密过程,无法同时满足加/解密需求;Akashi Satoh 方案工作速度最快,但芯片面积较大,功耗较高,不能满足嵌入式系统低成本低功耗的要求。本文的优化方案通过在加密模块基础上增加较少硬件资源,使芯片同时具有加/解密功能,虽然加解密过程需要较多时钟周期,但芯片最高工作频率可达 10 MHz,加解密过程数据吞吐率可达到较高水平,完全能够满足嵌入式此系统加解密应用的需求。

5 结束语

本文通过对传统 AES 算法的加解密流程进行深入分析,提出了一种轻量级 AES 加解密的实现方法,通过使用复合结构优化加解密模块,降低了芯片

整体面积。进行了 DC 综合与 FPGA 验证,结果表明,本文提出的轻量级 AES 加解密芯片设计方案具有硬件资源少,功耗低等优点,芯片处理速度满足嵌入式系统需求。由于同时实现了加解密算法,因此在同时有加解密需求的嵌入式系统中,本文提出的芯片设计方案将更具优势。

参考文献:

- [1] National institute of standards and technology. Specification for the advanced encryption standard (AES) [DB/OL]. (2001-11-26) [2013-04-20]. <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.
- [2] National Institute of standards and technology. Data encryption standard (DES) [DB/OL]. (1999-10-25) [2013-04-20]. <http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>.
- [3] Xinmiao Zhang, Keshab K Parhi. High-speed VLSI architectures for the AES algorithm[J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2004, 12(9): 957-967.
- [4] Saggese G P, Mazzeo A, Mazzocca N, et al. An FPGA-based performance analysis of the unrolling, tiling and pipelining of the AES algorithm[C] // Proceedings of the 13th International Conference on Field Programmable Logic and Applications. [s. l.]: IEEE, 2003: 292-302.
- [5] Standaert F X, Rouvroy G, Quisquater J J, et al. Efficient implementation of Rijndael encryption in reconfigurable hardware: Improvements and design tradeoffs [C] // Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems cologne, Germany: IEEE, 2003: 334-350.
- [6] Hodjat A, Verbauwhede I. Area-throughput trade-offs for fully pipelined 30 to 70 Gbits/s AES processors [J]. IEEE Transactions on Computers, 2006, 55(4): 366-372.
- [7] 刘晗嘉. AES 加密算法 IP 核的设计与验证[D]. 上海: 上海交通大学, 2009.
- [8] 赵跃华, 王益维, 李晓聪. 一种适合于低成本标签的 RFID[J]. 计算机应用研究, 2010, 27(5): 1885-1888.
- [8] 赵跃华, 王益维, 李晓聪. 一种适合于低成本标签的 RFID[J]. 计算机应用研究, 2010, 27(5): 1885-1888.
- [9] Lin Bing, Xia Kewei, Liang Wenli. Reconfigurable implementation of AES algorithm IP core based on pipeline structure [J]. Journal of Southeast University: English Edition, 2010, 26(1): 21-25.

(下转第 103 页)

5 结束语

文中所介绍的3D-IC时钟树综合布线算法和已有的3D-IC布线算法相比,在保证零漂移的同时,有效降低了布线的开销,提高了信号传输表现,这其中包括线长和延时的缩短以及TSV个数的缩减。

要让3DIC时钟树布线结果在各方面都有好的表现,就必须对它的每个步骤都进行最优化,抽象树生成、树节点的层嵌入以及缓冲器插入缺一不可。本文虽实现了零漂移布线,但在实际情况下时钟延时会因为温度的改变而改变,不可能让时钟漂移为零,因此还需要进一步深入研究以及优化来最小化各种情况下的时钟漂移。

参考文献:

- [1] Mondal M, Ricketts A J, Kirolos S, et al. Thermally robust clocking schemes for 3D integrated circuits [C]// Proceedings of the Conference on Design, Automation and Test in Europe. Los Alamitos, CA: IEEE, 2007: 1206-1211.
- [2] Arunachalam V, Burleson W. Low-power clock distribution in a multilayer core 3d microprocessor [C]// Proceedings of the 18th ACM Great Lakes Symposium on VLSI. New York: IEEE, 2008: 429-434.
- [3] Minz J, Zhao X, Lim S K. Buffered clock tree synthesis for 3D ics under thermal variations [C]// Proceed-

ings of the 13th Asia and South Pacific Design Automation Conference. Los Alamitos, CA: IEEE, 2008: 504-509.

- [4] Kim T-Y, Kim T. Clock tree embedding for 3d ics [C]// Proceedings of the 15th Asia and South Pacific Design Automation Conference. Los Alamitos, CA: IEEE, 2010: 486-491.
- [5] Kim T-Y, Kim T. Clock tree synthesis for TSV-based 3D IC designs [J]. Transactions on Design Automation of Electronic Systems (TODAES), 2011, 16 (4): 21-48.
- [6] Chao T-H, Hsu Y-C, Ho J-M, et al. Zero-skew clock routing with minimum wirelength. [J]. IEEE Transactions on Circuits and Systems, 1992, 39 (11), 799-814.
- [7] Jackson M A B, Srinnivasan A, Kuh E S. Clock routing for high-performance ics. [C]// Proceedings of the 27th Design Automation Conference. [s. l.]: IEEE, 1990, 573-579.

作者简介:

封成冬 男, (1989-), 硕士研究生. 研究方向为集成电路研究.

王琴 女, (1975-), 博士, 副教授. 研究方向为进行集成电路研究.

谢憬 男, (1981-), 博士研究生. 研究方向为进行集成电路研究.

毛志刚 男, (1962-), 博士, 教授. 研究方向为进行集成电路研究.

(上接第97页)

- [10] Moradi A, Poschmann A, Ling S, et al. Pushing the limits: A very compact and a threshold implementation of AES [J]. Eurocrypt 2011, 2011 (6632): 69-85.
- [11] Satoh A, Morioka S, Takano K, et al. A compact rijndael hardware architecture with S-Box optimization [J]. Asiacrypt 2001, 2001 (2248): 239-248.
- [12] P Hamalainen, Alho T, Hannikainen T, et al. Design and Implementation of Low-Area and Low-Power AES Encryption Hardware Core [C]// DSD [s. l.]: IEEE, 2006: 577 - 583.

作者简介:



彭浩 男, (1987-), 硕士. 研究方向为半导体芯片设计与工艺.