一种有效缩减AES算法S盒面积的组合逻辑优化设计

王 沁,梁 静,齐 悦
(北京科技大学信息工程学院,北京 100083)

摘 要: 通过对AES算法S盒构造原理的研究,利用其中仿射变换的系数具有循环移位的周期性特点对电路结构进行改进,提出一种面积优化的AES算法S盒组合逻辑电路设计方法.该方法基于流水线技术,采用倍频复用的电路结构,较传统结构减少了逻辑资源的使用.经过EDA工具综合仿真和实际系统验证,该方法比Wolkerstorfer和Satoh的S盒有限域实现的硬件规模分别缩减了47.53%和41.49%,比Morioka的S盒真值表实现的硬件规模缩减了21.43%.该设计方案已成功用于一种基于FPGA实现的密码专用处理器设计中.

关键词: S盒字节替换;仿射变换;组合逻辑;面积优化
中图分类号: TN918.4 **文献标识码:** A **文章编号:** 0372-2112 (2010) 04-0939-04

The Area Optimized Implementation of S-box in AES Algorithm

WANG Qin, LIANG Jing, QI Yue
(*Information Technology School*, *University of Science & Technology Beijing*, *Beijing* 100083, *China*)

Abstract: Based on the research on S-box constitution algorithm of Advanced Encryption Standard, we use the periodical characteristic of affine transformation in S-box to improve the circuit architecture and propose an area optimized combinational logic S-box implementation of AES. We multiply the circuit frequency and reuse the circuit with the pipeline technology. The synthesis result shows that the new S-box functional unit not only decreases the area of byte substitution compared with traditional S-box combinational logic by 47.53% and 41.49% and with truth table S-box combinational logic by 21.43%, but also maintains the critical delay of the circuit. Using the unit-gate model approximations, the hardware gate count of S-box is 880 gates. And the S-box scheme is applied to the application specific instruction processor for cryptography which is tested on Altera's FPGA Cyclone II EP2C20.

Key words: S-box subbytes; affine transformation; combinational logic; area optimization

1 引言

在无线传感器网络节点、智能卡这样资源受限和电池供电的嵌入式应用中,数据安全和硬件成本是决定性因素.高级加密标准AES因其具有低开销、安全性高、易于硬件实现等特点,被广泛应用于各种嵌入式应用环境中.因此,在存储和计算能力有限的嵌入式特征下,研究如何降低AES算法硬件开销是无线传感器网络安全算法实施的关键.

AES算法加密过程的四种主要运算分别是字节替换(SubBytes)、行移位(ShiftRows)、列混淆(MixColums)、轮密钥加(AddRoundKey)[1].解密过程是四种主要运算的反运算.其中,S盒在字节替换、反向字节替换和密钥扩展三个操作中使用[2],是AES算法中唯一的非线性变换,由于其作用在每一轮加密变换以及密钥扩展模块中,利用率非常高,所以S盒的硬件实现在很大程度上决定着整个AES芯片的性能优劣.

2 相关工作

从实现的角度看,AES的硬件实现效率主要由字节替换决定.通常使用查表法,但是查表法对硬件实现不是一个很有效的方法.AES算法的字节替换和逆字节替换的S盒不同,也就是说加密和解密的时候需要不同的真值表,为了达到高的数据吞吐率,文献[3]中采用并行架构,需要20个正向S盒(16个用于字节替换,4个用于密钥扩展)和16个逆向S盒(16个全部用于反向字节替换),这种硬件实现占用大量的实现空间,增加了芯片的面积,这是查表法S盒硬件实现的致命弱点.

为了降低字节变换实现代价,另一种实现S盒字节替换的方法是使用组合逻辑电路实现.定义S盒是一个建立在状态字节上的砖匠置换,S盒变换 S_{RD} 是用公式 $S_{RD}(x)=f(g(x))$ 构造的,其中 $g(x)$ 表示有限域 $GF(2^8)$ 上的乘法求逆变换,$f(\cdot)$ 是仿射变换,S盒构造函数由这两部分组成.在具体的硬件实现上,有限域 $GF(2^8)$ 上的乘法求逆运算的实现是S盒设计的难点.当前,很多文献围绕在算法层次上如何简化乘法求逆变换的计算复杂度,减少逻辑运算单元使用数量,从而达到减少硬件面积的效果.文献[4~6]中对乘法求逆变换研究工作的共同之处是将 $G(2^8)$ 上的求逆运算转化为低阶上

收稿日期:2009-02-18;修回日期:2009-07-29
基金项目:国家863高技术研究发展计划重点项目"工业无线技术及网络化测控系统研究与开发"(No.2007AA041201)

的求逆运算.例如,文献[4]中 Wolkerstorfer 把一个在有限域 $GF(2^8)$ 上的乘法求逆变换,转换成有限域 $GF((2^4)^2)$ 上的求逆变换,即通过有限域 $GF((2^4)^2)$ 上乘法、乘方、求逆等运算,计算出两个 $GF((2^4)^2)$ 上的 4 比特数,之后重新转换成一个 $GF(2^8)$ 的 8 比特数,完成 S 盒变换 S_{RD} 中的 $g(x)$ 乘法求逆变换,在硬件复杂度方面,其等效于 909 个 NAND2 门.文献[5]中 Satoh 把一个在有限域 $GF(2^8)$ 上的乘法求逆变换,转换成有限域 $GF(((2^2)^2)^2)$ 上的求逆变换,这样可以减少有限域上参与运算的比特位数到 2 位,即减少了求逆电路的运算单元占用面积,在硬件复杂度方面,其等效于 736 个 NAND2 门.上述文献定位于 S 盒的求逆变换的研究,文献[6]则基于整个 S 盒实现考虑,采用布尔函数的方法,得到 S 盒的真值表,再求解 S 盒的布尔函数表达式,用卡诺图简化该表达式后仿真,字节替换等效于 562 个 NAND2 门,反向字节替换等效于 558 个 NAND2 门,S 盒总计需要 1120 个 NAND2 门,组合逻辑的真值表方法与文献[4~6]中的伽罗华域上的复合变换实现方法相比,实现所需的逻辑门数要少,但是关键路径较长.

文献[4~6]的主要贡献是对乘法逆变换逻辑规模的缩减,其中文献[5]中占用门数最少,其乘法逆变换设计最优.而文献[4~6]对仿射变换没有采取优化措施,主要是因为 S 盒变换 S_{RD} 中的仿射变换 $f(\cdot)$ 公式上描述简单,从算法级上考虑降低计算复杂度有限,所以研究基于 S 盒仿射变换的降低芯片逻辑资源的文献并不多见.本文的主要贡献是从电路级上对仿射变换的优化,设计一种仿射电路优化方法,配合文献[5]中最优的逆变换设计,获得比文献[4~6]更小的 S 盒整体硬件面积.本文使用组合逻辑设计方法,研究如何优化仿射变换的硬件结构,设计出一种以降低芯片面积为目标的 S 盒仿射电路优化结构.

3 传统仿射变换的硬件实现

假设加密过程中正向 S 盒仿射变换的表达式为 $f(\alpha)$,解密过程中逆向 S 盒逆仿射变换的表达式为 $f^{-1}(\alpha)$,定义如下式所示[7],其中字节 $\alpha\in GF(2^8)$:

$$f(\alpha)=\begin{bmatrix}11111000\\01111100\\00111110\\00011111\\10001111\\11000111\\11100011\\11110001\end{bmatrix}\times\begin{bmatrix}\alpha_7\\\alpha_6\\\alpha_5\\\alpha_4\\\alpha_3\\\alpha_2\\\alpha_1\\\alpha_0\end{bmatrix}\oplus\begin{bmatrix}0\\1\\1\\0\\0\\0\\1\\1\end{bmatrix}$$

$$f^{-1}(\alpha)=\begin{bmatrix}01010010\\00101001\\10010100\\01001010\\00100101\\10010010\\01001001\\10100100\end{bmatrix}\times\begin{bmatrix}\alpha_7\\\alpha_6\\\alpha_5\\\alpha_4\\\alpha_3\\\alpha_2\\\alpha_1\\\alpha_0\end{bmatrix}\oplus\begin{bmatrix}0\\0\\0\\0\\0\\1\\0\\1\end{bmatrix}$$

通过分析发现,系数矩阵行向量分别循环右移一位后得到系数矩阵下一行的值,如此依次变换,针对系数的状态转移规律,仿射变换可以表示为系数矩阵行变量“与”上 α“异或”常量后得到的值.根据数学公式发现可以将仿射变换和逆仿射变换合二为一,使用同一套电路结构实现 AES 加密 S 盒和解密 S 盒的重构[8],缩减仿射电路的总面积.

仿射变换电路最简单的硬件实现方法如图 1 所式,用 8 个乘法器组成一个乘法器阵列,保证在每个采样时钟周期内完成 8 次乘运算,然后将计算结果进行求和运算.但是,串行计算每次只能得到输出字节中一位的数值,运算时间过长,不符合实际加密处理的要求.

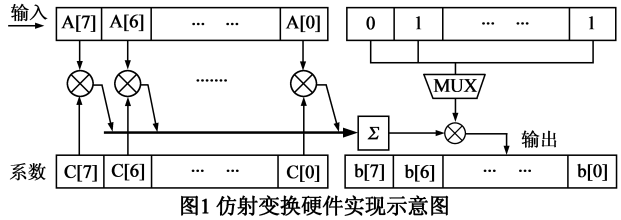


图1 仿射变换硬件实现示意图

为达到大数据量运算的要求,通常采用复用硬件的数据并行计算方法,即以缓冲写入频率为采样频率,从输入数据缓冲区中读入字节 A,送到多个并行乘法器阵列和加法器阵列,由每个累加器计算得出一位数值结果,将 8 组结构相同的乘法器和加法器阵列并行处理结果存储为一个字节的输出.采用流水线的传统仿射运算电路结构如图 2 所示.电路包括数据输入存储模块,数据处理模块和数据输出模块.

数据输入存储模块以采样时钟频率写入数据,数据采用存储单元循环覆盖方式写入,读取数据必须按周期地址循环读取,当 AES 算法处理 128 位数据分组时,共划分为 16 个字节,按地址从高到低写入缓冲区,下一个新的分组的 16 个字节以覆盖方式写入到上一个已完成仿射变换的 16 字节分组所在位置.数据输出模块以缓冲区数据写入频率为参照标准,给出仿射变换结果.数据处理模块包括数据选通器、乘法器阵列、加法器阵列和累加器.该方法的优点是控制逻辑简单,利于数据流水线处理,缺点是硬件规模大,为了达到提高数据吞吐率的目的,依靠并行处理的逻辑硬件单元体系结

构,复制了多个组合逻辑处理模块,增加了芯片面积.

4　改进仿射变换的硬件实现

针对上述实现方案的缺点,本节主要针对传统仿射变换体系结构进行改进,改进的仿射变换硬件结构主要是将矩阵乘法中 8 个系数的 8 轮乘累加计算,由并行 8 组乘累加阵列重复计算转为使用串行 1 组乘累加阵列倍频计算得到,达到缩减电路规模的目的.通过对仿射变换矩阵系数规律的分析,利用系数向量循环右移的周期性特点,调整数据运算顺序结构,提高内部处理电路的时钟频率,加快局部电路复用,提高数据处理能力;并结合流水线数据处理通路,简化控制逻辑,达到面积优化的效果.

数据流在经过逆变换和仿射变换模块时是由时钟同步控制,流水线不需要阻塞控制,逆变换模块在系统全局时钟的触发下,经过一个周期产生一个字节送到仿射模块输入端.而在仿射变换模块中,流水线划分为 4 级,内部时钟是外部全局时钟的 8 倍,内部倍频是为了新的电路达到原来并行电路的吞吐率,同时,各级流水线保持同步触发,不需要在逆变换和仿射变换之间设置数据缓冲器.

S 盒替换中改进的仿射变换模块结构如图 3 中所示,对比传统结构匹配滤波捕获电路,从体系结构上做了以下改进:

(1)整个数据处理过程以流水线方式完成.定义每个时钟上升沿时数据选通进入流水线.其中,在第 1 级流水,选通采样数据缓冲区的一个字节,该采样数据是前述逆变换电路的输出结果;在第 2 级流水,数据处理时钟的上升沿触发,在本地系数寄存器中,右循环移位 1 次后,与采样数据缓冲区中的数值按位相与,经过第 3 级流水的加法器阵列,计算出 *S* 盒替换后的字节.

(2)选通数据与对应系数 *A*[7:0]按位做“与”操作,等效于传统结构中乘法操作,简化了逻辑门数.并且在传统仿射电路中,需要 8 组相同的乘法器和加法器阵列,改进后加法器阵列规模与改进前相同,而整个模块只用 8 个与门,经复用完成所有的乘法运算,降低了乘法器使用的个数.

(3)传统仿射变换处理数据流量恒定,改进后则可以根据数据处理时钟频率调整倍频系数,改变流水线流量.

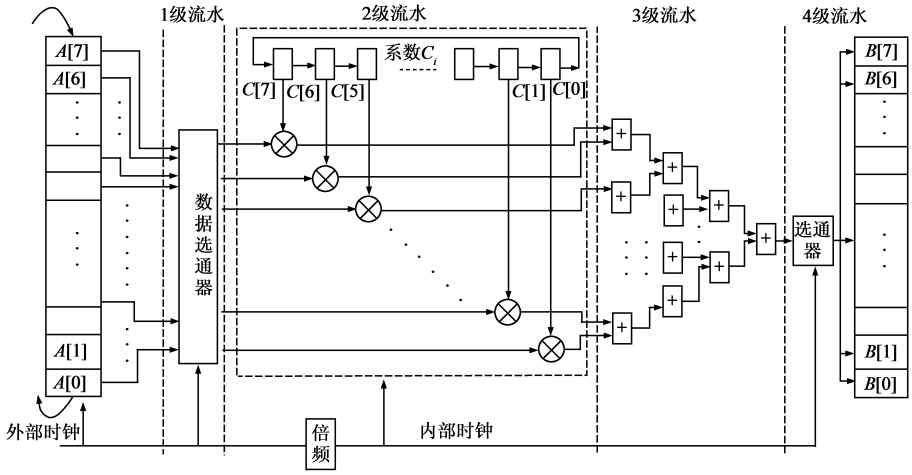


图3　采用流水线的改进仿射运算电路结构

5　仿真测试

S 盒的等效门数为乘法求逆变换和仿射变换门数之和,用硬件描述语言(HDL)进行描述,经 ModelSim 功能仿真正确后,采用 UMC 0.13um 1.8V 工艺库,用 Synopsys Design Compiler 工具进行综合,得到传统仿射变换的硬件规模是 768 个门,改进后仿射变换的硬件规模是 144 个门,优化比值为 81.25%.经仿真测试,对求逆变换和仿射变换的硬件电路中的触发器和逻辑门电路进行统计,共需要约 880 个门电路.而文献[4,5]中的求逆变换分别为 909 门和 736 门,与传统仿射变换 768 个门相加,两种变换一起配合使用的 *S* 盒电路分别需要

表 1　*S* 盒组合逻辑方法之间的面积比较

	乘法求逆变换		仿射变换		整体 S 盒实现	
	门数	优化比值	门数	优化比值	门数	优化比值
Wolkerstorfer 设计的 S 盒组合逻辑法[4]	909	19.03%	768	81.25%	1677	47.53%
Satoh 设计的 S 盒组合逻辑法[5]	736	–	768	81.25%	1504	41.49%
Morioka 设计的真值表组合逻辑法[6]	–	–	–	–	1120	21.43%
本文设计的 S 盒组合逻辑法	736	–	144	–	880	–

1677 和 1504 个门电路,本文设计的 S 盒组合逻辑电路比文献[4,5]的 S 盒硬件规模分别缩减了 47.53% 和 41.49%.文献[6]中根据真值表化简组合逻辑实现的整体 S 盒电路为 1120 门,本文设计的 S 盒组合逻辑电路比文献[6]的 S 盒硬件规模缩减了 21.43%,各种 S 盒组合逻辑方法之间的面积比较如表 1 所示.

6 结论

本文提出一种改进的组合逻辑实现的 S 盒替换功能单元方法,仅需要约 880 个门电路即可完成 S 盒的逆变换和仿射变换,采用改进的流水线复用结构实现硬件电路,在不增加时延的条件下,与文献[4,5]中使用传统仿射电路实现的基于有限域 S 盒组合逻辑相比较,在面积上减少了 47.53% 和 41.49%,与文献[6]中使用真值表实现的 S 盒组合逻辑相比较,在面积上减少了 21.43%,带来整个 S 盒硬件资源开销的降低.下一步将把 S 盒专用功能部件应用到其他常用密码算法中,测试硬件面积优化的效果.

参考文献:

[1] Daemen J,Rijmen V.高级加密标准(AES)算法-Rijndael 的设计[M].谷大武,徐胜波,译.北京:清华大学出版社,2003.

[2] Vincent Rijmen,Efficient implementation of the rijndael S-Box [R],2000.

[3] Hua Li.A parallel S-box architecture for AES byte substitution [A].2004 International Conference on Communications,Circuits and Systems[C].New York:IEEE Press,2004.1 – 3.

[4] Wolkerstorfer J,Oswald E,Lamberger M.An ASIC implementation of the AES S-boxes[C].ASIA-CRYPT2001.Heidelberg:Springer-Verlag.2001.239 – 254.

[5] Morioka S,Satoh A.An optimized S-box circuit architecture for low power AES design[C].Proceeding of Workshop of Cryptographic Hardware and Embedded System(CHES2002).San Francisco.USA:Springer-Verlag,2003.172 – 186.

[6] A Satoh,S Morioka.Hardware-focused Performance comparison for the Standard Block Ciphers AES,Camellia,and Triple-DES,Lecture Notes in Computer Science,Vol.2851,Springer 2003,pp.252 – 266,2003.

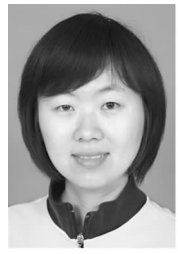
[7] 肖国镇,白恩健,刘晓娟.AES 密码分析的若干新进展[J].电子学报,2003,31(10):1549 – 1554.
Guozhen Xiao,Enjian Bai,Xiaojuan Liu.Some New Developments on the Cryptanalysis of AES[J].Acta Electronica Sinica,2003,31(10):1549 – 1554.(in Chinese)

[8] 高娜娜,李占才,王沁.一种可重构体系结构用于高速实现 DES、3DES 和 AES[J].电子学报,2006,34 (08):1386 – 1390.
Nana Gao,Zhancai Li,Qin Wang.A Reconfigurable Architecture for High-Speed Implementations of DES,3DES and AES [J].Acta Electronica Sinica,2006,34(08):1386 – 1390.(in Chinese)

[9] Atri Rudra,Pradeep K.Dubey,Charanjit S.Jutla.Efficient Rijndael Encryption Implementation with Composite Field Arithmetic[A].Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems[C].London:Springer-Verlag,2001.171 – 184.

作者简介:

王 沁 北京科技大学教授,博士生导师,主要研究方向为无线传感器网络、计算机体系结构、VLSI 和 SOC.



梁 静(通信作者) 女,1982 年 6 月生于北京,现为北京科技大学计算机应用专业博士研究生,研究方向:集成电路设计和嵌入式技术.
E-mail:liangjingjing826@163.com

齐 悦 北京科技大学讲师,博士,主要研究方向为集成电路设计、计算机体系结构、VLSI 和 SOC.