防御零值功耗攻击的 AES SubByte 模块设计及其 VLSI 实现

汪鹏君,郝李鹏,张跃军
(宁波大学电路与系统研究所,浙江宁波 315211)

摘 要: 密码器件在执行高级加密标准(Advanced Encryption Standard,AES)时常以能量消耗方式泄漏密钥信息,为有效降低其与实际处理数据之间的相关性,该文提出一种具有防御零值功耗攻击性能的 AES SubByte 模块设计及其 VLSI 实现方案.首先,在分析 GF(256)域求逆算法的基础上,采用关键模块复用的方法,提出一种更为有效的加法性屏蔽求逆算法;然后依此进一步得到一种新型的 SubByte 模块结构,实现在不影响对所有中间数据进行加法性屏蔽编码的同时,减少电路的芯片开销、提高电路的工作速度.实验结果表明,所设计的电路具有正确的逻辑功能.与传统 SubByte 模块比较,该设计的最高工作频率和面积都有较大的优化.

关键词: SubByte 模块; 零值功耗攻击; 差分功耗攻击; 加法性屏蔽; 高级加密标准
中图分类号: TN918.4 **文献标识码:** A **文章编号:** 0372-2112 (2012)11-2183-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.11.007

Design of AES SubByte Module of Anti-Zero Value Power Attack and Its VLSI Implementation

WANG Peng-jun, HAO Li-peng, ZHANG Yue-jun
(*Institute of Circuits and Systems, Ningbo University, Ningbo, Zhejiang* 315211, *China*)

Abstract: The secret information of cipherware leaks as energy consumption during AES implementation. To reduce the correlation between the secret information and the processing data effectively, this paper investigate a design of AES SubByte module of anti-zero value power attack and its VLSI implementation. First, by analyzing the traditional GF(256) inversion algorithm, an improved additive masking GF(256) inversion algorithm which adopts key module reuse method is proposed. Then a novel SubByte module structure is constructed by applying such algorithm, which has significant area and speed improvement and all data can be additive masked. The experimental results show that the novel scheme has correct logic function. Compared with traditional SubByte module, a remarkable improvement is achieved by the proposed approach on highest working frequency and area.

Key words: SubByte Module; zero-value power attack; differential power analysis(DPA); additive mask; advanced encryption standard(AES)

1 引言

差分功耗攻击(Differential Power Analysis,DPA)是一种高效、低成本的密码分析方法,对密码器件安全构成重大威胁[1~4].为防御差分功耗攻击,近年来人们采用乘法性屏蔽技术[5],在加密过程中引入与实际处理数据不相关的另一个变量,从而使得密码器件泄漏的功耗信息与实际处理数据相关性大大降低,以牺牲芯片开销和速度为代价,实现防御差分功耗攻击的目的.然而,以往改进的高级加密标准(Advanced Encryption Standard,AES)实现并不能抵御零值功耗攻击[6],另外随着具有认证和保密能力的便携式设备的普遍应用,面积和速度越来越成为安全芯片设计的挑战.因此,高速、低芯片开销的抗零值功耗攻击电路设计已受到学术界的普遍重视.SubByte 模块是 AES 中唯一的非线性转换结构,其实现方式决定 AES 协处理器诸如面积、速度和功耗等方面的性能,成为差分功耗攻击和零值功耗攻击的主要对象[7],提高 SubByte 模块防护密码分析的能力对 AES 的安全性具有重要意义.以前也有文献提出过具有抗差分功耗攻击以及抗零值功耗攻击性能的 SubByte 结构[8~10],但

收稿日期:2011-10-20;修回日期:2012-02-28
基金项目:国家自然科学基金(No.61274132;No.61076032);博士点基金(No.20113305110005);浙江省重点科技创新团队项目(No.2011R09021-04);浙江省大学生科技新创活动计划(新苗人才计划)项目资助课题

是其芯片面积开销较大.鉴此,在文献[8]和文献[10]研究的基础上,使用关键模块复用的策略,首先提出一种改进型 GF(256)域加法性屏蔽求逆算法;然后依此进一步提出一种新型 SubByte 模块结构,实现对所有中间数据加法性屏蔽编码的同时,减少芯片的面积并提高电路的工作速度.SMIC 0.13μm 标准 CMOS 工艺下,Synopsys Design Compiler 综合验证表明,该结构不仅具有良好的抗零值功耗攻击和抗差分功耗攻击性能,面积开销和电路速度更为合理.

2 零值功耗攻击原理及其防御措施

为了防御差分功耗攻击,近年来人们采用乘法性屏蔽技术改进 GF(256)域求逆算法,如图 1 所示,进而提出一种改进型 AES 算法[5].然而实践证明 GF(256)域乘法性屏蔽求逆算法存在安全漏洞,不能防御零值功耗攻击[6].零值功耗攻击就是利用全零字节经乘法性屏蔽模块运算产生的功耗与其他输入条件下的功耗存在显著差异的特点,采用差分功耗攻击的策略,获取加密算法密钥的密码分析技术[10].以图 1 所示 GF(256)域乘法性屏蔽求逆算法结构为例,输入字节 $\mathrm{in}+X=p\oplus k\oplus X$,其中 p 和 k 分别为 AES 算法每一轮运算中对应的输入数据和密钥,X 为随机数,若 $p=k$,那么有:

$$p=k\Rightarrow \mathrm{in}=0\Rightarrow(\mathrm{in}+X)*Y+X*Y=0$$
$$\Rightarrow(\mathrm{in}*Y)^{-1}=0 \tag{1}$$

由此得到的功耗与 $p\neq k$ 条件下功耗有明显差异,攻击者仅需使用差分功耗攻击的策略从所有可能明文中找出满足 $p=k$ 的明文,即可分析出加密算法密钥中一个字节,进而破解算法的全部密钥.

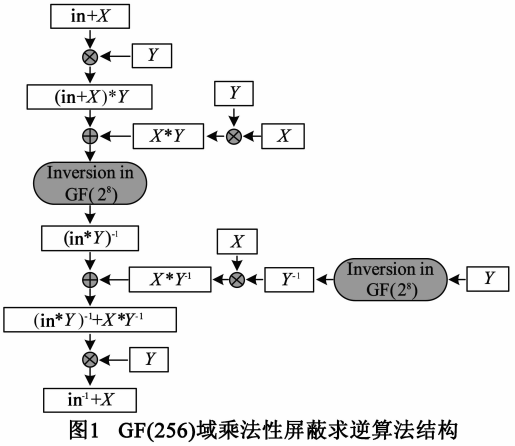


图1 GF(256)域乘法性屏蔽求逆算法结构

为了防御零值功耗攻击,Oswald 等人结合加法性和乘法性屏蔽技术,提出一种新型 GF(256)域求逆算法[8].具体过程如下:

设 GF(256)域的数据 y 可用 GF(16)域的线性多项式 a_hx+a_l 表示,其中 $a_h,a_l\in$GF(16),则:

$$y^{-1}=(a_hx+a_l)^{-1}=a_h'x+a_l' \tag{2}$$

其中:

$$a_h'=a_h\times d' \tag{3}$$
$$a_l'=(a_h+a_l)\times d' \tag{4}$$
$$d=(a_h^2\times p_0)+(a_h\times a_l)+a_l^2 \tag{5}$$
$$d'=d^{-1} \tag{6}$$

其中 p_0 根据从 GF(256)域映射到 GF(16)域生成多项式的不同而选取.

在加法性屏蔽 GF(256)域求逆算法中,操作数是 $y+mask$,其中 $mask$ 为屏蔽因子.操作数映射到 GF(16)域可表示为 $(a_h+m_h)x+(a_l+m_l)$,其中 m_h 和 m_l 为 $mask$ 在 GF(16)域内线性多项式的系数.该 GF(256)域加法性屏蔽求逆算法过程如下所示:

$$((a_h+m_h)x+(a_l+m_l))^{-1}=(a_h'+m_h)x+(a_l'+m_l) \tag{7}$$
$$a_h'+m_h=(a_h+m_h)(d'+m_l)+(d'+m_l)m_h+(a_h+m_h)m_l+m_h\times m_l+m_h \tag{8}$$
$$a_l'+m_l=(a_h\times d'+m_h)+(d'+m_h)(a_l+m_l)+(d'+m_h)m_l+(a_l+m_l)m_h+m_l\times m_h+m_l+m_h \tag{9}$$
$$d+m_h=(a_h+m_h)^2\times p_0+m_h^2\times p_0+(a_h+m_h)(a_l+m_l)+(a_l+m_l)^2+(a_h+m_h)m_l+(a_l+m_l)m_h+m_l\times m_h+m_l^2+m_h \tag{10}$$

其中 $d'+m_l=d^{-1}+m_l$,可以通过 GF(16)域加法性屏蔽求逆算法得到,计算过程与式(8)~式(10)类同,唯一区别在于 GF(4)域的求逆算法等价于该域的平方运算,即 $(d_1+m)^{-1}=(d_1+m)^2=d_1^2+m^2$,其中 $d_1,m\in$GF(4).

3 改进型 GF(256)域求逆算法

由于上述 GF(256)域求逆算法需要对运算过程中所有数据进行加法性屏蔽,因而其计算复杂度巨大.由式(8)~式(10)可知,基于 GF(256)域求逆算法的计算复杂度主要集中在 GF(16)域的乘法运算,文献[10]提出的改进算法通过减少 GF(16)域乘法运算的次数,以增加一个平方运算的代价,达到减小面积和计算复杂度的目的,然而效果并不明显.

通过对文献[8]和[10]提出的 GF(256)域求逆算法的研究,采用关键模块复用的方法,在满足所有数据均被屏蔽的前提下,提出一种改进型加法性屏蔽求逆算法,如下所示:

$$a_h'+m_h=(a_h+m_h)(d'+m_h)+(d'+m_h)m_h+(a_h+m_h)m_h+m_h^2+m_h \tag{11}$$
$$a_l'+m_l=(a_h+m_h)(d'+m_h)+(d'+m_l)(a_l+m_h)+(a_l+m_h)m_l+(a_h+m_h)m_h+m_l \tag{12}$$
$$d+m_l=(a_h+m_h)^2\times p_0+m_h^2\times p_0+(a_h+m_l)(a_l+m_h)$$

$$+(a_l+m_h)^2+(a_l+m_h)m_h+(a_l+m_h)m_l+m_l \tag{13}$$

对比式(11)~式(13)和式(8)~式(10)可知,改进型 GF(256)域求逆算法在保证对所有中间数据加法性屏蔽的同时,将 GF(16)域乘法模块的数量由 8 个减少至 6 个.表 1 给出了不同 GF(256)域求逆算法的芯片开销,与文献[10]相比,改进型算法的乘法模块数量由 7 个减少到 6 个,平方模块由 3 个减少到 2 个.由于 GF(16)域乘法模块和 GF(16)域平方模块在 GF(256)域求逆算法的硬件实现中占主要部分,因此乘法模块和平方模块数量的减少,使得整个密码器件的芯片开销显著减小,系统实现复杂度明显降低.

表 1　不同 GF(256)域求逆算法的芯片面积开销

	文献[8]	文献[10]	本文
乘法模块	8	7	6
平方模块	2	3	2
先平方、再与常数相乘的模块	2	2	2

4　改进型 GF(256)域求逆算法硬件架构

式(11)~式(13)对应改进型 GF(256)域求逆算法的结构框图如图 2 所示,其中⊗为 GF(16)域的乘法模块;X^2 为 GF(16)域平方模块;$X^2\times p_0$ 为 GF(16)域内首先进行平方操作然后与常数 p_0 相乘的模块;⊕为 GF(16)域的加法模块;Inversion in GF(16)为 GF(16)域的求逆模块,其结构与图 2 类同,唯一不同的在于 GF(4)域求逆过程等价于 GF(4)域的平方运算,可通过图 3 所示的结构得到.

从图 2 可以看出,与文献[10]的改进算法结构相比,所提出的 GF(256)域求逆算法结构中可复用乘法模块保持为 2 个,同时减少 1 个平方模块和一个乘法模块.由于 128 位 AES 算法中包括 16 个 GF(256)域求逆模块,因此改进算法带来的芯片面积开销减少是相当可观的.另外由于采用并行计算以及插入加法模块的方式,与文献[10]中求逆算法结构相比,图 2 所示结构具有两方面优点:一方面,由于并行计算以及关键模块复用策略的应用,电路关键路径上的模块数量由 15 个减少到 10 个,工作速度明显加快;另外一方面,通过调整加法模块的位置,在节点 $d'+m_l$ 到节点 $a_l'+m_l$ 计算过程中增加一个二输入加法模块(图中右上方的数字 4),从而节点 $d'+m_l$ 到电路输出两端均需经过五步操作(图中数字 1-5 代表不同计算模块),电路的两个输出信号实现基本同步.采用 SMIC 0.13μm 标准 CMOS 工艺,综合结果表明,该算法与文献[10]比较面积节省约 12.9%,速度提高 10.4%,因此本设计更加适用对芯片面积和工作速度要求严格的便携式设备.

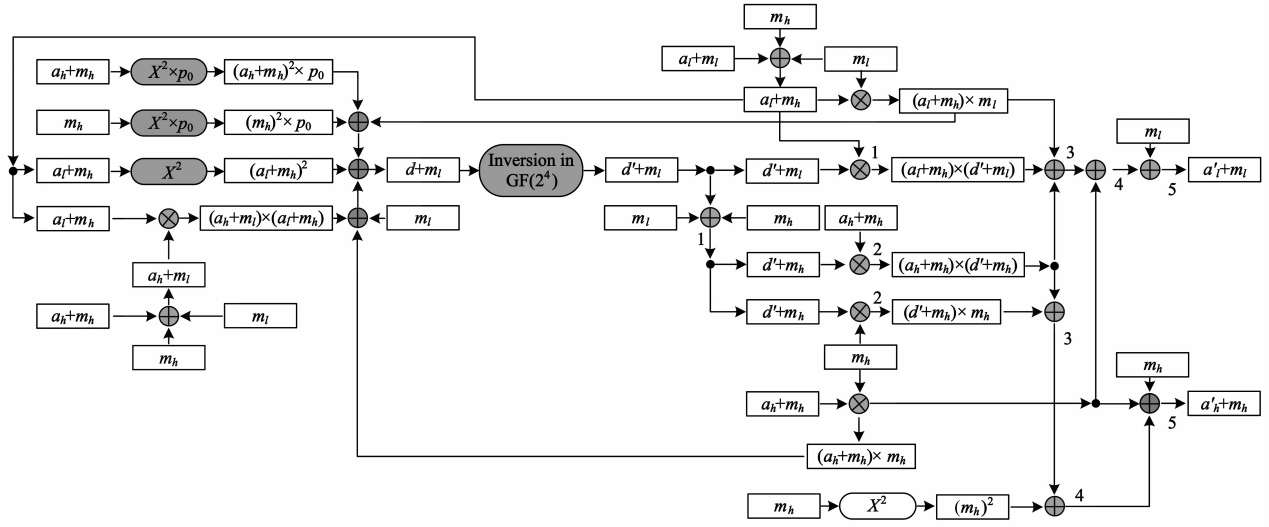


图2　改进型GF(256)域求逆算法结构

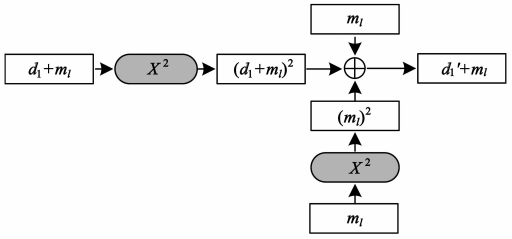


图3　GF(4)域求逆模块结构

5　防御零值功耗攻击 SubByte 模块的 VLSI 实现

通过对上述改进型 GF(256)域求逆算法硬件结构的研究,根据 SubByte 模块的工作特点,提出一种防御零值功耗攻击的 SubByte 模块设计,其结构框图如图 4 所示.它包括三个部分:改进型 GF(256)域求逆算法部分、仿射变换线性部分以及 mask 屏蔽模块.

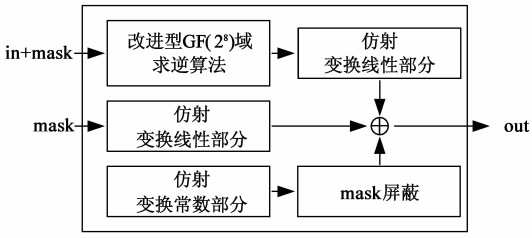


图4 防御零值功耗攻击的SubByte模块设计

其中 in 为输入字节,mask 为屏蔽因子,out 为输出字节,mask 屏蔽模块完成仿射变换中常数部分(63H)与屏蔽因子 mask 的异或操作,保证 SubByte 模块中间数据始终处于加法性屏蔽的要求.

在不同输入条件下,对上述所设计 SubByte 模块进行计算机模拟,模拟结果如表 2 所示.

表 2 防御零值功耗攻击的 SubByte 模块模拟结果

in	mask	SubByte(in)	SubByte(in) + mask	out
35	5	38	43	43
53	98	150	248	248
71	40	160	200	200
51	102	195	42	42
255	48	22	70	70

其中,SubByte(in)为输入字节 in 经 SubByte 模块操作后的理论值.从表 2 中可以看出,所设计 SubByte 模块的输出字节与相同输入条件下的理论值相同.经分析,证明所设计电路逻辑功能正确.

采用 SMIC 0.13μm 标准 CMOS 工艺,所设计 AES SubByte 模块最高工作频率可达 223.2MHZ,占用面积约为 $9.49\times10^{-3}mm^2$,不含随机数发生器.

将所设计的 SubByte 模块与传统 SubByte 模块[5,10,11]进行比较,经 Synopsys Design Compiler 在相同 CMOS 工艺下对不同设计进行综合验证,实验结果如表 3 所示.

表 3 不同 AES SubByte 模块比较

	文献[5]	文献[10]	文献[11]	本文
工艺/μm	0.13	0.13	0.13	0.13
频率/MHz	191.9	211.9	202.0	223.2
面积/$10^{-3}mm^2$	21.81	10.79	16.36	9.49
防御零值功耗攻击	否	是	否	是

由表 3 可知,该设计在芯片开销减少明显,最高工作频率增加显著的前提下,有效防御乘法性屏蔽设计无法实现的零值功耗攻击;与文献[10]中 SubByte 模块相比,在保持防御零值功耗攻击性能的同时,由于计算量大大减少,所提出的结构更加简单,系统最高频率和面积都有较大的优化.

6 结论

零值功耗攻击在实际中高效可行,对信息传输的安全性提出了更高要求,利用加法性屏蔽技术改进高级加密标准是一条有效途径.在分析传统改进型高级加密标准的基础上,采用关键模块复用技术提出一种硬件效率更高的 GF(256)域加法性屏蔽求逆算法,并在此基础上设计了一种新型的 SubByte 模块.实验结果表明,该算法具有抗零值功耗攻击的性能,同时面积开销和电路速度更合理,可广泛应用于协处理器等对面积、速度以及安全性等方面都有严格要求的领域.

参考文献

[1] 陈开颜,张鹏,邓高明,等.物理可观测下 DES 的安全性研究[J].电子学报,2009,37(11):2389 – 2395.
Chen K Y, Zhang P. Research on the DES Physical Observable Security[J]. Acta Electronica Sinica, 2009, 37(11): 2389 – 2395. (in Chinese)

[2] 臧玉亮,韩文报.线性反馈移位寄存器的差分能量攻击[J].电子与信息学报,2009,31(10):2406 – 2410.
Zang Yu-liang, Han Wen-bao. Differential power attack on liner feedback shift register[J]. Journal of Electronics and Information Technology, 2009, 31(10): 2406 – 2410. (in Chinese)

[3] Alioto M, Poli M, Rocchi S. A general power model of differential power analysis attacks to static logic circuits[J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2010, 18(5): 711 – 724.

[4] Wu K, Li H, Yu F. Retrieving lost efficiency of scalar multiplications for resisting against side-channel attacks [J]. Journal of computers, 2010, 5(12): 1878 – 1884.

[5] Akkar M L, Giraud C. An implementation of DES and AES, secure against some attacks[A]. Proceed of the 3rd International Workshop on Cryptographic Hardware and Embedded Systems[C]. Paris: 2001. 309 – 318.

[6] Golic J D, Tymen C. Multiplicative masking and power analysis of AES[A]. Proceed of the 4th International Workshop on Cryptographic Hardware and Embedded Systems[C]. Cologne: 2003. 198 – 212.

[7] Ors S B, Gurkaynak F, Oswald E, et al. Power analysis attack on an ASIC AES implementation[A]. Proceed of International Conference on Information Technology: Coding and Computing [C]. Las Vegas: 2004. 546 – 552.

[8] Oswald E, Mangard S, Pramstaller. A side channel analysis resistant description of the AES s-box[A]. Proceed of the 12th Annual Fast Software Encryption Workshop[C]. Paris: 2005. 413 – 423.

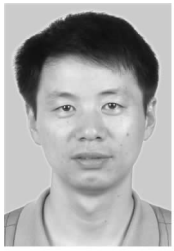
[9] 韩军,曾晓洋,赵佳.抗差分功耗分析和差分故障分析的 AES 算法 VLSI 设计与实现[J].通信学报,2010,31(1):20 – 29.
Han J, Zeng X Y, Zhao J. VLSI implementation of AES algorithm against differential power attack and differential fault at-

tack[J]. Journal on Communications, 2010, 31(1): 20 – 29. (in Chinese)

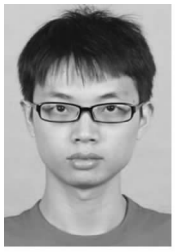
[10] 赵佳,曾晓洋,韩军,等.简化的抗零值功耗分析的 AES 算法及其 VLSI 实现[J].计算机工程,2007,33(16):220 – 222,233.
Zhao J, Zeng X Y, Han J, et al. Simplified AES algorithm of resistant to zero-value power analysis and its VLSI implementation[J]. Computer Engineering, 2007, 33(16): 220 – 222, 233. (in Chinese)

[11] Trichina E, Seta D, Germani L. Simplified adaptive multiplicative masking for AES[A]. Proceed of the 4th International Workshop on Cryptographic Hardware and Embedded Systems[C]. Cologne: 2003: 187 – 197.

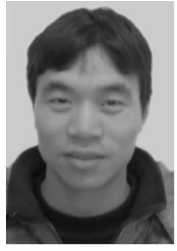
作者简介



汪鹏君　男,1966 年出生于浙江奉化,博士,教授,博士生导师,中国电子学会高级会员,中国计算机学会高级会员,中国电子学会电子线路与系统专业委员会委员,中国计算机学会多值逻辑与模糊逻辑专业委员会委员,目前主要从事多值逻辑电路和低功耗集成电路理论及设计方面的研究工作.
E-mail: wangpengjun@nbu.edu.cn



郝李鹏　男,1987 年出生于安徽安庆,硕士研究生,主要从事低功耗与高信息密度集成电路设计方面的研究工作.



张跃军　男,1982 年出生于浙江台州,博士研究生,主要从事低功耗与高信息密度集成电路设计、防御 DPA 攻击 VLSI 设计方面的研究工作.