

基于功耗感知隐藏技术的 SM4 算法 S 盒的实现

杨超群¹, 殷树娟¹, 李翔宇²

(1 北京信息科技大学 理学院, 北京 100192; 2 清华大学 微电子所, 北京 100084)

摘 要: 功耗感知隐藏技术(PAH)是一种低功耗的抗功耗攻击方法,用于 AES 算法的 S 盒保护显示了安全性和能量效率上的优势. SM4 是我国自主设计的专用分组密码算法,在芯片实现中同样需要进行侧信道攻击防护. 本文采用 PAH 技术,设计实现了 SM4 算法的 S 盒,设计了适用于 SM4 算法的补偿方案,并给出了自动化设计实现流程,将 PAH 技术推广应用到了 SM4 算法的 S 盒,版图后仿真结果表明所实现的 SM4 S 盒相对于其它方法功耗延时积降低了 76%,安全性达到与 AES S 盒电路相近的效果,证明了 PAH 方法的通用性.

关键词: SM4 算法; S 盒; PAH 技术; 补偿方案; 自动化设计实现流程

中图分类号: TN492

文献标识码: A

文章编号: 1000-7180(2018)06-0056-04

Implementation of SM4 Algorithm S-box Based on Power-aware Hiding Method

YANG Chao-qun¹, YIN Shu-juan¹, LI Xiang-yu²

(1 School of Applied Science, Beijing Information Science & Technology University, Beijing 100192, China;

2 Institute of Microelectronics, Tsinghua University, Beijing 100084, China)

Abstract: Power-aware hiding (PAH) is a low power and anti-power-analysis method. It shows the advantages in terms of security and energy efficiency when used for S box protection of AES algorithm. SM4 is a special block cipher algorithm designed independently in our country, and the protection of side channel attacks is also needed in the implementation of the chip. In this paper, the S box of SM4 algorithm is designed and implemented by using PAH method. The compensation scheme for SM4 algorithm is designed and the design flow of automation is given. The PAH technology is extended to the S-box of SM4 algorithm. The post-layout simulation results show that the power delay product of the implemented SM4 S box is 76% lower than other methods. And the security is similar to that of the AES S-box circuit. The generality of the PAH method is proved.

Key words: SM4 block cipher algorithm; S-box; PAH method; compensation scheme; automation design and implementation process

1 引言

在过去的几年里,侧信道攻击^[1]已经被证明是非常有效地作为攻击密码算法实现的一种实用手段. 攻击者可以从侧信道,如操作功耗、电磁辐射,获得密码芯片执行的加密算法的中间结果特征,并破解密钥. 相应的,一系列抵御攻击的对策被提出. 在众多功耗攻击对策中,马江莎等人提出的功耗感知

隐藏(Power-aware hiding, PAH)技术^[2],被应用于非线性操作(如 S 盒)时,具有低功耗的优点,更加适用于物联网等低功耗应用,而且相比于传统的功耗平衡技术,功耗平衡效果更好,是一种重要的防护技术. 但是,文献[2]中仅将 PAH 技术用于 AES 算法的 S 盒,存在局限性.

SM4 算法是我国自主设计的商用密码算法,广泛用于极敏感的内部信息、行政事务信息和经济信

息等的保护. 在我国, SM4 算法的防护技术研究比 AES 更具实用价值^[3].

因此,本文对功耗感知隐藏技术在 SM4 分组密码算法的 S 盒上的适用性进行研究,研究实现的可行性和电路的性能与安全性. 同时,介绍了 PAH 技术自动化设计流程的具体实现方法.

表 1 PAH 设计规则^[2]

原始 N 位 输出 HW	实际 N 位输出	标记位	$N/2$ 位补偿 输出 HW	总输出 HW
$h \leq N/2$	原始输出	0	$N/2-h$	$N/2$
$h > N/2$	原始输出取反	1	$h-N/2-1$	$N/2$

2 功耗感知隐藏技术

功耗感知隐藏技术适用于分组密码算法的非线性运算 S 盒,其基本思想是根据运算电路的输入输出预先计算出电路的翻转功耗,然后通过数据编码和补偿适当功耗相结合的方式实现功耗平衡效果,使得最终平衡的功耗等于一个预设值,该值理论上只有原始设计电路峰值功耗的一半.

ASIC 实现中操作的功耗大致上与寄存器数据的汉明距离 (Hamming Distance, HD)成正比,保持固定的汉明距离是功耗平衡的主要方面. 功耗感知隐藏技术通过补偿平衡输出数据的汉明重量 (Hamming Weight, HW)和在两个连续状态的有效数值之间插入间隔态,即对寄存器进行预充电的方式来实现固定的输出汉明距离.

表 1 是功耗感知隐藏技术的设计规则^[2],该方法假设一个运算原始的输出是 N 位的,如果原始输出的汉明重量 h 不大于输出位数的一半即 $N/2$ 时,实际输出就等于原始输出;而当原始输出的汉明重量 h 大于 $N/2$ 时,实际输出的值等于原始输出取反,这种设计规则的一个直接结果是实际输出的汉明重量总会小于 $N/2$. 为了得到运算的原始输出,该方法增加了一个标记位 f . 额外增加的 $N/2$ 个补偿位是将整体实际输出的汉明重量固定为 $N/2$.

文献[2]中给出了 AES S 盒的电路,通过规则的与门和或门阵列来实现电路,在整个电路中,与门阵列负责计算所有 256 个最小项,或门阵列负责将相应的最小项做和,得到最终的输出. 电路采用动态逻辑,所以,或门阵列包含一个 13×256 的 NMOS 阵列,每一列 NMOS 管的栅极连接同一个最小项,每一行并联的 NMOS 管组成一个或门的下拉网络,对应一个输出. 每一个输出信号由或门阵列中那些漏极接在输出节点上的晶体管决定,其余 NMOS 管

的漏极均接地. 整个电路很对称,有助于保证每个基本电路结构具有相同的寄生参数,从而实现高度的功耗平衡.

3 PAH 技术实现 SM4 算法 S 盒

SM4 算法是一种商用无线局域网分组密码算法^[3], SM4 同其他分组对称密码算法一样包含 S 盒运算. S 盒通过参与每一轮的加解密运算和密钥扩展,极大程度上影响着密码算法的性能. S 盒的防御也是安全防护工作的重点,所以,将功耗感知隐藏技术应用于 SM4 分组密码算法的 S 盒能够有效降低电路的功耗、提高芯片安全性.

根据 PAH 的设计原则,对于 SM4 算法的 S 盒,原始输出是 8 位的,其汉明重量可以通过查 S 盒置换表得到,分为 0 到 8 共 9 种情况. 当原始输出的汉明重量小于等于 4 时,实际输出的值即为原始输出,此时, $f=“0”$;而当原始输出的汉明重量大于 4 时,实际输出值为原始输出取反,此时, $f=“1”$. 实际的 8 位输出 Out[0:7]会限定在 0 到 4 内,加上标记位和 4 位补偿位 Cpt[0:3],总的 13 位输出的汉明重量固定为 4.

我们给出两个数据来具体介绍 PAH 技术的 SM4 算法 S 盒实现原理. 对于 S 盒输入“3C”,原 8 位输出为“0111 0101”,其汉明重量为 5,8 位实际输出应为“1000 1010”,其标志位为“1”,注意计算实际输出的汉明重量时,要把标志位考虑进去,这里实际 8 位输出和标志位的汉明重量已经达到 4,所以补偿位 Cpt 为“0000”补偿零位. 而对于输入“3A”,原 8 位输出为“1001 0100”,其汉明重量为 3,8 位实际输出应等于原始输出“1001 0100”,故标志位为“0”,这里实际 8 位输出和 f 的汉明重量只有 3,所以 Cpt 为“1000”补偿一位.

3.1 补偿位 Cpt 分配方案

理论上,补偿位在满足功能的条件下是可以任意选取的,但任意选取的补偿位不能实现最优的功耗平衡,因此,四位补偿位 Cpt 每一位被选为“1”的情况应该均匀分布,这样他们的逻辑才能够对称,进而保证电路功耗平衡. 为了确定补偿位 Cpt 的具体补偿分配方案,先给 256 组数据按补偿位 Cpt 的汉明重量分类. 显然,只有一组数据补偿位 Cpt 的汉明重量为 4;有 9 组数据补偿位 Cpt 的汉明重量为 3;有 36 组数据补偿位 Cpt 的汉明重量为 2;有 84 组数据补偿位 Cpt 的汉明重量为 1;其余的 126 组数据输出不需要补偿,即 $Cpt=“0000”$. 而各补偿位

Cpt[i]为“1”的个数的总和固定为 187,故最均衡的分配方案是给 Cpt[0]分配 46 个“1”,其余 3 个补偿位分配 47 个“1”。

本设计补偿信号 Cpt 每一位的具体补偿分配情况如表 2 所示. 按照 S 盒查找表输入 xy 从“00”到“ff”的顺序,对这 256 种情况进行补偿位 Cpt 每一位详细的分配. 对补偿位 Cpt 汉明重量为 n 的情况,按照表 2 中的补偿方案,先分配完表中靠上的组数,再分配下方的. 例如,共有 84 组 Cpt 汉明重量为 1 的输出数据,在这 84 组数据中,第 1 组 21 组数据的 Cpt 为“1000”,第 22 组到 42 组数据的 Cpt 为“0100”,第 43 组到 63 组数据的 Cpt 为“0010”,第 64 组到 84 组数据的 Cpt 为“0001”. 如此类推,直到分配完所有组数.

表 2 补偿位 Cpt 的补偿分配方案

Cpt[0:0]	对应数据数	补偿位汉明重量
1000	21	1
0100	21	1
0010	21	1
0001	21	1
1100	18	2
0011	18	2
1110	2	3
1101	2	3
1011	2	3
0111	3	3
1111	1	4

为了保证输出只发生正向翻转并且汉明距离固定,对输入数据采用 1/4 编码,即原码“00”,对应编码“0001”;原码“01”,对应编码“0010”;原码“10”,对应编码“0100”;原码“11”,对应编码“1000”. 编码后 4 位数据中有且仅有 1 位为“1”. 这样,就得到了输入 16 位、输出 13 位的 PAH SM4 S 盒的真值表.

3.2 自动化设计实现流程

我们按照 PAH 方法,设计实现了 SM4 的 S 盒电路和版图. PAH SM4 S 盒单元的结构是由与门阵列和或门阵列组成的规则逻辑阵列结构,电路和版图设计都具有高度的对称性. 而且该电路最终的功能可以通过改变或门阵列中 NMOS 管的连接而有所不同. 所以,单元晶体管级的 SPICE 网表和版图中连接单元的坐标可以通过 MATLAB 程序自动生成.

3.2.1 MATLAB 生成晶体管级 SPICE 网表

MATLAB 读入 S 盒矩阵后,将 S 盒矩阵转成二进制数矩阵,可以得到 PAH SM4 S 盒 256 种输入情况下各个输出的最小项矩阵. 因为电路中每个 AND 门和每个 OR 门的结构和晶体管尺寸完全相

同——晶体管尺寸通过对生成的 SPICE 网表的仿真,优化确定,因此,网表是由几种固定模式的语句构成,可以利用计算机程序自动生成——其中的内部节点名称可由计算机程序按照命名规则自动生成. 我们编写了一个读入任意 S 盒查找表,然后输出 PAH 电路 SPICE 网表的 MATLAB 程序.

SPICE 网表制作好后,采用 Hspice 对网表的功能进行验证,得到的部分波形如图 1,图中显示了 2 组不同输入对应的 13 位输出结果. 第一组输入数据为“3A”,其实际的 8 位输出 $Out[0:7]$ = “1001 0100”、标记位 f = “0”,4 位补偿位 $Cpt[0:3]$ = “1000”;第二组输入数据为“3C”,其实际的 8 位输出 $Out[0:7]$ = “1000 1010”、标记位 f = “1”,4 位补偿位 $Cpt[0:3]$ = “0000”. 这与我们之前给出的 2 个数据实例是一致的,说明自动化生成的网表功能正确,且其按照 PAH 规则生成的 SM4 S 盒电路具有固定的输出汉明重量.

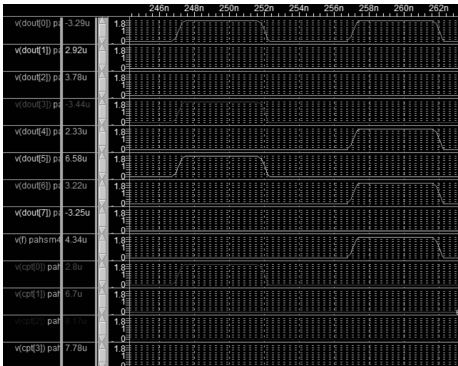


图 1 网表功能验证波形图

3.2.2 版图连接自动化

在版图设计中,与门阵列中各个连接单元与 S 盒无关,因为 AND 阵列总是包含所有最小项,所以只需要画一次就可以在不同 S 盒的版图中复用,也就是不用编程的固定部分. 而或门阵列的连接可以通过自动化的方式完成. 或门可编程阵列由 13 行 $\times$ 256 个 NMOS 组成,这些 NMOS 的栅极和漏级连接的端子类型由真值表决定,每一行对应 1 比特输出. 对于高 9 比特输出 $Out[7:0]$ 和 F ,共有 97 个最小项,所以,前 9 行的 256 个 NMOS 中有 159 个是虚管(dummy). 对于补偿位 $Cpt[0:3]$,最小项的数目是不一样的,按照本文的补偿方案, $Cpt[0]$ 的最小项有 46 个, $Cpt[1]$ 、 $Cpt[2]$ 和 $Cpt[3]$ 的最小项数目均为 47. 为了结构对称,它们对应的或门同样具有 97 个输入端,那些无用的输入端与地连接.

本文使用的是华大公司的版图设计工具 Aether,

该软件的 Generate Rom 功能可以按照配置文件所提供的坐标,自动放置版图单元.这就可以帮助我们自动放置接触单元实现 NMOS 管的栅极是连接与门阵列输出端还是地,NMOS 管的漏极是连接电路输出端还是地的编程.编程文件就是作为配置文件的文本文件.本文进行了版图后仿真,图 2 是 256 组数据的后仿功耗曲线与时间的关系.从图中可以直观地看到,不同输入数据有着近乎一致的功耗曲线,这将对抵御功耗攻击起到重要作用,进而提高安全性.

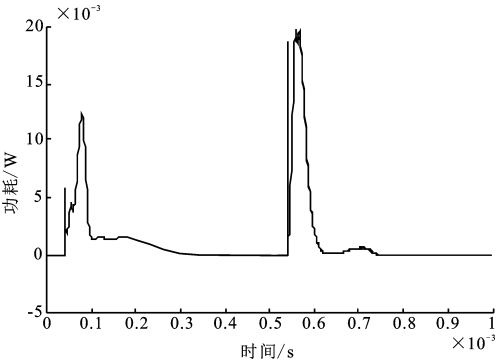


图 2 后仿功耗曲线

3.3 实验数据对比

我们在 SMIC 0.18 μm 的工艺库下进行仿真,同时用查找表方式实现了 SM4 S 盒,对比了文献[4]不同方案实现 SM4 S 盒的前仿结果,结果如表 3.由表中数据可知,我们的方案(PAH)与其他实现 SM4 S 盒的方案相比,具有更低的功耗开销与更小的延时,功耗延时积至少减少了 76%.

表 3 不同方案实现 SM4 S 盒参数对比

	延时 /ns	平均功耗 /(mW@10MHZ)	功耗延时积 /pJ	面积 / μm^2
无防护 LUT	1.43	0.30	0.43	4 980
塔域掩码 ^[4]	7.60	2.45	18.61	15 225
PPRM 掩码 ^[4]	4.20	0.74	3.10	18 395
PAH 后仿	1.43	0.51	0.73	38 637

除了在性能方面的优势,PAH 方案实现 SM4 S 盒的安全性同样优于已有功耗平衡逻辑.归一化能量偏差(NED)和归一化标准偏差(NSD)^[5]通常用来衡量抵抗功耗分析攻击的性能.二者的数值越小,则电路设计的抗功耗攻击能力越强,安全性越高.具体的计算公式如下:

$$\text{NED} = \frac{\max(E) - \min(E)}{\max(E)}$$

(1)

$$\text{NSD} = \frac{\delta E}{E}$$

(2)

式中,E 是电路一次计算的总能耗, δE 和 E 分别是它

的标准差和均值.表 4 是本文 PAH 技术实现 SM4 算法 S 盒与文献[2]PAH 技术实现 AES 算法 S 盒的 NED、NSD 值对比,这说明 PAH 技术应用于国内的 SM4 算法时,同样具有高安全性.

表 4 PAH SM4 S 盒安全性

	NED/%	NSD/%
PAH SM4 S 盒	0.72	0.14
PAH AES S 盒	1.8	0.42

4 结束语

本文基于功耗感知隐藏技术,用自动化方式实现了 SM4 S 盒的网表,并验证了其功能、性能和安全性.对比不同方案实现 SM4 算法 S 盒后,可以得出结论:功耗感知隐藏技术应用于 SM4 算法 S 盒时,在功耗和性能方面的表现高效,可达到与 AES S 盒电路相近的效果.本文工作一方面验证了 PAH 技术的通用性;另一方面,给出了一种低功耗高安全的 SM4 算法 S 盒实现方案.

参考文献:

[1] Kocher P, Jaffe J, Jun B. Differential power analysis: leaking secrets[C]//Proc. Crypto '99, Berlin, Springer-Verlag, LNCS 1999:388-397.

[2] Jiangsha M, Xiangyu L, Moyang W. Power-aware hiding method for S-box protection[J]. Electronics Letters, 2014, 50(22):1604-1606.

[3] 国家密码管理局. 无线局域网产品使用的 SMS4 密码算法[S]. 北京, 2006.

[4] 牛砚波,蒋安平. 一种低功耗抗差分功耗分析攻击的 SM4 算法实现[J]. 微电子学与计算机, 2014, 31(9): 28-32.

[5] Tiri K, Akmal M, Verbaauwhede I. A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards [C]// Solid-State Circuits Conference, 2002. Esscirc 2002. Florence, Italy, IEEE, 2002:403-406.

作者简介:

杨超群 女,(1993-),硕士研究生.研究方向为密码集成电路. E-mail:yangcq0124@163.com.

殷树娟 女,(1981-),副教授.研究方向包括混合信号集成电路设计、无源器件设计、核电子学和 IP 可重用设计.

李翔宇 男,(1977-),副研究员.研究方向包括嵌入式系统安全和信息安全、超大规模集成电路、物联网设备和低功耗集成电路.