

# 分组密码线性部件的抗功耗攻击特性

邱 爽, 白国强, 陈弘毅

(清华大学 微电子学研究所, 北京 100084)

**摘 要:** 通过对 FPGA 实现的分组密码 SM4 进行实际攻击, 发现了 SM4 的线性部件使其具有抗差分功耗攻击的能力, 研究并归纳了一般分组密码中线性部件的结构特性和其抗功耗攻击能力的关系, 从而提出了一种针对分组密码的算法设计层面的功耗攻击防护措施. 完成了对硬件实现的国密 SM4 算法的成功的 DPA 攻击.

**关键词:** SM4; 分组密码; 选择明文; 差分功耗攻击; 侧信道攻击

**中图分类号:** TP309.1

**文献标识码:** A

**文章编号:** 1000-7180(2015)02-0024-04

## DPA Resistance of Linear Component in Block Ciphers

QIU Shuang, BAI Guo-qiang, CHEN Hong-yi

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

**Abstract:** By mounting an actual DPA against FPGA implementation of SM4, the DPA resistance of linear component in SM4 has been discovered. Furthermore, the DPA resistance of linear component in block ciphers has been generalized, thus an algorithmic DPA countermeasures is proposed. This work also completes a successful DPA against a hardware implementation of SM4 for the first time.

**Key words:** SM4; block cipher; chosen-text; differential power analysis; side-channel attack

### 1 引言

差分功耗攻击 (differential power analysis, DPA)<sup>[1]</sup> 属于侧信道攻击的一种, 它利用硬件设备在执行加解密操作过程中泄露的功耗来恢复密钥, 对嵌入式系统的安全构成严重威胁<sup>[2]</sup>. 因此, 许多 DPA 防护措施诸如功耗平衡逻辑<sup>[3]</sup>、随机时延<sup>[4]</sup>、掩码<sup>[5]</sup>等相继被提出. 这些防护措施都是从硬件实现角度入手, 将敏感信息产生的特殊功耗进行掩盖, 使攻击者难以从功耗中恢复出敏感信息, 从而抵御 DPA 攻击. 目前人们对功耗攻击硬件防护措施的研究很充分, 但对算法自身抗功耗攻击特性的研究却还寥寥无几. 针对这一问题, 本文发现并归纳了 SM4 算法中线性部件的抗 DPA 特性, 提出了一种算法层面的 DPA 防护措施.

### 2 SM4 算法介绍

分组密码是现代密码研究的一个重要领域, 由于其高效、标准、便于实现等优点, 在加密系统中的应用十分普遍. 本文主要研究对象是 DES、AES 和国内官方公布的第一个商用分组密码 SM4, 本节我们以 SM4 算法为例对分组密码进行介绍.

SM4 算法具有 128 比特的明密文和 128 比特的密钥. 加密、解密算法都采用 32 轮非线性迭代结构. 128 比特数据分组被划分成 4 个 32 比特字, 并以字为单位进行加密运算. 用  $Z_2^e$  表示  $e$  比特向量集, 则字属于  $Z_2^{32}$  向量集, 字节属于  $Z_2^8$  向量集. 在加密 (或解密) 过程中, 输入明文 (或密文) 可表示为  $(X_0, X_1, X_2, X_3) \in (Z_2^{32})^4$ , 轮密钥  $rk \in Z_2^{32}$ , 进行一轮加密 (或解密) 运算的结果  $F$  为

$$F(X_0, X_1, X_2, X_3, rk) = X_0 \oplus T(X_0 \oplus X_1 \oplus X_2 \oplus X_3 \oplus rk) \quad (1)$$

收稿日期: 2014-04-27; 修回日期: 2014-06-18

基金项目: 国家自然科学基金项目 (U1135004)

式中,  $T$  为合成置换, 有  $T: Z_2^{32} \rightarrow Z_2^{32}$ , 是非线性函数  $\tau$  和线性函数  $L$  的复合函数, 记作  $T(\cdot) = L(\tau(\cdot))$ .  $\tau$  是四个并行的相同的 S 盒, 每个 S 盒有 8 比特输入 8 比特输出, 如图 1 所示. 设输入  $A = (a_0, a_1, a_2, a_3) \in (Z_2^8)^4$ , 输出  $B = (b_0, b_1, b_2, b_3) \in (Z_2^8)^4$ , 有

$$(b_0, b_1, b_2, b_3) = \tau(A) = (\text{Sbox}(a_0), \text{Sbox}(a_1), \text{Sbox}(a_2), \text{Sbox}(a_3)) \quad (2)$$

线性变换  $L$  是将输入分别循环左移 2 位、10 位、18 位、24 位后与原始的输入异或到一起, 得到一个新的 32 比特输出. 设输入为  $B \in Z_2^{32}$ , 输出为  $C \in Z_2^{32}$ ,  $\ll$  为循环移位符号, 有

$$C = L(B) = B \oplus (B \ll 2) \oplus (B \ll 10) \oplus (B \ll 18) \oplus (B \ll 24).$$

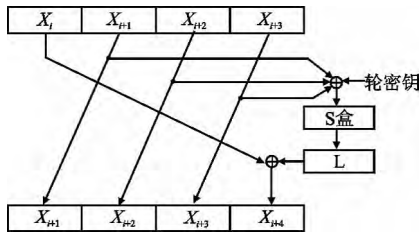


图 1 SM4 算法轮结构

综上, SM4 加密算法的轮函数结构如图 1 所示, 每一轮(第  $i$  轮)迭代产生一个新的 32 比特状态字  $X_{i+4}$ . 输入的四个状态中的第一个字  $X_i$  舍弃, 后三个字  $X_{i+1}, X_{i+2}, X_{i+3}$  与新产生的状态  $X_{i+4}$  构成下一轮加密(或解密)的输入. 在如此迭代 32 轮之后, 再经过反序变换处理, 输出即为密文(或明文). 反序变换  $F$  定义为

$$R(A_0, A_1, A_2, A_3) = (A_3, A_2, A_1, A_0) \quad (3)$$

式中,  $A_i \in Z_2^{32} (i = 0, 1, 2, 3)$ . 假设输入明文(或密文)为  $(X_0, X_1, X_2, X_3) \in (Z_2^{32})^4$ , 输出密文(或明文)为  $(Y_0, Y_1, Y_2, Y_3) \in (Z_2^{32})^4$ , 轮密钥  $rk_i \in Z_2^{32} (i = 0, 1, \dots, 31)$ , 完整的 SM4 加密(或解密)过程可表示为

$$\begin{aligned} X_{i+4} &= F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i) = X_i \oplus \\ &T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i), i = 0, 1, \dots, 31, \\ (Y_0, Y_1, Y_2, Y_3) &= R(X_{32}, X_{33}, X_{34}, X_{35}) = \\ &(X_{35}, X_{34}, X_{33}, X_{32}). \end{aligned} \quad (4)$$

### 3 差分功耗攻击

DPA 于 1999 年首次被 Paul Kocher<sup>[1]</sup> 提出, 从此开启了功耗攻击的先河. DPA 是功耗攻击中最基本的一种, 后来衍生出的 CPA<sup>[6]</sup> 可被视为高阶(High-order)DPA. 因此本文以 DPA 作为功耗攻击

的主要手段进行研究. 对分组密码进行功耗攻击的一般步骤如下:

(1) 采集功耗. 采集到的功耗集合可记作  $W = \{\omega_1, \omega_2, \dots, \omega_N\}$ , 其中每一条功耗  $\omega_i \in W$  对应一个明文, 因此对应的明文集合可记作  $P = \{p_1, p_2, \dots, p_N\}$ .

(2) 对密钥进行划分. 加密算法的中间结果一般都是明文(或密文)和部分密钥的函数, 这部分密钥被称为根密钥. 在攻击过程中, 首先要将一个轮密钥划分为多个根密钥, 再以根密钥为单位进行 DPA 攻击. 一般情况下, 划分的依据是 S 盒的规模.

(3) 破解每个根密钥. 根密钥的长度一般远小于总的密钥, 假设根密钥的长度为  $n$ ,  $2^n$  种可能的根密钥构成猜测密钥集合  $K = \{k_0, k_1, \dots, k_{2^n-1}\}$ , 也即  $K = \{\underbrace{00\dots00}_{n\text{位}}, \underbrace{00\dots01}_{n\text{位}}, \dots, \underbrace{11\dots11}_{n\text{位}}\}$ . 对每一个猜测密钥  $k_i \in K (i = 0, 1, \dots, 2^n - 1)$  都进行一次均值差试验并得到一个均值差(Difference of Means, DoM)  $DoM(k_i)$ . 所有猜测密钥的均值差构成均值差集合  $DoM(K) = \{DoM(k_0), DoM(k_1), \dots, DoM(k_{2^n-1})\}$ . 如果猜测密钥  $k_c \in K$  满足  $DoM(k_c) > \overline{\{DoM(k_i)\}} (i = 0, 1, \dots, 2^n - 1)$ , 则此次 DPA 攻击认定猜测密钥  $k_c$  为正确的根密钥.

显然, 均值差  $DoM$  是差分功耗攻击中最重要的部分, 均值差集合  $DoM(K)$  直接决定了功耗攻击的结果. 求均值差第一步是要对采集的功耗进行分组, 也就是对功耗对应的明文  $p_i \in P (i = 1, 2, \dots, n)$  进行分组. 其中分组的依据为选择函数  $D$ , 分成的两组可表示为  $\{p_i \mid D(p_i, k_j) = 1\}$  和  $\{p_i \mid D(p_i, k_j) = 0\}$ , 其中  $k_j \in K (j = 0, 1, \dots, 63)$  为猜测密钥. 分组过程完成后, 再将两组中的明文对应的功耗分别求平均值作差, 得到的就是均值差  $DoM$ . 设  $\omega_i$  为采集到的第  $i$  个功耗样本,  $N$  为采集的功耗样本条数,  $DoM$  定义如下:

$$DoM(k) = \frac{\sum_{i=0}^{N-1} D(p_i, k) \omega_i}{\sum_{i=0}^{N-1} D(p_i, k)} - \frac{\sum_{i=0}^{N-1} (1 - D(p_i, k)) \omega_i}{\sum_{i=0}^{N-1} (1 - D(p_i, k))} \quad (5)$$

### 4 线性部件的抗 DPA 特性

根据对 SM4 算法的线性部件 L 的抗 DPA 特性的研究, 归纳并建立了分组密码的线性部件特征与其抗 DPA 能力的函数关系, 并据此提出了一种

针对分组密码的抗 DPA 算法设计方案.

#### 4.1 SM4 算法的抗 DPA 特性

本文中对分组密码的抗 DPA 特性的研究都是建立在合理的硬件假设基础上的. 该假设指的是: S 盒的输出结果不存储在寄存器中. 由于忽略了合理硬件假设, 前人在对 SM4 算法进行 DPA 攻击研究时并未发现其抗 DPA 特性<sup>[7]</sup>. 合理硬件假设是我们研究 SM4 算法抗 DPA 特性的前提.

基于合理硬件假设, 在进行功耗攻击时我们不能利用 S 盒输出作为选择函数, 只能利用每一轮输出的结果(轮状态)作为选择函数. 然而在 SM4 算法中, S 盒输出需要经过线性变换 L 才能输出为轮状态. 以轮状态的第一比特为例, 选择函数为

$$D = X_{01} \oplus S_{11}(p_{18} \oplus k_{18}) \oplus S_{13}(p_{18} \oplus k_{18}) \oplus S_{23}(p_{28} \oplus k_{28}) \oplus S_{33}(p_{38} \oplus k_{38}) \oplus S_{41}(p_{48} \oplus k_{48}) \quad (6)$$

式中,  $X_{01}$  表示  $X_0$  的第一比特,  $S_{ij}(x)$  表示当第  $i$  个 S 盒输入为  $x$  时, 第  $j$  比特输出值,  $p_{i8}$  和  $k_{i8}$  分别表示明文和密钥中输入到第  $i$  个 S 盒的 8 比特. 由式(6)可知, 所有四个根密钥  $k_{18}, k_{28}, k_{38}, k_{48}$  都是 D 函数的输入, 因此, 猜测密钥有 32 位, 猜测密钥集合  $K = \{k_0, k_1, \dots, k_n\}$  中元素的个数为  $2^{32}$ . 换句话说, 攻击者如果想要得到密钥, 必须进行  $2^{32}$  次猜测. 对如此庞大的数据进行计算和比较不仅占用资源、难以实现, 而且错误率也极高. 因此, 由于运算时间和存储空间限制, SM4 算法加密硬件难以被传统 DPA 攻破.

#### 4.2 选择明文 DPA 及其局限性

由上文可知 SM4 算法中的线性结构 L 对传统 DPA 具有抵抗性. 本节提出了针对 SM4 算法的选择明文 DPA 攻击法, 它的有效性经过理论和实验证实. 选择明文 DPA 并不是第一次提出, Messerges<sup>[8]</sup> 曾经利用选择明文 DPA 降低攻击过程中的算法噪声. 然而本文中首次利用选择明文 DPA 作为唯一可以破解具有抗 DPA 特性的 SM4 算法的功耗攻击手段.

选择明文的目的是控制住多余的根密钥, 使其在选择函数的表达式中变成常量, 最后只留一个需要攻击的根密钥. 举例说明, 以轮状态的第一比特作为选择函数, 则令明文中输入第 2、3、4 个 S 盒的明文变为常量, 只令输入第一个 S 盒的明文变化. 此时, 选择函数变为

$$D = X_{01} \oplus S_{11}(p_{18} \oplus k_{18}) \oplus S_{13}(p_{18} \oplus k_{18}) \oplus S_{23} \oplus S_{33} \oplus S_{41} \quad (7)$$

后面三项为常数. 输入选择明文后, 选择函数只与第

一个根密钥有关, 此时进行 DPA 只需猜测  $2^8$  次. 选择明文 DPA 的攻击复杂度相较普通 DPA 大大下降, 从而使破解 SM4 算法成为可能. 第 5 节中我们给出了选择明文 DPA 的实验结果.

尽管选择明文 DPA 可以破解 SM4 算法, 但这并不影响 SM4 算法的抗 DPA 特性. 选择明文攻击可以通过合理的通信协议来阻止. 为阻止选择明文攻击, 加密硬件中必须设置为先校验后加密模式, 校验码错误则不进行加密计算, 这种情况下选择明文 DPA 无法进行.

#### 4.3 复杂度与混合系数

SM4 算法中 L 函数将不同 S 盒的输出混合, 从而导致 DPA 的复杂度升高, 产生抗 DPA 特性. 将分组密码中具有此类特性的线性结构称为“混合结构”. 定义“混合结构”的特性参数混合系数

$$\varphi = \frac{\text{混合的 S 盒个数}}{\text{总 S 盒个数}} \quad (8)$$

式中, 混合度  $\varphi$  是列混合结构混合的 S 盒占总 S 盒数量的百分比.

为定量衡量分组密码线性部件对抗 DPA 特性的影响, 定义攻击复杂度  $\lambda$  为攻击全过程中需要进行的运算的轮数. 假设分组密码轮密钥位数为  $n$ , 容易得到混合系数和复杂度之间的关系  $\lambda = \text{取整}[\varphi^{-1}]2^{\varphi}$ , 其中  $2^{\varphi}$  为进行一次 DPA 的复杂度, 系数“取整 $[\varphi^{-1}]$ ”为得到全部密钥信息需要进行的 DPA 次数. 据此可知, “混合结构”的混合系数  $\varphi$  越大, 轮密钥长度  $n$  越大, 复杂度  $\lambda$  也就越大, 该分组密码抗 DPA 特性也就越强.

表 1 针对分组密码的不同攻击方式的复杂度  $\lambda$

| $\lambda$ | 数学攻击                | DPA                            |                 |
|-----------|---------------------|--------------------------------|-----------------|
|           |                     | 传统 DPA                         | 选择明文 DPA        |
| DES 算法    | $16 \times 2^{56}$  | $8 \times 2^6 + 2^8 \times 16$ | —               |
| AES 算法    | $10 \times 2^{128}$ | $16 \times 2^8$                | —               |
| SM4 算法    | $32 \times 2^{128}$ | $4 \times 2^{32}$              | $16 \times 2^8$ |

由表 1 可以看出: (1) 由于 DPA 攻击过程中将密钥划分成若干个根密钥, 因而 DPA 攻击复杂度大大低于普通代数攻击手段; (2) 使用选择明文 DPA 大大降低了 SM4 算法的攻击复杂度.

#### 4.4 一种算法层面的 DPA 防护策略

根据以上分析, 我们可以得到一种算法层面抗 DPA 攻击策略, 包括三个方面: (1) 分组密码具有较大的轮密钥位数; (2) 分组密码中线性结构具有较高的混合度  $\varphi$ ; (3) 加密硬件遵从合理硬件假设, 且采用先校验后加密方式.

## 5 实验结果

根据以上分析,在 Vertex-II FPGA 上实现了 SM4 算法并对其进行实测数据下的 DPA 攻击.图 2 为采用选择明文 DPA 攻击时,256 个猜测密钥产生均值差随样本量的演变图,从图中可以看出,正确密钥的均值差是均值差集合中最大的,选择明文 DPA 成功.图 3 为利用普通 DPA 对 SM4 算法进行攻击时(S 盒输出为选择函数),256 个猜测密钥产生的均值差随样本量的演变图.从图 3 中可以看出直接针对 SM4 的 FPGA 进行普通 DPA 无法得到任何密钥信息,从而破解失败.

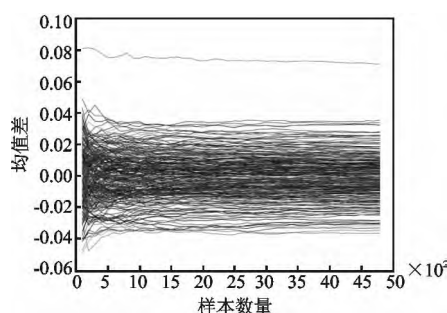


图 2 选择明文 DPA 的均值差演化图

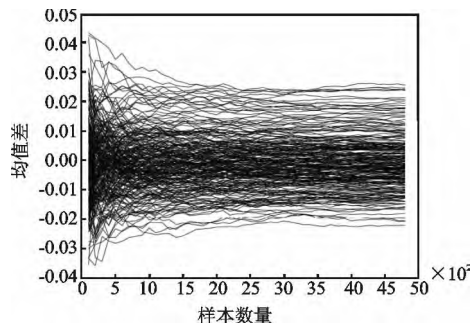


图 3 普通 DPA 的均值差演化图

## 6 结束语

在合理硬件假设的基础上分析 SM4 算法的 DPA 特性,发现其由于具有线性结构 L 从而具备抗 DPA 特性.归纳了“混合结构”的混合特性与抗 DPA 特性的数学关系,从而得到一套算法层次的 DPA 防护方案.以上研究不仅得到了 SM4 算法的抗 DPA 特性,也为新算法的抗 DPA 设计提供了参考.

(上接第 23 页)

[7] 赵永锋,王毅刚.采用手指的三维人机交互方法[J].微电子学与计算机,2009,26(6): 21-24.

作者简介:

郑毅 男,(1988-),硕士研究生.研究方向为 3D 测量、图

## 参考文献:

- [1] Kocher P, Jaffe J, Jun B. Differential power analysis [C]//Advances in Cryptology—CRYPTO'99. Berlin, Heidelberg; Springer, 1999: 388-397.
- [2] 李浪,焦铭,李仁发,等.一种 ECC 加密芯片抗功耗攻击研究[J].微电子学与计算机,2011,28(1): 2-6.
- [3] Tiri K, Verbauwhede I. A VLSI design flow for secure side-channel attack resistant ICs[C]//Proceedings of the conference on Design, Automation and Test in Europe—Volume 3. Germany: Munich, IEEE Computer Society, 2005: 58-63.
- [4] Clavier C, Coron J S, Dabbous N. Differential power analysis in the presence of hardware countermeasures [C]//Cryptographic Hardware and Embedded Systems—CHES 2000. Berlin, Heidelberg; Springer, 2000: 252-263.
- [5] Chari S, Jutla C S, Rao J R, et al. Towards sound approaches to counteract power-analysis attacks [C]//Advances in Cryptology—CRYPTO'99. Berlin, Heidelberg; Springer, 1999: 398-412.
- [6] Brier E, Clavier C, Olivier F. Correlation power analysis with a leakage model [C]//Cryptographic Hardware and Embedded Systems—CHES 2004. Berlin, Heidelberg; Springer, 2004: 16-29.
- [7] Bai X, Guo L, Li T. Differential power analysis attack on SMS4 block cipher [C]//Circuits and Systems for Communications, ICCSC 2008, 4th IEEE International Conference on. China; Shanghai, IEEE, 2008: 613-617.
- [8] Messergers T S, Dabbish E A, Sloan R H. Examining smart-card security under the threat of power analysis attacks[J]. Computers, IEEE Transactions on, 2002, 51(5): 541-552.

## 作者简介:

邱爽 女,(1990-),硕士.研究方向为侧信道攻击.

白国强 男,(1963-),博士,副教授,博士生导师.研究方向为信息安全芯片.

陈弘毅 男,(1942-),硕士,教授.研究方向为集成电路(IC)设计.

像处理和人机交互方式. E-mail: zhengy4446@163.com.

宋玮 男,(1988-),硕士研究生.研究方向为 3D 测量、图像处理和人机交互.

谢翔 男,(1971-),副研究员.研究方向为集成电路系统设计、图像处理、无线通信、生物医学电子学等.