·网络空间安全· 文章编号: 1000-3428(2020)01-0102-06 文献标志码: A 中图分类号: TP393.08

针对分组密码的攻击方法研究

朱文锋[1],王 琴[1],郭 筝[1,2],刘军荣[1,2]

(1.上海交通大学 微电子学院,上海 200240; 2.智巡密码(上海)检测技术有限公司,上海 201100)

摘 要: 为提升旁路攻击对分组密码算法硬件实现电路的攻击效果,增大正确密钥与错误密钥间的区分度,提出一种针对分组密码的旁路攻击方法。结合差分功耗分析(DPA)攻击和零值攻击的特点,通过分类来利用尽可能多的功耗分量,以攻击出全部密钥。在 FPGA 上实现 AES 硬件电路并进行实验,结果表明,在 20 万条全随机明文曲线中,该方法恢复出了全部密钥,相比 DPA 攻击方法,其正确密钥与错误密钥间的区分度更大。

关键词: 旁路攻击方法;硬件实现;分组密码算法;组合逻辑功耗;信噪比

开放科学(资源服务)标志码(OSID):

中文引用格式:朱文锋,王琴,郭筝,等.针对分组密码的攻击方法研究[J].计算机工程,2020,46(1):102-107,113.
英文引用格式:ZHU Wenfeng, WANG Qin, GUO Zheng, et al. Research on attacks method for block ciphers[J]. Computer Engineering,2020,46(1):102-107,113.

Research on Attacks Method for Block Ciphers

ZHU Wenfeng[1], WANG Qin[1], GUO Zheng[1,2], LIU Junrong[1,2]

(1. School of Microelectronics, Shanghai Jiao Tong University, Shanghai 200240, China;
2. Zhixun Cipher(Shanghai) Detection Technology Co., Ltd., Shanghai 201100, China)

【**Abstract**】In order to improve the effect of Side Channel Attacks(SCAs) on the hardware implementation of block cipher algorithm, and increase the discrimination between correct keys and wrong keys, this paper proposes a SCAs method for block ciphers. This method combines the characteristics of Differential Power Analysis(DPA) attack and zero-value attack, and utilizes as many power components as possible through classification, thus obtaining all keys by attacking. Then, the AES hardware circuit is implemented on the FPGA and experiments are carried out. The results show that the proposed method successfully recovers all keys in 200,000 full random plaintext curves. Besides, the correct keys and wrong keys are more distinguishable in this method than those in the DPA attack method.

【**Key words**】Side Channel Attacks(SCAs) method; hardware implementation; block cipher algorithm; combinational logic power; Signal to Noise Ratio(SNR)
DOI:10.19678/j.issn.1000-3428.0053229

0 概述

近年来,信息安全问题逐渐成为人们关注的焦点。由于密码算法的计算依赖物理载体(如 CPU 和密码芯片),在运算过程中,物理器件总会泄露各种与密码系统相关的物理信息,如运行时间、能量消耗和电磁辐射等[1],攻击者可以采集和利用这些旁路信息,根据它们与密钥信息间的关联性来进行密钥恢复[2]。一些先进的攻击手段可以绕开数学推理过程而通过其他途径获得秘密信息,其中的典型代表就是旁路攻击(Side Channel Attacks,SCAs)[3]。

文献[4]提出了一种旁路功耗攻击方法,该方法通过采集密码设备运行时的瞬时功耗,分析它们与算法处理的数据和进行的操作之间的关联,进而获取设备存储的秘密信息。功耗攻击一般分为 2 种,一种为简单功耗分析(Simple Power Analysis, SPA),另一种为差分功耗分析(Differential Power Analysis, DPA)[4]。SPA 通过直接观测少量曲线形态的方式获取与密钥相关的信息,而 DPA 则采集大量功耗信息,运用数理统计分析恢复密钥,该攻

基金项目:国家自然科学基金"针对 S 芯片验证模块引脚信息的自动分析技术"(U1536103);上海市闵行区中小企业技术创新计划"基于区块链技术的金融业务平台"(2018MH110)。
作者简介:朱文锋(1994—),男,硕士研究生,主研方向为旁路攻击方法、硬件木马检测;王 琴,副教授、博士;郭 筝、刘军荣,博士。
收稿日期:2018-11-23 **修回日期**:2019-02-20 **E-mail**:zhuwenfengzi@foxmail.com

击也是目前比较流行和常见的旁路攻击方式[5]。文献[6]提出了一种模板攻击方法,模板是描述设备能量消耗特征的最优方法。文献[7]指出基于相关性系数的差分功耗分析(CPA)相比传统 DPA 的优势。文献[8]讨论了基于互信息和线性回归的通用 DPA(对攻击的密钥模板不做任何假设)具有一定局限性,并提出了一种近似通用 DPA 的概念[8]。近年来,基于深度学习的攻击方法也得到学者们的广泛关注[9-11]。

由于分组密码算法在硬件实现过程中存在大量的并行计算,噪声中和中间值相关的真实功耗信息难以被区分出来。现有针对硬件实现的分组密码算法攻击大多具有一定的局限性,如 SPA 适合信噪比很大且已知功耗模型的情况[12],DPA 能利用的功耗占总功耗的比例较小,当信噪降低到原先信噪的 $1/\theta$ 时,攻击成功所需的曲线数则降为原先的 $1/\theta^2$,模板攻击在噪声特别大的情况下所描述的设备能量消耗特征也并非很准确[13]。

在实际攻击中,可以将与中间值不相关的噪声近似看成是随机的,并根据中间值对这一部分功耗进行分类,使每一类的功耗平均值都近似相等。本文以充分利用与中间值相关的功耗、消除和中间值无关的功耗分量为出发点,提出一种针对分组密码的攻击方法,即功耗最小分类方法。该方法通过尽可能多地利用和中间值相关的功耗分量来增大信噪比并提升攻击效果。

1　旁路功耗分析的基本原理

能够实现旁路功耗分析的原因在于,芯片产生的功耗与芯片在运算过程中进行的操作和处理的中间值数据存在关联[14]。

1.1　密码设备的电路基础

现代密码设备通常由数字电路构成,数字电路(包括 ASIC 和 FPGA)的基本单元是逻辑元件[15]。数字电路本质上由电子开关组成,通常通过晶体管或 MOS 管实现。CMOS 晶体管的 NMOS 管和 PMOS 管不会在同一时刻一起导通,因此,能够保证 CMOS 晶体管的输出电压具有稳定的逻辑 1 电平或者逻辑 0 电平。CMOS 电路能构造出复杂的组合逻辑和时序逻辑电路,最终形成完整电路。

1.2　功耗的产生与组成

数字 CMOS 逻辑单元的功耗主要由 2 个部分组成,一部分为负载电容充放电时引起的功耗,称为动态功耗,另一部分为漏电流引起的功耗,称为静态功耗。动态功耗在电路总功耗中占主要部分[16]。

在某一个固定的时刻,CMOS 器件输出端的电平会出现 4 种情况:保持原先的 0 不变,保持原先的 1 不变,发生 0→1 的变化,发生 1→0 的变化。这 4 种情况对应的动态功耗种类如图 1 所示。

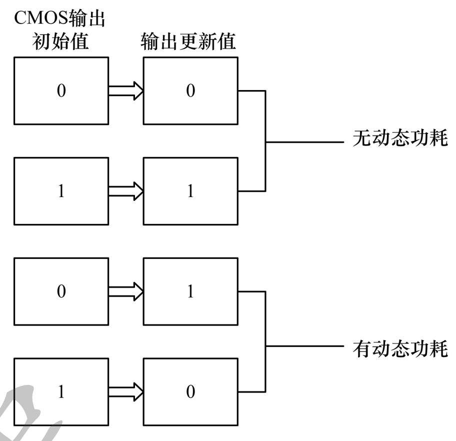


图 1　CMOS 器件输出端 4 种情况对应的功耗种类
Fig. 1　Power consumption types corresponding to 4 cases of CMOS device output

由于数字电路中所用到的 CMOS 电路的宽长比都一样,因此可以简单地用输出端是否发生翻转来近似模拟 CMOS 电路的动态功耗,若发生翻转则将功耗记为 1,否则将功耗记为 0。

1.3　旁路功耗的统计特征

旁路功耗分析的主要依据是密码芯片的瞬时功耗值与执行的操作和处理的数据间有一定的关联[17]。对这 2 种依赖性进行细分,将功耗曲线上的每个点对操作的依赖分量记为P_{op},对数据的依赖分量记为P_{data}。另外,在现实中的每次功耗测量中均会存在电子噪声,从而对功耗分析造成干扰,本文将该分量记为$P_{el.\,noise}$。还有一些功耗与操作和数据都无关,相对于操作和数据都是随机的,将该功耗分量记为P_{random}。除此之外,每个点还包含一些功耗常量部分,记为P_{const}。将上述分量叠加,可得到每个点的总功耗,如下:

$$P_{total} = P_{op} + P_{data} + P_{el.\,noise} + P_{random} + P_{const} \tag{1}$$

电子噪声$P_{el.\,noise}$服从正态分布,通过平均可以去除$P_{el.\,noise}$和P_{random}的影响。用P_{exp}表示给定攻击场景中可以利用的功耗分量,将该场景中除电子噪声外而无法利用的功耗分量表示为$P_{sw.\,noise}$(称为转换噪声),则有:

$$P_{data} = P_{exp} + P_{sw.\,noise} \tag{2}$$

在数字电路中,信噪比(Signal to Noise Ratio, SNR)是一个重要的参数,其表示电子系统中信号与噪声的比例。信噪比的一般定义如式(3)所示。

$$S_{SNR} = \frac{V(\mathrm{signal})}{V(\mathrm{noise})} \tag{3}$$

其中,$V(\cdot)$表示方差。

对于一个给定的攻击场景,功耗曲线中某一点的信噪比如式(4)所示[18]。信噪比越高,攻击者能利用的有用信息就越多。

$$S_{SNR} = \frac{V(P_{exp})}{V(P_{sw.\,noise} + P_{el.\,noise} + P_{random})} \tag{4}$$

2 最小功耗分类方法

2.1 DPA 攻击与零值攻击

DPA 的目标是记录密码设备对大量不同数据分组进行加密或解密时的能量迹，并基于能量迹恢复出密码设备中的密钥。其攻击过程描述为[19]：

1）在密码芯片系统中，将 N 组不同的明文（密文）数据和密钥进行加密或解密，并获取密码设备的能耗，将其记为 T。

2）基于猜测的密钥和明文（密文），通过密码算法产生相应的中间值，根据功耗模型（汉明重量模型或者汉明距离模型），将中间值映射为能量消耗值 H。

3）计算假设的能量消耗与实测能量迹间的线性相关系数。

一个操作数为 0 的乘法器往往需要很少的功耗，可以假设一个操作数为 0 的乘法器，其能量消耗就为 0[20]。利用该特性，能够通过类似 DPA 攻击的方法攻击出算法密钥，这种攻击方式称为零值攻击。

2.2 功耗分类方法

功耗最小分类方法具有通用的攻击策略，与 DPA 攻击的步骤类似，但两者选取中间值时依据的功耗模型有很大差别。功耗最小分类方法分为以下 5 个步骤：

1）选择算法硬件实现电路中的某个寄存器变化量作为中间值，要求该寄存器变化前后的值都可以通过已知的非常量数据和猜测的少量密钥而获得，且要求该寄存器值改变的同时能引起足够多的组合逻辑电路中间值发生改变，产生尽量多的功耗，在该寄存器值不变的情况下，这些组合逻辑电路中间值也不发生改变。

2）测量密码设备在加密或解密 D 个不同数据分组时产生的瞬时功耗。

3）对于每一个可能的密钥 k 值和 D 次加密过程，根据密码算法计算出假设的中间值矩阵 $\boldsymbol{V}$。

4）对于猜测密钥k_j对应的矩阵 $\boldsymbol{V}$ 中的列，将中间值为 0 的曲线放入猜测密钥k_j对应的曲线集合中，每一个猜测密钥k_j都得到一组曲线集合，如图 2 所示。在中间值为 0 的情况下，寄存器没有翻转功耗，组合逻辑功耗也相对较小

5）对于曲线上每一个确定的位置，都存在一个曲线集合T_j，其在该位置上的功耗平均值最小（相对于其他密钥对应的曲线集合在该点上的功耗平均值），则这个平均值最小的集合对应的密钥就是该位置攻击出的密钥结果。

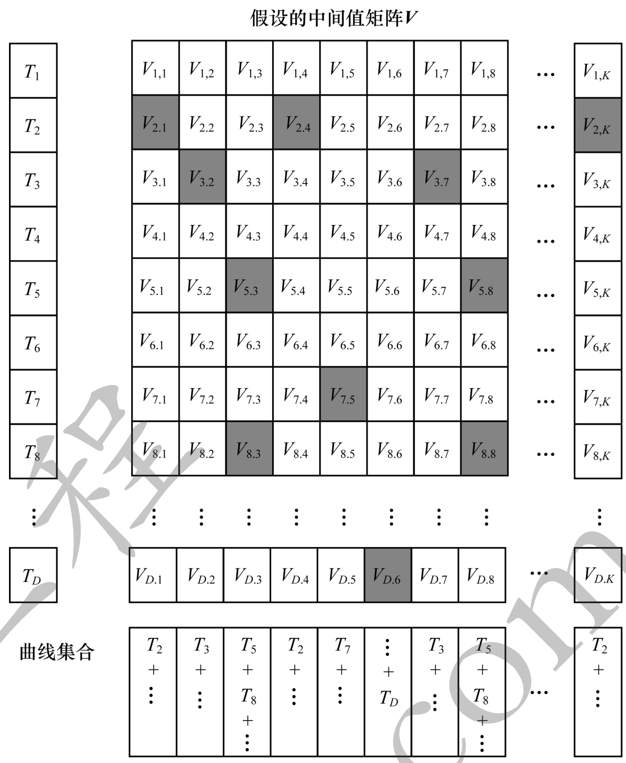


图 2 功耗曲线分类示意图

Fig. 2 Classification diagram of power consumption curve

2.3 最小功耗分类方法优势

本文最小功耗分类方法优势分析如下：

1）具有足够大的P_{exp}。从 2.2 节可以看出，在中间值不为 0 的情况下，有足够大的寄存器翻转功耗和组合逻辑电路计算功耗，而在中间值为 0 的情况下，这些功耗都为 0，从而保证了该方法具有足够大的P_{exp}，在给定攻击场景中能利用更多的功耗分量。

2）能够消除和中间值无关的功耗的影响。将功耗曲线组的功耗进行平均之后，能够消除电子噪声$P_{el.\ noise}$、与操作和数据都无关的功耗P_{random}、固定功耗P_{const}，这些功耗和中间值没有关联，在曲线集合中，它们的平均值近似相等。

3）正确密钥和错误密钥之间的系数差异很大。当中间值为非线性函数（不是密钥）时，DPA 方法应用相关性系数的方法求正确密钥的相关系数，正确密钥和错误密钥间的区分度较小。而在最小功耗分类方法下，如果密钥正确，寄存器和组合逻辑电路的中间值都未发生改变，变量的改变引起的功耗最小，即分类方法中可以利用到的功耗分量P_{exp}当前值最小；如果密钥错误，任何一个错误密钥对应的中间值为 0 曲线的P_{exp}值远大于正确密钥对应的中间值为 0 曲线的P_{exp}。

3 针对 AES 的最小功耗分类方法

在分组密码中，AES 具有代表性且攻击难度较高，其首轮运算在全随机明文的情况下很难攻击，因此，本文选取 AES 进行攻击。

3.1 AES 硬件实现

AES 算法可在不同的软硬件平台上进行实现，

由于 FPGA 具有配置硬件资源可重构、运算速度快等优点,因此,本文选择在 FPGA 上实现 AES 硬件电路,如图 3 所示[21],其中,阴影部分为寄存器,每一轮执行 SubBytes、ShiftRows、MixColumns 及 AddRoundKey 后将新生成的 AES 状态存入寄存器。图 3 为 AES 硬件实现时的一种通用架构,能够节省电路面积,且运算速度较快。

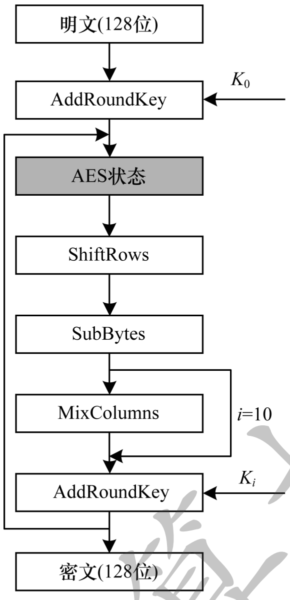


图 3　AES 硬件实现原理图

Fig. 3　Schematic diagram of AES hardware implementation

3.2　AES 每轮的整体功耗拆分

AES 每一轮的 SubBytes、ShiftRows、MixColumns 及 AddRoundKey 计算,可以近似拆分成 16 个单独的功耗模块。如图 4 所示,每个模块的功耗由其输入所决定。上述功耗模块分别用模块 1 ~ 模块 16 表示,模块 1 对应 AES 状态寄存器的第 1 个字节 state[127:120]和密钥的第 1 个字节 key[127:120]。

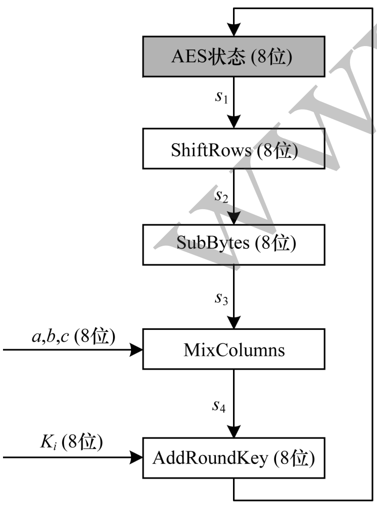


图 4　一个功耗模块对应的硬件架构

Fig. 4　Hardware architecture of a power consumption module

3.3　最小功耗分类方法应用

在应用最小功耗分类方法时,首先选择攻击算法的中间值。本文选择的寄存器是 AES 状态(8 位)寄存器,时间节点为第 1 轮。在攻击密钥的第 1 个字节时,中间值的表达式如下:

$$v = T_{\text{text\_out}}(D-1,0) \oplus T_{\text{text\_in}}(D,0) \oplus K_{\text{key}} \tag{5}$$

其中,$T_{\text{text_out}}(D-1,0)$表示第 $D-1$ 条曲线的密文的第 1 个字节,$T_{\text{text_in}}(D,0)$表示第 D 条曲线的明文的第 1 个字节,K_{key}表示猜测的 8 位密钥。

由图 4 可以看出,该寄存器的变化也会引起中间变量表 $s_1 \sim s_4$ 的变化,且 s_1、s_2、s_3 只会随 X 的变化而变化,s_4 会受到 X 变化的影响。$s_1 \sim s_4$ 的变化会引起较大的组合逻辑电路功耗,当寄存器变化前后的值一样,即异或值为 0 时,寄存器翻转功耗为 0,$s_1 \sim s_3$ 保持不变,此时产生的动态功耗分量较小。

然后,参照 2.2 节的内容完成余下步骤。选择 AES 功耗曲线的第 2 个尖峰附近的点进行分类和平均,攻击出密钥,中间值 $\boldsymbol{V}$ 引起的寄存器翻转泄露和组合逻辑泄露都发生在该时刻附近。

3.4　算法伪代码

针对 AES 的最小功耗分类方法的实现伪代码如算法 1 所示。其中,T_{trace} 为二维数组,存储曲线上各个点的功耗信息,D_{data} 存储曲线的明密文信息。算法输出选定位置各密钥对应的曲线集合的功耗平均值。

算法 1　最小功耗分类方法

输入　T_{trace}, D_{data}

输出　r_4

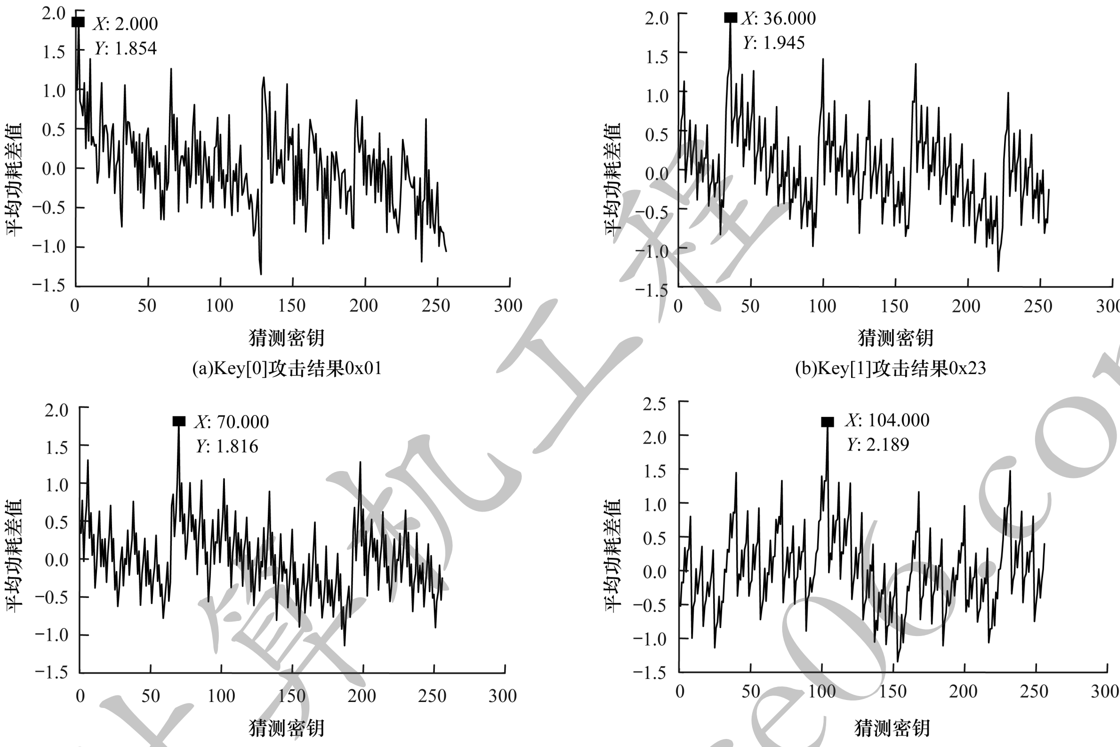
```
for t_i = 1:tracenum
sample (t_i) = trace(t_i, point );
end
for byte = 1:16
for k_0 = 0:255
r_2 = 0;
r_3 = 0;
for t_i = 2:tracenum
a = data(t_i, byte) ⊕ data(t_i - 1, byte + 16) ⊕ k_0;
if  a = = 0
r_2(k_0 + 1) = r_2(k_0 + 1) + sample(t_i);
r_3(k_0 + 1) = r_3(k_0 + 1) + 1;
end
end
r_4(k_0 + 1) = r_2(k_0 + 1)/r_3(k_0 + 1);
end
figure:plot(r_4);
end
```

4　实验结果与分析

本文通过一款专门用于研究硬件电路旁路安全的开发板 SAKURA-G 来模拟 AES 功耗曲线,以进行实验对比与分析。

4.1 针对 AES 的最小功耗分类方法性能分析

对不带防护的 AES 算法硬件实现电路的首轮运算进行攻击,在 100 万条全随机明文的功耗曲线数量下(功耗曲线的密钥为 0x012345789abcdef、0x012345789 abcdef),攻击结果如图 5 所示,其中,纵坐标表示猜测密钥对应的曲线集合的平均功耗和全部曲线的平均功耗的差值,曲线的纵坐标越高,表示平均功耗越小,(X,Y)为最高点坐标。从图 5 可以看出,各猜测密钥对应的曲线集合的平均功耗差异较大,且正确密钥与错误密钥区分明显。图 5 只选取了 4 个字节的攻击结果,在实际实验中攻击出了 AES 算法的全部密钥。



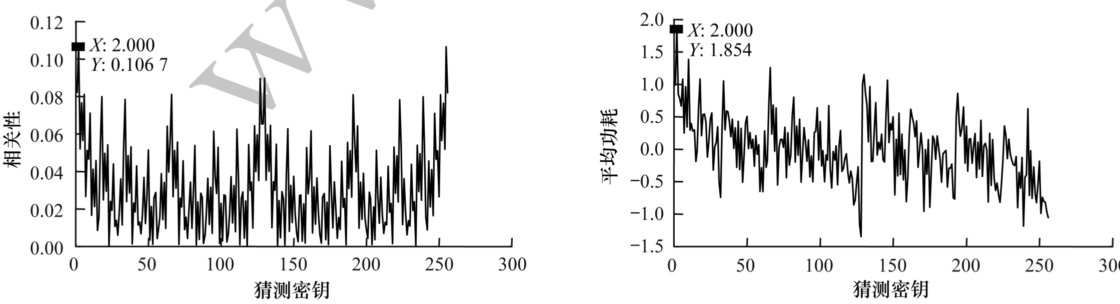
(a)Key[0]攻击结果0x01　(b)Key[1]攻击结果0x23　(c)Key[2]攻击结果0x45　(d)Key[3]攻击结果0x67

图 5 最小功耗分类方法攻击结果

Fig. 5 Attack results of minimum power consumption classification method

4.2 与 DPA 攻击的比较

对不带防护的 AES 算法硬件实现电路的 20 万条全随机明文功耗曲线,分别应用最小功耗分类方法和基于中间值的汉明重量模型 DPA 方法进行首轮攻击,密钥第 1 个字节的攻击结果对比如图 6 所示,全部密钥的攻击结果对比如表 1 所示。其中,图 6(a)中的纵坐标是猜测密钥中间值矩阵和功耗矩阵的相关性,图 6(b)中的纵坐标是猜测密钥对应的曲线集合的平均功耗。在表 1 中,系数差百分比为负数表示正确密钥未排名第一,值的大小为正确密钥相对排名第一的错误密钥的系数差百分比。从图 6 和表 1 可以看出,最小功耗分类方法相比 DPA 方法具有更好的区分度,前者排名第二的错误密钥相对正确密钥的系数差百分比大多都超过 10%,平均超过 20%,而 DPA 方法排名第二的错误密钥相对正确密钥的系数差百分比都在 0.2% 以内,两者相差 100 个数量级。



(a)DPA方法攻击结果　(b)最小功耗分类方法功击结果

图 6 2 种方法对密钥第 1 个字节的攻击结果对比

Fig. 6 Comparison of attack results of 2 methods on the first byte of key

表 1　2 种方法对全部密钥的攻击结果对比

Table 1　Comparison of attack results of 2 methods on all keys

密钥字节	排名第二的错误密钥相对正确密钥的系数差百分比/%	
	最小功耗分类方法	DPA 方法
0	39.33	0.10
1	23.70	0.10
2	29.40	0.10
3	34.10	0.10
4	32.60	0.10
5	11.30	0.20
6	11.90	0.01
7	-0.67	0.20
8	6.20	0.13
9	16.00	0.02
10	29.10	0.01
11	28.50	0.01
12	25.20	0.09
13	31.50	0.18
14	19.30	0.17
15	17.00	0.16

5　结束语

本文提出一种针对分组密码的最小功耗分类方法。相对 DPA 攻击方法,该方法能利用更多的组合逻辑功耗和寄存器翻转功耗,提高有用功耗的比例。实验结果表明,最小功耗分类方法对不带防护的 AES 算法硬件实现电路的攻击具有有效性,可以恢复出全部密钥,且恢复出的密钥存在较高的区分度。由于分组密码算法结构类似,硬件实现时也存在寄存器功耗和组合逻辑功耗,因此在理论上最小功耗分类方法对其他分组密码算法同样有效。下一步将研究该方法对带防护的分组密码算法硬件实现电路的攻击性能。

参考文献

[1] LI Lang. Research on power analysis attacks and defense issues of block ciphers chip[D]. Changsha: Hunan University,2010. (in Chinese)
李浪. 分组密码芯片功耗攻击与防御问题研究[D]. 长沙:湖南大学,2010.

[2] YANG Jing. Differential power analysis and countermeasures on ultra-lightweight block cipher--PRESENT[D]. Chengdu: Southwest Jiaotong University,2013. (in Chinese)
杨静. 超轻量级密码 PRESENT 的差分功耗攻击及其防护[D]. 成都:西南交通大学,2013.

[3] GU Xingyuan. Research on resistance to side channel attack in software implemented cryptographic system[D]. Shanghai: Shanghai Jiao Tong University,2013. (in Chinese)
顾星远. 软件实现的密码系统的旁路攻击防护研究[D]. 上海:上海交通大学,2013.

[4] KOCHER P,JAFFE J,JUN B. Differential power analysis[C]// Proceedings of the 19th Annual Inter-national Cryptology Conference on Advances in Cryptology. Berlin, Germany: Springer,1999:388-397.

[5] HUANG Luyun. Principle and simulation of differential power analysis attack based on AES encryption device[J]. Information Technology,2013(12):170-173. (in Chinese)
黄露昀. AES 加密设备的差分能量攻击原理与仿真[J]. 信息技术,2013(12):170-173.

[6] LI Peizhi. The research on template attack for block cipher chips [D]. Zhengzhou: PLA University of Information Engineering,2013. (in Chinese)
李佩之. 分组密码芯片模板攻击关键技术研究[D]. 郑州:解放军信息工程大学,2013.

[7] BRIER E,CLAVIER C,OLIVIER F. Correlation power analysis with a leakage model[C]//Proceedings of the 6th International Workshop on Cryptographic Hardware and Embedded Systems. Washington D. C. ,USA:IEEE Press,2004:11-13.

[8] WHITNALL C,OSWALD E,FRANÇOIS-XAVIER S. The myth of generic DPA…and the magic of learning [EB/OL]. [2018-11-05]. https://eprint. iacr. org/2012/256. pdf.

[9] HOSPODAR G,GIERLICHS B,MULDER E D,et al. Machine learning in side-channel analysis:a first study[J]. Journal of Cryptographic Engineering,2011,1(4):293-302.

[10] LERMAN L,MEDEIROS S F,VESCHCHIKOV N,et al. Semi-supervised template attack [C]//Proceedings of the 4th International Conference on Constructive Side-Channel Analysis and Secure Design. Berlin,Germany: Springer,2013:256-263.

[11] LERMAN L,BONTEMPI G,MARKOWITCH O. A machine learning approach against a masked AES[J]. Journal of Cryptographic Engineering,2015,5(2):123-139.

[12] CHEN Zhimin. Side channel power analysis on secure integrated circuits and countermeasures[D]. Shanghai: Shanghai Jiao Tong University,2006. (in Chinese)
陈志敏. 安全芯片旁路功耗分析及抗攻击措施[D]. 上海:上海交通大学,2006.

[13] MANGARD S, OSWALD E, POPP T. Power analysis attacks[EB/OL]. [2018-11-05]. http://www. springerlink. com/content/g01q1k.

[14] MANGARD S, OSWALD E, POPP T. Energy analysis attack[M]. Translated by FENG Dengguo,ZHOU Yongbin, LIU Jiye. Beijing:Science Press,2010. (in Chinese)
MANGARD S,OSWALD E,POPP T. 能量分析攻击[M]. 冯登国,周永彬,刘继业,译. 北京:科学出版社,2010.

[15] WANG Yunfeng. Research on chaos based cryptography and key technologies[D]. Hangzhou:Zhejiang University,2006. (in Chinese)
王云峰. 基于混沌的密码算法及关键技术研究[D]. 杭州:浙江大学,2006.

(下转第 113 页)

（上接第 107 页）
[16] MAO Jinliang. Design and implementation of dynamic clock-gating management strategy [D]. Nanjing: Southeast University, 2014. (in Chinese)
茅锦亮. 动态时钟门控管理策略的设计与实现[D]. 南京:东南大学, 2014.
[17] LE Daheng. Research on circuit-level design against power analysis attack for cryptographic chip [D]. Changsha: National University of Defense Science and Technology, 2011. (in Chinese)
乐大珩. 抗功耗攻击的密码芯片电路级防护关键技术研究[D]. 长沙:国防科技大学, 2011.
[18] HAN Xueyang. Improved correlation energy analysis attack based on preprocessing energy trace [D]. Jinan: Shandong University, 2016. (in Chinese)
韩学洋. 基于预处理能量迹的改进相关能量分析攻击[D]. 济南:山东大学, 2016.
[19] CHU Jie, DING Guoliang, DENG Gaoming, et al. Design and realization of differential power analysis for DES[J]. Journal of Chinese Computer Systems, 2007, 28(11): 2070-2073. (in Chinese)
褚杰, 丁国良, 邓高明, 等. DES 差分功耗分析攻击设计与实现[J]. 小型微型计算机系统, 2007, 28(11): 2070-2073.
[20] WANG Pengjun, HAO Lipeng, ZHANG Yuejun. Design of AES subbyte module of anti-zero value power attack and its VLSI implementation [J]. Acta Electronica Sinica, 2012, 40(11): 2183-2187. (in Chinese)
汪鹏君, 郝李鹏, 张跃军. 防御零值功耗攻击的 AES SubByte 模块设计及其 VLSI 实现[J]. 电子学报, 2012, 40(11): 2183-2187.
[21] LU Langru, KUANG Youhua, YANG Qianghao, et al. How to implement AES by using FPGA[J]. Computer and Communications, 2001, 19(5): 14-17. (in Chinese)
陆浪如, 匡友华, 杨强浩, 等. AES 算法的 FPGA 实现[J]. 交通信息与安全, 2001, 19(5): 14-17.

编辑　吴云芳