Journal of Computer Applications
计算机应用, 2020, 40(7): 1977 - 1982
ISSN 1001-9081
CODEN JYIIDU
2020-07-10
http://www.joca.cn

文章编号:1001-9081(2020)07-1977-06
DOI:10.11772/j.issn.1001-9081.2019122209

SM4密码算法的阶梯式相关能量分析

丛　旌[1,2],韦永壮[1,2*],刘争红[1,2]

(1. 广西密码学与信息安全重点实验室(桂林电子科技大学),广西 桂林 541004;
2. 广西无线宽带通信与信号处理重点实验室(桂林电子科技大学),广西 桂林 541004)

(*通信作者电子邮箱walker_wyz@guet.edu.cn)

摘　要:针对相关能量分析(CPA)易受噪声干扰、分析效率低的问题,提出了一种阶梯式CPA方案。首先,通过构造一种新的阶梯式方案提高CPA中信息的利用率;其次,通过引入confidence指标提升每一次分析的正确率,解决前几次分析正确率得不到保证的问题;最后,基于SM4密码算法结构给出了一个阶梯式CPA方案。模拟实验结果表明,在达到90%分析成功率的前提下,阶梯式CPA比传统CPA减少了25%能量迹条数的需求。现场可编程门阵列(FPGA)上的实验表明,阶梯式CPA恢复完整轮密钥的能力已经非常接近将搜索空间扩展到最大时的极限。阶梯式CPA能以足够小的计算量减少噪声的干扰、提高分析的效率。

关键词:侧信道分析;相关能量分析;SM4分组密码算法;并行实现;阶梯式方案

中图分类号:TN918.1; TP309　　**文献标志码**:A

Stepwise correlation power analysis of SM4 cryptographic algorithm

CONG Jing[1,2], WEI Yongzhuang[1,2*], LIU Zhenghong[1,2]

(1. *Guangxi Key Laboratory of Cryptography and Information Security* (*Guilin University of Electronic Technology*), *Guilin Guangxi* 541004, *China*;
2. *Guangxi Key Laboratory of Wireless Wideband Communication and Signal Processing* (*Guilin University of Electronic Technology*), *Guilin Guangxi* 541004, *China*)

Abstract: Focused on the low analysis efficiency of Correlation Power Analysis (CPA) interfered by noise, a stepwise CPA scheme was proposed. Firstly, the utilization of information in CPA was improved by constructing a new stepwise scheme. Secondly, the problem that the accuracies of previous analyses were not guaranteed was solved by introducing the confidence index to improve the accuracy of each analysis. Finally, a stepwise CPA scheme was proposed based on the structure of SM4 cryptographic algorithm. The results of simulation experiments show that, on the premise of the success rate up to 90%, stepwise CPA reduces the demand of power traces by 25% compared to classic CPA. Field Programmable Gate Array (FPGA) based experiments indicate that the ability of stepwise CPA to recover the whole round key is very close to the limit of expanding the search space to the maximum. Stepwise CPA can reduce the interference of noise and improve the efficiency of analysis with a small amount of calculation.

Key words: Side Channel Analysis (SCA); Correlation Power Analysis (CPA); SM4 block cryptographic algorithm; parallel implementation; stepwise scheme

0　引言

2012年3月,国家密码管理局发布SM4作为密码行业的标准。过去十年,专家学者们已经对SM4密码算法的实现展开了一系列分析研究,特别是在侧信道分析(Side Channel Analysis, SCA),如差分能量分析[1]、相关能量分析(Correlation Power Analysis, CPA)[2-3]等方面取得了若干重要进展。

侧信道分析通过分析密码算法实现过程中的中间值的信息泄露进行破译。时间[4]、功耗[5]、电磁波[6-7]等信息均可被用于分析密码系统。简单能量分析是侧通道分析中最经典的一种,即:不同的操作可能产生不同的功耗。通过观察采集到的设备加密过程中的能量波形,可以直接得到设备执行的具体操作,并进一步推测设备中的数据。1999年,差分能量分析由Kocher等[5,8]首先提出,后来由Messerges等[9]将其形式化。差分能量分析仅利用1位功率信息对能量迹进行分类[10],是侧通道分析中使用最广泛的分析方法。为了改进原有的差分能量分析,Bevan等[11]、Messerges等[12]引入了多位差分功耗分析(Differential Power Analysis, DPA)。然后,基于汉明距离泄漏模型的相关能量分析在文献[13]中提出,该方案通过计算功率样本与密码算法中间值汉明距离之间的相关系数确定正确的密钥。该泄漏模型同样适用于以S盒为单位的部分密钥;故当密钥空间较大时,可以通过分而治之的方法逐个恢复部分密钥,从而获得完整密钥。近几年,人工智能(Artificial Intelligence, AI)算法也开始应用于侧通道分析当中[14-15]。

收稿日期:2020-01-02;**修回日期**:2020-03-02;**录用日期**:2020-03-11。　**基金项目**:国家自然科学基金资助项目(61872103);广西重点研发计划项目(桂科AB18281019);桂林电子科技大学研究生科研创新项目(2018YJCX45)。

作者简介:丛旌(1993—),男,江苏南通人,硕士研究生,主要研究方向:分组密码算法、侧信道分析;　韦永壮(1976—),男,广西田阳人,教授,博士,主要研究方向:对称密码算法设计与分析;　刘争红(1979—),男,湖北红安人,讲师,硕士,主要研究方向:无线宽带通信、FPGA、GPU并行运算。

注意到，为了追求效率，密码算法在硬件实现时通常采用并行实现的方案。此时，传统的基于单个S盒的泄漏模型不再足够精确。文献[16]将传统相关能量分析中基于单个S盒的泄漏模型改进为基于多个S盒的泄漏模型，并通过引入遗传算法以对抗扩大的搜索空间。文献[17]在此基础上进行了改进，设计了基于多种群遗传算法的相关能量分析，以应对遗传算法过早收敛的问题。两者均大幅降低了恢复密钥所需的能量迹的条数，但都存在离线计算量较大、样本不足时得不到任何结果等问题。如何以尽可能小的计算量减少噪声，提高泄漏信息的利用率，成为研究的难点。

本文针对密码算法并行实现下相关能量分析效率低下的现象分析了原因，并提出了新的方法：阶梯式相关能量分析。其核心思想是优化传统相关能量分析的流程，提高能量迹的利用率，从而提高分析效率，减少能量迹的条数需求。阶梯式相关能量分析通过构造一种新的阶梯式方案并引入confidence指标，可以在分析时回避正确性较低的分析结果，以确保每一次分析的结果有尽可能高的正确率。同时，随着阶梯式流程的推进，原本作为干扰项的部分噪声也将被逐一消除。整个分析过程变得越来越准确，这使得原本容易受噪声干扰的部分密钥的恢复过程变得不再容易出错。将阶梯式相关能量分析应用于SM4密码算法的分析，本文得到了优于传统相关能量分析的结果。其计算量与传统相关能量分析相当，但明显减少了恢复完整轮密钥所需求的能量迹条数。

1 预备知识

1.1 SM4密码算法

SM4密码算法与数据加密标准(Data Encryption Standard, DES)[18]及高级加密标准(Advanced Encryption Standard, AES)[19]类似，均为分组密码。SM4的分组长度和密钥长度均为128比特，加密算法与密钥扩展算法均采用32轮非线性迭代结构，以32比特为单位进行加密运算。SM4密码算法的加、解密算法的结构相同、使用的轮密钥相反，其解密轮密钥是加密轮密钥的逆序。

SM4密码算法的整体结构如图1所示。

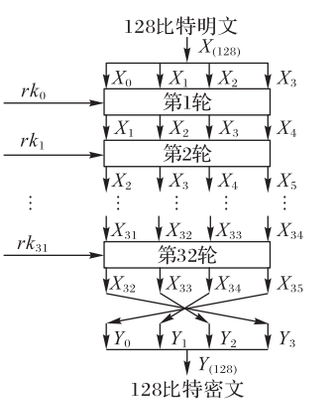


图1 SM4算法结构

Fig. 1 Structure of SM4 algorithm

明文输入为：

$X_{(128)} = (X_0, X_1, X_2, X_3) \in (GF(2^{32}))^4$

密文输出为：

$Y_{(128)} = (Y_0, Y_1, Y_2, Y_3) \in (GF(2^{32}))^4$

第i轮运算输入为：

$X_i, X_{i+1}, X_{i+2}, X_{i+3}$

轮密钥为：

$rk_i \in GF(2^{32})$; $i = 0, 1, \cdots, 31$

则轮函数定义为：

$$X_{i+4} = F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i) = X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i)$$

其中T为非线性变换和线性变换复合而成的合成置换。非线性变换由4个平行的S盒构成，S盒的数据均采用16进制。线性变换公式如下：

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

其中B为非线性变换得到的字。

最后一轮加密变换时，输出为：

$$(Y_0, Y_1, Y_2, Y_3) = R(X_{32}, X_{33}, X_{34}, X_{35}) = (X_{35}, X_{34}, X_{33}, X_{32})$$

其中R为反序变换。

1.2 相关能量分析

文献[20]给出了相关能量分析的具体分析步骤，概括如下：

步骤1 选择中间值。选择合适的分析点是进行具体相关能量分析的前提。通过分析具体的密码算法，找到加解密过程中的一个中间值。这个中间值通常由一个函数$f(p,k)$生成，其中p是明文的一部分，k是与p相对应的密钥的一部分。满足这种条件的中间值可以泄露k。

步骤2 采集能量迹。搭建实验平台，进行d次加密或解密，每次采集长度为l的能量迹，构成大小为$d \times l$的矩阵$\boldsymbol{T}$。同时记录每次加密或解密时计算中间值$f(p,k)$所需的p，构成长度为d的向量$\boldsymbol{P} = (p_1, p_2, \cdots, p_d)$。采集到的能量迹需要进行预处理(如对齐操作等)，确保矩阵$\boldsymbol{P}$中每一列数据对应的功耗均由相同的操作产生。

步骤3 计算假设中间值。对k进行穷举，记为向量$\boldsymbol{K} = (k_1, k_2, \cdots, k_n)$，其中$n$表示$k$所能取到的所有值的数量。根据所有$d$次加密或解密对应的$p$和所有$n$个密钥假设，计算$v = f(p,k)$，构成大小为$d \times n$的矩阵$\boldsymbol{V}$。

步骤4 将中间值映射为功耗。选择合适的功耗模型，对$\boldsymbol{V}$中的每个假设中间值计算对应的假设功耗值，得到由中间值矩阵$\boldsymbol{V}$映射而成的功耗矩阵$\boldsymbol{H}$，其大小依然为$d \times n$。

步骤5 求相关系数。对矩阵$\boldsymbol{H}$中的每一列h_i与矩阵$\boldsymbol{T}$中的每一列t_j求相关系数，构成大小为$n \times l$的矩阵$\boldsymbol{R}$。其中的元素$r_{i,j}$越大，表示h_i与t_j的匹配性越好。最大元素所对应的列标即为所求密钥。相关系数计算公式如下：

$$r_{i,j} = \frac{\sum_{d=1}^{D}(h_{d,i} - \overline{h_i})(t_{d,j} - \overline{t_j})}{\sqrt{\sum_{d=1}^{D}(h_{d,i} - \overline{h_i})^2 \sum_{d=1}^{D}(t_{d,j} - \overline{t_j})^2}} \tag{1}$$

2 阶梯式相关能量分析

2.1 并行实现下的相关能量分析

在相关能量分析中，采集到的能量分为两部分：信息与噪声。信息，即分析对象对应的S盒在运行时产生的能量；噪声，包括密码设备运行时其他模块产生的能量与白噪声。特别的，在密码算法并行实现的条件下，其他S盒的能量信息也会包含在采集到的能量中。这些能量将被视为该次分析中的

噪声,对分析结果产生干扰。

从图2中可以明确得知,单次分析的密钥比特数越多,噪声越小,但相应的搜索空间也会越大;反之,搜索空间减小,但受噪声的影响更大。如何权衡两者之间的关系,或者找到新的方法在同一数量级的计算量上提高分析的效率是研究的关键。传统相关能量分析采用分而治之的思想,每一次分析恢复一个S盒对应的部分密钥,多次分析恢复完整轮密钥。但实际上在每一次部分密钥的恢复后,一些本可以被利用的信息被忽略掉了。

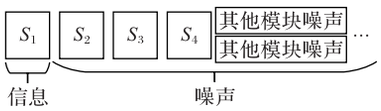


图2　采集能量的构成

Fig. 2　Composition of collected power

2.2　阶梯式方案

相关能量分析的传统方案通过分而治之的思想,利用多次分析分别恢复每个S盒对应的部分密钥,如图3所示:第一次分析第一个S盒对应的部分密钥,之后每次分析下一个S盒对应的部分密钥,直到分析完所有S盒对应的部分密钥,构成完整轮密钥。图3中 m 表示完整轮密钥包含的数据字的个数。每一次分析的过程是相互独立的,即一次分析的结果不会对其他分析造成任何影响。当噪声较大或能量迹条数过少时,分析的成功率降低。而任意一次分析的失败都将导致完整密钥恢复的失败,这是相关能量分析失败最常见的原因。

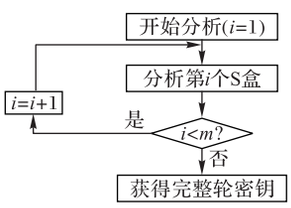


图3　传统相关能量分析方案

Fig. 3　Classic CPA scheme

然而,成功完成其中任意一次分析后,所获的部分密钥对下一次分析而言并不是没有任何意义的。将一次分析的结果纳入下一次的分析目标,将在维持搜索空间不变的前提下,有效减少噪声、增加信息。如:第一次分析以第一个字节的密钥为分析目标,得到分析结果:k_1 = 01010101。第二次分析,将第一字节与第二字节同时作为分析目标。其中第一字节固定为 k_1 = 01010101 不变,第二字节 k_2 从 00000000 遍历至 11111111。每次分析的密钥字节数越来越长,由图2可知噪声将会减少。但是因为每次分析只添加一个字节的新密钥,其他密钥都是已知的、固定不变的,所以搜索空间依然是 2^8 = 256。具体方案为:第一次分析第一个S盒对应的8比特密钥,之后每次分析都将下一个S盒对应的8比特密钥纳入攻击范围。在保持前一次分析结果不变的前提下,遍历下一个S盒对应的8比特密钥,直到最后一次分析,获得完整的轮密钥。

阶梯式方案的优势在于:随着阶梯式流程的推进,分析的密钥字节数越来越长,噪声越来越少。这意味着后分析的部分密钥将有越来越高的正确率。但相关能量分析的成功,即完整密钥的恢复,取决于每一次对部分密钥分析的成功与否,而非单次分析成功率的最大值。前几次分析的正确性成了阶梯式方案的短板。单纯的阶梯式方案并不能对前几次分析的成功率产生有效影响,而后几次分析成功率的提升对完整密钥恢复的成功率提升非常有限,所以需要进一步引入文献[21]中提及的confidence指标(下文中简称c指标):

$$confidence = r_1 - r_2 \tag{2}$$

其中:r_1 为一次相关能量分析中获得的最大的相关系数;r_2 为同一次相关能量分析中获得的第二大的相关系数。c指标为两者之差,它可以有效地衡量这一次相关能量分析结果的正确性。指标数值越大,结果为正确的可能性越大,反之则越有可能是受噪声干扰所得的错误结果。

具体分析流程如图4。描述如下:第一次分析,依次对4个S盒对应的部分密钥进行分析,并计算每次分析的c指标。保留c指标最高的一次分析所得的密钥。第二次分析,将已恢复的密钥纳入分析目标,继续分析其余3个S盒对应的部分密钥,并计算每次分析的c指标。如:第一次分析已恢复 k_3,则依次分析 $k_1|k_3$, $k_2|k_3$, $k_4|k_3$,其中 k_3 固定为已恢复的值,k_1, k_2, k_4 依次遍历256种候选值。保留c指标最高的一次分析所得的密钥。以此类推,直到第四次分析结束,恢复出完整轮密钥。为了便于理解具体流程,表1给出了阶梯式相关能量分析实例中每一次分析的具体参数。

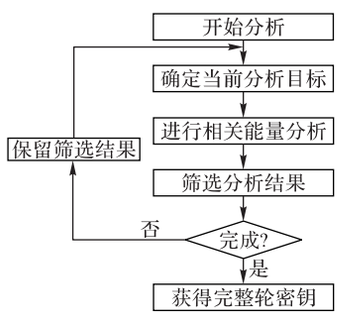


图4　阶梯式相关能量分析方案

Fig. 4　Stepwise CPA scheme

表1　阶梯式相关能量分析实例

Tab. 1　Example of stepwise CPA

序号	已恢复	当前目标	固定位	恢复结果
1	无	k_1, k_2, k_3, k_4	无	k_3
2	k_3	$k_1\|k_3$, $k_2\|k_3$, $k_4\|k_3$	k_3	$k_1\|k_3$
3	$k_1\|k_3$	$k_2\|k_1\|k_3$, $k_4\|k_1\|k_3$	$k_1\|k_3$	$k_1\|k_2\|k_3$
4	$k_1\|k_2\|k_3$	$k_4\|k_1\|k_2\|k_3$	$k_1\|k_2\|k_3$	$k_1\|k_2\|k_3\|k_4$

c指标的引入在一定程度上解决了前几次分析正确率得不到保证的问题。可以说,依据c指标筛选分析结果是在资源已定的情况下被动地提升成分析的功率,而阶梯式方案的推进则是主动消除噪声的影响,提升成功率。两者的结合有效提高了相关能量分析的成功率,尤其是在噪声较大、能量迹条数较少的情况下。

传统相关能量分析的基本思想是“分而治之”,但在分治的过程中,任何一次分析的错误都将导致最终完整轮密钥恢复的失败。本文提出的阶梯式相关能量分析,其基本思想是“步步为营”。相较于传统相关能量分析,只要有一次分析成功,就可以继续分析下去。而且随着阶梯式流程的推进,一些本可能发生错误的分析也将在接下来的分析中因噪声的减少而被进一步修正。

2.3　阶梯式相关能量分析的构造

阶梯式相关能量分析包含以下主要步骤:确定分析目标、

相关能量分析、筛选分析结果、状态更新。

相关数据定义如下：

1）m表示完整轮密钥包含的数据字的个数（以SM4密码算法为例，m=4）；

2）数组*key*存储所有已恢复的部分密钥；

3）数组*state*存储密钥恢复的状态（具体是一个长度为m的布尔数组，true表示当前下标对应的S盒对应的部分密钥已被恢复，反之则为false）；

4）数组*target*存储本次分析的目标（具体是一个长度为m的布尔数组，true表示当前下标对应的S盒对应的部分密钥被包含在本次分析的目标之内，反之则为false）；

5）数组*data*存储相关能量分析的结果和相应的精确系数；

6）数组*result*存储本次分析保留的恢复的部分密钥及其在完整轮密钥中的位置。

相关函数定义及其基本功能如下：

1）函数target()根据密钥恢复的状态返回本次分析的目标。若还没有任何部分密钥被恢复，则分析目标为分别为所有部分密钥；否则分析目标为所有未被恢复的部分密钥分别与已恢复的密钥合并。

2）函数cpa()根据分析目标、明文、S盒函数及能量迹返回相关能量分析的结果和相应的c指标。

3）函数select()根据相关能量分析的结果和相应的c指标返回本次分析保留的恢复的部分密钥及其在完整密钥中的位置。

4）函数update()根据本次分析结果更新数组*key*和数组*state*，以存储本轮恢复的部分密钥和当前密钥恢复的情况。

上述函数均为作者在C语言环境下编写而得。

下面给出阶梯式相关能量分析的伪代码：

算法1 阶梯式相关能量分析。

输入：能量迹W、明文P、S盒函数S；

输出：轮密钥。

```
1) FOR i:=1 TO m DO
2)     target:= target(state);
3)     data:= cpa(target, W, P, S);
4)     result:=select(data);
5)     update(result);
6) END FOR
7) RETURN key;
```

3 实验与结果分析

3.1 模拟实验

在模拟实验中，在C语言仿真平台上对SM4算法的S盒操作进行了模拟，并分别添加两种不同程度的噪声，其标准差分别为σ = 3.0和σ = 5.0。在这两组数据上分别执行了传统相关能量分析和本文提出的阶梯式相关能量分析。实验按照不同的给定能量迹条数分组进行，从100到1 000，间隔为10，每组实验取1 000次实验结果的平均值。图5给出了这两种方案的成功率。表2总结了在成功率达到50%和90%的前提下，两种方案对能量迹条数的需求和相应的计算量。由于计算量主要取决于相关系数的计算次数，所以这里忽略了排序操作的计算量，只记录恢复完整轮密钥所需计算相关系数的次数。

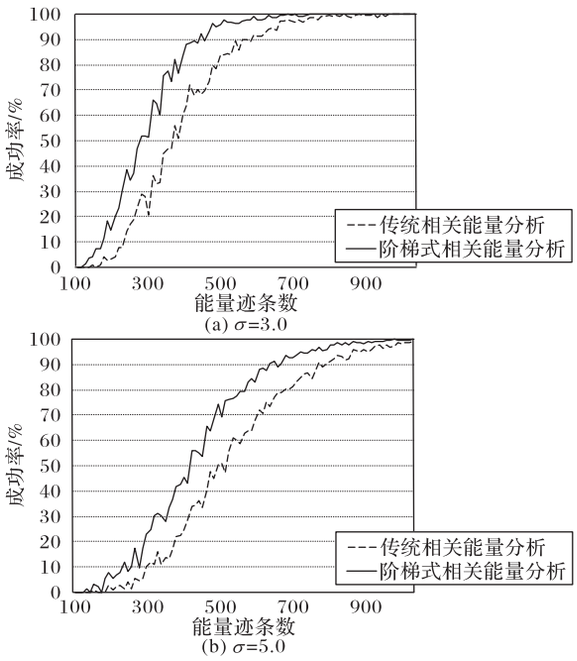


图5 不同噪声下能量迹条数与成功率的关系

Fig. 5 Relationship between the number of power traces and success rate under different noises

表2 阶梯式相关能量分析与传统相关能量分析对比

Tab. 2 Comparison of stepwise CPA and classic CPA

方案	成功率/%	能量迹		计算量
		σ=3.0	σ=5.0	
传统相关能量分析	50	360	490	1 024
	90	560	760	
阶梯式相关能量分析	50	270	410	2 560
	90	420	630	

实验结果表明，在能量迹条数相同的前提下，本文提出的阶梯式相关能量分析的成功率明显优于传统相关能量分析。当σ = 3.0时，阶梯式相关能量分析只需要420条能量迹就可以达到90%的成功率，而传统相关能量分析需要560条，减少了25%的能量迹条数需求。当σ = 5.0时，阶梯式相关能量分析只需要630条能量迹就可以达到90%的成功率，而传统相关能量分析需要760条，减少了17%的能量迹条数需求。值得一提的是，阶梯式相关能量分析的计算量为2 560次，是传统相关能量分析的2.5倍。相较于计算量达到几万甚至几十万的基于遗传算法的相关能量分析（Correlation Power Analysis based on Simple Genetic Algorithm, SGA-CPA）[16]和基于多种群遗传算法的相关能量分析（Correlation Power Analysis based on genetic algorithm and Multiple Sieve method, MS-CPA）[17]，阶梯式相关能量分析的计算量非常小，可以认为是与传统相关能量分析的计算量处于同一数量级上。

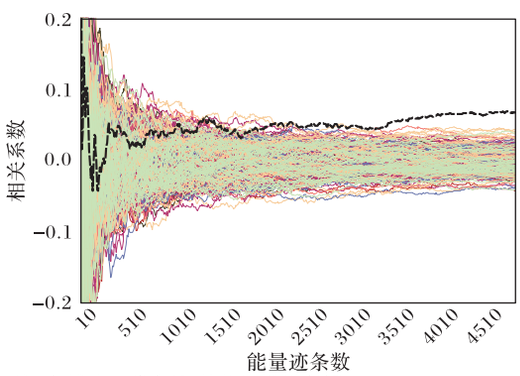
3.2 FPGA上的实验

在实际实验中，使用SAKURA-G自主搭建实验平台。SAKURA-G是一款专门为硬件安全方面的研究和开发而设计的FPGA板。它由两块Spartan-6 FPGA集成而来：主FPGA用于密码算法的实现；控制FPGA用于相应控制逻辑的实现。超低噪声的设计使能量分析变得更加容易。

在具体的相关能量分析实验中，把SM4硬件电路下载到SAKURA-G开发板上，然后将其触发输出和信号输出分别与

示波器相连,并将主控制口通过USB连接线与电脑相连。对固定的密钥和已知的随机明文执行SM4密码算法,并通过使用 LeCroy WaveRunner 610Zi 示波器与旁路分析软件SCAnalyzer完成5 000条能量迹的采集。实际采集到的每一条能量迹为一个长度为30 000的数组,记录了电压随时间变化的曲线。为了降低噪声和减少计算量,需要对能量迹进行重采样,即数组中的每10个点取平均数,记为一个点。

首先,对这5 000条能量迹进行传统相关能量分析,计算单字节部分密钥的所有可能值对应的中间值与能量迹的相关系数。图6给出了实验结果:虚线表示正确密钥,不同灰度的实线表示其他错误密钥。用于计算相关系数的能量迹条数为10~5 000,间隔为10。当能量迹条数大于3 430条时,正确密钥对应的相关系数始终大于错误密钥对应的相关系数,这意味着本次实验中使用传统相关能量分析恢复密钥至少需要3 430条能量迹。



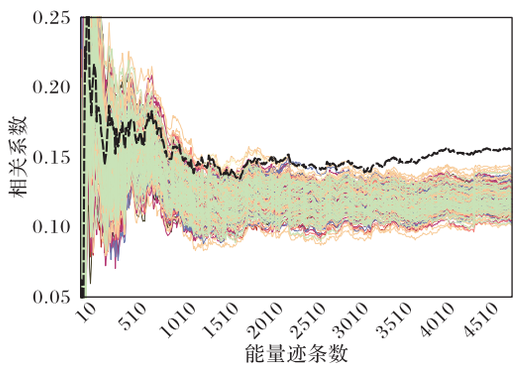
注:虚线为正确密钥;其他为错误密钥。

图6　相关系数与能量迹条数的关系(传统相关能量分析)

Fig. 6　Relationship between the number of power traces and correlation coefficient (classic CPA)

其次,对同样的5 000条能量迹计算其与完整密钥对应的中间值的相关系数,旨在找出同等实验环境下通过相关能量分析恢复完整轮密钥所需能量迹的最小数量。由于完整轮密钥长度为32比特,穷尽所有可能的计算量较大且没有必要,所以只选择部分最具"竞争力"的错误密钥与正确密钥进行对比。文献[17]已给出相关结论,即候选密钥中正确的字节数越多,其对应的相关系数越大。故本次实验中只选择$2^8 \times 4$个只含有3个正确字节的候选密钥与正确密钥做对比。经过实验结果的分析与对比发现,在本实验中,当第2个S盒对应的部分密钥错误、其他部分密钥正确时,错误密钥对应的相关系数与正确密钥对应的相关系数最接近。所以为了精简图表数据,图7将只给出这部分实验结果的数据:其中虚线表示正确密钥,不同灰度的实线表示其他错误密钥。用于计算相关系数的能量迹条数为 10~5 000,间隔为10。当能量迹条数大于3 100条时,正确密钥对应的相关系数始终大于错误密钥对应的相关系数,这意味着本次实验中以相关能量分析为基本思想恢复完整密钥最少需要3 100条能量迹。当然这是建立在将相关能量分析的搜索空间扩大到2^{32}的前提下的。这是通过巨大计算量换取分析精度的一种方式。

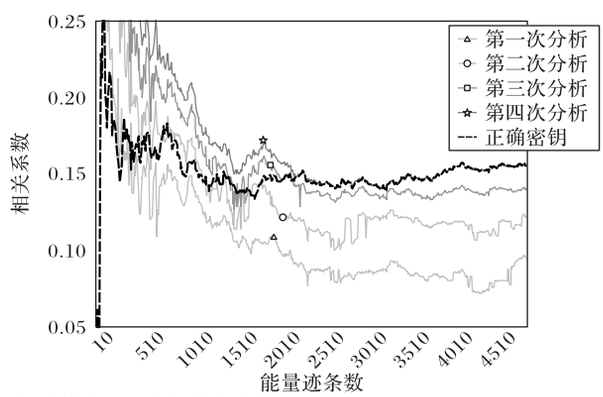
最后,同样是这5 000条能量迹,对其进行阶梯式相关能量分析,记录每一次分析的结果对应的相关系数,并与正确密钥对应的相关系数进行对比。图8给出了实验结果:其中虚线表示正确密钥,4种灰度的实线由浅至深分别表示4次分析的结果。用于计算相关系数的能量迹条数为10~5 000,间隔为10。当能量迹条数达到2 370条时,最后一次分析的结果对应的相关系数已基本与正确密钥对应的相关系数重合。当能量迹条数大于3 100条时,两者完全重合。这说明阶梯式相关能量分析恢复正确密钥的能力已经非常接近将搜索空间扩展到最大时的极限。



注:虚线为正确密钥;其他为错误密钥。

图7　相关系数与能量迹条数的关系(完整轮密钥)

Fig. 7　Relationship between the number of power traces and the correlation coefficient (whole round key)



注:虚线为正确密钥;其他为错误密钥。

图8　相关系数与能量迹条数的关系(阶梯式相关能量分析)

Fig. 8　Relationship between the number of power traces and correlation coefficient (stepwise CPA)

本次实验中,使用传统相关能量分析恢复密钥至少需要3 430条能量迹,而将搜索空间扩大到2^{32}时,对能量迹条数需求的极限是3 100条。阶梯式相关能量分析的结果在能量迹条数达到2 370条时基本与正确密钥吻合,在达到3 100条时完全吻合。不同实验中的数据存在细微的差别,但数据间的关系和比例大致不变。由此可以看出阶梯式相关能量分析相对于传统相关能量分析有明显的优越性。

4　结语

本文讨论了相关能量分析在并行实现下分析效率低下的原因,提出了阶梯式方案,并通过引入confidence指标,基于SM4密码算法的结构,构造了阶梯式相关能量分析。实验结果表明阶梯式相关能量分析以较小的计算量有效降低了传统相关能量分析对能量迹条数的需求,是一种精确、快捷的分析方案。接下来进一步的研究可以考虑对能量迹进行分析和筛

选,以减少计算量、提高分析效率。

参考文献(References)

[1] 沈薇. SMS4算法的能量分析攻击及其防御研究[D]. 西安:西安电子科技大学, 2009:13-34. (SHEN W. Investigations of power analysis attacks and its countermeasures on SMS4 cipher algroithm [D]. Xi'an: Xidian University, 2009:13-34.)

[2] 胡文静,王安,乌力吉,等. 基于SAKURA-G实验板的SM4硬件电路能量攻击研究[J]. 微电子学与计算机, 2015, 32(4):15-20. (HU W J, WANG A, WU L J, et al. Power attack of SM4 hardware implementation based on SAKURA-G board [J]. Microelectronics and Computer, 2015, 32(4): 15-20.)

[3] 王欢. 面向SM4密码算法智能卡实现的能量分析攻击与评估方法研究[D]. 北京:中国科学院大学, 2016:21-40. (WANG H. Study of the side-channel analysis against the smartcard implementation of SM4 algorithm and its security evaluation techniques [D]. Beijing: University of Chinese Academy of Sciences, 2016:21-40.)

[4] KOCHER P. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems[C]// Proceedings of the 16th Annual International Cryptology Conference, LNCS 1109. Berlin: Springer, 1996: 104-113.

[5] KOCHER P, JAFFE J, JUN B. Differential power analysis [C]// Proceedings of the 19th Annual International Cryptology Conference, LNCS 1666. Berlin: Springer, 1999: 388-397.

[6] GANDOLFI K, MOURTEL C, OLIVIER F. Electromagnetic analysis: concrete results[C]// Proceedings of the 3rd International Workshop on cryptographic Hardware and Embedded Systems, LNCS 2162. Berlin: Springer, 2001: 251-261.

[7] QUISQUATER J J, SAMYDE D. ElectroMagnetic Analysis (EMA): measures and counter-measures for smart cards[C]// Proceedings of the 2001 International Conference on Research in Smart Cards, LNCS 2140. Berlin: Springer, 2001: 200-210.

[8] KOCHER P, JAFFE J, JUN B, et al. Introduction to differential power analysis[J]. Journal of Cryptographic Engineering, 2011, 1(1): 5-27.

[9] MESSERGES T S, DABBISH E A, SLOAN R H. Investigations of power analysis attacks on smartcards[C]// Proceedings of the 1999 USENIX Workshop on Smartcard Technology. Berkeley: USENIX Association, 1999: 151-161.

[10] MAYER-SOMMER R. Smartly analyzing the simplicity and the power of simple power analysis on smartcards[C]// Proceedings of the 2nd International Workshop on Cryptographic Hardware and Embedded Systems, LNCS 1965. Berlin: Springer, 2000:78-92.

[11] BEVAN R, KNUDSEN E. Ways to enhance differential power analysis[C]// Proceedings of the 5th International Conference on Information Security and Cryptology, LNCS 2587. Berlin: Springer, 2002: 327-342.

[12] MESSERGES T S, DABBISH E A, SLOAN R H. Examining smart-card security under the threat of power analysis attacks[J]. IEEE Transactions on Computers, 2002, 51(5): 541-552.

[13] 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, LNCS 3156. Berlin: Springer, 2004: 16-29.

[14] PICEK S, HEUSER A, JOVIC A, et al. Side-channel analysis and machine learning: a practical perspective[C]// Proceedings of the 2017 International Joint Conference on Neural Networks. Piscataway: IEEE, 2017: 4095-4102.

[15] SHAN W, ZHANG S, HE Y. Machine learning based side-channel-attack countermeasure with hamming-distance redistribution and its application on advanced encryption standard[J]. Electronics Letters, 2017, 53(14): 926-928.

[16] ZHANG Z, WU L, WANG A, et al. A novel bit scalable leakage model based on genetic algorithm[J]. Security and Communication Networks, 2015, 8(18): 3896-3905.

[17] DING Y, WANG A, YIU S M. An intelligent multiple sieve method based on genetic algorithm and correlation power analysis[EB/OL]. [2019-04-23]. https://eprint. iacr. org/2019/189. pdf.

[18] MORRIS R, SLOANE N J A, WYNER A D. Assessment of the national bureau of standards proposed federal data encryption standard[J]. Cryptologia, 1977, 1(3): 281-291.

[19] DAEMEN J, RIJMEN V. The advanced encryption standard process[M]// The Design of Rijndael: AES—the Advanced Encryption Standard. Berlin: Springer, 2002:1-8.

[20] MANGARD S, OSWALD E, POPP T. Differential power analysis [M]// Power Analysis Attacks: Revealing the Secrets of Smart Cards. Boston: Springer, 2007:119-165.

[21] ROBYNS P, QUAX P, LAMOTTE W. Improving CEMA using correlation optimization[J]. IACR Transactions on on Cryptographic Hardware and Embedded Systems, 2019(1): 1-24.

This work is partially supported by the National Natural Science Foundation of China (61872103), the Key Research and Development Program of Guangxi (GUIKEAB18281019), the Graduate Research Innovation Project of Guilin University of Electronic Technology (2018YJCX45).

CONG Jing, born in 1993, M. S. candidate. His research interests include block cryptographic algorithm, side channel analysis.

WEI Yongzhuang, born in 1976, Ph. D., professor. His research interests include symmetric cryptographic algorithm design and analysis.

LIU Zhenghong, born in 1979, M. S., lecturer. His research interests include wireless broadband communications, FPGA, GPU parallel computing.