针对 AES 加密算法的安全检测

何利文,安　聪,国海轮
(南京邮电大学,江苏 南京 210003)

摘　要:侧信道攻击(side channel attack,SCA)是一种新兴的密码分析方法,主要通过加密软件或硬件运行时产生的各种泄漏信息获取密文信息,其中相关功耗分析(CPA)是较为强大的一种攻击方法,可以用来实现 AES 加密算法的安全检测。CPA 需要假设猜测密钥,然后根据示波器采集到的能量迹,使用具有数据相关性的汉明模型,并计算实际能量值与假设能量消耗之间的皮尔逊相关系数,利用皮尔逊相关系数来判断猜测密钥的正确与否。CPA 可以把皮尔逊相关系数的计算结果限制在[-1,1]之间且 CPA 过程自带标准化,不需要额外对数据进行标准化。此外,还利用 python 的 pandas 库和 style 方法对获得的结果进行刻画,更好地实现了相关系数和正确的密钥之间的关系。本案例使用 NewAE Technology Inc 的芯片物理攻击平台 ChipWhisperer 实施 CPA 攻击来检测加密算法的安全性,成功破解了预设的 AES-128 的 16 字节的密钥。实验表明,CPA 在针对未加防护的 AES 加密算法时有显著的效果,可以检测 AES 加密算法的安全性。

关键词:ChipWhisperer;高级加密标准;能量迹;相关功耗分析;相关系数
中图分类号:TP31　　**文献标识码**:A　　**文章编号**:1673-629X(2022)05-0087-06
doi:10.3969/j.issn.1673-629X.2022.05.015

Security Detection of AES Encryption Algorithm

HE Li-wen,AN Cong,GUO Hai-lun
(Nanjing University of Posts and Telecommunications,Nanjing 210003,China)

Abstract:Side channel attack (SCA) is a new cryptanalysis method,which mainly obtains ciphertext information through various leakage information generated by encryption software or hardware during operation. Among them,correlation power analysis (CPA) is a relatively powerful attack method,which can be used to realize the security detection of AES encryption algorithm. CPA needs to guess the key hypothesis,and then according to the energy trace collected by the oscilloscope,the Hamming model with data correlation is used,and the Pearson correlation coefficient between the actual energy value and the assumed energy consumption is calculated,and the Pearson correlation coefficient is used to judge the correctness of the guess key. CPA can limit the calculation result of Pearson correlation coefficient to between [-1,1] and the CPA process has its own standardization,so there is no need for additional standardization of data. In addition,we also use Python's Pandas library and style method to characterize the results obtained,better realizing the relationship between the correlation coefficient and the correct key. This case uses NewAE Technology Inc's chip physical attack platform ChipWhisperer to implement CPA attack to detect the security of encryption algorithm,and successfully cracked the preset 16-byte key of AES-128. The experiment shows that CPA has a significant effect on the unprotected AES encryption algorithm,and can detect the security of the AES encryption algorithm.

Key words:ChipWhisperer;advanced encryption standard;trace;correlation power analysis;correlation coefficient

0　引　言

近年来,信息安全问题日益突出,已成为人类共同面临的挑战,侧信道攻击对信息安全构成了巨大的威胁。密码芯片在工作过程中不可避免地会产生时间、功耗、电磁辐射等旁道信息[1]。这些信息与芯片内部的数据和操作有关。因此,侧信道信息可用于攻击密码芯片。利用侧信道信息破解密文信息的方法最早由 Kocher 于 1996 年提出,随后逐渐发现了差分功耗分析(DPA)、相关功耗分析(CPA)等侧信道攻击方法[2]。目前,已经成功地在许多设备上实现了多种侧信道攻击[3]。

差分功耗分析(differential power analysis,DPA)[4]可以从功耗曲线微小的差分信号分析出所需的关键信息,但需要采集大量的信息,并采集多组功耗

收稿日期:2021-04-17　　**修回日期**:2021-08-20
基金项目:2018 年国家重点研发计划项目(2018YFB2100200)
作者简介:何利文(1968-),男,博士,教授,研究方向为网络、信息安全、云计算大数据分析与应用;通信作者:安　聪(1996-),男,硕士研究生,研究方向为信息安全。

曲线以及每条曲线对应的明文、密文记录,通常需要很强的分析经验和较长时间的分析运算,对分析平台的设备要求也比较高。而相关功耗分析(correlation power analysis,CPA)[5]是选择一个未知但是恒定的参考态,建立一个具有数据相关性的汉明模型,利用功耗样点与被处理数据的汉明权重之间的相关因子进行分析。因此 CPA 攻击的准确性要比 DPA 高很多。

1 背景介绍

1.1 高级加密标准

高级加密标准[6](advanced encryption standard,AES)是最常见的对称加密算法,加解密使用相同的密钥,可以在不同的平台上实现:

明文(p),可理解的消息或数据,机密算法的输入,解密算法的输出。AES-128 的明文长度为 128 位。

密钥(k),在将明文转换为密文或者将密文转换为明文算法中输入的数据。AES-128 的密钥长度为 128 位。

轮数(r),AES-128 的加密轮数为 10 轮。

其中 AES-128 加密算法由 10 轮组成,每一轮使用一个由原始密钥产生的密钥。每一轮由四个基本步骤组成:字节替换、行移位、列混合变幻、轮密钥加密变换。

密文(c),加密算法的输出,解密算法的输入,其依赖于明文和密钥。AES-128 的密文长度为 128 位。

1.2 相关功耗分析(CPA)

相关系数攻击模型是经典差分攻击的一个延伸[7],它选择一个未知但是恒定的参考态,建立一个具有数据相关性的汉明模型,利用功耗样点与被处理数据的汉明权重之间的相关性因子进行分析。其主要思路是攻击者已知明文,并可变化明文并采集相应的功耗曲线。攻击者猜测密钥,根据明文和密钥计算出某中间变量[8]。以中间变量的汉明权重(逻辑 1 的个数)和功耗的相关系数做分析,相关系数最高的即猜测正确的密钥。否则由于错误的密钥,导致中间变量必然与功耗没有预期的正比关系。这种分析是以功耗与处理的 1 的个数成正比为理论前提的,由芯片原理可知[9]:功耗是与逻辑门输出的 0、1 的转换次数(汉明距)成正比的,而不是与处理的 1(汉明权重)的个数成正比。

1.3 侧信道分析攻击

侧信道分析攻击技术是相对于传统意义上基于通信的密码分析而言的。传统的密码分析是通过对密码处理器的算法进行破解分析,并对输入输出等数据辅之以监听等手段,在流程内实现攻击[10]。侧信道分析攻击技术的对象则是密码处理器的实现,即不是对加解密数据本身分析,而是对加解密过程中的时序、功耗等其他信道的信息进行分析,从而得到密钥等敏感信息[11]。

和传统的密码分析相比,侧信道分析攻击技术有成本上的优势。密码分析虽然通过一些分析方法可降低密码破解的强度,即缩小穷举密钥的空间,但目前通常采取的延长密钥位的办法可使实现穷举攻击需要的时间远远长于密钥的生存期。侧信道分析攻击技术的破解效率与密钥长度无关或只是线性相关,而非传统密码分析中,其效率与密钥长度的幂相关。若集成电路没有保护措施,那么侧信道分析攻击技术可能仅需很小的代价就能得到密钥。

1.4 ChipWhisperer

ChipWhisperer[12]是一种开源工具链,使学习侧信道攻击变得简单。它还充当一个平台,以有据可查、经济高效且可重复的方式执行侧信道研究。ChipWhisperer 主要侧重于电源分析攻击以及电压和时钟故障,这些故障会中断设备的电源或时钟信号,从而导致意外行为。

1.5 Jupyter Notebook

Jupyter Notebook 是基于网页的用于交互计算的应用程序。其可被应用于全过程计算:开发、文档编写、运行代码和展示结果[13]。Jupyter Notebook 是以网页的形式打开,可以在网页页面中直接编写代码和运行代码,代码的运行结果也会直接在代码块下显示。如在编程过程中需要编写说明文档,可在同一个页面中直接编写,便于作及时的说明和解释。同时 Jupyter Notebook 也支持 python 语言, ChipWhisperer 的 Version5 就是使用的 Jupyter Notebook。

2 CPA 攻击检测算法安全性

2.1 CPA 攻击步骤

第一步:将密钥分成 16 个子密钥分别破解,每一子密钥为一个字节[14]。首先考虑第一个子密钥 GuessKey 的破解。根据能量迹随机地选择明文中的字节 $P_1,P_2,\cdots,P_N$,将 P 输入到目标密码算法的执行单元。

第二步:猜测 K 的候选值,然后每遍历一个值,参照 AES 的一轮加密过程,将其与明文 P 进行异或得到 X,异或之后再经过 S-BOX 的字节替换即可得到用于求解汉明重量的输入 Y,求出 Y 的汉明重量后最终得到 h 的样本值[15],如图 1 所示。

第三步:计算 V 和 h 的 person 相关系数 $r(v,h)$,相关性最大的那个点就是 S 盒的输出。

在 CPA 攻击中,根据不同采样点位置的电压值与

汉明重量的关系可以判断正确和错误密钥[16],也就是有无明显的尖峰。只需要对全部的位置都做相关系数,然后找到最大值,这样就找到了正确的密钥,S 盒的输出位置也就找到了

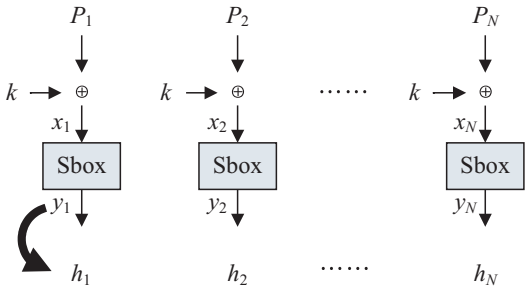

图 1　样本值 h

2.2　CPA 完整攻击流程

高级加密标准是最常见的对称加密算法,加解密使用相同的密钥,可以在不同的平台上实现。

CPA 完整攻击流程[17]程序的主体是两个循环,随机选择明文 $P_1,P_2,\cdots,P_N$,采集加密规程中的能量迹:电压 V,每条能量迹上有 M 个采样点。

For byte = 1∶16//外部循环:循环猜测 16 个 byte 的密钥;

For K = 0∶255 //内部循环:每个猜测的密钥共有 256 种可能需要将其从 0 遍历到 255;

$H = HW(\mathrm{Sbox}(P_{\mathrm{byte}} \oplus K))$ //猜测密钥与明文异或,经过 S 盒处理后计算汉明重量,P_{byte} 表示各 P_N 的第 byte 个字节[18];

For m = 1∶M//计算每个采样点的 person 相关系数;

$V = V_m$ // V_m 各能量迹 V 的第 m 个采样点;

Corr(K) = $r(V,h)$Rightkeybyte = find(max(corr)) // 取相关系数最大的值。

3　ChipWhisperer 使用 CPA 检测 AES-128 加密算法

3.1　捕获部分

首先在命令行下启动 Jupyter Notebook,启动成功后可以在网页上打开。在 Jupyter Notebook 下找到 ChipWhisperer 的项目位置,打开 ChipWhisperer 里面的 CPA 攻击脚本,这个脚本里的内容是 CW 预设的一些参数和攻击步骤,需要根据攻击环境进行更改。

在 CPA 的攻击脚本中,需要修改 PLATFORM 的值,这个值是根据目标板的种类修改的,本实验使用的是 CW303 的目标板,因此需要把 PLATFORM 的值改为 PLATFORM = 'CW303'。

ChipWhisperer 的连接是写在脚本 Setup_Generic.ipynb 中的,里面含有一些参数的设置,例如:PLATFORM 值、间隔时间、时钟频率等。如果要在攻击脚本里进行连接,需要运行这个脚本进行连接。但是单独运行其他的脚本会使实验结构复杂化,每次调试都要去重启它,增加实验的难度,本实验利用 run 命令在攻击脚本中直接调用 Setup_Generic. ipynb 连接设备,避免了每次调试都需要单独连接设备。

本实验使用 XMEGA 目标进行实验,XMEGA 目标需要对 XMEGA 进行编程,XMEGA 编程需要首先将 XMEGA 设备里的内容清空,然后重新写入需要的内容[19],成功写入后并给出提示。

成功连接并确认内容已编程到 XMEGA 设备中,就可以捕获目标的能量迹了。为了更好地展示能量迹的捕获进程,该文利用 python 里面的 tqdm 模块,构建进度条[20]。因此从运行结果中可以看到捕获能量迹的进度,成功运行后还需要把捕获到的能量迹保存下来。本实验统一把能量迹保存在 project 下,方便后续的使用。

本实验使用 Python 中的 holoviewsSuJu 数据分析/可视化库具有快速生成交互性和高维可视化非常适合于数据的交互式探索的特点,利用其功能对捕获到的能量迹进行制作[21],以采样点位 5 000 为例,捕获到的能量迹如图 2 所示。

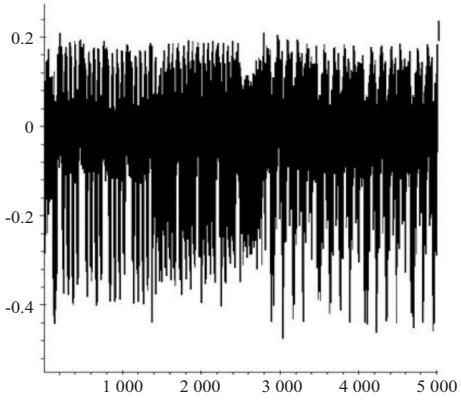

图 2　捕获能量迹

3.2　分析部分

计算相关性之前需要获取一个字节的输入和一个字节的猜测密钥,并且返回 S-Box 的输出,根据猜测密钥计算其汉明权重,利用下面的公式:

HW = [bin(n).count("1") for n in range(0, 256)]

来计算汉明权重。

首先是计算相关性问题。Personal 相关系数[22](皮尔逊相关系数)的计算方法如下:

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

其中，d 表示能量迹的数目；i 表示猜测子密钥，$h_{d,i}$ 表示密钥 i（猜测子密钥）对应的假设中间值汉明重量；j 表示采样点，$\bar{t}_j$ 表示能量迹第 j 个采样点的均值；h 表示功率消耗猜测；t 表示能量迹。

根据皮尔逊相关系数的计算方法可以得到每个猜测密钥的相关性，利用这些相关性可以找出那些猜测密钥符合捕捉到的能量轨迹。对于相关系数而言，只需要关注其绝对值[23]（即存在线性相关性），而不关心符号。此外，虽然没考虑到相关性的计算，但是每条记录的 trace 实际上是由一堆样本点组成的，这意味着实验实际拥有的是每个子猜测密钥与每个样本点的相关性[24]。通常只有跟踪中的几个点是相关的，它是需要关注的整个跟踪中的最大值，因此本实验通过获取最大值的方式选择每个子猜测密钥的相关性。最后，通过找到相关性最大的子猜测密钥确定与数据最匹配的子猜测密钥[25]。

经过以上部分计算皮尔逊相关系数并得出相关性最大的猜测子密钥，本实验将这些猜测子密钥存在 results 中，利用 print 函数可以输出这些猜测子密钥，输出的内容为最大猜测子密钥的值以及相关系数的值。本实验还使用 python 里面的 pandas 库，更好地在数据帧中输出它们[26]。

除此之外，还使用 style 方法来进一步刻画它，使它可以链接格式化函数。例如，由于猜测密钥是从 0-255，因此有很多相关性很小甚至无限趋近于 0 的数据，可以删除多余的 0 并清理数据。本实验更进一步地对得到的密钥进行处理，如输出不同颜色的密钥，并把正确密钥用红色输出且在表格的最顶部。这样，就完成了对 AES-128 的 CPA 攻击。

4 相关系数方法的改进

相关函数的实现可以作为一个遍历所有跟踪的循环运行。理想情况下，希望将相关系数作为一种“在线”计算。为了实现这种“在线”计算，可以添加一个跟踪，观察输出，再添加另一个跟踪，观察输出[27]。当生成部分猜测熵（PGE）与轨迹数量的图时，这是非常可取的，如果没有这种输出的存储方法，在得到最后的结果时需要多次运行循环，这些循环是用来计算不同阶段的输出[28]。

根据上面这种情况，可以使用相关方程的另一种形式，它会显式地存储变量的和，这更容易执行在线计算。它把每次添加跟踪得到的结果保存起来，当添加新的跟踪时，根据之前存储的计算结果，很容易更新这些总和，而不需要循环地运行之前得到的计算结果[29]。

下面两个公式就是改进后显式的存储变量的和。

$$D\sum_{d=1}^{D} h_{d,i}t_{d,j} - \sum_{d=1}^{D} h_{d,i}\sum_{d=1}^{D} t_{d,j}$$

$$\left(\left(\sum_{d=1}^{D} h_{d,i}\right)^2 - \left(D\sum_{d=1}^{D} h_{d,i}^2\right)\right)$$

$$-\left(\left(\sum_{d=1}^{D} t_{d,j}\right)^2 - \left(D\sum_{d=1}^{D} h_{d,j}^2\right)\right)$$

5 实验结果分析

通过捕获到的能量迹上的采样点设置猜测密钥，计算各个明文在猜测密钥下的 S 和输出得到的样本值，并利用能量迹和样本值计算相关系数。实验成功破解出 AES 的 16 组密钥，如图 3 和图 4 所示。

1A	1B	1C	1D	2A	2B	2C	2D
0.752	0.949	0.763	0.792	0.776	0.913	0.763	0.814
2D	5B	41	87	FA	A7	F8	C9
0.658	0.621	0.632	0.629	0.686	0.623	0.670	0.619
93	B3	1D	D1	C2	D3	95	A5
0.617	0.614	0.617	0.628	0.602	0.607	0.636	0.617
87	47	6E	B4	F2	91	57	43
0.609	0.612	0.608	0.621	0.598	0.601	0.622	0.612
77	43	2F	0F	DA	7B	15	C2
0.599	0.599	0.600	0.621	0.586	0.593	0.621	0.603

（a）前 8 组

3A	3B	3C	3D	AA	AB	AC	AD
0.658	0.914	0.829	0.910	0.702	0.844	0.818	0.906
4E	40	0B	5B	5E	54	92	0C
0.639	0.657	0.611	0.607	0.622	0.595	0.648	0.622
39	19	AB	F6	D1	07	9E	69
0.634	0.621	0.605	0.602	0.621	0.594	0.635	0.617
34	85	82	FA	E1	DC	31	34
0.627	0.611	0.604	0.579	0.608	0.594	0.628	0.617
54	02	E4	14	94	5F	F6	EF
0.606	0.604	0.603	0.566	0.600	0.593	0.605	0.603

（b）后 8 组

图 3 密钥

1A	1B	4F	1D	B6	2B	56	2D
0.881	0.876	0.801	0.925	0.840	0.906	0.797	0.940
C1	15	32	C2	B4	51	02	20
0.816	0.802	0.780	0.846	0.807	0.792	0.786	0.852
1D	74	60	C8	C8	B7	D2	9D
0.813	0.793	0.777	0.840	0.804	0.789	0.785	0.819
78	DE	28	4C	8F	0F	84	72
0.803	0.792	0.765	0.835	0.798	0.782	0.774	0.789
E6	40	93	D4	7D	7A	2C	F1
0.798	0.783	0.763	0.818	0.797	0.776	0.770	0.766

（a）前 8 组

BD	3B	3C	3D	26	AB	AC	AD
0.797	0.855	0.856	0.906	0.844	0.917	0.860	0.894
C1	A4	A4	4C	07	D5	FF	53
0.792	0.806	0.781	0.824	0.821	0.838	0.830	0.822
B3	30	D8	49	4B	95	ED	1A
0.781	0.803	0.776	0.786	0.809	0.801	0.777	0.800
DE	52	89	98	C2	39	55	1B
0.780	0.799	0.772	0.780	0.805	0.798	0.764	0.781
42	B6	3A	7E	A8	AC	2A	59
0.768	0.790	0.772	0.779	0.795	0.777	0.759	0.780

（b）后 8 组

图 4 密钥

CPA 破解密钥的成功率与能量迹的条数和采样点的个数有很大的关系,实验首先固定能量迹的数量对采样点的数量进行修改,得到图 4(3 000 采样点)和图 5(4 000 采样点)的密钥破解结果。

1A	1B	B3	1D	2A	2B	2C	2D
0.840	0.931	0.840	0.880	0.838	0.935	0.808	0.863
80	77	63	87	5B	51	91	54
0.800	0.800	0.810	0.839	0.792	0.832	0.805	0.840
EE	2D	A1	33	D2	A1	6A	B3
0.782	0.787	0.789	0.782	0.782	0.805	0.786	0.794
C7	44	55	28	CC	17	11	14
0.767	0.783	0.784	0.778	0.772	0.785	0.783	0.785
B4	08	A5	A0	08	06	DA	63
0.763	0.780	0.784	0.772	0.772	0.785	0.781	0.780

(a)前 8 组

F6	3B	3C	3D	33	AB	AC	AD
0.876	0.924	0.863	0.915	0.856	0.870	0.905	0.959
7F	49	91	E1	F6	1D	B3	1C
0.809	0.788	0.784	0.851	0.782	0.836	0.851	0.815
96	45	8D	C1	AD	50	D1	6B
0.793	0.787	0.781	0.776	0.772	0.791	0.799	0.796
03	AF	15	7F	87	66	36	EA
0.792	0.785	0.779	0.755	0.769	0.783	0.788	0.795
61	56	6F	6E	0B	FA	43	42
0.784	0.775	0.772	0.753	0.769	0.779	0.785	0.794

(b)后 8 组

图 5　密钥

固定能量迹的条数以及调整采样点的大小反复实验,最终得到采样点与成功率之间的关系图。根据实验结果可以发现,在采样点数量为 0 到 5 000 之间时,成功率会随着采样点数量的增加而增加,超过 5 000 之后,成功率基本处于平稳状态,如图 6 所示。

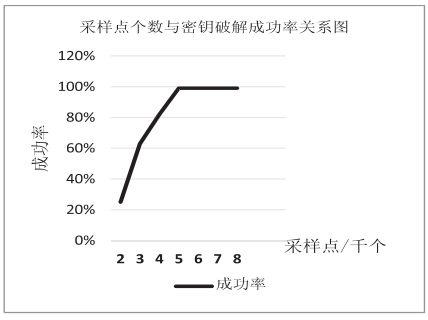

图 6　采样点个数和密钥破解成功率

固定最佳采样点 5 000,调整能量迹的条数,每次增加 5 条能量迹,实验得到具体的密钥破解结果如图 7(20 条能量迹)和图 8(25 条能量迹)。

1A	1B	28	1D	0A	2B	CB	2D
0.939	0.950	0.850	0.909	0.825	0.963	0.843	0.861
89	C7	1C	74	2A	E0	F1	26
0.808	0.831	0.811	0.829	0.788	0.820	0.822	0.809
DE	7D	AA	E8	B0	73	AE	BF
0.794	0.818	0.806	0.826	0.784	0.786	0.820	0.799
CE	9D	5A	9B	A2	66	3C	35
0.793	0.800	0.783	0.810	0.783	0.779	0.809	0.796
F6	28	6A	AD	F3	D7	30	1A
0.782	0.792	0.779	0.790	0.781	0.776	0.803	0.789

(a)前 8 组

5A	3B	3C	3D	16	AB	10	AD
0.828	0.932	0.814	0.859	0.839	0.914	0.823	0.964
F6	EB	D6	B2	5F	BE	4F	88
0.801	0.798	0.797	0.805	0.835	0.797	0.817	0.807
3A	B3	3F	74	6F	05	9B	B1
0.784	0.785	0.775	0.773	0.805	0.786	0.806	0.800
11	46	C2	D8	ED	E3	3B	FA
0.782	0.776	0.770	0.773	0.788	0.770	0.788	0.790
34	C0	ED	36	37	D2	0B	A6
0.774	0.773	0.765	0.770	0.787	0.762	0.782	0.782

(b)后 8 组

图 7　密钥

1A	1B	1C	CD	2A	2B	2C	2D
0.908	0.821	0.833	0.830	0.852	0.908	0.815	0.883
C7	D5	7C	6F	9E	CD	0A	5F
0.890	0.780	0.826	0.829	0.834	0.845	0.815	0.814
B5	B3	8E	1D	D5	4B	22	08
0.835	0.775	0.800	0.821	0.814	0.803	0.813	0.805
D5	86	05	EE	AC	42	9A	C6
0.783	0.762	0.795	0.820	0.793	0.803	0.812	0.784
D9	90	67	8A	A8	00	7E	3C
0.774	0.761	0.789	0.804	0.790	0.791	0.783	0.757

(a)前 8 组

3A	3B	3C	3D	AB	AB	AC	AD
0.795	0.912	0.852	0.839	0.799	0.908	0.843	0.917
AF	C1	E5	77	AE	A5	3A	AE
0.791	0.810	0.840	0.797	0.789	0.812	0.822	0.841
E5	A8	47	CA	82	55	4A	C8
0.782	0.794	0.819	0.793	0.789	0.789	0.806	0.809
CF	95	20	ED	35	93	EF	C5
0.781	0.793	0.811	0.770	0.780	0.776	0.792	0.809
DE	5D	3B	EF	4D	78	5D	09
0.766	0.781	0.810	0.767	0.780	0.773	0.786	0.800

(b)后 8 组

图 8　密钥

实验中固定采样点的大小以及调整能量迹的条数实验,最终得到能量迹与成功率之间的关系图。根据实验结果可以发现,在采样点数量为 0 到 30 之间时,成功率会随着采样点数量的增加而增加,超过 30 之后,成功率处于平稳状态,如图 9 所示。

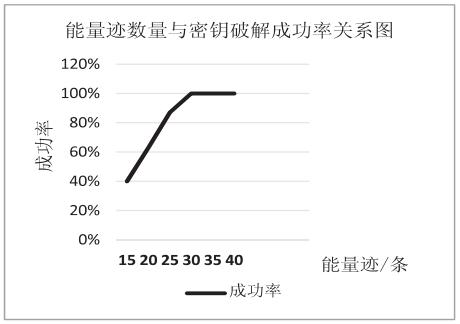

图 9　能量迹条数和密钥破解成功率

CPA 攻击的成功率正常情况下会随着采样点和能量迹数量的增加而增加,但同时运算速度也会下降,本实验在保证成功率的同时提高了运算速度,采用不同的采样点和能量迹进行反复实验,最终得到能量迹为 30 条、采样点位 5 000 时,CPA 对 AES 的密钥破解情况最好,此时几乎可以达到 100% 的密钥破解率,再

增加数量就会导致运算速度降低。

6 结束语

随着信息化水平的不断提高,AES 加密算法的安全问题尤为重要。虽然 AES 加密算法可以防御一些基本的攻击方式,但针对侧信道攻击的防御还是较为薄弱的。该文针对 AES-128 加密算法实施了相关功耗分析攻击,并成功破解了 128 位完整的密钥。攻击过程中使用 ChipWhisperer 成功捕获了功耗曲线,通过计算汉明权重,得出了功耗数据的相关系数,并推测密钥是否正确。实验结果表明,对 AES-128 加密算法的破解成功率达到了 90% 以上。AES-128 加密算法容易受到相关功耗分析的攻击,因此,在实际中使用 AES 加密算法时需要考虑芯片的安全测试,增加芯片抗侧信道攻击的防护。

参考文献:

[1] GANDOLFI K,MOURTEL C,OLIVIER F. Electromagnetic analysis:concrete results[C]//Third international workshop on cryptographic hardware and embedded systems - CHES 2001. Paris,France:[s. n.],2001:251-261.

[2] YAN Yingjian, LI Moran, GUO Jianfei. Implementation of multi-bit DEMA attack on AES cryptographic chip[J]. Computer Engineering and Applications,2014,50(14):92-95.

[3] LEE T F,LIU C M. A secure smart-card based authentication and key agreement scheme fortelecare medicine information systems[J]. Journal of Medical Systems,2013,37(3):1-8.

[4] FEI Y,LUO Q,DING A A. A statistical model for DPA with novel algorithmic confusion analysis [M]//Cryptographic hardware and embedded systems-CHES 2012. Berlin:Springer,2012

[5] BRIER E,CLAVIER C,OLIVER F. Correlation power analysis with a leakage model[C]//Cryptographic hardware and embedded systems. Massachusetts,USA:[s. n.],2004:16-29.

[6] 张仕斌. 应用密码学[M]. 西安:西安电子科技大学出版社,2009:75-79.

[7] 蔡泽民,王 奕,李仁发. 基于代数表达式功耗模型的差分功耗分析攻击[J]. 计算机应用,2014,34(2):448-451.

[8] MORADI A,MISCHKE O,EISENBARTH T. Correlation enhanced power analysis collision attack[C]//Cryptographic hardware and embedded systems, CHES 2010. Berlin:Springer,2010:125-139.

[9] KUTZNER S,POSCHMANN A. On the security of RSM-presenting 5 first-and second-order attacks[C]//Constructive side-channel analysis and secure design. Paris, France: Springer,2014:299-312.

[10] STANDAERT F X. Introduction to side-channel attacks [M]//Secure integrated circuits and systems. Berlin:Springer,2010:27-42.

[11] LERMAN L,MEDEIROS S F,BONTEMPI G,et al. A machine learning approach against a masked AES[C]//Smart card research and advanced applications. Berlin,Germany:Springer,2014:61-75.

[12] LEE J,KIM J,LEE J,et al. Most significant bit is most significant power - case study:ChipWhisperer[C]//Conference on information security and cryptography 2018 summer. Naju,Republic of Korea:[s. n.],2018:362-366.

[13] ZADEH A A,HEYS H M. Simple power analysis applied to nonlinear feedback shift registers[J]. IET Information Security,2014,23(8):188-198.

[14] ÖRS S B,GÜRKAYNAK F G,OSWALD E,et al. Power-analysis attack on an ASIC AES implementation[C]//Proceedings of the international conference on information technology:coding and computing (ITCC'04). Seoul,Kores:IEEE,2004.

[15] RATHNALA P, WILMSHURST T, KHARAZ A. A practical approach to differential power analysis using PIC micrcontroller based embedded system[C]//6th Computer science and electronic engineering conference (CEEC). West Bengle, Indian:IEEE,2014.

[16] 刘会英,赵新杰,王 韬,等. 基于汉明重的 SMS4 密码代数旁路攻击研究[J]. 计算机学报,2013,36(6):1183-1193.

[17] LIU P C,CHANG H C,LEE C Y. A true random-based differential power analysis countermeasure circuit for an AES engine[J]. IEEE Transactions on Circuits and Systems II:Express Briefs,2012,59(2):103-107.

[18] 刘 鸣. 密码芯片的功耗分析及抗功耗分析研究[D]. 北京:清华大学,2005.

[19] TAYLOR G,MOORE S,Anderson R,et al. Improving smart card security using self-timed circuits[C]//Proceedings of the eighth international symposium on asynchronous circuits and systems (ASYNC 02). Manchester, United Kingdom: IEEE,2002:211-218.

[20] ELDIB H,WANG C,SCHAUMONT P. SMT-based verification of software countermeasures against side-channel attacks [C]//Tools and algorithms for the construction and analysis of systems. Grenoble,France:Springer,2014:62-77.

[21] CHEN Kaiyan,ZHANG Peng,DENG Gaoming. Correlation electromagnetic analysis attack and minimum sample size analysis[J]. Journal of Huazhong University of Science and Technology(Natural Science),2011(1):32-35.

[22] 冯登国,周永斌. 能量分析攻击[M]. 北京:科学出版社,2010.

[23] CHOU J W,CHU M H,TSAI Y L,et al. An unsupervised learning model to perform side channel attack[M]//Advances in knowledge discovery and data mining. Gold Coast,Australia:Springer,2013:414-425.

[24] WANG Danhui,WANG An,ZHENG Xuexin. Fault-tolerant linear collision attack:a combination with correlation power analysis[M]//Information security practice and experience.

(下转第 129 页)