基于聚类的密码芯片频域侧信道分析

蔡爵嵩,严迎建,朱春生,郭朋飞
(战略支援部队信息工程大学,河南 郑州 450002)

摘 要:能量迹的对齐问题是影响侧信道分析成功率的关键因素之一,频域侧信道分析能够有效解决能量迹在时域内的对齐问题,但由于频域内一个点对应着时域内多个点,频域侧信道分析通常需要比时域侧信道分析更多的能量迹条数。为了减少频域侧信道分析所需能量迹条数,提出基于聚类的密码芯片频域侧信道分析方法,通过机器学习中的聚类算法分离出有效信号频率后,再进行侧信道分析,从而减少所需能量迹条数。实验表明,所提方法能够在不同程度上减少频域侧信道分析所需能量迹条数。

关键词:侧信道分析;频域;机器学习;聚类;能量迹
中图分类号:TN407;TP309.7 **文献标识码**:A DOI:10.16157/j.issn.0258-7998.200300

中文引用格式:蔡爵嵩,严迎建,朱春生,等. 基于聚类的密码芯片频域侧信道分析[J].电子技术应用,2021,47(3):61-64,70.
英文引用格式:Cai Juesong,Yan Yingjian,Zhu Chunsheng,et al. Side-channel analysis in frequency domain with clustering[J]. Application of Electronic Technique,2021,47(3):61-64,70.

Side-channel analysis in frequency domain with clustering

Cai Juesong,Yan Yingjian,Zhu Chunsheng,Guo Pengfei
(PLA Information Engineering University,Zhengzhou 450002,China)

Abstract: The alignment of power traces is one of the key factors affecting the success of side-channel analysis. Frequency-domain side-channel analysis can effectively solve the alignment of power traces in the time domain. However, frequency-domain side-channel analysis usually requires more power traces. In order to improve this problem, this paper proposes a frequency-domain side-channel analysis method based on clustering. After the effective signal frequencies are separated through the clustering algorithm in machine learning, side-channel analysis is carried out to reduce the number of power traces. Experiments show that this method can reduce the number of power traces required for frequency-domain side-channel analysis in different degrees.
Key words: side-channel analysis;frequency domain;machine learning;clustering;power traces

0 引言

侧信道分析(Side-channel Analysis,SCA)是一种不仅利用算法本身,更依赖于密码算法物理实现中的侧信道泄漏的分析方法,严重威胁到密码芯片的安全性。能量分析是一种最流行的侧信道分析方式,包括简单能量分析(Simple Power Analysis,SPA)[1]、差分能量分析(Differential Power Analysis,DPA)[2]、模板攻击(Template Attacks,TA)[3]、相关能量分析(Correlation Power Analysis,CPA)[4]等。现有文献主要是针对密码芯片的能量消耗在时域上进行分析。但时域分析有一定的局限性,如能量迹的对齐问题。通常采集设备的不稳定或者芯片加入时钟随机化防护措施,都会导致能量迹需要进行对齐处理。因此,能量迹的对齐成为影响侧信道分析成功率的关键因素之一。

密码芯片有效信号的频率由时钟频率决定,不会受到采集设备和手段的影响,所以使用有效信号的频率能量大小代替能量迹采样点的功耗大小作为密钥的特征是可行的。2000 年,AIGNER M 等人表示在对密码芯片侧信道分析中,时域内的能量消耗差异在频域内同样会体现出来[5]。2005 年,GEBOTYS C H 等人在 CHES 会议上通过对电磁信号的频域进行分析首次验证了频域侧信道分析的可行性[6]。近年来,将能量迹转换到频域进行侧信道分析已经被证明是一种解决能量迹对齐问题的有效途径[7-9]。虽然频域侧信道分析能够解决时域侧信道分析的对齐问题,但由于噪声频率可能与有效信号频率相同或相近,因此频域侧信道分析通常需要更多的能量迹,如文献[7]采集了 70 000 条能量迹,文献[8]采集了 10 000 条能量迹。

文献[10]~[14]表明将机器学习引入侧信道分析,能够有效找到能量迹上的特征点,提高侧信道分析的成功率。2017 年,ZHANG R N 等人[14]直接使用机器学习中的无监督学习算法 k-means 对时域内的能量迹进行了分

析，并成功获得其密钥。本文将机器学习中的聚类算法引入频域侧信道分析中，寻找信号频率内在的分布，对有效信号频率进行分离，从而减少频域侧信道分析所用能量迹条数。

1 基础知识

1.1 相关能量分析(CPA)

2004 年，BRIER E 等人提出了相关能量分析(Correlation Power Analysis，CPA)[4]，工作原理是基于芯片能量消耗 W 与中间值模型 H 之间具有线性相关性。通过计算 W 与 H 之间的皮尔逊相关系数 $\rho(W,H)$ 来评估中间值模型与实际能量消耗的匹配程度。

一般地，分析者采用的中间值模型为汉明重量模型(Hamming Weight，HW)或汉明距离模型(Hamming Distance，HD)。分析者通过计算猜测密钥对应的中间值与芯片实际能量消耗之间的相关系数来进行分析，相关系数最大的对应密钥值即被认为是正确密钥。

1.2 频域侧信道分析

密码芯片的频域侧信道分析就是对傅里叶变换后的能量迹进行分析。由于能量迹是由采集设备采样得到的数字信号，在时域内是离散的有限时间序列，因此本文采用的是离散傅里叶变换(Discrete Fourier Transform，DFT)。

一般地，信号的时域波形表示信号随时间的变化，而其频域图则显示了在一个频率范围内每个给定频带内的信号量，所以频域内的信息更集中。这也是频域侧信道分析一般需要比时域侧信道分析更多的能量迹条数的原因。

1.3 k-means 算法

机器学习中的无监督聚类算法可以利用样本数据内在的相似性对样本数据进行自动分类。将每一类称为一个簇，则有簇内相似性高、簇间相似性低的特点。本文选取应用最广、算法实现最简单的 k-means 算法进行聚类分析。

给定样本集 $D=\{\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_m\}$，k-means 算法从中选择 k 个样本作为初始聚类中心 $\{\boldsymbol{\mu}_1,\boldsymbol{\mu}_2,\cdots,\boldsymbol{\mu}_k\}$，计算样本 $\boldsymbol{x}_j(1\leqslant j\leqslant m)$ 与各初始聚类中心 $\boldsymbol{\mu}_i(1\leqslant i\leqslant k)$ 之间的距离：

$$d_{ji}=||\boldsymbol{x}_j-\boldsymbol{\mu}_i||_2 \tag{1}$$

根据距离最近的聚类中心确定样本 $\boldsymbol{x}_j$ 的簇标记 λ_j $(1\leqslant j\leqslant m)$：

$$\lambda_j=\underset{i\in\{1,2,\cdots,k\}}{\operatorname{argmin}} d_{ji} \tag{2}$$

将样本 $\boldsymbol{x}_j$ 划入相应的簇 $C_{\lambda_j}(1\leqslant j\leqslant m)$：

$$C_{\lambda_j}=C_{\lambda_j}\cup\{\boldsymbol{x}_j\} \tag{3}$$

计算新聚类中心 $\boldsymbol{\mu}_i'(1\leqslant i\leqslant k)$：

$$\boldsymbol{\mu}_i'=\frac{1}{|C_i|}\sum_{x\in C_i}\boldsymbol{x}(i=1,2,\cdots,k) \tag{4}$$

假如新的聚类中心 $\boldsymbol{\mu}_i'$ 与原聚类中心 $\boldsymbol{\mu}_i$ 不同，则将 $\boldsymbol{\mu}_i$ 更新为 $\boldsymbol{\mu}_i'$。重复以上步骤，直到聚类中心不发生变化为止。

1.4 轮廓系数(Silhouette Coefficient)

1986 年，ROUSSEEUW J 等人提出了轮廓系数(Silhouette Coefficient)[15]，用来衡量一个点与它所属聚类类别的相似程度，可以用来在相同数据的基础上来评价不同算法或者算法不同参数对聚类结果产生的影响。

(1)计算样本 $\boldsymbol{x}_j(1\leqslant j\leqslant m)$ 到同一簇 C_{λ_j} 内其他样本的平均距离 a_j。a_j 越小，表明样本 $\boldsymbol{x}_j$ 越应该被聚类到该簇。a_j 被称为样本 $\boldsymbol{x}_j$ 的簇内不相似度。

(2)计算样本 $\boldsymbol{x}_j$ 到其他簇 $C_i(i=1,2,\cdots,k;i\neq j)$ 内所有样本的平均距离 b_{ij}，称之为样本 $\boldsymbol{x}_j$ 与簇 $C_i(i=1,2,\cdots,k;i\neq j)$ 的不相似度，即样本 $\boldsymbol{x}_j$ 的簇间不相似度。

$$b_j=\min\{b_{1j},b_{2j},\cdots,b_{kj}\} \tag{5}$$

b_j 为样本 $\boldsymbol{x}_j$ 到其他簇 $C_i(i=1,2,\cdots,k;i\neq j)$ 内所有样本的最小平均距离。可以知道，b_j 越大，说明样本 $\boldsymbol{x}_j$ 越不属于其他簇 $C_i(i=1,2,\cdots,k;i\neq j)$。

(3)根据样本 $\boldsymbol{x}_j$ 的簇内不相似度 a_j 和簇间不相似度 b_j，就可以定义样本 $\boldsymbol{x}_j$ 的轮廓系数 S_j：

$$S_j=\begin{cases}1-a_j/b_j & a_j<b_j\\ 0 & a_j=b_j\\ b_j/a_j-1 & a_j>b_j\end{cases} \tag{6}$$

容易知道，$-1\leqslant S_j\leqslant 1$，当 S_j 越接近于 1 时，簇内越紧凑，簇间越稀疏，聚类效果越优。所有样本的轮廓系数 S_j 的均值为聚类结果的轮廓系数，是评价该聚类是否合理、有效的指标之一。

2 基于聚类的频域侧信道分析

2.1 使用聚类算法分离有效信号的可行性分析

现在来分析能量迹中的有效信号与噪声信号相似度是否较低，即能否在能量迹中有效分离出有效信号。设能量迹中某一点的信噪比(Signal to Noise Ratio，SNR)为：

$$\mathrm{SNR}=\frac{\mathrm{Var}(P_{\mathrm{exp}})}{\mathrm{Var}(P_{\mathrm{sw.noise}}+P_{\mathrm{el.noise}})} \tag{7}$$

其中，P_{exp} 为侧信道分析所利用的有效信号能量，$P_{\mathrm{sw.noise}}$ 为转换噪声，$P_{\mathrm{el.noise}}$ 为电子噪声。显而易见，SNR 越高，从全部信号分离出 P_{exp} 越容易。一般地，在采集密码芯片能量消耗时通过低通滤波技术来提高能量迹的 SNR，确保侧信道分析能够成功。因此，对于一个能够成功进行频域侧信道分析的能量迹来说，P_{exp} 是能够从全部信号中分离出来的。

本文的研究是在能够成功实施频域侧信道分析的前提下进行的，所以有效信号 P_{exp} 是能够从全部信号中分离出来的。由于噪声频率和有效信号频率均为基频的倍数，因此，将能量迹进行傅里叶变换后，有效信号的频率与大部分噪声信号的频率的相似度低，只有很小一部分噪声与有效信号同频或频率接近，但这并不妨碍进行侧信道分析。因此，使用聚类算法能够有效分离出有效

信号的频率。

2.2 基于聚类的频域侧信道分析方法

结合频域侧信道分析方法和聚类算法，本文提出基于聚类的频域侧信道分析方法，流程图如图 1 所示。现给出该方法的具体实施步骤：

(1)使用采集设备对密码芯片能量消耗进行采集，得到 n 条能量迹 $t_i(i=1,2,\cdots,n)$，组成能量迹集 $T=\{t_1,t_2,t_3,\cdots,t_n\}$。

(2)对能量迹集 $T=\{t_1,t_2,t_3,\cdots,t_n\}$中的每一条能量迹 $t_i(i=1,2,\cdots,n)$进行离散傅里叶变换(DFT)，得到：

$$T'=\{\mathrm{DFT}(t_1),\mathrm{DFT}(t_2),\cdots,\mathrm{DFT}(t_n)\} \tag{8}$$

(3)对 T'使用 k-means 算法进行聚类。k-means 算法非常简单且使用广泛，运行速度快，可用于处理大型的数据集。但该算法存在对初始参数比较敏感，需要找到相似程度低的类别才能进行较好的聚类。

由于只存在有效信号频率和噪声频率，因此聚类类别数设置为 2。

(4)由于能量迹中噪声频率分布更广，有效信号频率占比较少，因此选择其中簇内数量较少的一类进行侧信道分析，一般采用 1.1 节所描述的相关能量分析(CPA)方法进行侧信道分析。

(5)如果失败，则回到步骤(3)。因为聚类算法是根据数据内在特征进行自动分类，所以有可能会出现无法得到预期结果的情况。因此，在失败时，应该重新进行聚类分析，或者在对聚类算法进行优化改进[16]。

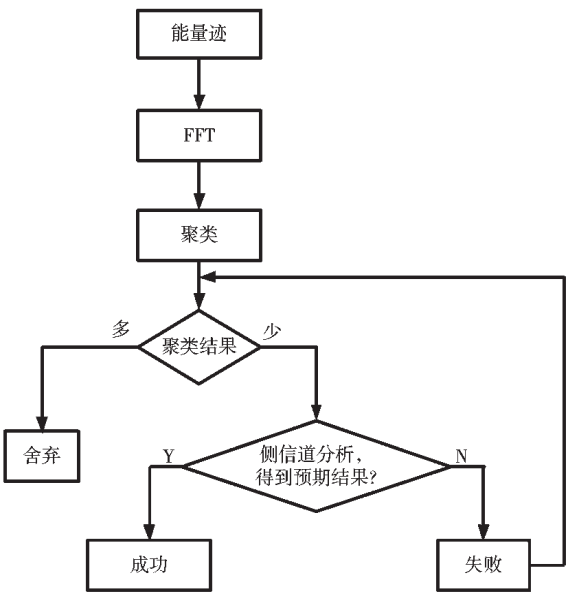


图 1 基于聚类的频域侧信道分析方法流程图

3 实验验证及分析

本文使用 ChipWhisperer 系列侧信道分析开发板[17]进行实验，验证基于聚类的密码芯片频域侧信道分析方法的可行性。

3.1 实验数据采集

本节使用 CW1173 ChipWhisperer-Lite 开发板[18]进行能量迹采集，目标设备为 ATMEGA XMEGA128，密码算法为 128 位 AES 算法，共采集 60 000 条能量迹用作分析。实验平台为 MATLAB R2018b，傅里叶变换使用的是 MATLAB 自带的 fft 和 fftshift 函数。

图 2 为 AES 算法第一轮的能量迹曲线，图 3 为经过傅里叶变换后的频域幅值谱。

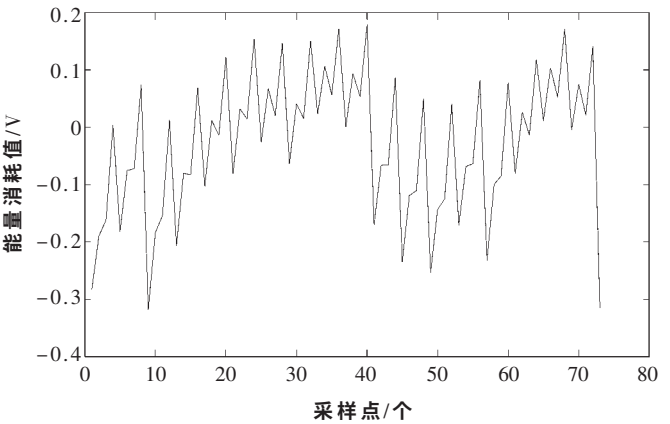


图 2 AES 算法第 1 轮能量迹曲线

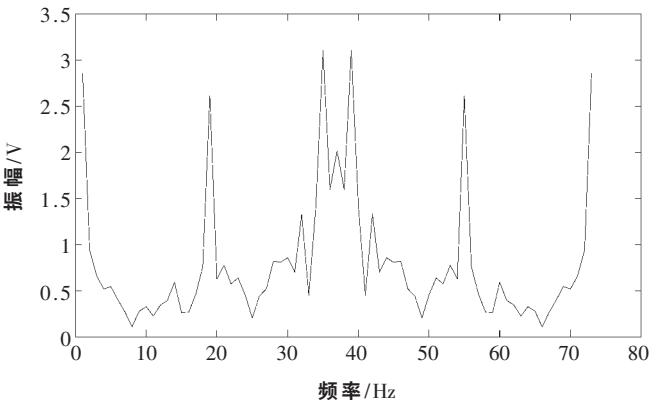


图 3 AES 第 1 轮能量迹经过傅里叶变换后的频域幅值谱

3.2 实验过程及结果

对 AES 算法前 4 轮分别进行傅里叶变换后，利用 1.1 节描述的相关能量分析(CPA)方法进行分析，中间值模型选择为 S 盒输出的汉明重量(HW)值，然后计算中间值模型与傅里叶变换后的能量迹之间的相关系数。当连续使用多条能量迹进行分析得到的最大相关系数对应的猜测密钥值 key_guess 不变时，即认为是正确密钥。

采取对比实验，设定 3 组实验，第 1 组为全部能量迹，第 2 组为聚类后数量较多的能量迹，第 3 组为聚类后数量较少的能量迹，分别记为 I、II、III。在实验中，将第 I 组作为基准，第 II 组和第 III 组都与第 I 组进行比较，看本文方法是否会减少能量迹条数，同时第 II 组与第 III 组进行比较，看本文方法是否能够准确分离出有

效信号频率，结果如表 1 所示。其中，表内失败是指使用60 000 条能量迹无法分析得到正确密钥；表 1 结果为最少所需能量迹条数；由于聚类算法是根据数据内在特征进行自动分类，因此会出现结果与表 1 结果不一致的情况。

表 1　3 组实验分析成功所需能量迹条数

组别	I	II	III
第 1 个 S 盒所需条数	59	59	47
第 2 个 S 盒所需条数	28 000	失败	780
第 3 个 S 盒所需条数	16 500	失败	12 400
第 4 个 S 盒所需条数	31 500	失败	31 250

3.3 实验结果分析

本文引入 1.4 节介绍的轮廓系数(Silhouette Coefficient)对聚类算法参数设置和聚类后的结果进行评价。图4~图 7 分别对应 AES 算法第一轮的第 1 个 S 盒、第 2 个 S 盒、第 3 个 S 盒、第 4 个 S 盒聚类后的轮廓系数图。

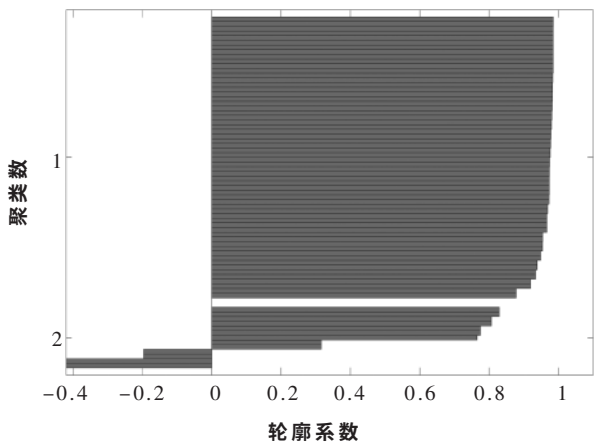


图 4　AES 算法第一轮第 1 个 S 盒聚类后轮廓系数示意图

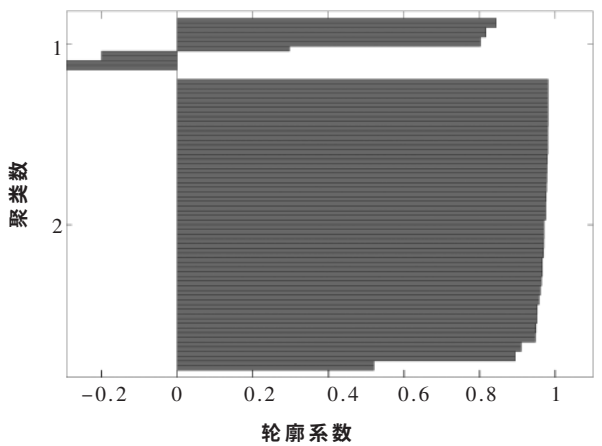


图 5　AES 算法第一轮第 2 个 S 盒聚类后轮廓系数示意图

从图 4~图 7 可以看出，4 次聚类后的轮廓系数均接近 1，说明文中聚类参数设置合理、有效，聚类效果较好，进一步说明本文所提方法的步骤(3)将聚类类别设

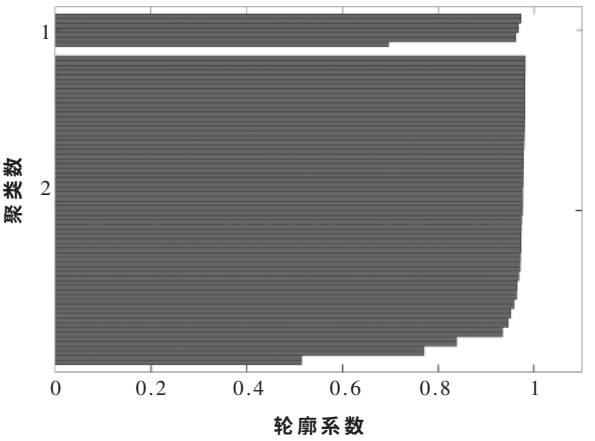


图 6　AES 算法第一轮第 3 个 S 盒聚类后轮廓系数示意图

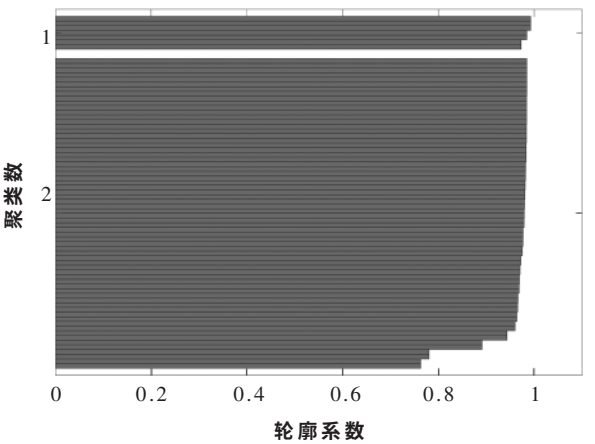


图 7　AES 算法第一轮第 4 个 S 盒聚类后轮廓系数示意图

为 2 是正确的，同时表明通过聚类算法能够从全部信号中分离出有效信号。

通过对表 1 的分析可知，第 III 组分析成功所需能量迹条数明显少于第 I 组和第 II 组，并且第 II 组还存在不能成功分析的情况，说明能量迹中的有效信号频率确实在第 III 组当中，即能准确分离出有效信号频率，从而进行有效侧信道分析，减少频域侧信道分析所需能量迹条数。

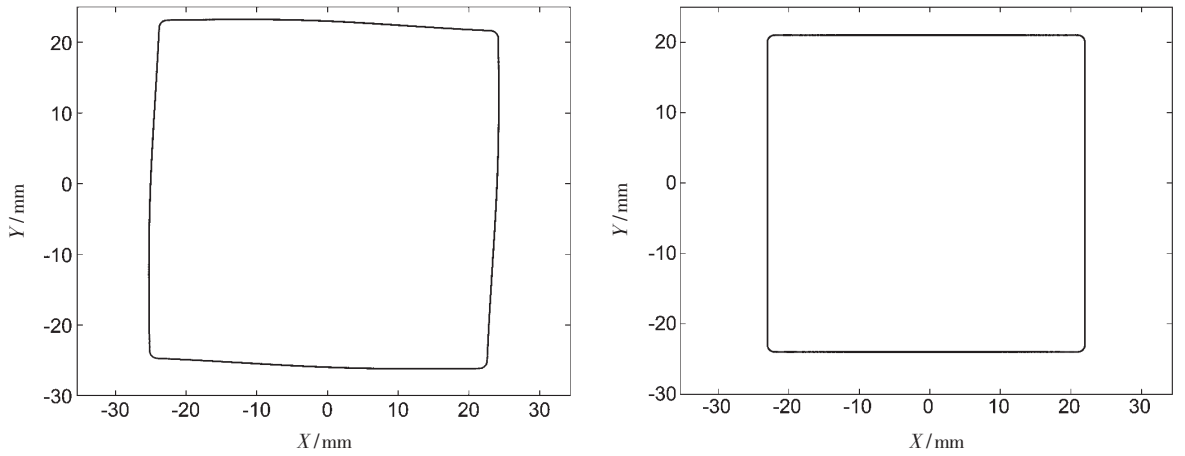
4 结论

将密码芯片的能量消耗转换到频域进行侧信道分析，能够有效解决能量迹对齐问题，但由于频域内的一个点对应时域内的多个点，因此频域侧信道分析往往需要更多的能量迹条数。本文针对这个问题，提出使用机器学习中的聚类算法找出有效信号的频率后进行分析。实验结果表明，本文方法能够减少密码芯片频域侧信道分析所需的能量迹条数。将本文方法应用于密码芯片频域侧信道分析中，能够提高分析性能，使频域侧信道分析更加实用。

参考文献

[1] KOCHER P C.Timing attacks on implementations of Diffie-

(下转第 70 页)



(a)未标定　　(b)标定后

图 11　轮廓坐标图

自标定方法[J].仪器仪表学报,2016,37(11):2459-2464.
[7] 朱嘉齐,章家岩,冯旭刚.柔性臂测量机的圆光栅偏心参数标定算法[J].电子测量与仪器学报,2019,33(8):1-7.
[8] 于源,卢军,王小椿.自由曲面测量中曲面匹配的建模及算法分析[J].机械科学与技术,2001,20(3):467-468,471.

(下转第 74 页)

(上接第 64 页)

Hellman, RSA, DSS, and other systems[C]. Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology, 1996.
[2] KOCHER P C, JAFFE J M, JUN B C. Differential power analysis[M]. Springer-Verlag, 2009.
[3] CHARI S, RAO J R, ROHATGI P. Template attacks[C]. Cryptographic Hardware and Embedded Systems-CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers. Springer, Berlin, Heidelberg, 2002.
[4] BRIER E, CLAVIER C, OLIVIER F. Correlation power analysis with a leakage model[C]. Cryptographic Hardware and Embedded Systems-CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004.
[5] AIGNER M, OSWALD E. Power analysis tutorial[D]. Graz, Austria: University of Technology Graz, 2000.
[6] GEBOTYS C H. EM analysis of Rijndael and ECC on a wireless Java-based PDA[C]. Proceedings of CHES 2005, 2005, 3659: 250-264.
[7] 乌力吉,张振宾,董刚,等.基于侧信道相关能量分析的频域分析方法:中国,CN104052590A[P].2014-09-17.
[8] 王敏,饶金涛,吴震,等.SM4 密码算法的频域能量分析攻击[J].信息网络安全,2015(8):20-25.
[9] 向春玲,吴震,饶金涛,等.针对一种 AES 掩码算法的频域相关性能量分析攻击[J].计算机工程,2016,42(10):146-150.
[10] LERMAN L, MEDEIROS S F, VESHCHIKOV N, et al. Semi-supervised template attack[C]. Proceedings of the 4th International Conference on Constructive Side-Channel Analysis and Secure Design. Springer-Verlag, 2013.
[11] 刘飚.基于机器学习的密码芯片电磁攻击技术研究[D].北京:北京邮电大学,2014.
[12] 唐明,王欣,李延斌,等.针对轻量化掩码方案的功耗分析方法[J].密码学报,2014,1(1):51-63.
[13] 唐明,王欣,胡晓波,等.基于聚类分析的轻量化掩码分析方法[J].武汉大学学报,2016,62(3):230-234.
[14] ZHANG R N, ZHANG Q M, CHEN J H. A power attack method based on clustering[C]. 2017 International Conference on Computer, Electronics and Communication Engineering(CECE 2017), 2017: 418-424.
[15] ROUSSEEUW P J. SilHouettes: a graphical aid to the interpretation and validation of cluster analysis[J]. Journal of Computational and Applied Mathematics, 1987, 20: 53-65.
[16] 张素洁,赵怀慈.最优聚类个数和初始聚类中心点选取算法研究[J].计算机应用研究,2017,34(6):1617-1620.
[17] NewAE Technology Inc. ChipWhisperer main page[EB/OL]. [2020-04-14]. https://wiki.newae.com/Main_Page.
[18] NewAE Technology Inc. CW1173 ChipWhisperer-Lite[EB/OL]. [2020-04-14]. https://wiki.newae.com/CW1173_ChipWhisperer-Lite.

(收稿日期:2020-04-14)

作者简介:
蔡爵嵩(1992-),男,硕士,主要研究方向:安全专用芯片设计、机器学习。
严迎建(1973-),男,博士,教授,主要研究方向:芯片安全防护。
朱春生(1988-),男,博士,讲师,主要研究方向:芯片安全防护。

版权声明