一种基于奇异值分解的功耗轨迹筛选方法

周新平[1,2],孙德刚[1,2],王 竹[1,2],欧长海[1,2]
(1. 中国科学院信息工程研究所,北京 100093; 2. 中国科学院大学网络空间安全学院,北京 100049)

摘 要: 功耗分析攻击是侧信道分析中针对密码设备最有效的分析手段之一,它利用密码设备消耗的功耗来分析密码设备的敏感信息.差分功耗分析是最早提出的功耗分析方法,也是目前最基本的分析方法之一.但是在实际使用差分功耗分析过程中,由于功耗轨迹存在噪声等因素,往往使得花了较多的功耗轨迹,差分功耗分析的效果一般,难以恢复出正确密钥.针对这个问题,本文提出了一种基于奇异值分解的选择功耗轨迹方法,这种方法可以选择一些质量好的功耗轨迹用于差分功耗分析,提高差分功耗分析的攻击效率.本文的实验验证了该方法的有效性,在同等分析条件下,对于我们自己采集的功耗数据,使用该方法情况下仅需124条功耗轨迹就可以达到80%的成功率,而普通差分功耗分析需要490条;对于DPA Contest 2008/2009提供的数据,使用该方法仅需53条功耗轨迹可以达到80%的成功率,而普通差分功耗分析需要195条.两个不同的实验对象都说明了该方法的有效性.

关键词: 差分功耗分析; 选择功耗轨迹; 奇异值分解
中图分类号: TP309.7 **文献标识码:** A **文章编号:** 0372-2112 (2017)09-2250-06
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.09.028

A Method Based on Singular Value Decomposition for Enhancement of Differential Power Analysis

ZHOU Xin-ping[1,2], SUN De-gang[1,2], WANG Zhu[1,2], OU Chang-hai[1,2]
(1. *Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093, *China*;
2. *School of Cyber Security University of Chinese Academy of Sciences, Beijing* 100049, *China*)

Abstract: Power analysis is one of the most effective techniques in side channel analysis. This technique utilizes the power consumption that are relative to the intermediate state of cryptographic algorithm to recover the secret information in the cryptographic devices. Differential power analysis is the first method of power analysis and it is one of the most fundamental analysis techniques. However, in practical scenario, the efficiency of differential power analysis is largely affected by the noise of power traces. Consequently, this leads to the low efficiency of differential power analysis and it is hard to recover the secret key. To address this issue, a new method that is based on singular value decomposition to select power traces is proposed. The power traces of high quality can be selected when this method is applied to improve the efficiency of differential power analysis. The experiments verify the validity of the method. Further, the experimental results show that our method is much better compared with the existing method. Using the method of this paper only 124 power traces is needed to achieve the success rate of 80%, while the normal differential power analysis needs 490 power traces. In addition, when analyzing the data of DPA Contest V1, using the method of this paper only 53 power traces is needed to achieve the success rate of 80%, while the normal differential power analysis needs 195 power traces. Two experiments on different subjects verify the effectiveness of our method.

Key words: differential power analysis; selecting power traces; singular value decomposition

收稿日期:2016-06-12;修回日期:2016-11-15;责任编辑:梅志强
基金项目:国家自然科学基金项目(No.61372062)

1 引言

传统的密码分析侧重于密码算法本身的分析,分析算法的输入输出来寻找漏洞,进而破解密钥. 侧信道分析攻击利用密码设备在运行过程中的一些与数据操作相关的物理泄漏,结合输入输出,分析密码算法的实现安全性,对密码设备安全性构成严重的威胁. 功耗分析是一种较为普遍的侧信道分析方法. 差分功耗分析(Differential Power Analysis, DPA)是 Paul Kocher 等人在 1999 年提出[1],它是功耗分析攻击中最基本的方法之一[2~7]. 其思想是利用密码设备工作过程中,功耗和数据有依赖关系,将采集到的功耗数据按猜测值分为两类,然后求这两类的均值差. 若猜测密钥正确,均值差会出现明显的尖峰,否则均值差接近于 0. DPA 之所以广泛被使用在于它的操作简单,攻击方便. 但是假如采集的功耗数据噪声过大,正确密钥和错误密钥经过差分后的结果区分度不大,难以区分出正确密钥.

针对这个问题,本文提出了一种基于奇异值分解(Singular Value Decomposition, SVD)的方法用在 DPA 上. 利用奇异值分解技术,选择一部分质量好的功耗轨迹数据进行差分分析,这样很大程度上提高 DPA 的分析效率.

2 相关工作

DPA 的效率受功耗轨迹的噪声影响较大,目前已有文献研究数字信号处理(Digital Signal Processing, DSP)技术应用在 DPA 上. 文献[8,9]使用傅里叶变换(FFT)将时域信号转换成频域信号进行分析,文献[10,11]利用低通滤波器降低功耗轨迹的噪声,文献[12]利用小波变换的思想对 CPA 进行预处理,从而提高分析效率. 然而,这些 DSP 技术的使用需要确定各种参数,并而要求信号和噪声在频域没有重叠的情况,实现起来比较复杂.

文献[13]首次提出选择功耗轨迹的想法. 这种方法是基于与处理数据相关的时间点附近的平均值和方差来选择功耗轨迹. 此方法要求事先确定与处理数据最相关的时间点,故在实际分析中实现难度大. 文献[14]提出一种基于原始数据的主成分分析的来提高相关性系数分析[15](CPA)的想法. 这种方法首先求原始数据的主成分,根据主成分选择功耗轨迹,效率比普通 CPA 有很大提高. 文献[16]提出了一种自适应的选择明文相关性分析方法来选择功耗轨迹进行分析,对文献[13]的方法有所改进,但是操作难度依然大.

本文提出的方法基于奇异值分解,奇异值分解在侧信道分析方面也有诸多应用. 文献[17]利用 SVD 作为预处理工具构造 DPA 的区分器,SVD 也可以被用来确定电磁分析中的时钟信号[18].

3 差分功耗分析

3.1 相关符号

本文使用 $\boldsymbol{L}=\{\boldsymbol{l}_1,\boldsymbol{l}_2,\cdots,\boldsymbol{l}_m\}\in\mathbf{R}^{m\times n}$ 代表功耗轨迹数据,其意义是随机加密 m 个明文,分别采集加密过程中密码设备消耗的功耗 $\boldsymbol{l}_i(1\leqslant i\leqslant m)$,每次采样包含 n 个采样点. $P=\{p_1,p_2,\cdots,p_m\}$ 代表随机加密的 m 个明文. $K=\{k_1,k_2,\cdots,k_S\}$ 表示密钥空间,S 代表所有可能的密钥的个数.

3.2 DPA 原理

其基本思想是,将功耗轨迹按某种方式(与密钥有关)分为两个组,分别求这两个组的平均功耗轨迹,然后相减,根据相减后的结果确定猜测密钥正确与否. 具体步骤如下:

(1)确定一个中间值函数 $x=F(p,k)$,这个函数是密钥和明文的函数;

(2)对于密钥空间 K 中每个密钥 k,计算它与所有明文的加密的中间值;

(3)设计一个区分函数 D,这个区分函数可以将中间值函数得到的结果分为两个类;

(4)根据区分函数和步骤(2)中得到的中间值将原始功耗轨迹数据 $\boldsymbol{L}$ 分为两类;

(5)分别求这两类的平均功耗轨迹,然后求均值差;

(6)确定正确密钥,对于所有的均值差,如果出现了明显的尖峰说明此时的猜测密钥就是正确密钥 k^*,错误的密钥对应的均值差几乎趋于 0.

上述步骤可以表示成下式:

$$\Delta_D[j]=\frac{\sum_{i=1}^{m}D(p_i,k_t)\boldsymbol{L}_i[j]}{\sum_{i=1}^{m}D(p_i,k_t)}-\frac{\sum_{i=1}^{m}(1-D(p_i,k_t))\boldsymbol{L}_i[j]}{\sum_{i=1}^{m}(1-D(p_i,k_t))} \tag{1}$$

其中 Δ 表示差值,$1\leqslant j\leqslant n$,$1\leqslant t\leqslant S$.

DPA 利用的原理是不同的数据对应的功耗消耗不同,若猜测密钥错误,中间值是随机计算的,那么分类也是随机的,这样造成分类后求的均值差不会有明显的功耗特征. 假设猜测密钥正确,这样中间值计算结果是对的,分类也是正确的,这样大量采集的数据会产生明显的功耗特征,因为两组数据对应的中间值数据在事实上是不同的. 这样 DPA 能够成功分析出密码设备的密钥.

DPA 效率受噪声的影响比较大,假如噪声较大,那

么即使猜测密钥正确,明显的尖峰也会被噪声掩盖,造成密钥难以被区分. 假如能通过预处理的方式选择一些噪声较低的功耗轨迹作为 DPA 分析的数据,就可以提高 DPA 分析效率.

4 奇异值分解

4.1 特征值分解

特征值分解是一种特征提取方法,主要用在在信号处理、统计学和数据挖掘等方面,用于提取数据的特征.

向量 $\boldsymbol{\nu}$ 是方阵 $\boldsymbol{A}$ 的特征向量,将一定可以表示成下面的形式:

$$\boldsymbol{A\nu}=\lambda\boldsymbol{\nu} \tag{2}$$

其中 λ 是实数. 由于特征值分解仅对数据矩阵是方阵时有效,故对于数据不是方阵时需要用奇异值分解.

4.2 奇异值分解

奇异值分解可以提取出非方阵的特征. 假设原始数据是 $\boldsymbol{A}\in\mathbf{R}^{m\times n}$,它可以分解成三个矩阵的乘积

$$\boldsymbol{A}=\boldsymbol{U\Sigma V}^{\mathrm{T}} \tag{3}$$

其中 $\boldsymbol{U}\in\mathbf{R}^{m\times m}$是 $\boldsymbol{A}$ 的左奇异向量组成的矩阵,$\boldsymbol{V}\in\mathbf{R}^{n\times n}$是 $\boldsymbol{A}$ 的右奇异向量组成的矩阵,$\boldsymbol{\Sigma}\in\mathbf{R}^{m\times n}$除了对角线的元素都是 0,对角线上的元素称为奇异值.

以上三个矩阵可以通过如下求出,首先将一个矩阵 $\boldsymbol{A}$ 的转置乘以 $\boldsymbol{A}$,将会得到一个方阵,利用这个方阵求特征值可以得到

$$(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A})\boldsymbol{\nu}=\lambda\boldsymbol{\nu} \tag{4}$$

$\boldsymbol{\nu}$ 即右奇异向量,所有的 $\boldsymbol{\nu}$ 构成 $\boldsymbol{V}$ 矩阵.

$$\sigma=\sqrt{\lambda} \tag{5}$$

σ 就是奇异值,构成矩阵 $\boldsymbol{\Sigma}$. 矩阵 $\boldsymbol{U}$ 如下求出

$$\boldsymbol{\mu}=\frac{1}{\sigma}\boldsymbol{A\nu} \tag{6}$$

所有的$\boldsymbol{\mu}$ 组成 $\boldsymbol{U}$ 矩阵.

这种方法给出求取任意矩阵的特征,更多关于 SVD 的细节可参照文献[19,20].

4.3 奇异值分解的假设

从前面关于 SVD 的介绍来看,SVD 可以是看作是一种特征的提取方式. 通过它可以求得原始数据一系列的特征向量. 特征向量在某些情况下是可以表征原始数据的性质,其中最大的特征值对应的特征向量所包含的信息最多. 最大的特征值对应的特征向量可以被认为是原始数据的一种投影.

我们可以利用这个投影对原始数据进行排序,其中投影值越大,对应原始采样数据的质量越高(噪声越小). 利用这些高质量的采样数据作为 DPA 分析的数据,分析的效率越高.

5 基于 SVD 的 DPA

通过前一节的介绍,可以了解如何通过奇异值分解提取特征. 用在 DPA 上具体如下. 首先计算 $\boldsymbol{LL}^{\mathrm{T}}$,这样得到了方阵. 在进行特征值分解前,先对 $\boldsymbol{LL}^{\mathrm{T}}$ 进行标准化,消除这个方阵中的巨大差异,使得数据处于同一数量级上. 这里使用 Z-score 标准化,其转化函数如下:

$$\boldsymbol{x}^{*}=\frac{\boldsymbol{x}-\boldsymbol{u}}{\delta} \tag{7}$$

其中 $\boldsymbol{x}^{*}$ 是转化后的结果,$\boldsymbol{x}$ 是原始数据的一行,$\boldsymbol{u}$ 是原始数据的均值向量,δ 是 $\boldsymbol{x}$ 的标准差.

假设 $\boldsymbol{LL}^{\mathrm{T}}$ 经过标准化后的结果用 $\boldsymbol{B}\in\mathbf{R}^{m\times m}$表示,则有:

$$\boldsymbol{B}=\mathrm{normalize}(\boldsymbol{LL}^{\mathrm{T}}) \tag{8}$$

此时可以直接求得 $\boldsymbol{B}$ 的特征向量以及特征值

$$\boldsymbol{B\nu}=\lambda\boldsymbol{\nu} \tag{9}$$

这样可以得到所有的特征值 λ_i 和 $\boldsymbol{\nu}_i\in\mathbf{R}^{m\times 1}$($i\in[1,m]$).

如前面所述,特征值大时对应的特征向量包含原有数据的最多信息,那么可以根据该特征向量确定原始功耗轨迹的好坏. 假设最大的特征值对应的特征向量是 $\boldsymbol{\nu}'=(\nu'_1,\nu'_2,\nu'_3,\nu'_4,\nu'_5)=(3,1,2,4,5)$,对其进行从大到小排序可得到 $\boldsymbol{\nu}''=(\nu'_5,\nu'_4,\nu'_1,\nu'_3,\nu'_2)=(5,4,3,2,1)$. 这样就可以认为第五条功耗轨迹质量最好,第四条次之,以此类推. 当进行 DPA 分析前,可以用此方法选择一些高质量的功耗轨迹进行分析,提高分析效率. 具体算法如算法 1.

算法 1 (SVD 选择功耗轨迹)

输入:功耗轨迹数据 $\boldsymbol{L}\in\mathbf{R}^{m\times n}$,需要的功耗数量 k
输出:$S\in\mathbf{R}^{k\times 1}$,代表 k 条功耗轨迹的下标
1:计算 $\boldsymbol{A}=\boldsymbol{LL}^{\mathrm{T}}$
2:计算 $\boldsymbol{B}=\mathrm{normalize}(\boldsymbol{A})$
3:计算 $\boldsymbol{B}$ 的特征值 λ_i 和特征向量 $\boldsymbol{\nu}_i$,$\boldsymbol{B\nu}_i=\lambda\boldsymbol{\nu}_i(i=1,2,\cdots,m)$
4:选择最大的 λ_i对应的特征向量 $\boldsymbol{\nu}'$
5:对 $\boldsymbol{\nu}'$ 进行从大到小排序,得到所有的下标 $\mathrm{Order}\in\mathbf{R}^{m\times 1}$
6:$S=\mathrm{Order}(1:k)$
7:返回 S

算法 1 用于实现选择 DPA 分析的功耗轨迹,整个分析流程如图 1 所示.

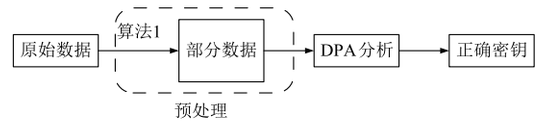

图1 基于SVD的DPA流程图

6　实验

6.1　AES 实验分析

6.1.1　实验平台

本实验分析的是 AES-128 在单片机 STC89C58RD 上的实现. 单片机 STC89C58RD 是 8 位处理器,其泄漏的功耗模型可以近似看为汉明重量模型(Hamming Weight,HW). 采样设备是 Tektronix DPO 7254 示波器,采样率是 50MSa/s,采样 2000 次,每次采样 10000 个点. 实验的攻击点是 AES 算法第一轮各个 S 盒输出(如图 2 所示),采用多比特 DPA 分析(按中间值的汉明重量或者汉明距离将功耗轨迹分类作差分)方法,对 S 盒的输出的汉明重量做区分,大于 4 的分为一组,剩下的分为一个组,求均值差.

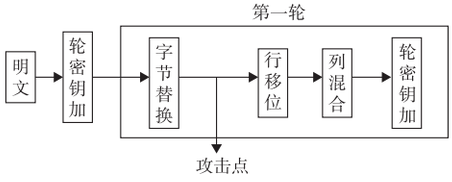

图2　DPA攻击方案

6.1.2　实验结果

从密码设备采集到的原始功耗轨迹数据如图 3 所示.

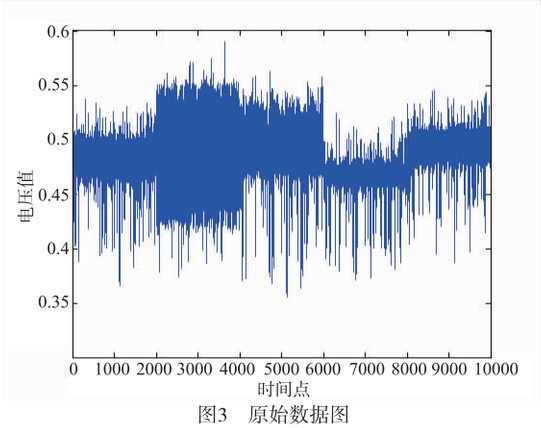

图3　原始数据图

在实验过程中,每次随机选择 1000 条功耗轨迹数据组成算法1的输入,然后根据流程图1进行分析,本实验采用侧信道通用的评估标准成功率进行评估. 该评估标准在文献[21]中被提出,其核心思想是在不同数量的功耗轨迹情况下,恢复出正确子密钥的概率. 这个评估方式是目前侧信道分析普遍的评估标准,为了简单起见,本文采用的是部分成功率(Partial Success Rate,PSR),即恢复一个子密钥的成功率.

由于总共采集了 2000 条功耗轨迹,而成功率是需要多次分析求概率,故本实验每次随机抽取 1000 条功耗轨迹作为算法 1 的输入,然后按照流程图 2 进行分析. 作为对比,本实验与传统无预处理 DPA 和文献[13]的方法来改进 DPA 即基于 PCA 的 DPA 方法作对比实验,当选择后的功耗轨迹数目都是 200 条时,其结果分别如图 4 ~ 6 所示.

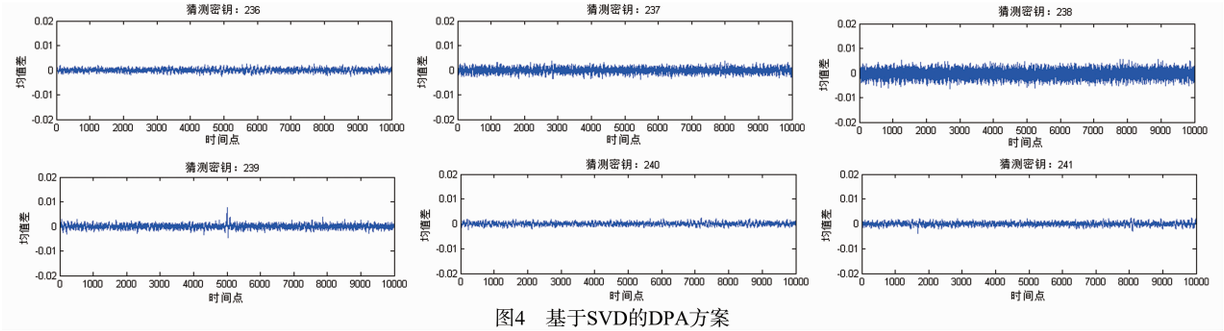

图4　基于SVD的DPA方案

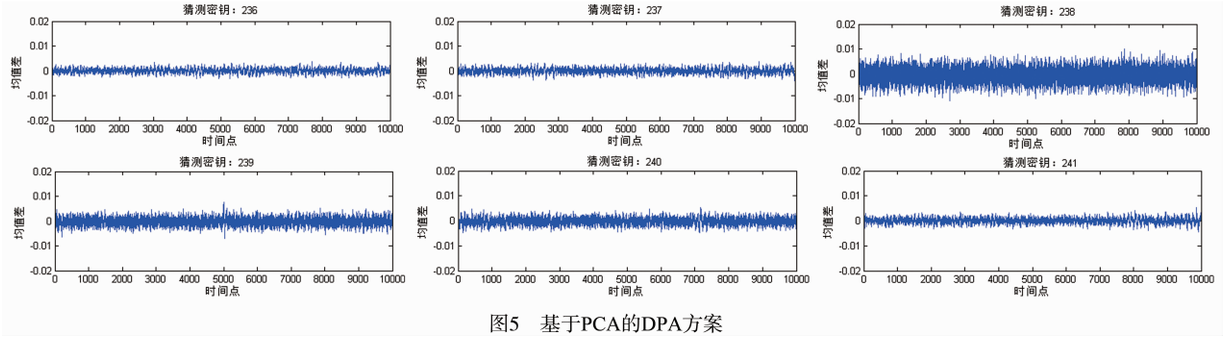

图5　基于PCA的DPA方案

本实验中,正确密钥是 239,攻击点处于 5000 点左右,　　图 4 显示,经过 SVD 选择的功耗轨迹进行差分后,正确密

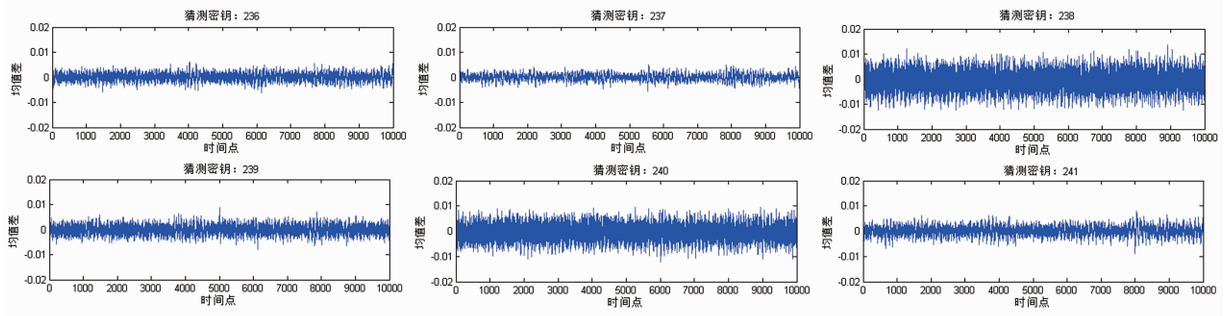

图6 DPA方案

钥对应的差分图相比较其他错误密钥,区分度很明显,可以正确得到密钥. 而图 5 ~6 得到的差分图在正确密钥时,尖峰不是很明显,与错误密钥的结果区分度不大.

这三种方案的部分成功率如图 7 所示.

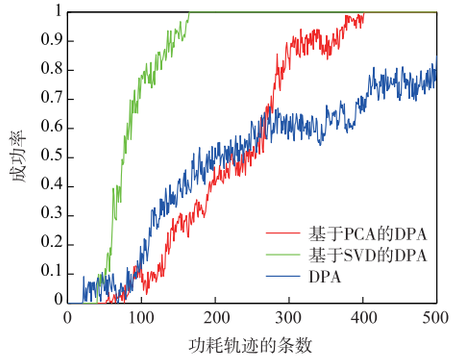

图7 各种方案的成功率(单片机STC89C58RD)

从图 7 可以看出,经过大量的实验,利用 SVD 选择功耗轨迹后进行 DPA 分析相比较其余两种方法在恢复密钥的效率上有很大提高.

6.2 DES 实验分析

6.2.1 实验平台

此外,为了进一步验证本方法的有效性,本文使用 DPA Contest(http://www.dpacontest.org/home/)提供的数据作为实验对象. DPA Contest 提供的数据在功耗分析领域具有较高认可度,本文采用的是 DPA Contest 2008/2009(DPA 大赛第一阶段) 的 secmatv1_2006_04_0809 数据. 该数据是从 ASIC 设备上执行 DES 算法时采集下的功耗值,符合汉明距离模型(Hamming Distance,HD). 本文针对 DES 的攻击点是 DES 算法中的 f 函数.

6.2.2 实验结果

本实验随机选择 DPA Contest V1 提供的数据中的 500 条作为算法 1 的输入,与实验一相同,使用通用标准部分成功率来对比各种方法的优劣,其结果如图 8 所示. 从图 7 可以看出,经过大量的实验,利用 SVD 选择功耗轨迹后对 DPA Contest V1 数据进行 DPA 分析相比较其余两种方法在恢复密钥的效率上有很大提高.

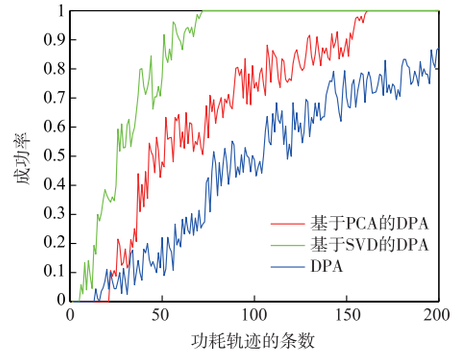

图8 各种方案的成功率(DPA Contest V1)

7 结论

本文针对 DPA 在实际分析过程中,效率不是很高的问题,提出了一种基于 SVD 的选择功耗轨迹的方法,利用这种方法可以选择一些质量较高的功耗轨迹用于做 DPA 分析. 从理论上分析了该方法可以提取数据的特征的性质,故而可以用于做功耗轨迹排序以及选择. 本文在实际应用中对运行 AES 算法的单片机采集的数据和国际上认可度较高的 DPA 大赛数据,并做实验分析了该方法的有效性,与其余方法做了对比,效率方面有了较大的提高. 在未来研究中,我们将利用此方法在其他密码算法的实现上进行分析,此外,也应用此方法在分析对加保护的设备二阶分析中,提高二阶分析的效率. 另一方面,将此方法应用在模板分析中,用此方法选择功耗轨迹来刻画模板,解决模板分析中刻画阶段的不精确,提高模板分析的效率.

参考文献

[1] Kocher P,Jaffe J,Jun B. Differential power analysis[A]. Advances in Cryptology—CRYPTO'99[C]. Berlin Heidelberg:Springer,1999. 388 –397.

[2] Clavier C,Coron J S,Dabbous N. Differential power analysis in the presence of hardware countermeasures[A]. Cryptographic Hardware and Embedded Systems—CHES 2000[C]. Berlin Heidelberg:Springer,2000. 252 –263.

[3] Joye M, Paillier P, Schoenmakers B. On second-order differential power analysis[A]. Cryptographic Hardware and Embedded Systems-CHES 2005[C]. Berlin Heidelberg: Springer, 2005. 293 – 308.

[4] Tiri K, Akmal M, Verbauwhede I. A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards [A]. Solid-State Circuits Conference, 2002. ESSCIRC 2002 [C]. Florence Italy: IEEE, 2002. 403 – 406.

[5] Guilley S, Hoogvorst P, Pacalet R. Differential power analysis model and some results[A]. CARDIS[C]. Berlin Heidelberg: Springer, 2004, 4. 127 – 142.

[6] Prouff E, Rivain M, Bévan R. Statistical analysis of second order differential power analysis [J]. Computers, IEEE Transactions on, 2009, 58(6): 799 – 811.

[7] Fischer W, Gammel B M, Kniffler O, et al. Differential power analysis of stream ciphers[A]. Topics in Cryptology-CT-RSA 2007[C]. Berlin Heidelberg : Springer, 2006. 257 – 270.

[8] Gebotys C H, Ho S, Tiu C C. EM analysis of Rijndael and ECC on a wireless Java-based PDA [A]. Cryptographic Hardware and Embedded Systems – CHES 2005[C]. Berlin Heidelberg: Springer, 2005. 250 – 264.

[9] Plos T, Hutter M, Feldhofer M. On comparing side-channel preprocessing techniques for attacking RFID devices[A]. Information Security Applications[C]. Busan, Korea: Springer, 2009. 163 – 177.

[10] Barenghi A, Pelosi G, Teglia Y. Improving first order differential power attacks through digital signal processing [A]. Proceedings of the 3rd International Conference on Security of Information and Networks [C]. New York USA: ACM, 2010. 124 – 133.

[11] Kasper T, Oswald D, Paar C. Side-Channel Analysis of Cryptographic RFIDs with Analog Demodulation [M]. RFID. Security and Privacy. Berlin Heidelberg: Springer, 2012: 61 – 77.

[12] Cao, Yuchen, Yongbin Zhou, Zhenmei Yu. On the negative effects of trend noise and its applications in side-channel cryptanalysis[J]. Chinese Journal of Electronics, 2014, 23(2): 366 – 370.

[13] Kim Y, Sugawara T, Homma N, et al. Biasing power traces to improve correlation power analysis attacks[A]. First International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE 2010)[C]. Berlin Heidelberg: Springer, 2010. 77 – 80.

[14] Kim Y, Ko H. Using principal component analysis for practical biasing of power traces to improve power analysis attacks [A]. Information Security and Cryptology-ICISC 2013[C]. Berlin Heidelberg: Springer, 2014. 109 – 120.

[15] Brier E, Clavier C, Olivier F. Correlation power analysis with a leakage model[A]. Cryptographic Hardware and Embedded Systems-CHES 2004[C]. Berlin Heidelberg: Springer, 2004. 16 – 29.

[16] Hu W, Wu L, Wang A, et al. Adaptive chosen-plaintext correlation power analysis [A]. Computational Intelligence and Security (CIS), 2014 Tenth International Conference on[A]. Kunming: IEEE, 2014. 494 – 498.

[17] Batina L, Hogenboom J, van Woudenberg J G J. Getting more from PCA: First results of using principal component analysis for extensive power analysis[A]. Topics in Cryptology-CT-RSA 2012[C]. Berlin Heidelberg: Springer, 2012. 383 – 397.

[18] Hongying L I U, Xin J I N, Tsunoo Y. Correlated noise reduction for electromagnetic analysis[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2013, 96(1): 185 – 195.

[19] Andrews H C, Patterson III C L. Singular value decomposition (SVD) image coding[J]. Communications, IEEE Transactions on, 1976, 24(4): 425 – 432.

[20] Golub G H, Reinsch C. Singular value decomposition and least squares solutions[J]. Numerische mathematik, 1970, 14(5): 403 – 420.

[21] Standaert F X, Malkin T G, Yung M. A unified framework for the analysis of side-channel key recovery attacks[A]. Advances in Cryptology-EUROCRYPT 2009[C]. Berlin Heidelberg : Springer, 2009. 443 – 461.

作者简介

周新平　男,1990 年出生于江西樟树,现为中国科学院信息工程研究所博士研究生. 主要研究领域为密码学,侧信道分析.
E-mail: zhouxinping@ iie. ac. cn

孙德刚　男,1970 年出生于吉林磐石,现为中国科学院信息工程研究所研究员,博士生导师,主要研究领域为信号处理理论与技术、电磁检测与防护.

王　竹(通信作者)　女,1972 年出生于山西太原,博士,现为中国科学院信息工程研究所副研究员,主要研究领域为应用密码学及其应用.
E-mail: wangzhu@ iie. ac. cn

欧长海　男,1989 年出生于贵州铜仁,现为中国科学院信息工程研究所博士研究生. 主要研究领域为密码学与侧信道分析.