新的抵抗鬼峰的关联矩阵差分能量分析

姜子敬，丁群
（黑龙江大学电子工程学院，黑龙江 哈尔滨 150080）

摘 要：差分能量分析（DPA）是对芯片中分组密码实现安全性的最主要威胁之一，当采集的能量迹不足时，DPA 容易受到错误密钥产生的差分均值影响产生鬼峰。基于 DPA，提出了一种可以有效抵抗鬼峰的关联矩阵差分能量分析（IMDPA）。通过构造预测差分均值矩阵，利用猜测密钥在非泄露区间的弱相关性，避免非泄露区间对泄露区间内密钥猜测的影响。对 IMDPA 在 AES-128 算法的不同泄露区间进行了实验验证，结果表明，与传统的 DPA 相比，IMDPA 需要更少（达到 85%）的能量迹来猜测正确的密钥。同时 IMDPA 在实施防护措施下的 AES-128 的密钥猜测效率仍然存在显著的优势。为了进一步验证 IMDPA 在分组密码中的通用性，在 SM4 算法上进行了实验验证，与传统的 DPA 相比，IMDPA 需要更少（达到 87.5%）的能量迹来猜测正确的密钥。

关键词：AES；鬼峰；差分能量分析；SM4
中图分类号：TN918
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2023063

Nove lincidence matrix differential power analysis for resisting ghost peak

JIANG Zijing, DING Qun
College of Electronic Engineering, Heilongjiang University, Harbin 150080, China

Abstract: At present, differential power analysis (DPA) is one of the most important threats to the security of block ciphers in chips. When the collected power trace is insufficient, DPA is vulnerable to ghost peak caused by the difference mean value generated by the wrong key. Based on DPA, a incidence matrix differential power analysis (IMDPA) was proposed which could effectively resist ghost peak. The prediction difference mean matrix was constructed to avoid the influence of the non leaking interval on the key guessing of the leaking interval by using the weak correlation of the guessing key in the non leaking interval. The proposed IMDPA was tested in different leak intervals of AES-128 algorithm. The results show that compared with traditional DPA, IMDPA requires less (up to 85%) power trace to guess the correct key. At the same time, the key guessing efficiency of AES-128 under the implementation of protective measures by IMDPA still has obvious advantages. In order to further verify the universality of IMDPA in block ciphers, experimental verification is conducted on SM4 algorithm. Compared with traditional DPA, IMDPA requires less (up to 87.5%) power traces to guess the correct key.

Keywords: AES, ghost peak, differential power analysis, SM4

0 引言

自 1996 年 Kocher[1]提出密码分析方法以来，侧通道分析作为一种区别于经典密码分析的加密分析方法，经过 20 多年的发展，以其强大的分析能力和广泛的应用范围，已成为密码领域的研究热

收稿日期：2022−10−24；**修回日期**：2023−01−20
通信作者：丁群，qunding@aliyun.com
基金项目：国家自然科学基金资助项目（No.61471158）；黑龙江省自然科学基金优秀青年基金资助项目（No.YQ2020F012）
Foundation Items: The National Natural Science Foundation of China (No.61471158), The Natural Science Foundation of Heilongjiang Province for Distinguished Young Scholars (No.YQ2020F012)

点。侧信道分析一般包括定时分析、功率分析[2-4]、模板分析[5]、电磁分析[6-7]、碰撞攻击[8-9]、故障分析[10-12]和人工智能侧信道分析[13-15]等。其中，差分能量分析（DPA, differential power analysis）是对芯片中分组密码实现安全性的最主要威胁之一。因此，在评估芯片中分组密码侧信道安全性的时候，分组密码算法的 DPA 安全性是衡量的要素之一。DPA 由 Kocher 等[2]基于中间变量一个比特的均值距离（差分均值）模型提出。

传统的 DPA 通常比较不同采样点的差分均值。这意味着不同采样点的非均匀侧信道信号强度可能会显著影响结果，非泄露区间可能存在鬼峰的情况。鬼峰定义为非泄露区间错误密钥猜测的差分均值比泄露区间正确密钥猜测的差分均值高。2004 年，Brier 等[3]提出当 DPA 用于攻击 DES 时，鬼峰导致攻击效能受到影响。2006 年，Schramm 等[16]提出 DES 的 S 盒操作的低非线性可能会导致鬼峰。2017 年，Lo 等[17]提出当 DPA 应用于具有高非线性的 S 盒时，鬼峰仍然存在。由于非泄露区间可能存在鬼峰对密钥猜测的影响，只能采集更多的能量迹来猜测正确的密钥。为了减少 DPA 所需能量迹数目和提高 DPA 效率，2018 年，Mahanta 等[18]提出基于 Canberra 距离解决 DPA 出现的鬼峰问题。2021 年，Chen 等[19]通过对差分均值矩阵进行标准化抑制鬼峰的产生。

针对 DPA 可能会受到鬼峰[3, 16-20]影响攻击效能的问题，本文提出了一种新的侧信道分析方法，通过构造预测差分均值矩阵，利用皮尔森相关系数的特点，根据相关性的强弱猜测正确密钥，利用猜测密钥在非泄露区间的弱相关性，从而避免非泄露区间对泄露区间内密钥猜测的影响。这样即使非泄露区间的密钥猜测相关联的差分均值高于泄露区间，也不会被鬼峰现象影响到密钥猜测。该方法对鬼峰导致的密钥猜测错误问题和提高猜测密钥的效率具有重要意义。

1　差分能量分析

1.1　能量模型

在侧信道分析中，通常需要在设备的操作数据和功耗的模拟值之间建立对应关系来表征密码设备的功耗。在功耗攻击中，汉明权重模型和汉明距离模型是描述电路功耗的 2 个重要模型。

如果密码运算中的中间值用 v 表示，则其汉明权重为 $\mathrm{HW}(v)$，汉明权重指的是 v 的二进制表示中数字 1 的数量。汉明权重模型更适用于使用预充电总线的微控制器。当密码算法的中间值从内存复制到寄存器，或发生与数据相关的其他操作时，将发生汉明权重泄露，由此产生的电路功耗通常与汉明权重有关，如式(1)所示。

$$T = a\mathrm{HW}(v) + b \tag{1}$$

其中，T 表示功耗，a 表示功耗的比例系数，b 表示与处理数据无关的泄露和噪声。

汉明距离是指 2 个值异或后的汉明重量。汉明距离模型适用于硬件实现中的寄存器比特翻转。当时钟到达时，寄存器比特发生翻转，翻转的比特数用于描述当时的功耗值。该功耗通常与汉明距离有关，如式(2)所示。

$$T = a\mathrm{HD}(v_1, v_2) + b \tag{2}$$

其中，$\mathrm{HD}(v_1, v_2)$ 表示 v_1 和 v_2 的汉明距离，v_1 被记录为电路改变之前的状态，v_2 被记录为改变之后的状态。

综上所述，汉明距离模型更适合描述 FPGA 中寄存器比特翻转引起的功耗。

1.2　差分能量分析

DPA 将密钥的猜测问题转换为随机变量概率分布的差值计算问题。不同数据操作下得到的功耗曲线存在微小差异，DPA 利用这一特性，通过假设密钥和明文构建的区分函数将功耗曲线分为 2 个独立的向量样本，通过计算两者的均值差将微小差异进行累积放大，从而推测出正确的猜测密钥。DPA 需要依次完成下面 4 个步骤。

步骤 1　信息采集。采集一组固定密钥随机明文的能量迹 $t = \{t_i \mid i \in [1, n]\}$，每一条能量迹对应 m 个采样点。第 i 条能量迹的第 j 个采样点表示为 $t_{i,j}$，其对应的明文为 $p = \{p_i \mid i \in [1, n]\}$，密文为 $c = \{c_i \mid i \in [1, n]\}$。

步骤 2　数据分区。由于密码算法采用硬件实现，其能量消耗依赖于时钟沿到来时同一寄存器比特位的翻转，因此使用汉明距离模型计算预测功耗。假设猜测密钥 $k = \{k \mid k \in [0, 2^n - 1]\}$，计算猜测密钥 k 与 n 条能量迹相对应寄存器位置的汉明距离矩阵 $\boldsymbol{h} = \{h_{i,j} \mid i \in [0, 2^n - 1], j \in [1, n]\}$，将 n 条能量迹按汉明距离矩阵 $\boldsymbol{h}$ 分为 2 个集合，如式(3)所示。

$$T_1=\{t_i \mid h_i<4\},\ T_2=\{t_i \mid h_i>4\}, i=1,2,\cdots,n \quad (3)$$

步骤 3　均值差异计算。求出 2 个集合中的曲线各自的均值，然后对均值作差。

$$\boldsymbol{D}=\frac{\sum\limits_{t_i\in T_1} t_i}{|T_1|}-\frac{\sum\limits_{t_i\in T_2} t_i}{|T_2|} \quad (4)$$

步骤 4　正确密钥确定。DPA 攻击的结果可以表示为矩阵 $\boldsymbol{D}=\{D_{i,j} \mid i\in[0,2^n-1], j\in[1,m]\}$，矩阵 $\boldsymbol{D}$ 的行记为 $\boldsymbol{D}_i$，对应于猜测密钥 k；列记为 $\boldsymbol{D}_j$，对应于能量迹 t_i 的 m 个采样点。矩阵中元素绝对值的最大值对应的猜测密钥确定为正确密钥。

在 DPA 攻击过程中，鬼峰现象是比较常见的。DPA 是从密码设备中提取密钥信息，然后将能量消耗值与猜测密钥的预测值进行比较，找到对应的尖峰，尖峰所对应的位置就是正确的密钥值。然而在采集到的能量迹中存在许多采样点，这些采样点分别对应算法的不同阶段，本文将这些采样点的位置分组为泄露区间，其余采样点的位置可以分组为非泄露区间。当泄露区间中的正确密钥猜测相关联的差分均值高于采样点中的其他密钥猜测相关联的差分均值时，密钥猜测正确，而泄露区间中的正确密钥猜测相关联的峰值可能低于非泄露区间中的错误密钥猜测相关联的假峰值。那些高于正确密钥猜测相关联的峰值的假峰值被称为鬼峰。如图 1 所示，非泄露区间中的尖峰比正确密钥猜测生成的尖峰具有更高的差分均值。所以即使正确密钥猜测在泄露区间产生最高峰值，但该峰值低于非泄露区间的错误密钥猜测产生的峰值，DPA 也会输出鬼峰所对应的错误猜测密钥，导致密钥猜测错误。

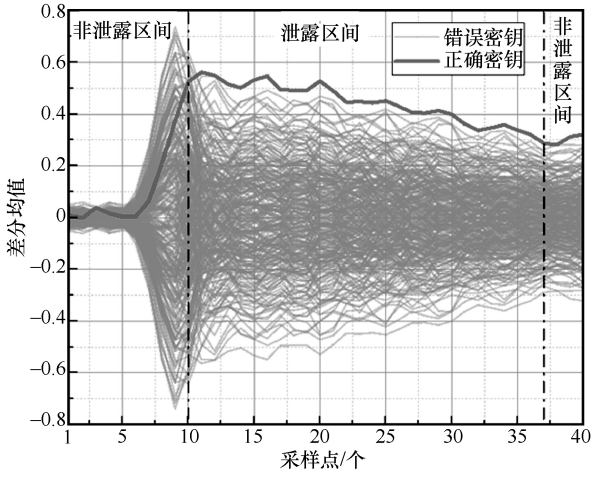


图 1　基于差分能量分析差分均值曲线

标准化预处理是目前最有效的抑制鬼峰的预处理方法。数据的标准化预处理如式(5)所示。图 2 为 AES-128 算法在 FPGA 运行时采集到的 100 条功耗曲线。

$$t'_{ij}=\frac{t_{ij}-\mu_j}{\sigma_j} \quad (5)$$

其中，t_{ij} 表示采集的 AES-128 算法第 i 条第 j 个采样点的能量消耗，t'_{ij} 表示标准化预处理后的能量迹，μ_j 表示第 j 个采样点的能量均值，σ_j 表示第 j 个采样点的能量方差。μ_j 和 σ_j 分别为

$$\mu_j=\frac{\sum\limits_{i=1}^{n} t_{ij}}{n} \quad (6)$$

$$\sigma_j=\sqrt{\frac{\sum\limits_{i=1}^{n}(t_{ij}-\mu_j)^2}{n-1}} \quad (7)$$

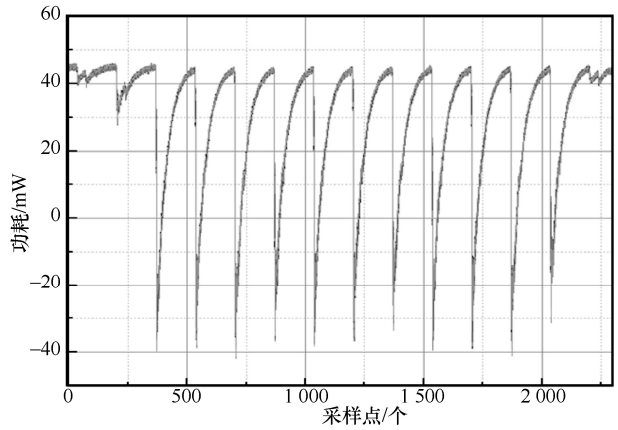


图 2　AES-128 算法的功耗曲线

图 3 为图 2 中 AES-128 算法 100 条功耗曲线经过标准化预处理后的功耗曲线，不同颜色的功耗曲线代表一条独立的能量迹。

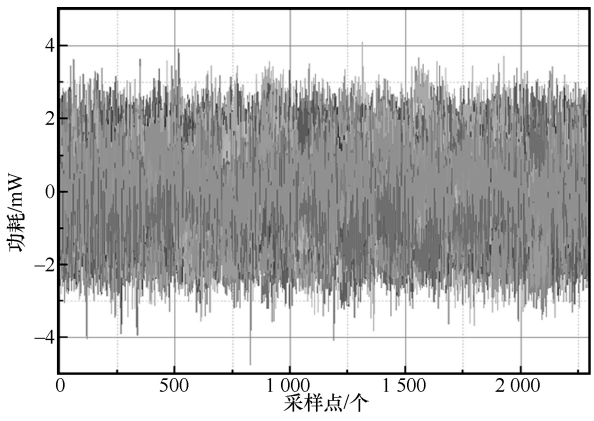


图 3　AES-128 算法标准化预处理后的功耗曲线

经过标准化预处理后的差分均值曲线如图 4 所示。标准化预处理后错误密钥原本非泄露区间的鬼峰得到有效抑制，正确密钥在整个采样区间获得最大的差分均值，即可成功猜测出正确密钥。

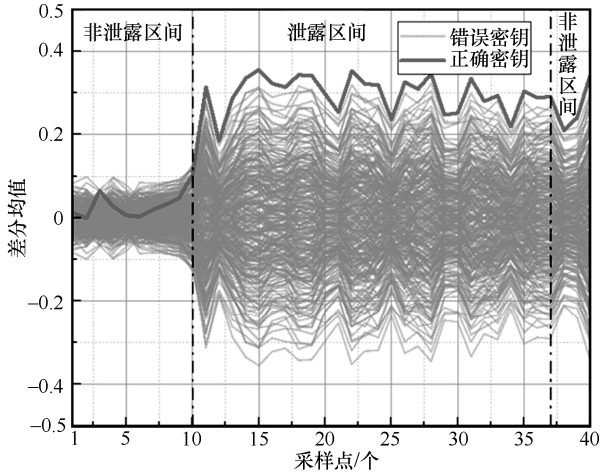


图 4　标准化预处理后的差分均值曲线

2　关联矩阵差分能量分析

目前已经提出的解决方案大都致力于降低在能量迹采集过程中噪声的影响，包括滤除大噪声、能量迹对齐技术、能量迹标准化处理。这些方法作为 DPA 的预处理可以有效抑制鬼峰现象，减少 DPA 所需能量迹数量并提高 DPA 效率。

第 1 节已经详细介绍了 DPA 的攻击过程。一般情况下，泄露区间中正确密钥相关联的差分均值达到峰值，但同时非泄露区间中产生更高的差分均值则会导致密钥猜测错误的问题。为解决鬼峰问题，Chen 等[19]提出基于差分均值矩阵标准化的 MDPA，但其实际上是标准化后处理方法，本质上与标准化预处理一样仍然是致力于降低在能量迹采集过程中噪声的影响而非抑制鬼峰。Mahanta 等[18]提出基于 Canberra 距离的差分能量分析，通过利用欧几里得相似度的 Canberra 距离抑制鬼峰的值，留下可能揭示密钥的实际峰值来解决鬼峰问题。

为解决鬼峰问题，本文提出了一种新的解决思路，即关联矩阵差分能量分析（IMDPA, incidence matrix differential power analysis），它是建立在标准 DPA 攻击之上的一种有效改进。不同于 EDPA 通过抑制鬼峰来解决密钥猜测错误的问题，本文通过增强正确密钥在泄露区间关联的峰值来解决密钥猜测错误的问题。为了在差分能量分析中增强正确密钥在泄露区间关联的差分均值，由于寄存器翻转比特数与功耗呈线性关系这一特点，相较上述方法，本文构造出一个在泄露区间与差分均值矩阵有着强关联对应关系的中间值矩阵，使猜测密钥的差分均值在泄露区间产生强关联效果。由于这种强关联性只存在于泄露区间，非泄露区间鬼峰的影响被减弱。因此可以根据差分均值和中间值相关性的强弱猜测正确密钥，利用猜测密钥在非泄露区间的弱相关性，从而避免非泄露区间对泄露区间内密钥猜测的影响。这样即使非泄露区间的密钥猜测相关联的差分均值高于泄露区间，也不会被鬼峰现象影响密钥猜测。

IMDPA 攻击需要依次完成下面 5 个步骤，具体如算法 1 所示。

步骤 1　实际功耗 DPA。根据汉明距离模型通过遍历 2^8 种猜测密钥计算其与 n 条随机明文能量迹的汉明距离矩阵 $\boldsymbol{h}$。矩阵 $\boldsymbol{h}$ 的行记为 $\boldsymbol{h}_i$，对应于猜测密钥 $k=\{k\,|\,k\in[0,2^8-1]\}$；列记为 $\boldsymbol{h}_j$，对应于能量迹 $t=\{t_i\,|\,i\in[1,n]\}$。

根据矩阵 $\boldsymbol{h}$ 的行 $\boldsymbol{h}_i$ 对能量迹 t 划分集合并利用式(3)和式(4)计算差分均值。DPA 攻击的结果可以表示为矩阵 $\boldsymbol{D}$，矩阵 $\boldsymbol{D}$ 的行记为 $\boldsymbol{D}_i$，对应于猜测密钥 k；列记为 $\boldsymbol{D}_j$，对应于能量迹 t_i 的 m 个采样点。

步骤 2　构造预测差分均值矩阵所需的预测功耗矩阵。根据式(2)中汉明距离模型可知，汉明距离和功耗呈线性关系，所以本文直接将汉明距离矩阵 $\boldsymbol{h}$ 作为预测功耗矩阵 $\tilde{\boldsymbol{h}}$。此时的预测功耗矩阵 $\tilde{\boldsymbol{h}}$ 大小为 $[2^8,n]$。预测功耗矩阵 $\tilde{\boldsymbol{h}}$ 中不仅包括正确密钥的预测功耗，同样也包括错误密钥的预测功耗，且矩阵中的元素仅代表泄露区间的预测功耗，矩阵 $\tilde{\boldsymbol{h}}$ 的行记为 $\tilde{\boldsymbol{h}}_i$，列记为 $\tilde{\boldsymbol{h}}_j$，分别对应于猜测密钥 k 和能量迹 t。

步骤 3　预测功耗分类。通过对 2^8 种密钥可能结果与 n 条随机明文能量迹的汉明距离对相应的 n 条预测功耗信息进行分类，由于预测功耗矩阵不仅包括正确密钥的预测功耗，同样也包括错误密钥的预测功耗，因此要逐行对预测功耗矩阵 $\tilde{\boldsymbol{h}}$ 的 n 个预测功耗进行分类，如式(8)所示。当外部用于遍历正确密钥的 k 和预测功耗矩阵所处的行向量同时属于正确密钥时，n 个预测功耗分类结果接近实际能量迹的分类。

$$H_1=\{\tilde{h}_j \mid h_j<4\}, H_2=\{\tilde{h}_j \mid h_j>4\}, j=1,2,\cdots,n \tag{8}$$

步骤 4 预测差分均值矩阵构造。求出 $2^8\times 2^8$ 种可能的分类结果各自的均值，然后对均值作差，即可得到预测差分均值矩阵 $\boldsymbol{C}=\{C_{i,j} \mid i\in[1,2^8], j\in[1,2^8]\}$，如式(9)所示。矩阵 $\boldsymbol{C}$ 的行记为 $\boldsymbol{C}_i$，列记为 $\boldsymbol{C}_j$，分别对应于猜测密钥 k 和预测功耗矩阵所在的行。

$$\boldsymbol{C}=\frac{\sum\limits_{h_j\in H_1}\tilde{h}_j}{|H_1|}-\frac{\sum\limits_{h_j\in H_2}\tilde{h}_j}{|H_2|} \tag{9}$$

步骤 5 正确密钥确定。根据皮尔森相关系数计算IMDPA结果矩阵 $\boldsymbol{D}$ 和本文构造的预测差分均值矩阵 $\boldsymbol{C}$ 的相关系数矩阵 $\boldsymbol{\rho}=\{\rho_{i,j} \mid i\in[1,2^8], j\in[1,m]\}$。矩阵 $\boldsymbol{\rho}$ 的行记为 $\boldsymbol{\rho}_t$，列记为 $\boldsymbol{\rho}_j$，分别对应于猜测密钥 k 和能量迹 t 的 m 个采样点。矩阵中元素绝对值最大值对应的行确定为正确密钥，列对应采样点为泄露位置。皮尔逊相关系数的数学表达式为

$$\rho_{XY}=\frac{\mathrm{Cov}[X,Y]}{\sqrt{\mathrm{Var}[X]\mathrm{Var}[Y]}} \tag{10}$$

算法 1 关联矩阵差分能量分析

输入 明文 p，密文 c，能量迹 t，S 盒 S

输出 猜测密钥

```
for Sbox = 1:16
    for k = 0:255
        for p = 1:num
        h = HW[S^{-1}(c ⊕ k) ⊕ c]
        T1 = {t | h < 4}, T2 = {t | h > 4}
        end for
    end for
D = mean(T1) − mean(T2)
end for
for k = 0:255
    for k̃ = 0:255
        for p = 1:num
        H1 = {h | h < 4}, H2 = {h | h > 4}
        end for
    end for
    C = mean(H1) − mean(H2)
 end for
for k̃ = 0:255
    for Sampling point = 1:m
    ρ = corr(C, D)
    end for
end for
ρ_{i,j} = max(max(ρ)) //i 为猜测密钥，j 为泄露点
```

假设功耗 DPA 结果矩阵 $\boldsymbol{C}$ 对应的猜测密钥 $\tilde{k}$ 确实为真实密钥，那么列向量 $\boldsymbol{C}_j$ 的假设差分均值和矩阵 $\boldsymbol{D}$ 列向量 $\boldsymbol{D}_j$ 的实际功耗差分均值一定有较强的相关性，而 m 个采样点中相关性最强的点对应需要的泄露位置，这样就可以无视非泄露区间产生的高差分均值对密钥猜测的影响。

3 实验结果

为了验证 IMDPA 的可行性，本文构建了基于 FPGA 的能量消耗采集平台。由于 FPGA 具有高灵活性和低成本的特点，因此在生产密码芯片之前适合进行硬件实现算法仿真实验，发现问题和改进可能的薄弱环节，降低设计时间和成本。本节实验采用 SAKURA-G FPGA 开发板。FPGA 被设计为采用功耗采集模块，便于实验在芯片操作过程中采集和处理功耗信息。

3.1 AES-128 密钥猜测效率

为探究 Kocher 等[2]的标准 DPA、Mahanta 等[18]的基于 Canberra 距离的差分能量分析 EDPA、Chen 等[19]的基于差分均值矩阵标准化的 MDPA 及本文提出的 IMDPA 的效率，本节选取 AES-128 算法分别通过实验复现 DPA、EDPA、MDPA 这 3 种方法与本文提出的 IMDPA 进行密钥猜测对比实验，以此验证抵抗鬼峰的效果。在进行能量波形仿真时，由于密码算法采用硬件实现，其能量消耗依赖于时钟沿到来时同一寄存器比特的翻转，假设仿真波形服从汉明距离模型，噪声服从高斯分布。本节在不同波形数量下均进行了多次实验，波形数量的范围为[0, 5 000]和[0, 10 000]。在各个波形数量下均进行 100 次实验，统计 4 种方法的密钥全部字节收敛、密钥猜测成功率和计算复杂度，其中，计算复杂度由猜测全部 16 B 的时间表示。

3.1.1 AES-128 不同泄露区间

为了探究 S 盒对 DPA 效率的影响，分别选取 AES-128 算法异或白化密钥输出寄存器（图 5 的寄存器 A）和第 10 轮轮函数输出寄存器（图 5 的寄存器 B）作为攻击目标。

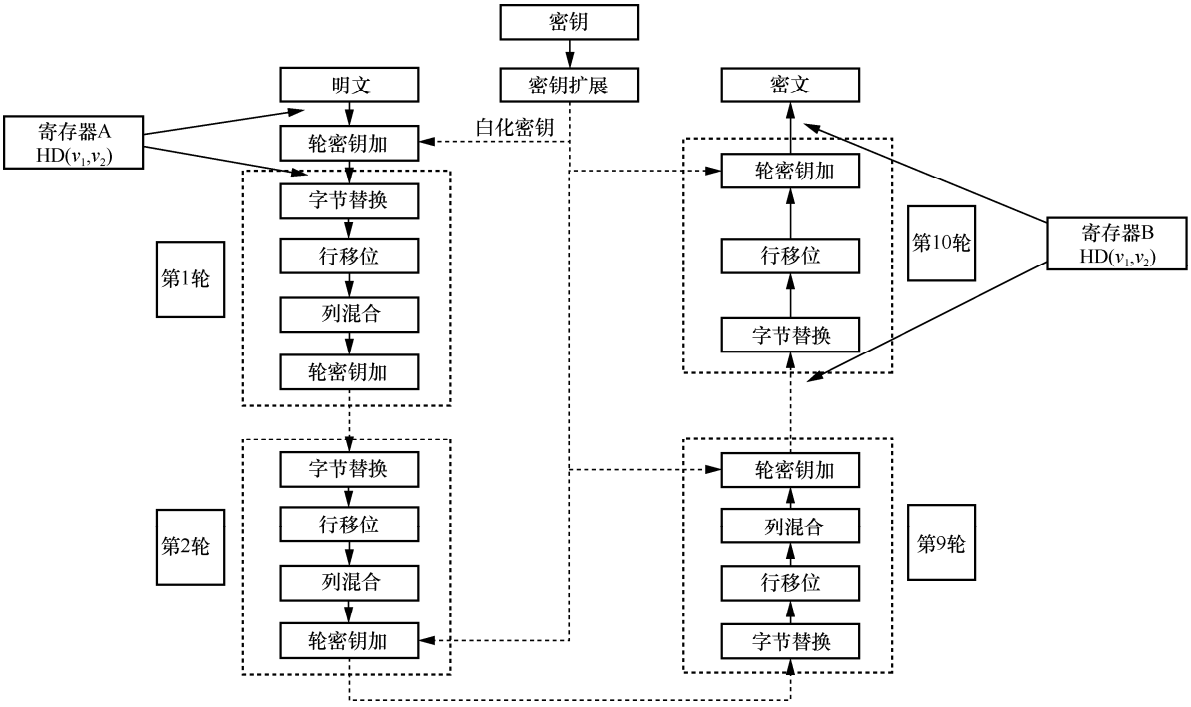


图 5　AES-128 算法

泄露点分析如图 6 所示。由图 6 可知，AES-128 算法在整个加密过程中寄存器 A 和寄存器 B 分别对应 AES-128 算法的第 1 个和第 11 个尖峰。

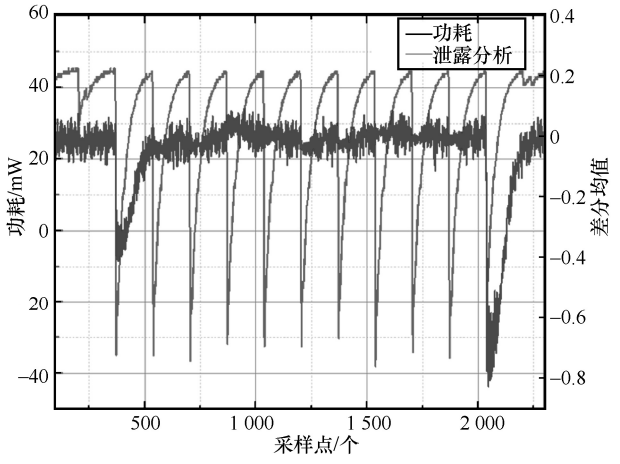


图 6　泄露点分析

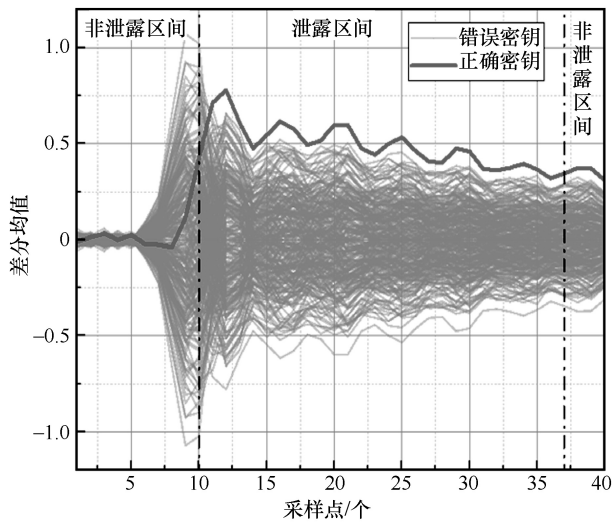
图 7 分别为 AES-128 算法寄存器 A 和寄存器 B 标准 DPA 和 IMDPA 的攻击结果。由图 7(a)和图 7(b)可知，DPA 攻击位置的选取会直接影响密钥猜测的结果。由于第 10 轮轮函数包含非线性部件 S 盒，当攻击位置取寄存器 A 时，非泄露区间产生的鬼峰数量要明显多于攻击位置取寄存器 B 时非泄露区间产生的鬼峰数量。由图 7(c)和图 7(d)可知，IMDPA 最高的峰值落在泄露区间，有效抵抗了非泄露区间鬼峰对密钥猜测的影响。

AES-128 算法的不同寄存器位置下 4 种方法全部 16 B 密钥的收敛情况如图 8 所示。从图 8 可以看出，4 种方法中的 16 B 的猜测密钥随着能量迹数量的增加而逐渐收敛。对比图 8(a)和图 8(b)可知，攻击位置的选择影响密钥收敛。由于第 10 轮存在非线性变换–字节替换操作，即使 S 盒的输入仅发生 1 bit 的翻转，其输出将截然不同，导致功耗产生巨大差异。因此，当选择寄存器 B 作为攻击位置时，密钥收敛速度明显更快。

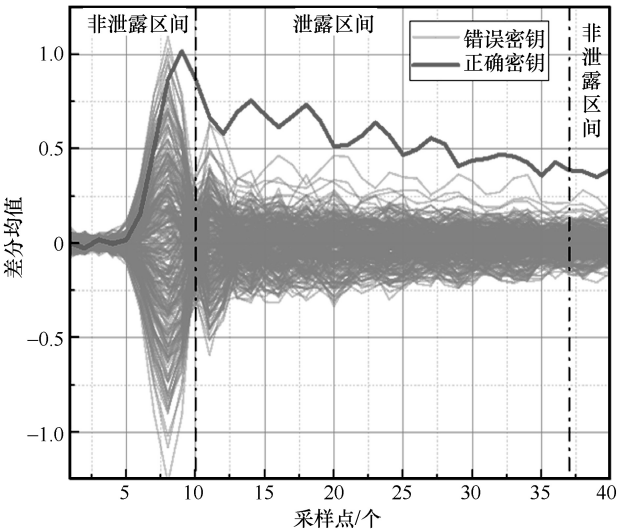
对比图 8(a)和图 8(b)可知，尽管 EDPA 的密钥收敛相较标准 DPA 有显著提高，但与 IMDPA 相比仍有明显差距。MDPA 在寄存器 B 所在的泄露区间与 IMDPA 密钥猜测效率相差不大，但在寄存器 A 所在的泄露区间时其密钥猜测效率甚至不如未经改造的 DPA。本文提出的 IMDPA 具有最快的收敛速度并且完全收敛时所需的能量迹数量最少。当寄存器 A 受到攻击时，3 000 条能量迹即可完成密钥全部字节的收敛。当寄存器 B 受到攻击时，1 500 条能量迹即可完成密钥全部字节的收敛。

3.1.2　AES-128 不同防护方案

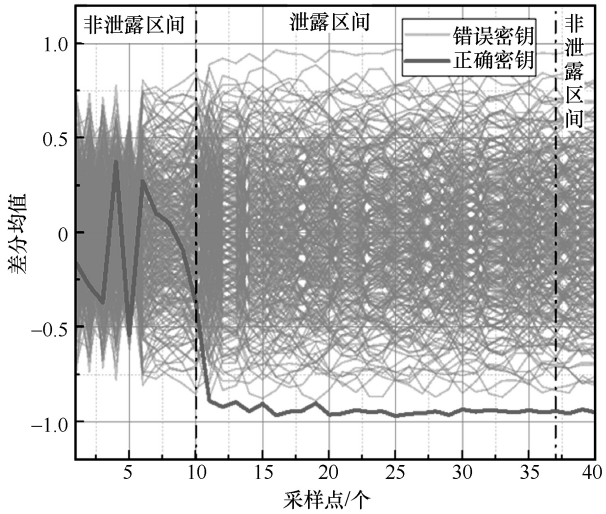
随着侧信道分析技术的蓬勃发展，其相应的防护技术也层出不穷。侧信道攻击能够成功的本



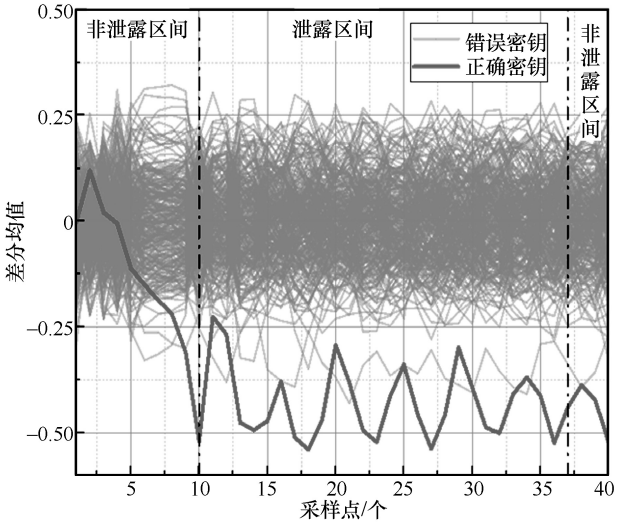
(a) 寄存器A处标准DPA攻击结果



(b) 寄存器B处标准DPA攻击结果

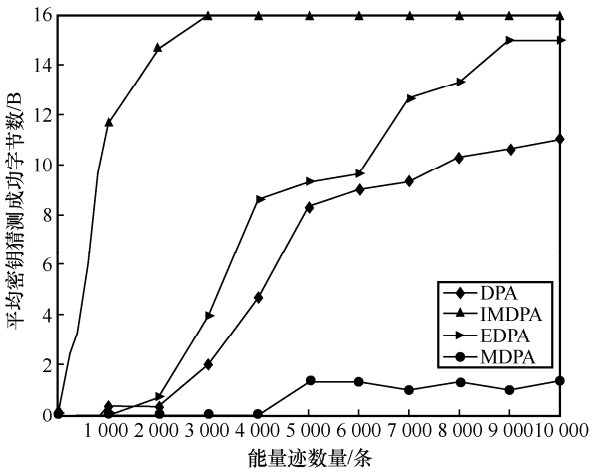


(c) 寄存器A处IMPA攻击结果

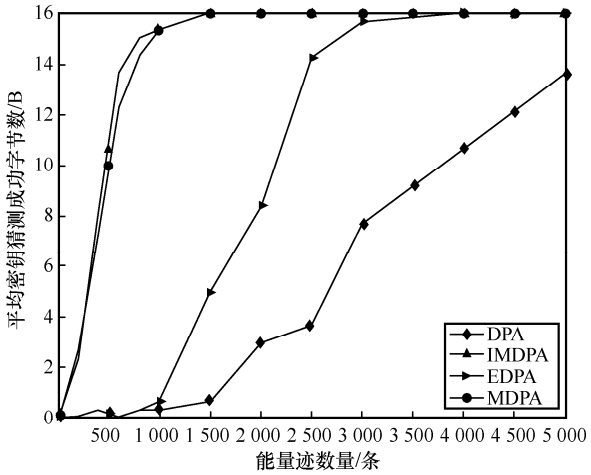


(d) 寄存器B处IMPA攻击结果

图 7　AES-128 算法寄存器 A 和寄存器 B 标准 DPA 和 IMDPA 的攻击结果



(a) 寄存器A



(b) 寄存器B

图 8　AES-128 算法的不同寄存器位置下 4 种方法全部 16 B 密钥的收敛情况

质原因在于芯片在运算过程中处理的中间值与芯片产生的功耗有关联。所以，降低或者消除中间值与芯片运行时产生的功耗的相关性可以有效提高加密芯片的安全性。为探究实施防护技术对 4 种差分能量分析方法的影响，本节通过引入噪声[21]、插入冗余操作[22]、双轨逻辑电路[23]、随机时钟[24]实施防护手段后的 AES-128 算法分别进行密钥猜测实验，以此验证在施加防护措施的条件下改进差分能量分析抵抗鬼峰的效果。

引入噪声通过引入大电容网络，利用外部随机数控制网络随机充放电，来增加能量消耗中的噪声分量或采用并行执行多个不相关操作等方式实现。AES-128 算法引入噪声后密钥猜测效果如图 9 所示。

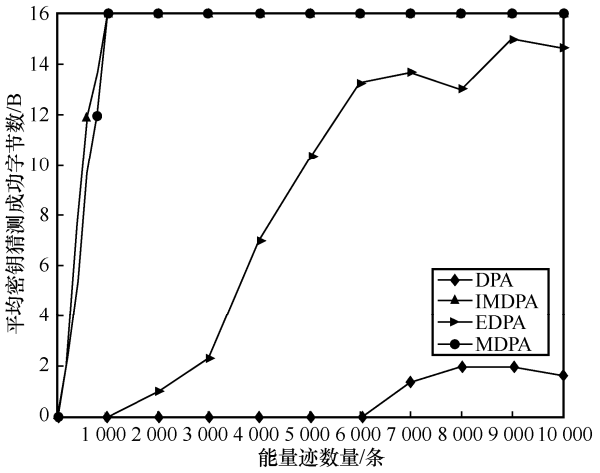


图 9　AES-128 算法引入噪声后密钥猜测效果

插入冗余操作是在算法运行的过程中随机插入伪操作，即通过外部随机数来控制算法在不同位置进行冗余操作，该方法会降低数据的吞吐量，影响计算效率。AES-128 算法插入冗余操作后密钥猜测效果如图 10 所示。

双轨逻辑电路主要是指在电路设计过程中，通过对所有逻辑信号进行互补编码，实现电路在每个时钟周期拥有恒定的能量消耗。AES-128 算法通过双轨逻辑电路达到功耗平衡后密钥猜测效果如图 11 所示。

随机时钟方案通过影响系统内部晶振或使系统在多个时钟频率下进行切换的方式，使同一操作随机出现在不同的时间点，从而无法进行有效攻击。随机时钟的 AES-128 加密功耗曲线如图 12 所示。随机时钟导致相同操作发生在不同的时间点，因此需要提前对功耗波形进行预处理操作才能进行能量分析。随机时钟预处理后相关的 DPA 密钥猜测结果如图 13 所示。

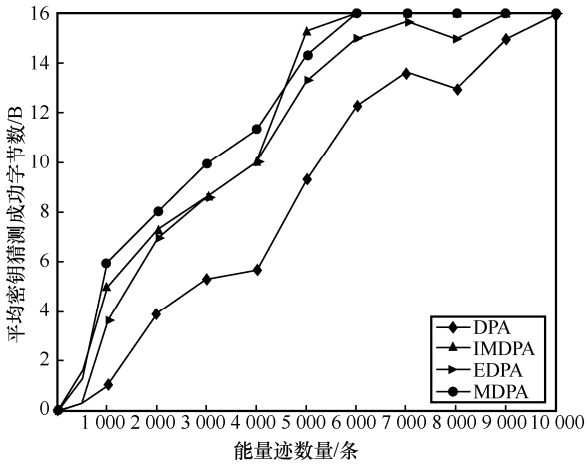


图 10　AES-128 算法插入冗余操作后密钥猜测效果

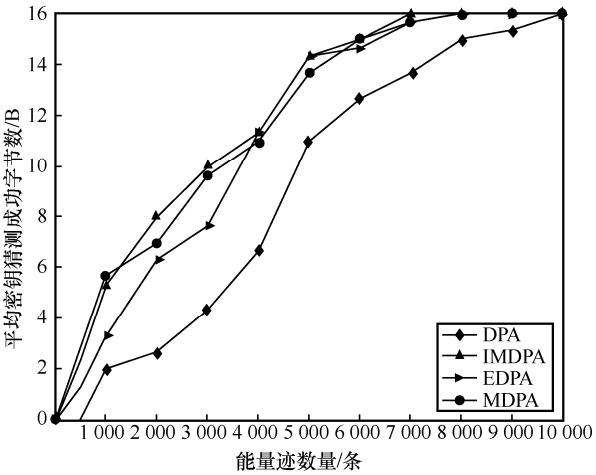


图 11　AES-128 算法通过双轨逻辑电路达到平衡后密钥猜测效果

对比图 9~图 11、图 13 可知，AES-128 算法实施了防护方案后的密钥猜测效率。引入噪声、插入冗余操作、双轨逻辑电路 3 种防护方案具有一定的防护作用，可使猜测出密钥全部字节所需的能量迹数量显著增加。随机时钟下的 AES-128 在对功耗信息进行数据对齐处理后 4 种方法猜测密钥所需的能量迹数量代价相同，由此可知数据对齐处理对差分能量分析中产生的鬼峰有着不错的抵抗效果。MDPA 和 IMDPA 在 AES-128 实施防护的条件下密钥猜测效率相差不大。本文提出的 IMDPA 在 AES-128 施加防护后抵抗鬼峰密钥猜测的效果相对最好，相对其他 3 种差分能量分析方法猜测出全部字节密钥所需的能量迹数量最少。

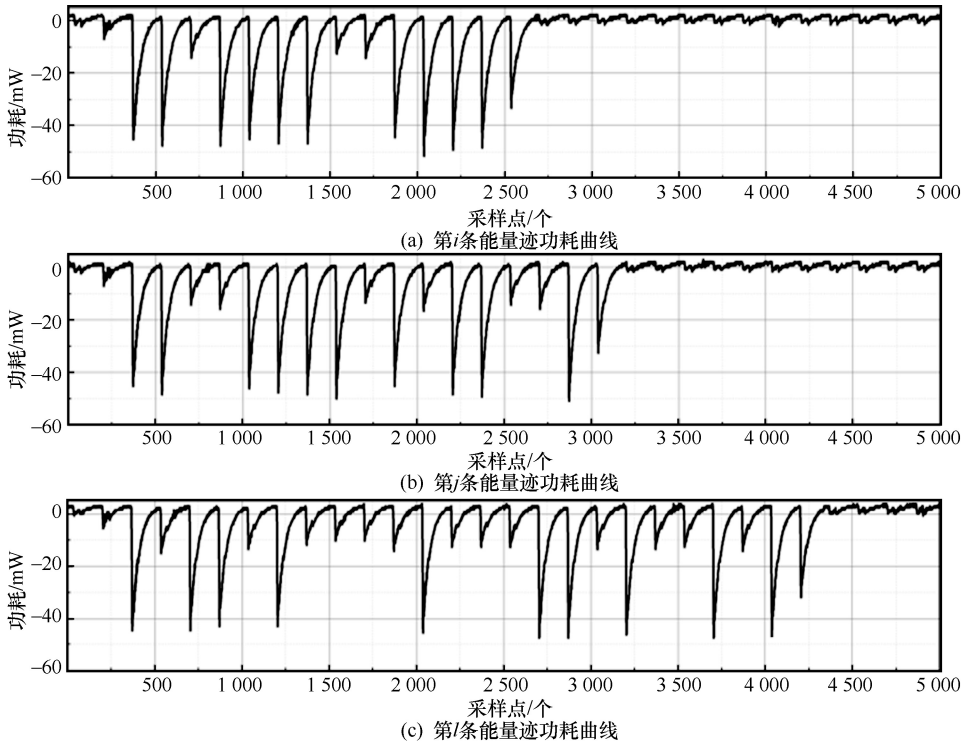


图 12　随机时钟的 AES-128 加密功耗曲线

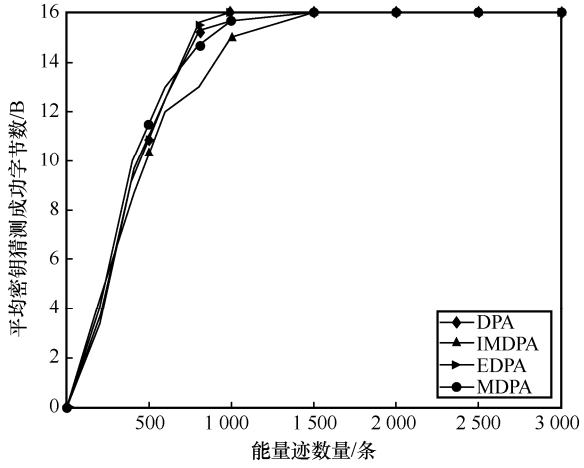


图 13　随机时钟预处理后相关的 DPA 密钥猜测结果

3.1.3　AES-128 预处理

目前，抑制鬼峰产生的最有效的预处理方法包括对能量迹进行标准化处理。由于在能量波形采集时能量会发生抖动，数据对齐也是一种有效抑制鬼峰产生的预处理方法，其预处理后相关的 DPA 密钥猜测结果如图 14 所示。当对能量波形进行预处理后，无论是标准化预处理还是数据对齐都有一定的抑制鬼峰的作用，且相较标准 DPA 密钥收敛速度明显提升，然而标准化处理相较数据对齐的鬼峰抑制效果更明显。本文提出的 IMDPA 收敛速度仍然最快，由于皮尔逊相关系数给出了标准化结果（相关系数范围为[–1, 1]），因此标准化处理与 IMDPA 猜测密钥字节完全收敛所需的能量迹数量相同。

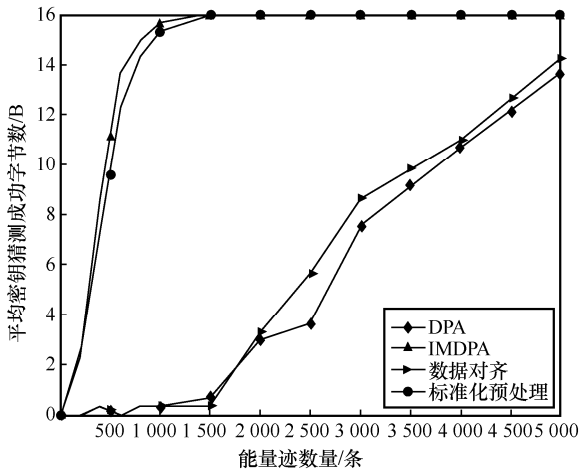


图 14　预处理后相关的 DPA 密钥猜测结果

3.2　SM4 密钥猜测效率

为了进一步验证 IMDPA 在分组密码算法上的通用性，本节选取 SM4 算法分别对上述 4 种方法进行密钥猜测实验，以此验证其抵抗鬼峰的效果，SM4 算法如图 15 所示。

攻击选取 SM4 算法首轮轮函数寄存器位置，其所在泄露区间 4 种方法的密钥猜测收敛情况如图 16 所示。从图 16 中可以看出，EDPA 在 SM4 算法中抵抗鬼峰的效果并不好，其密钥收敛甚至不如标准

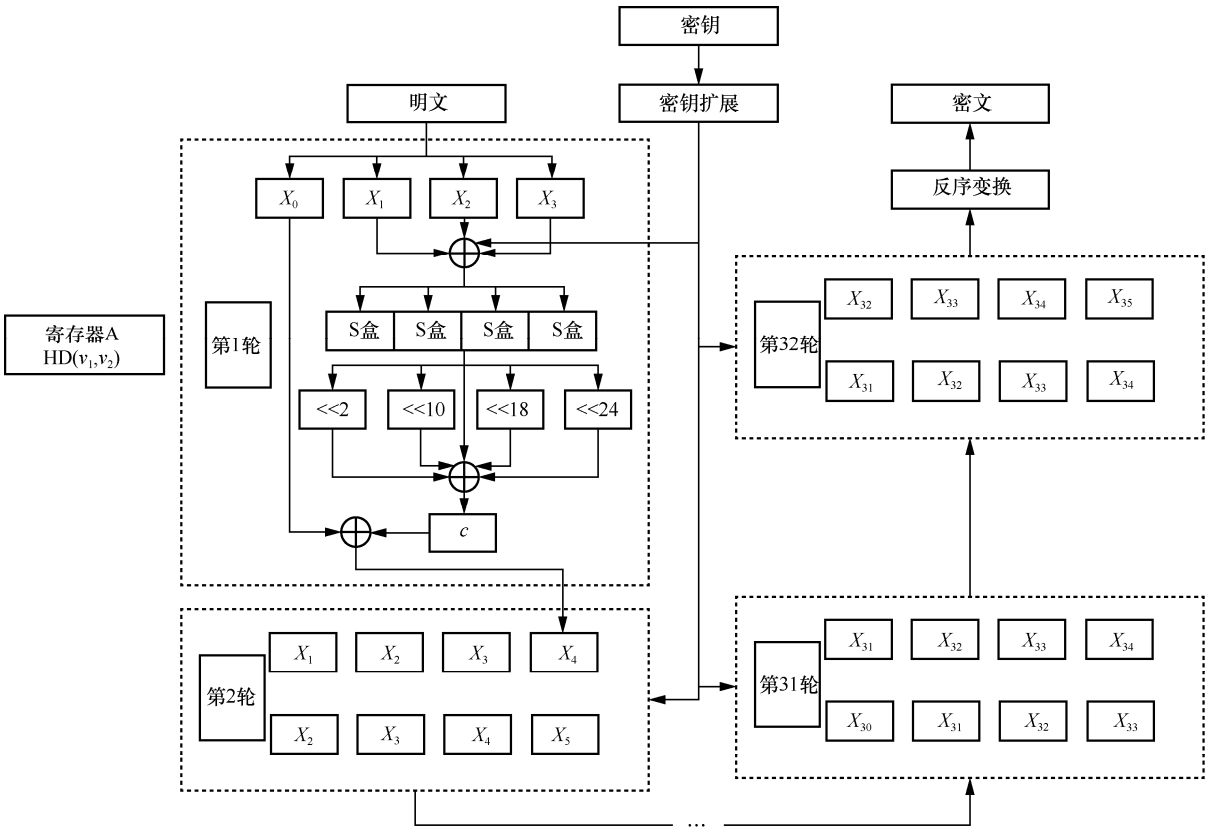


图 15　SM4 算法

DPA。由于分组密码大都由唯一的非线性操作 S 盒、异或运算、移位操作等线性运算组成，因此 MDPA 在 SM4 算法中与 AES-128 在寄存器 B 所在的泄露区间的密钥猜测情况一样，其与 IMDPA 密钥猜测效率相差不大。本文提出的 IMDPA 仍然具有最快的收敛速度并且完全收敛时所需的能量迹最少。当 SM4 首轮轮函数输出所在寄存器受到攻击时，1 000 条能量迹即可完成密钥全部字节的收敛。

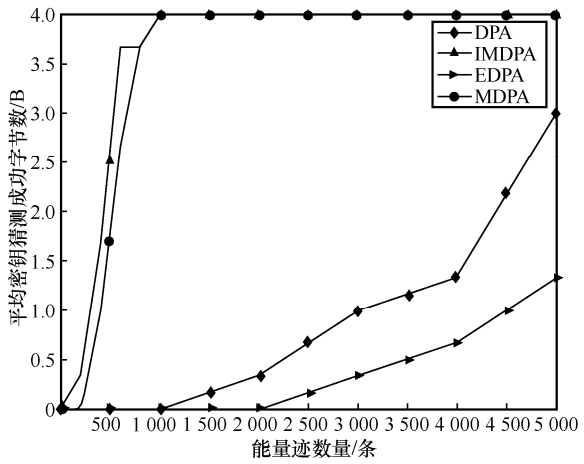


图 16　SM4 密钥猜测收敛情况

3.3　密钥猜测成功能量迹代价

为了使实验结论更具说服力，本节统计分析了不同分组密码实施不同侧信道防护后不同差分能量分析恢复正确密钥的能量迹代价。由于 Kocher 等[2]的标准 DPA、Mahanta 等[18]的基于 Canberra 距离的差分能量分析 EDPA、Chen 等[19]的基于差分均值矩阵标准化的 MDPA 在相应文献中并未体现不同场景下的密钥猜测效率，因此本文通过实验复现 DPA、EDPA、MDPA 得到实验数据。在不同算法实施不同的防护措施攻击不同位置时，4 种方法密钥猜测成功率达到 100%时所需的能量迹数量如表 1 所示。由表 1 可知，在 SM4 的首轮轮函数寄存器位置，EDPA 密钥恢复成功所需的能量迹代价甚至高于标准 DPA。结合密钥收敛情况和表 1，MDPA 在 AES-128 算法的寄存器 A 位置抵抗鬼峰作用失效，其密钥猜测效率甚至远低于标准 DPA。本文提出的 IMDPA 适用于不同算法、不同泄露区间、不同防护措施的多种场景，其密钥恢复成功率达到 100%所需的能量迹数量最少。

表 1 密钥猜测成功率达到 100%时所需的能量迹数量

算法	攻击位置	防护措施	IMDPA/条	DPA/条	EDPA/条	MDPA/条
AES-128	寄存器 A	无防护	3 000	10 000+	10 000+	10 000+
AES-128	寄存器 B	无防护	1 500	10 000	4 000	1 500
AES-128	寄存器 B	引入噪声	1 000	10 000+	10 000+	1 000
AES-128	寄存器 B	插入冗余操作	6 000	10 000	9 000	6 000
AES-128	寄存器 B	双轨逻辑电路	7 000	10 000	8 000	8 000
AES-128	寄存器 B	随机时钟	1 500	1 500	1 500	1 500
SM4	首轮轮函数输出寄存器	无防护	1 000	8 000	10 000+	1 000

3.4 计算复杂度

AES-128 算法的寄存器 B 位置 4 种方法的计算复杂度比较如图 17 所示。从图 17 可以看出，标准 DPA 和 MDPA 的计算复杂度的最小值几乎相同。由于需要额外计算预测差分均值矩阵，IMDPA 计算复杂度最高。尽管 IMDPA 和 EDPA 的计算复杂度均高于标准 DPA，但在密钥收敛速度和密钥恢复成功所需的能量迹代价方面却远非标准 DPA 可比。

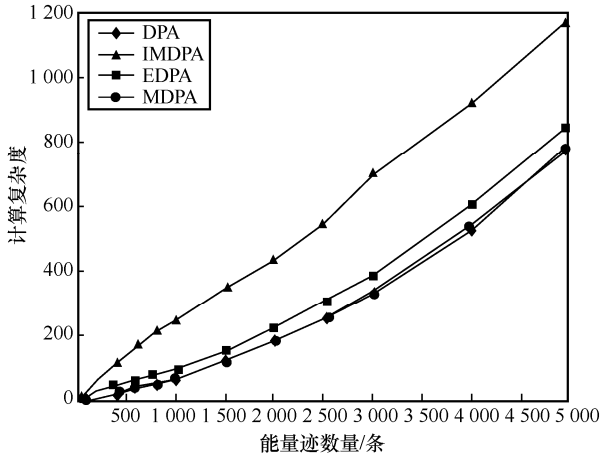


图 17 计算复杂度比较

4 结束语

针对分组密码在差分能量分析中可能受到鬼峰影响导致密钥猜测错误的问题，本文提出了一种新的解决方案——IMDPA。通过构造预测差分均值矩阵，利用猜测密钥在非泄露区间的弱相关性，从而避免非泄露区间对泄露区间内密钥猜测的影响，以此解决非泄露区间产生鬼峰带来的影响。本文在不同泄露区间、不同防护措施、不同算法条件下开展实验，结果表明，EDPA 在 SM4 密码算法中密钥收敛效果并不理想，在分组密码中不具有通用性。MDPA 在 AES-128 算法的寄存器 A 位置所在的泄露区间密钥很难完成收敛，不适于仅有线性操作的泄露区间。本文提出的 IMDPA 由于皮尔逊相关系数给出了标准化结果（相关范围为[−1, 1]），因此不需要对能量迹进行预处理即可适用于各种场景下的应用，是抵抗鬼峰最好的解决方案，且其密钥猜测效率有显著优势。

参考文献：

[1] KOCHER P C. Timing attacks on implementations of diffie-Hellman, RSA, DSS, and other systems[C]//Advances in Cryptology — CRYPTO ’96. Berlin: Springer, 1996: 104-113.

[2] KOCHER P, JAFFE J, JUN B. Differential power analysis[C]//Advances in Cryptology — CRYPTO’ 99. Berlin: Springer, 1999: 388-397.

[3] BRIER E, CLAVIER C, OLIVIER F. Correlation power analysis with a leakage model[C]//International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2004: 16-29.

[4] CHÉRISEY E D, GUILLEY S, RIOUL O, et al. Best information is most successful[C]//Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2019: 49-79.

[5] CHARI S, RAO J R, ROHATGI P. Template attacks[C]// Cryptographic Hardware and Embedded Systems - CHES 2002. Berlin: Springer, 2003: 13-28.

[6] AGRAWAL D, ARCHAMBEAULT B, RAO J R, et al. The EM side—channel(s)[C]//Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2002: 29-45.

[7] MONTMINY D P, BALDWIN R O, TEMPLE M A, et al. Differential electromagnetic attacks on a 32-bit microprocessor using software defined radios[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(12): 2101-2114.

[8] SCHRAMM K, WOLLINGER T, PAAR C. A new class of collision attacks and its application to DES[C]//International Workshop on Fast Software Encryption. Berlin: Springer, 2003: 206-222.

[9] BOGDANOV A, KIZHVATOV I. Beyond the limits of DPA: combined side-channel collision attacks[J]. IEEE Transactions on Computers, 2012, 61(8): 1153-1164.

[10] BIHAM E, SHAMIR A. Differential fault analysis of secret key cryptosystems[C]//Advances in Cryptology — CRYPTO’97. Berlin: Springer, 1997: 513-525.

[11] LI Y, SAKIYAMA K, GOMISAWA S, et al. Fault sensitivity analysis[C]//International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2010: 320-334.

[12] WANG A, CHEN M, WANG Z Y, et al. Fault rate analysis: breaking masked AES hardware implementations efficiently[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2013, 60(8): 517-521.

[13] PROUFF E, STRULLU R, BENADJILA R, et al. Study of deep learning techniques for side-channel analysis and introduction to ASCAD database[J]. IACR Cryptology ePrint Archive, 2018, 2018: 53.

[14] ROBYNS P, QUAX P, LAMOTTE W. Improving CEMA using correlation optimization[C]//Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2018: 1-24.

[15] CARBONE M, CONIN V, CORNÉLIE M A, et al. Deep learning to evaluate secure RSA implementations[C]//Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2019: 132-161.

[16] SCHRAMM K, PAAR C. Higher order masking of the AES[C]// Topics in Cryptology – CT-RSA 2006. Berlin: Springer, 2006: 208-225.

[17] LO O, BUCHANAN W J, CARSON D. Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA)[J]. Journal of Cyber Security Technology, 2017, 1(2): 88-107.

[18] MAHANTA H J, KHAN A K. Improving power analysis peak distribution using Canberra distance to address ghost peak problem[J]. International Journal of Information Security and Privacy, 2018, 12(3): 27-41.

[19] CHEN J C, NG J S, CHONG K S, et al. A novel normalized variance-based differential power analysis against masking countermeasures[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 3767-3779.

[20] GUILLEY S, HOOGVORST P, PACALET R. Differential power analysis model and some results[C]//IFIP International Federation for Information Processing. Boston: Springer US, 2004: 127-142.

[21] KAMOUN N, BOSSUET L, GHAZEL A. Correlated power noise generator as a low cost DPA countermeasures to secure hardware AES cipher[C]//Proceedings of 2009 3rd International Conference on Signals, Circuits and Systems (SCS). Piscataway: IEEE Press, 2010: 1-6.

[22] STEFAN M, ELISABETH O, THOMAS P. 能量分析攻击[M]. 冯登国, 周永彬, 刘继业, 等译, 北京: 科学出版社, 2010.
STEFAN M, ELISABETH O, THOMAS P. Energy analysis attack[M]. Translated by FENG D G, ZHOU Y B, LIU J Y, et al. Beijng: Science Press, 2010.

[23] BELLIZIA D, SCOTTI G, TRIFILETTI A. Implementation of the PRESENT-80 block cipher and analysis of its vulnerability to side channel attacks exploiting static power[C]//Proceedings of 2016 MIXDES - 23rd International Conference Mixed Design of Integrated Circuits and Systems. Piscataway: IEEE Press, 2016: 211-216.

[24] HOMMA N, NAGASHIMA S, SUGAWARA T, et al. A high-resolution phase-based waveform matching and its application to side-channel attacks[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2008, 91(1): 193-202.

[作者简介]

姜子敬（1994– ），男，黑龙江哈尔滨人，黑龙江大学博士生，主要研究方向为网络信息安全及硬件加密侧信道分析。

丁群（1957– ），女，黑龙江哈尔滨人，黑龙江大学教授、博士生导师，主要研究方向为硬件逻辑加密与系统集成、混沌保密通信和网络信息安全等。