基于TSDM的抗时间维度随机化方法研究

高　博[1,2]，陈　琳[1]，严迎建[1]
（1.信息工程大学，河南 郑州 450001；2.中国人民解放军92957部队，浙江 舟山 316000）

摘　要： 时间维度随机化技术通过插入随机延迟、冗余操作和变频时钟等操作，使得侧信息在时域难以对齐，进而降低了侧信道攻击效率。针对时间维度随机化技术引起的能量迹时域失调的问题，提出了基于趋势序列动态匹配（Trend Series Dynamic Matching，TSDM）的抗时间维度随机化方法，分析了攻击兴趣点的分布，提取了能量迹的趋势信息，刻画了能量迹的形状特征，压缩了能量迹的维度，抑制了噪声的负面影响，实现了数据的动态对齐，进而提高侧信道攻击的效率。面向3种典型时间随机化技术开展方法验证和性能分析，该方法相较多种经典对齐方法在不同噪声环境下的数据对齐效果更好，能量攻击成功率达到100%所需的能量迹数量分别减少了23.8%、24.2%、11.3%。

关键词： 侧信道攻击；时间维度随机化；动态时间扭曲；成功率
中图分类号： TP309.7　　**文献标志码：** A　　**DOI：** 10.16157/j.issn.0258-7998.222866

中文引用格式： 高博，陈琳，严迎建. 基于TSDM的抗时间维度随机化方法研究[J]. 电子技术应用，2023，49(2)：86-91.
英文引用格式： Gao Bo，Chen Lin，Yan Yingjian. Research on anti-time dimension randomization method based on TSDM[J]. Application of Electronic Technique，2023，49(2)：86-91.

Research on anti-time dimension randomization method based on TSDM

Gao Bo[1,2]，Chen Lin[1]，Yan Yingjian[1]
(1.Information Engineering University，Zhengzhou 450001，China；2.92957 Troops of PLA，Zhoushan 316000，China)

Abstract： Time-domain randomization makes side channel attacks difficult to align side information by inserting random delays, redundant operations, and variable frequency clocks, thereby reducing the efficiency. Aiming at the problem of time-domain misalignment of energy traces caused by time-dimensional randomization technology, this paper proposes an anti-time-domain randomization method based on Trend Series Dynamic Matching (TSDM). This method analyzes the distribution of attack interest points, and describes the shape feature of the energy trace, compresses the dimension of the energy trace, preserves the sensitive information of energy attacks, suppresses the negative impact of noise, realizes the dynamic alignment of data, and improves the efficiency of side channel attacks. This paper, conducts method verification and performance analysis for three typical time randomization techniques. Compared with various classical alignment methods, this method has better data alignment effect in different noise environments, and the number of energy traces required for the success rate of energy attack to reach 100% respectively decreased by 23.8%, 24.2%, 11.3%.

Key words： side channel attack；time-domain randomization；dynamic time warping；success rate

0 引言

侧信道攻击(Side Channel Attack, SCA)通过分析加密操作过程中泄漏的物理敏感信息与运算中间值假定功耗的统计特性，可轻松获取嵌入式设备的秘密数据，已经成为嵌入式设备主要安全威胁之一。目前，侧信道攻击方法包括简单能量攻击、差分能量攻击和相关能量攻击等，均需要分析侧信道信息中的所有泄漏点，攻击效率的高低取决于对应于同一操作的泄漏点在时域上对齐质量。为了保证嵌入式设备的安全性，研究学者提出了众多安全防护方法，包括盲化、隐藏、掩码、平衡等，降低、掩盖甚至消除侧信道信息与数据的相关性，提高侧信道攻击的难度。目前，隐藏技术因其计算代价小、方法迁移性好和成本开销低等优点，已经成为抗侧信道攻击的主要方法之一。作为典型的隐藏技术，时间维度随机化技术包括随机延迟[1]、乱序操作[2]、随机插入伪操作[3]和随机变化工作时钟频率[4]等，使侧信道信息在时域上失调，达到降低侧信道攻击的攻击效率，甚至可能导致攻击失败。

为了解决由时间维度随机化导致攻击效率低的问题，高效的时域对齐方法应运而生。Clavier[5]等针对随机插入伪操作，提出了基于滑动窗口的差分能量分析（Sliding Window Differential Power Analysis, SW-DPA）；通过一个滑动窗口将多个相似泄漏点合并成一个，但该方法容易丢失部分的关键信息，且窗口大小的设置严重依赖于个人经验。Gennaro[6]等提出了静态对齐(Static Alignment, SA)的方法，然而该方法只能用来消除触发信号与时钟信号不同步带来的泄漏信号失调问题，且对噪声极其敏感。Le[7]等提出了整合分析(Integrated Analysis, IA)的方法，但该方法抗噪性差，对齐效果欠佳。Woudenberg[8]等提出了基于动态时间扭曲(Dynamic Time Warping, DTW)的弹性对齐技术，有效地解决了由随机插入伪操作和随机变化工作时钟频率引起的泄漏信号失调问题，但该方法的计算代价较大，难以应用在实际场景中。Shiple[9]等提出了一种基于四阶统计量的对齐方法，实现了失调泄漏信号的动态和局部对齐，但会丢失部分与密钥相关的泄漏信息。Schfer[10]提出了结合小波变换和模拟退火算法的对齐方法，但模拟退火算法执行速度严重影响了对齐算法的效率。Yang[11]等提出了基于shotgun距离的局部泄漏信号对齐算法，但该方法仅能解决随机插入伪操作导致的失调问题。Abdellatif[12]在电磁轨迹上证明了结合小波变换、包络检测预处理的弹性对齐方法能够获得更高的分析成功率，但需要的轨迹数量巨大。Jia[13]等提出了基于最长共同子序列的对齐方法，并在单通道、多通道泄漏分别验证了方法的有效性，但该方法的时间复杂度和空间复杂度较高。总体上，目前提出的数据对齐方法虽然从一定程度上解决了侧信息时域失调的问题，但仍存在对噪声敏感、通用性差、效率低等问题。

针对现有时域对齐方法存在的问题，本文从泄漏信号形状相似性度量角度出发，将泄漏信号数据点间的对齐转化为趋势序列间的匹配，提出了一种基于趋势序列动态匹配(Trend Series Dynamic Matching, TSDM)的对齐方法。在插入随机延迟、伪操作、变频时钟及不同噪声环境下的失调能量迹上验证了本方法的性能，结果表明本方法的侧信道关键信息保存度高、数据对齐效果好、抗噪性强。

1 时间维度随机化技术概述及分析

时间维度随机化技术通过改变同一操作的执行周期，使得密码设备泄露的侧信道信息在时域上随机化，消除、减弱甚至掩盖敏感信息与泄露的侧信道信息之间的相关性，进而实现降低侧信道攻击效率的目的。时间维度随机化方法包括随机插入伪操作、随机延迟、改变时钟频率等，已经成为主要防护技术之一。本节介绍3种时间维度随机化技术的工作原理，分析其工作特性、优势与主要应对策略，为提出本文的抗时间维度随机化技术提供思路。

1.1 随机插入伪操作

随机插入伪操作技术通过在密码算法执行过程中插入若干个的随机指令，利用随机指令执行泄露的侧信道信息来降低、消除泄露信息与执行过程间的相关性。插入指令的类型越私密，指令执行的数量越随机，呈现的随机性就越强，防护的效果就越好。图1为由插入伪操作引发的能量迹时域失调，其中能量迹1为插入随机伪操作的能量迹，能量迹2为原始能量迹。从图1中可以明显看出，由于随机伪操作的插入，使得能量迹1和2存在一定的时域偏移，这在一定程度上弱化了真实的相关性，进而降低侧信道攻击效率。

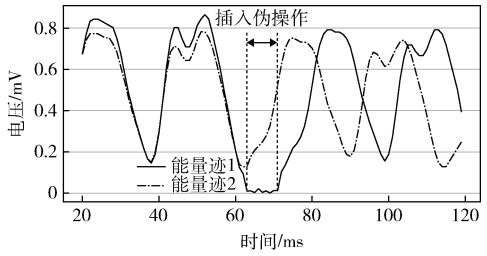

图1 随机插入伪操作导致的能量迹时域失调

1.2 随机延迟插入

随机延迟插入技术通过在密码算法执行序列中添加随机的等待时间，使关键信息点分散在时域上，进而掩盖真实的侧信息。与插入伪操作不同的是，插入的随机延迟导致侧信道信息的关键信息点在时域上更为分散，随机性更强，防护效果更好。图2为由插入延迟导致的能量迹时域失调，其中能量迹1为原始能量迹，能量迹2为插入了随机延迟的能量迹。从图中可以看出，由于延迟的插入，使得能量迹1和2存在一定的时域偏移。

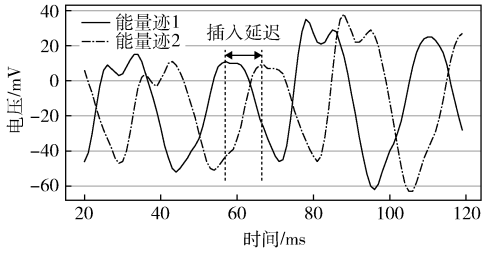

图2 插入随机延迟导致的能量迹时域失调

1.3 随机变化时钟频率

随机变化时钟频率技术通过控制变化密码芯片加密过程的工作时钟信号频率，改变加密过程的执行速度，降低攻击效率。其安全性取决于工作时钟频率的变化，通常由内部产生的随机数确定。图3为变化时钟频

率导致的能量迹时域失调。其中能量迹1为时钟频率为24 MHz时加密能量迹，能量迹2为时钟频率为48 MHz时加密能量迹。从图中可以看出，由于时钟工作频率的改变，使得能量迹1和2的长度存在较大差异，对应于同一操作的功耗点发生了明显的时域偏移，如果采用统一的分析过程和参数，将会无法准确分析出正确的密钥。

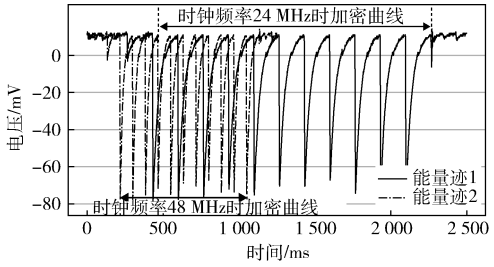

图3　变化时钟频率导致的能量迹时域失调

1.4 时间维度随机化应对分析

若将能量迹当作多维随机变量，时间维度的随机化技术改变了密码算法执行过程中操作的执行时刻，使得多个样本在同一时刻的量值属于不同维度变量；但包含最显著相关性兴趣点的尖峰形状未受影响。因此，可以将各功耗点间的对齐转化为变化趋势的相似性度量、尖峰形状间相似性匹配。通过提取趋势信息，匹配尖峰形状特征，便可攻破时间维度随机化的防护。本文将从这一思路出发，融合角度关键点的线性表示方法和余弦距离的动态时间扭曲方法，依据数据的趋势和形状特性，寻找并匹配趋势一致的侧信道信息，实现数据的高效对齐。

2 基于趋势序列动态匹配的对齐方法

该方法受基于形状的时间序列相似性度量[14]启发，利用角度关键点对能量迹进行分段线性表示，提取能量迹中尖峰形状；并利用基于余弦距离的DTW进行趋势序列间的相似性度量，得到趋势序列间的扭曲距离后，便可依照扭曲路径完成能量迹对齐。接下来详细介绍该对齐方法的原理。

本文以采用时间维度随机化防护技术的密码芯片为研究对象，工作过程中泄露的能量迹集为 $\mathbf{Traces}=\{\boldsymbol{T}_1,\boldsymbol{T}_2,\cdots,\boldsymbol{T}_N\}$，$\boldsymbol{T}_i$ 为第 i 条能量迹。

为了消除各功耗点间幅值上的偏移和尺度差别的影响，对每条能量迹进行了零均值归一化处理。对于归一化后的能量迹 $\boldsymbol{T}_i'$，依次利用3个连续功耗点形成的夹角变化值提取反映能量迹趋势变化的关键点，得到能量迹关键点序列。

$\boldsymbol{T}_i'=\{x_1,x_2,\cdots,x_m\}$ 中任意连续的3个样本点 x_{j-1}、x_j、x_{j+1}，由 x_{j-1}、x_j 和 x_j、x_{j+1} 构成的两条直线在 x_j 处的夹角为 α_j，α_j 的计算方法如式(1)所示：

$$\alpha_j=\left|\theta_{j1}-\theta_{j2}\right| \tag{1}$$

式中，$\theta_{j1}=\arctan\left(\frac{x_j-x_{j-1}}{\Delta t}\right)\times 180/\pi$，$\theta_{j2}=\arctan\left(\frac{x_{j+1}-x_j}{\Delta t}\right)\times 180/\pi$，$\Delta t$ 为相邻两点间时间差。

若 x_j 处的角度变化值 α_j 越小，x_{j-1}、x_j、x_{j+1} 3点连线越趋近于一条直线，趋势变化越小；当 α_j 大于设定的角度变化阈值 η 时，x_j 是关键点。

为了剔除噪声引入的关键点，依照式(2)对所有关键点进行了筛选：

$$x_j=\begin{cases}x_j, & \Delta A_j\geqslant\varepsilon\\ \varnothing, & \Delta A_j<\varepsilon\end{cases} \tag{2}$$

式中，幅度变化值 $\Delta A_j=\left|x_j-\frac{x_{j-1}+x_{j+1}}{2}\right|$，$\varepsilon$ 为幅度变化阈值。噪声点间的幅值波动小，如果连续3点幅值变化 ΔA_j 小于设定的幅度变化阈值 ε，则 x_j 是噪声引入的关键点。

将能量迹第一点 x_1、所有关键点和最后一点 x_m 按照时间顺序进行合并，得到能量迹的关键点序列 $\overrightarrow{\boldsymbol{T}_i'}$ 和关键点时间索引序列 I_i。其对应表征趋势信息的向量序列为：

$$\overrightarrow{\boldsymbol{T}_i}=\bigcup_{j=1}^{L_i}\{(\overrightarrow{\boldsymbol{T}_i'}[j+1]-\overrightarrow{\boldsymbol{T}_i'}[j],I_i[j+1]-I_i[j])\} \tag{3}$$

式中，L_i 为 $\overrightarrow{\boldsymbol{T}_i'}$ 的长度。为了方便后续描述，简化表示为：$\overrightarrow{\boldsymbol{T}_i}=\{\overrightarrow{V_{i1}},\overrightarrow{V_{i2}},\cdots,\overrightarrow{V_{iL_i}}\}$。

在经典DTW算法的基础上，以趋势信息的向量序列为匹配对象，使用余弦距离来度量两个向量的相似性。选取一条能量迹趋势向量序列 $\overrightarrow{\boldsymbol{T}_R}=\{\overrightarrow{V_{R1}},\overrightarrow{V_{R2}},\cdots,\overrightarrow{V_{RL_R}}\}$ 作为参考，待度量向量序列 $\overrightarrow{\boldsymbol{T}_i}=\{\overrightarrow{V_{i1}},\overrightarrow{V_{i2}},\cdots,\overrightarrow{V_{iL_i}}\}$，向量 $\overrightarrow{V_{ij}}$ 和 $\overrightarrow{V_{Rk}}$ 间的余弦距离的计算公式如式(4)所示。

$$d(\overrightarrow{V_{ij}},\overrightarrow{V_{Rk}})=\begin{cases}\cos\alpha=\dfrac{\overrightarrow{V_{ij}}\cdot\overrightarrow{V_{Rk}}}{\left|\overrightarrow{V_{ij}}\right|\left|\overrightarrow{V_{Rk}}\right|}, & \alpha<\dfrac{\pi}{2}\\ 0, & \alpha\geqslant\dfrac{\pi}{2}\end{cases} \tag{4}$$

式中，$\overrightarrow{V_{ij}}$ 为 $\overrightarrow{\boldsymbol{T}_i}$ 的第 j 个向量，$\overrightarrow{V_{Rk}}$ 为 $\overrightarrow{\boldsymbol{T}_R}$ 的第 k 个向量，α 为 $\overrightarrow{V_{ij}}$ 和 $\overrightarrow{V_{Rk}}$ 间的夹角。夹角 α 越小，两向量表征的形状相似度越高。当夹角 α 为0时，$\overrightarrow{V_{L_i}}$ 与 $\overrightarrow{V_{L_R}}$ 完全平行，表征的形状相同，余弦距离为1。同时，为了限制夹角过大的向量的影响，当两向量的夹角大于90°时，将两向量的距离设为0。

依照递推公式(5)，计算累积距离矩阵 $\boldsymbol{R}_{iR}$，$\boldsymbol{R}_{iR}$ 的表示如式(6)所示：

$$r(\overrightarrow{V_{ij}},\overrightarrow{V_{Rk}})=d(\overrightarrow{V_{ij}},\overrightarrow{V_{Rk}})+\max\{r(\overrightarrow{V_{i(j-1)}},\overrightarrow{V_{Rk}}),r(\overrightarrow{V_{i(j-1)}},\overrightarrow{V_{R(k-1)}}),r(\overrightarrow{V_{ij}},\overrightarrow{V_{R(k-1)}})\} \tag{5}$$

$$\boldsymbol{R}_{iR}=\begin{bmatrix} r(\overrightarrow{V_{i1}},\overrightarrow{V_{R1}}) & r(\overrightarrow{V_{i1}},\overrightarrow{V_{R2}}) & \cdots & r(\overrightarrow{V_{i1}},\overrightarrow{V_{RL_R}}) \\ r(\overrightarrow{V_{i2}},\overrightarrow{V_{R1}}) & r(\overrightarrow{V_{i2}},\overrightarrow{V_{R2}}) & \cdots & r(\overrightarrow{V_{i2}},\overrightarrow{V_{RL_R}}) \\ \vdots & \vdots & \ddots & \vdots \\ r(\overrightarrow{V_{iL_i}},\overrightarrow{V_{R1}}) & r(\overrightarrow{V_{iL_i}},\overrightarrow{V_{R2}}) & \cdots & r(\overrightarrow{V_{iL_i}},\overrightarrow{V_{RL_R}}) \end{bmatrix}_{L_i\times L_R} \tag{6}$$

根据构造的累积距离矩阵 $\boldsymbol{R}_{iR}$，以 $r(\overrightarrow{V_{iL_i}},\overrightarrow{V_{RL_R}})$ 为起点 p_1，向上、左和对角 3 个方向进行最大值寻优，将 3 个方向累积距离最大值作为下一个路径点 p_2，具体如式(7)所示。循环寻优，直到回到 $r(\overrightarrow{V_{i1}},\overrightarrow{V_{R1}})$，即可找到最优 DTW 路径 $P_i=\{p_s,\cdots,p_2,p_1\}$。

$$p_2=\max\{r(\overrightarrow{V_{i(L_i-1)}},\overrightarrow{V_{RL_R}}),r(\overrightarrow{V_{iL_i}},\overrightarrow{V_{R(L_R-1)}}),r(\overrightarrow{V_{i(L_i-1)}},\overrightarrow{V_{R(L_R-1)}})\} \tag{7}$$

依据扭曲路径 P_i，完成向量序列间的匹配，进而对齐两条能量迹。具体实现过程如算法 1 所示。

算法 1: 基于趋势序列动态匹配的对齐方法

输入:能量迹 $\mathbf{Traces}=\{\boldsymbol{T}_1,\boldsymbol{T}_2,\cdots,\boldsymbol{T}_N\}$，角度阈值 η，幅度变化阈值 ε；

输出:对齐后的能量迹 $\overline{\mathbf{Traces}}$。

(1) for i=1 to N do
(2) $\boldsymbol{T}_i'=f(\boldsymbol{T}_i)$
(3) end for
(4) for $\boldsymbol{T}_i'$ in $\{\boldsymbol{T}_i'\}$ do
(5) for $x_j\in\boldsymbol{T}_i'$ do
(6) if $\alpha_j>\eta$ and $\Delta A_j>\varepsilon$ then
(7) $\overline{\boldsymbol{T}_i'}\leftarrow x_j$
(8) end if
(9) end for
(10) end for
(11) for $\overline{\boldsymbol{T}_i'}$ in $\{\overrightarrow{\boldsymbol{T}_1'},\overrightarrow{\boldsymbol{T}_2'},\cdots,\overrightarrow{\boldsymbol{T}_N'}\}$ do
(12) $\overrightarrow{\boldsymbol{T}_i}=\{\overrightarrow{V_1},\overrightarrow{V_2},\cdots,\overrightarrow{V_{L_i}}\}\leftarrow\overrightarrow{\boldsymbol{T}_i'}$
(13) end for
(14) 任选一条趋势向量序列作为参考，记作 $\overrightarrow{\boldsymbol{T}_R}=\{\overrightarrow{V_{R1}},\overrightarrow{V_{R2}},\cdots,\overrightarrow{V_{RL_R}}\}$
(15) for $\overrightarrow{\boldsymbol{T}_i}=\{\overrightarrow{V_{i1}},\overrightarrow{V_{i2}},\cdots,\overrightarrow{V_{iL_i}}\}$in $\{\overrightarrow{\boldsymbol{T}_1'},\overrightarrow{\boldsymbol{T}_2'},\cdots,\overrightarrow{\boldsymbol{T}_N'}\}$ do
(16) 依照 DTW 返回 P_i
(17) $\overline{\boldsymbol{T}_i}\leftarrow\overrightarrow{\boldsymbol{T}_i}$
(18) end for
(19) return $\overline{\mathbf{Traces}}=\{\overline{\boldsymbol{T}_1},\overline{\boldsymbol{T}_2},\cdots,\overline{\boldsymbol{T}_N}\}$

算法 1 中，第 1~3 行完成了能量迹所有样本点的零均值归一化；第 4~10 行筛选出能量迹角度关键点，得到了关键点序列；第 11~13 行得到了能量迹形状向量序列；第 14~17 行依照式(6)、式(7)获得扭曲路径，返回对齐后的能量迹。

3 实验与分析

本文以典型的 AES-128 加密算法为例，在单片机和 FPGA 两种实现平台上，采集了由随机延迟、随机插入伪操作及变化芯片工作时钟频率引起的时域失调能量迹；利用 TSDM 来对齐能量迹，并使用相关能量攻击来攻击对齐后的能量迹，计算出一阶成功率[15]来比较其对齐效果。

3.1 能量迹采集与实验设置

本文分别采集了 2 000 条、2 000 条、30 000 条由随机延迟、随机插入伪操作及变化工作时钟频率引起的时域失调能量迹，具体信息如表 1 所示。

表 1 能量迹信息

实现平台	失调原因	能量迹数量	泄露模型
Chip Whisperer	随机延迟	2 000	汉明重量
Chip Whisperer	随机插入伪操作	2 000	汉明重量
SAKURA-G	变化时钟频率	30 000	汉明距离

为了体现 TSDM 对齐方法的性能，本文以经典的静态对齐 SA[1]方法、整合对齐 IA[7]方法、SW_DPA[6]方法、基于 DTW[9]的弹性对齐方法作为对比。同时，为了验证提出的 TSDM 对齐算法的抗噪性，本文在原始能量迹中添加了适当的噪声(假设原始信号的信噪比为无穷大)。经典方法的参数设置参考了文献[13]。其中，IA 对齐方法的窗口长度设置为 8；SW_DPA 对齐方法的时钟周期长度设置为 18，并将 15 个样本点合并为 1 个样本点；基于 DTW 对齐方法的半径设置为 150。对于 TSDM 方法，阈值 η、ε 的设定需要通过最小化拟合误差综合设定。阈值 η 取值过小会增加关键点数量降低对齐效率，取值过大会丢失敏感信息，降低对齐精度。经反复实验，将 η 设定为 150°。由于能量迹进行了归一化处理，限定在较小的数值区间里，ε 设定为 0.05。

3.2 实验结果与分析

图 4、图 5、图 6 分别为各对齐方法消除随机延迟插入、随机插入伪操作、改变时钟频率引发的能量迹失调影响后 CPA 攻击成功率对比图。从图 4(a)中可以看出，在信噪比较高时，SA 对齐方法能够精确地完成对应于第一个 S 盒输出泄漏点间的模式匹配，且对齐效果非常理想，攻击成功率达到 100% 需要能量迹数量约为 105 条；SW_DPA 方法完全没有效果；DTW 方法攻击成功率到 100% 需要能量迹约为 500 条；IA 方法攻击成功率在使用 800 条能量迹时仍未达到 100%。本文所提出的 TSDM 对齐方法，依照能量迹的形状趋势完成了尖峰间的精准匹配，对齐后的分析效果优于 SA，攻击成功率达到 100% 需要能量迹数量减少了约 23.8%。从图 4(b)中可以看出，在噪声较大时，SA 对齐方法由于无法准确选

择能量迹中特征突出的功耗点用于模式匹配，从而导致对齐效果较差；IA 对齐方法匹配后使用接近 1 000 条能量迹的攻击成功率仅为 20%；SW_DPA、基于 DTW 弹性的对齐方法也表现不佳，而 TSDM 对齐方法剔除了噪声引入的角度关键点，性能依旧稳定，攻击效果较好。

从图 5(a)中可以看出，在信噪比较高时，IA 方法优于基于 DTW 的对齐方法，攻击成功率达到 100%需要能量迹约 595 条；SW_DPA 方法的性能出现较大的波动，在能量迹数量大约为 1 150 条时成功率不升反降；TSDM 对齐方法效果明显优于其他对齐算法，相比 IA 方法，攻击成功率达到 100%需要能量迹数量减少了约 24.2%。从图 5(b)中可以看出，在信噪比较低时，TSDM 对齐方法性能依旧稳定，而基于 DTW 的对齐方法完全失效，抗噪性较差。

图 6 为各对齐方法消除改变时钟频率引发的能量迹失调影响后攻击成功率对比图。由于 IA 和 SW_DPA 方法不适用于处理变频时钟导致的能量迹失调，未进行对比。基于 DTW 的对齐方法对噪声极为敏感，性能下降明显；TSDM 对齐方法性能依旧稳健，相比 DTW 方法，攻击成功率达到 100%需要能量迹数量减少了约 11.3%。

各对齐方法在消除 3 种时间维度随机化技术引发能量迹失调影响后效果较大差异的原因可以总结为：SA 方法需要选择能量迹最明显的特征通过左右平移来实现模式匹配，所以在信噪比低时，SA 方法因无法准确选择用于攻击的兴趣点而完全失效；IA 和 SW_DPA 方法在对能量迹中功耗点整合时会丢失部分敏感信息，同时引入无用的累加噪声；基于 DTW 对齐方法需要完成逐点的匹配，使得计算复杂度高，并且容易受到噪声和孤立点的干扰。本文提出的 TSDM 对齐方法精确刻画了能量迹的形状特征，高质量地保存了攻击敏感信息，降低了能量迹的维度，在一定程度上抑制了噪声干扰，使得该方法对齐效果准确高效、性能稳健。

4 结论

针对由随机延迟插入、随机插入伪操作、改变时钟频率等时间维度随机化技术引起的能量迹时域失调问题，本文提出了 TSDM 的对齐方法，将泄漏信号电压值间的对齐转化为趋势序列的匹配，并在常见的实现平台上及不同噪声环境下验证了该方法的性能。实验结果表明，TSDM 对齐方法能够在保存原有与密钥相关泄漏

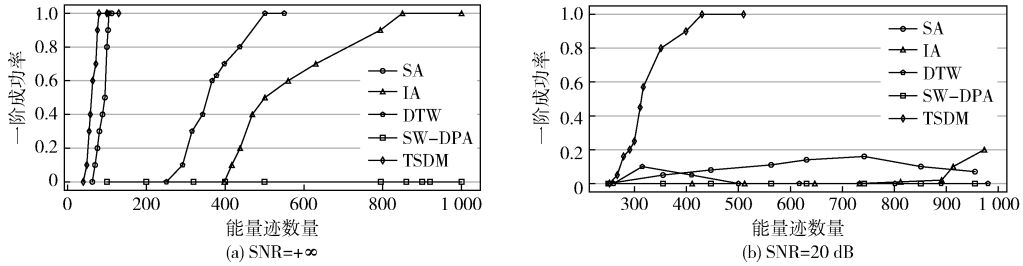

图 4　消除随机延迟插入引发能量迹失调影响后攻击效果对比

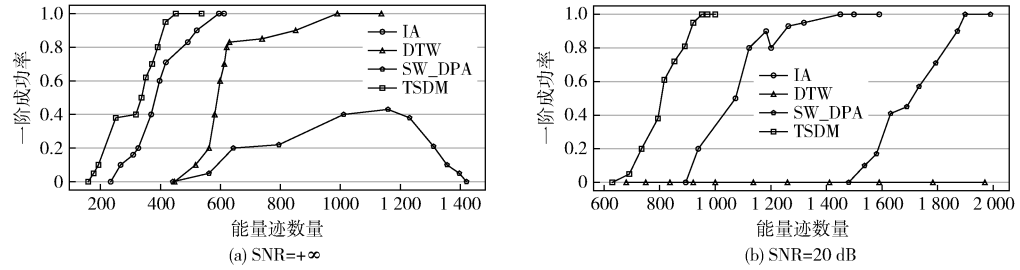

图 5　消除随机插入伪操作引发能量迹失调影响后攻击效果对比

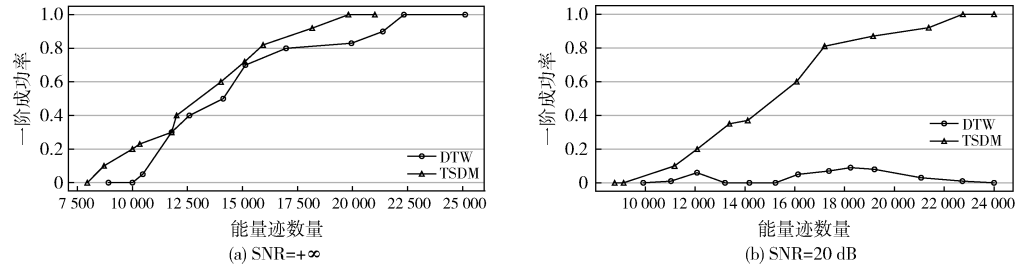

图 6　消除改变时钟频率引发能量迹失调影响后攻击效果对比

的同时避免冗余信息的引入，信息利用率高，对齐效果好，并且抗噪性能好，通用性强。

本文仅用TSDM对齐方法在3种常见时间维度随机化技术引起失调的能量迹上进行了验证，下一步将使用TSDM对齐方法对在采用组合防护策略(隐藏、掩码)能量迹上进行攻击。

参考文献

[1] MANGARD S, OSWALD E, POPP T. Power analysis attacks: revealing the secrets of smart cards[M]. Springer Science & Business Media, 2008.

[2] MORADI A, SCHNEIDER T. Side-channel analysis protection and low-latency in action[C]// Springer, Berlin, Heidelberg. Springer, Berlin, Heidelberg, 2016.

[3] TUNSTALL M, BENOIT O. Efficient use of random delays in embedded software[C]// IFIP International Workshop on Information Security Theory and Practices. Springer, Berlin, Heidelberg, 2007.

[4] ZAFAR Y, PARK J, HAR D. Random clocking induced DPA attack immunity in FPGAs[C]// 2010 IEEE International Conference on Industrial Technology, 2010.

[5] CLAVIER C, CORON J S, DABBOUS N, et al. Differential power analysis in the presence of hardware countermeasures[C]//Proceedings of the Second International Workshop on Cryptographic Hardware and Embedded Systems, 2000: 252-263.

[6] GENNARO R, ROBSHAW M. Algebraic decomposition for probing security[M]. Springer Berlin Heidelberg, 2015:742-763.

[7] LE T H, CLÉDIÈRE J, SERVIÈRE C, et al. Efficient solution for misalignment of signal in side channel analysis[C]// 2007 IEEE International Conference on Acoustics, Speech and Signal Processing, 2007.

[8] WOUDENBERG J G J V, WITTEMAN M F, BAKKER B. Improving differential power analysis by elastic alignment[C]// International Conference on Topics in Cryptology: Ct-rsa. Springer-Verlag, 2011.

[9] SHIPLE E, ASHOUR I S, AMMAR A A. Attacking misaligned power tracks using fourth-order cumulant[J]. International Journal of Advanced Computer Science & Applications, 2013, 4(12):8-14.

[10] SCHFER P. Towards time series classification without human preprocessing[C]// MLDM 2014, 2014.

[11] YANG W, CAO Y, ZHOU Y, et al. Distance based leakage alignment for side channel attacks[J]. IEEE Signal Processing Letters, 2016, 23(4):419-423.

[12] ABDELLATIF K M. Towards efficient alignment for electromagnetic side channel attacks[C]// 2019 31st International Conference on Microelectronics (ICM) , 2019.

[13] JIA A, YANG W, ZHANG G. Side channel leakage alignment based on longest common subsequence[C]// 2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE). IEEE, 2020.

[14] ESLING P, AGON C. Time-series data mining[J]. ACM Computing Surveys, 2013, 45(1): 1-34.

[15] STANDAERT F X, MALKIN T, YUNG M. A unified framework for the analysis of side-channel key recovery attacks [C] // Proceedings of the 28th Annual International Conference on Advances in Cryptology, 2009: 443-461.

（收稿日期：2022-04-15）

作者简介：

高博（1990-），男，硕士研究生，工程师，主要研究方向：芯片安全防护。

陈琳（1975-），女，博士，副教授，主要研究方向：安全专用芯片。

严迎建（1973-），男，博士，教授，主要研究方向：芯片安全防护。

扫码下载电子文档

版权声明