基于流形学习能量数据预处理的模板攻击优化方法

袁庆军[①②] 王 安[③] 王永娟*[①②] 王 涛[①②]

[①](战略支援部队信息工程大学 郑州 450001)

[②](河南省网络密码技术重点实验室 郑州 450001)

[③](北京理工大学计算机学院 北京 100081)

摘 要：能量数据作为模板攻击过程中的关键对象，具有维度高、有效维度少、不对齐的特点，在进行有效的预处理之前，模板攻击难以奏效。针对能量数据的特性，该文提出一种基于流形学习思想进行整体对齐的方法，以保留能量数据的变化特征，随后通过线性投影的方法降低数据的维度。使用该方法在Panda 2018 challenge1标准数据集进行了验证，实验结果表明，该方法的特征提取效果优于传统的PCA和LDA方法，能大幅度提高模板攻击的成功率。最后采用模板攻击恢复密钥，仅使用两条能量迹密钥恢复成功率即可达到80%以上。

关键词：信息安全；模板攻击；流形学习；能量数据；对齐算法；降维算法

中图分类号：TP309.7 **文献标识码**：A **文章编号**：1009-5896(2020)08-1853-09

DOI: 10.11999/JEIT190598

An Improved Template Analysis Method Based on Power Traces Preprocessing with Manifold Learning

YUAN Qingjun[①②] WANG An[③] WANG Yongjuan[①②] WANG Tao[①②]

[①](*PLA Strategic Support Force Information Engineering University* , *Zhengzhou* 450001, *China*)

[②](*Henan Key Laboratory of Network Cryptography Technology*, *Zhengzhou* 450001, *China*)

[③](*School of Computer Science*, *Beijing Institute of Technology*, *Beijing* 100081, *China*)

Abstract: As the key object in the process of template analysis, power traces have the characteristics of high dimension, less effective dimension and unaligned. Before effective preprocessing, template attack is difficult to work. Based on the characteristics of energy data, a global alignment method based on manifold learning is proposed to preserve the changing characteristics of power traces, and then the dimensionality of data is reduced by linear projection. The method is validated in Panda 2018 challenge1 standard datasets respectively. The experimental results show that the feature extraction effect of this method is superior over that of traditional PCA and LDA methods. Finally, the method of template analysis is used to recover the key, and the recovery success rates can reach 80% with only two traces.

Key words: Information security; Template analysis; Manifold learning; Power traces; Alignment algorithm; Dimension reduction algorithm

1 引言

侧信道分析[1]技术利用密码设备运行过程中产生的物理信息泄露恢复密码设备中的秘密，能有效威胁密码设备的安全。为了更加全面地评估密码产品，提高密码产品安全性，密码产品安全测评领域也引入了侧信道攻击的相关技术，如欧洲的CC认证[2]和美国FIPS-140标准[3]中，就要求密码产品具备抗能量分析和故障分析的能力。

模板攻击[4]是侧信道攻击的经典方法之一，其攻击过程可分为两个阶段：建模和匹配。在建模阶段，利用已知明文和密钥的能量数据建立模板，刻画数据与能量数据之间的依赖关系。在匹配阶段，将目标设备的运行时能量数据与建立的模板进行模式匹配，恢复目标设备的密钥。与相关能量分析

收稿日期：2019-08-07；改回日期：2019-10-31；网络出版：2019-11-27

*通信作者： 王永娟 pinkywyj@163.com

基金项目：国家自然科学基金(61872040)，河南省网络密码技术重点实验室开放基金(LNCT2019-S02)，“十三五”国家密码发展基金(MMJJ20170201)

Foundation Items: The National Natural Science Foundation of China (61872040), The Fund of Henan Key Laboratory of Network Cryptography Technology (LNCT2019-S02), The National Cryptographic Development Fund of the 13th Five-Year Plan (MMJJ20170201)

(CPA)[5]、差分能量分析(DPA)[1]、碰撞分析(CA)[6]等其他侧信道分析方法相比，模板攻击的条件较强，主要体现在建立攻击模型时需要实现对目标设备(或与目标设备极其类似)的完全掌控，并采集指定明文和密钥进行运算时的能量数据。模板攻击的优势主要在对能量数据的数量需求小，能更大限度地挖掘能量数据中的密钥相关信息，具有更高的密钥恢复效率。

能量数据是模板攻击中的研究对象，是对目标设备在密码算法运行过程中消耗能量情况的直观描述。能量数据预处理的成功与否将直接影响模板攻击的计算复杂度和恢复成功率。在实践中，密码设备往往作为功能系统的一部分出现，研究人员难以精确采集密码模块运算过程中的功耗，系统中其他模块的能量消耗也会被示波器收录，以噪声分量的形式存在于能量数据中。此外，采集环境中存在的天然电磁辐射和示波器的采样误差也影响着能量数据精确性。除了这些天然的因素，指令偏移[7]、随机时延[8]和掩码防护[9]等侧信道防护机制，同样会造成能量数据的变化。在这种情况下，信息将被大量的噪声分量和关键信息的偏移而掩盖，增加模板分析的难度。在能量数据的维数上，受示波器的采样率和加密算法的运行时间的影响，其维数往往高达数万维。攻击者不能确定密钥在什么时刻参与了运算，因此在进行侧信道分析时，研究者必须以高维能量数据作为分析对象。为了提升分析效率，能量数据的预处理至关重要。

能量数据的预处理通常包括降噪、对齐和降维。在实际工作中，降噪主要通过采用高斯滤波和带通滤波实现，通过对特定频率的信号的筛选，过滤指定频率的信息，从而降低高斯噪音的影响。本文不涉及降噪方法的改进。对齐算法的思想是选择某条能量迹的关键特征(如第1个波峰)作为参照，平移其他能量迹，使所有能量迹的关键特征对齐，从而对齐能量数据。采用的算法一般是最小二乘法或者Person相关系数法。这种方法对添加了随机时延的能量数据对齐效果较差。数据降维的主要思想是通过摒弃与密钥信息无关的维度，在保持密钥信息的前提下压缩数据。在实践中，通常采用选择兴趣区间的方法，即以密钥或与密钥有关的中间值作为筛选对象，摒弃与之相关性差的数据维。

模板攻击本质上是以密钥或中间值为标签的能量数据分类过程，而机器学习和神经网络技术在图像等数据分类领域的独特优势，使得研究人员将其引入侧信道分析领域[10]，取代传统的基于均值和协方差的模板建立方法，转而通过机器学习模型建立能量模板，并取得了较好的研究成果。与之相对的，机器学习领域的数据处理方法也应用到能量数据预处理中，其中被广泛采用的特征提取方法是PCA(Principal Component Analysis)[11]和LDA(Linear Discriminant Analysis)[12]。这两种方法通过线性空间投影的方法，在尽可能保留数据特征的前提下，降低数据的维度。研究表明[13]，PCA和LDA方法同样可以用于传统模板攻击的降维。在此基础上，王燚等人[14]提出了分段PCA的方法，即结合兴趣区间方法，对区间内外的点分别设立PCA取点比例。在机器学习侧信道攻击领域，数据的对齐仍然是数据预处理中的重要环节，无论是PCA, LDA还是分段PCA的方法，都需要先对数据进行对齐处理，以尽量保留有效信息。应用深度学习技术进行密钥恢复时，数据对齐虽然不是必要的[15]，但是对密钥的恢复成功率有很大的影响[16]。

Panda 2018 challenge1[17]能量数据集是PANDA 2018国际会议组织的竞赛中发布的公开数据集，采集自软件实现的AES-128算法，并添加了指令偏移和随机时延防护对策。本文主要针对能量数据的预处理进行了优化，进而提高模板攻击效率和恢复成功率，对以Panda 2018 challenge1能量数据集为例进行了验证试验，主要研究贡献为：(1)借鉴流形学习[18]思想，提出了一种利用能量数据局部关系进行整体对齐和降维的预处理方法，相比于PCA和LDA算法，该方法对能量数据的预处理结果具有更小的类内差分和更大的类间差分，区分效果更加明显；(2)采用经典模板攻击对Panda 2018 challenge1公开数据集进行密钥恢复，使用两条能量迹时恢复成功率即可达80%，在同样条件下，采用传统预处理方法进行模板攻击时，密钥恢复成功率仅为1%。本文其余部分的组织结构如下：第2节介绍了能量数据的特性和能量数据的常用预处理方法；第3节对改进的能量数据预处理方法进行了介绍；第4节以Panda 2018 challenge1公开数据集为研究对象，对改进的预处理方法进行了实验分析；第5节总结了本文的研究结论和下一步的研究工作。

2 相关知识

2.1 能量数据

能量数据是包含密码算法运算能量消耗的数据，在实践中，能量数据是将示波器与目标设备恰当地连接，以捕捉其瞬时电压值。根据欧姆定律，电压值与目标设备的能量消耗成正比，因此，示波器采集的电压数据即表示了设备的即时能量消耗。此外，采用电磁探头采集设备运行时电磁逸散也是

收集能量数据的通用方法之一。相比采集电压方法，电磁信号受到天然环境中的电磁影响，采集到的能量数据信噪比更低。在密码工程实践中，密码芯片往往作为功能模块的重要组成部分，集体参与运算。系统中其他模块的能量消耗也会被示波器收录，以噪声分量的形式存在于能量数据中。此外，采集环境中存在的其他电磁辐射和示波器的采样误差也影响着能量数据精确性。

除了天然噪音和误差外，针对能量分析的防护措施，如指令偏移和随机时延等，通过改变指令的执行顺序或者加入冗余指令，增加能量数据中的噪声分量比例，降低能量数据中的信噪比。如图1所示，是具有指令偏移和随机时延的AES算法一轮加密过程中的3条能量迹。

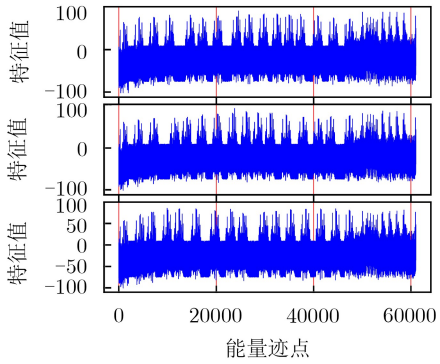


图 1 PANDA 2018 Challenge1 前3条能量迹

由图1分析可知，能量数据具有如下特征：噪声大、不对齐、维度高。能量数据的预处理的过程就是降噪、对齐和降维的过程。对能量数据的有效预处理能提高能量数据信噪比，降低分析复杂度，提高密钥恢复成功率。

2.2 预处理

对能量数据预处理的目的是从表现复杂的能量数据中提取与密钥信息相关的特征值(或矩阵)，其研究主要分为以下几个方向：

(1) 对齐：数据对齐是预处理的首要步骤，更是兴趣区间选择等降维方法的必要前置。对齐算法的思想是选择某条能量迹的关键特征作为参照，对齐能量数据。文献[19]和文献[20]提出的AOC和POC，分别选择了能量迹中的相位表现和振幅表现为关键特征，通过对时域的平移操作对齐能量迹。能量迹维度过高或指令间的随机时延机制都会对此类方法的效果造成影响。文献[21]提出的频域上的数据处理是另一个解决思路，时域上的延迟不会对指令频率造成影响。在机器学习领域的广泛应用PCA方法，也是一种另类的对齐思路，它的主要思想是从数据中提取对结果影响最大的“主成分”，并将这些成分按从大到小进行排序。

(2) 降维：过高的数据维度将造成建模和匹配过程的运算量过大，难以成功恢复密钥，因此，有效的数据降维是进行模板攻击的关键步骤。降维的过程则必然意味着有效信息的丢失，如何在尽量少的丢失有效信息的前提下降低数据维度，是研究人员的重要课题。如第1节所述，常用的兴趣区间选择算法有T-检验算法[22]和ρ-检验算法[23]，其算法如下：

设能量数据集$\boldsymbol{T}$是由n条能量迹组成的矩阵$[T_1, T_2, \cdots, T_n]^{\mathrm{T}}$

(a) T-检验：将能量迹分为p组，则第i组能量迹$(0 < i \leq p)$可以表示为$\{T_{i_1}, T_{i_2}, \cdots, T_{i_q}\}$，其中$iq$为第$i$组中能量迹的数量，则有第$i$组能量迹的均值向量$\boldsymbol{M}_i = \dfrac{1}{i_q}\sum_{j=1}^{i_q} T_j$，方差向量$\boldsymbol{V}_i = \dfrac{1}{i_q}\sum_{j=1}^{i_q}(T_j - M_i)^2$。则T-test矩阵的计算公式为

$$\boldsymbol{T}_{\mathrm{st}} = \sum_{i_1=1}^{p-1}\sum_{i_2=i_1+1}^{p}\frac{(M_{i_1} - M_{i_2})^2}{\dfrac{V_{i_1}}{i_{1q}} + \dfrac{V_{i_2}}{i_{2q}}} \tag{1}$$

则T-检验矩阵中的显著特征点为T-检验方法选择的兴趣点。

(b) ρ-检验：相比于T-检验，ρ-检验掌握了能量迹对应的密钥信息，因此可以采用与相关能量攻击相类似的方法，计算中间值与能量迹的相关系数矩阵，选择相关系数矩阵中的显著特征点。

无论是T-检验还是ρ-检验方法，都是利用已知中间值与能量数据的对应关系进行降维的方法，在处理有掩码防护机制的能量数据时，如果其采用的掩码值未知，则无法对能量数据进行降维。在大部分掩码实现方案中，掩码依赖于设备在运行过程中生成的随机数，在非实验室条件下，研究人员难以掌握确切的掩码值。

(3) 机器学习特征提取：PCA和LDA是有学习的数据预处理方法，能尽可能保留数据特征的线性降维方法，其原理是将数据投影到超平面上，使高维数据在该超平面上尽量保留原有的特性。在模板攻击中，功耗曲线的表现与中间值线性相关，因此，PCA和LDA能尽量保留原有数据的特性，在泛用性上强于传统的数据预处理方法。实践表明，使用PCA或LDA方法对数据进行降维，能显著提升密钥恢复成功率。LDA与PCA的最大区别是LDA是有监督的降维方法，它通过标签自主调节坐标轴的维度，获得最大类间方差的同时降低类内方差。

PCA和LDA是广泛应用于机器学习的数据预处理方法，与机器学习经常处理的其他数据不同，能量数据的有效维度如图2所示，其占比少于5%，而其他的数据如人脸识别、医疗、生物等数据的有效维度占比达70%以上。也就是说，对能量数据进行PCA和LDA时，能量数据中的大多数维度作为噪声分量，因为同样具有明显的特征，也被保留下来。当使用PCA和LDA算法，提取能量数据中的特征向量时，也会因噪声分量过大而影响密钥恢复的效率。

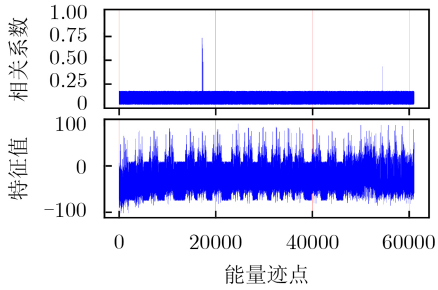


图 2 PANDA 2018 Challenge1 能量迹与密钥相关系数

3 基于流形学习与线性降维的预处理方法改进

在对能量数据进行分析时，可以将每条能量迹视作高维空间中的一个点，而预处理的过程，就是将这个点映射到低维空间的过程。能量数据中超过95%的维度与密钥无关，因此，能量数据预处理的最理想情况是，在保留有效的数据特性的基础上(即高维空间中点与点之间的相对位置)，将其映射到低维空间。本文改进的预处理算法主要包括对齐和降维两部分，其关键步骤为：(1)使用改进的对齐算法将待处理能量数据集进行对齐；(2)将对齐后的能量数据集进行降维，输出能量数据特征值。该特征值即为经过预处理后的能量数据。

3.1 对齐算法

模板攻击的建模过程至少需要应用上千条能量迹，即以256个中间值为标签建立模板时，每类标签对应的能量迹数量超过4条。在这上千条非对齐的能量迹中，根据统计学原理，也存在数条能量迹相互对齐或接近对齐。根据能量数据中的泄露特性，即使这些能量迹类属不同的标签，其数据的走向也极其相似。借鉴流形学习的数据处理方法，对能量数据进行对齐处理。流形学习将数据视作由一个低维流形映射到高维空间的数据点，是低维空间中的数据扭曲到高维空间的表现，在这个过程中产生了部分维度的冗余。流形具备欧氏空间的性质，在进行流形运算时，保持该流形数据的欧氏空间性质，并将其还原为低纬度的数据。在本方法中，将每条能量迹视为高维空间中的一个数据点，则越对齐的能量迹，其对应的数据点之间的欧式距离越近。在进行流形算法时，将欧式距离最近的点，视为在同一个流形区间上的点，在保留同区间点的相对位置的情况下，拉伸该流形曲面，在此过程中，对齐数据的欧氏空间性质仍然得到保持。

对包含α条能量迹的数据集$T_\alpha=\{T_i,0\le i\le\alpha,i\in N\}$，对目标能量迹$T_j$，使用K-means算法进行聚类，计算出与所选能量迹最接近对齐的k条能量迹，记做$\{T_{j1},T_{j2},\cdots,T_{jk}\}$。假设在高维空间中，他们之间具有线性关系，即

$$T=w_{j1}\cdot T_{j1}+w_{j2}\cdot T_{j2}+\cdots+w_{jk}\cdot T_{jk} \tag{2}$$

其中，w表示权重系数(实践中，通常根据数据集情况，设置k为3～20间的某个数值)。

表1是关系向量矩阵$\boldsymbol{W}$的计算方法法和对齐数据的算法：

表 1 向量矩阵计算算法

输入：能量数据$T_\alpha=\{T_i,0\le i\le\alpha,i\in N\}$，对齐参数$k$。
输出：对齐后的能量数据T'_α
(1) for j in range(α), do
(2) 计算与T_j 欧式距离最近的k条能量迹$\{T_{j1},T_{j2},\cdots,T_{jk}\}$;
(3) end
(4) for j in range (α), do
(5) 计算关系向量矩阵$\boldsymbol{W_j}=\dfrac{\left(\boldsymbol{C}_i^{-1}\cdot\boldsymbol{1}_k\right)}{\boldsymbol{1}_k^{\mathrm{T}}\cdot\boldsymbol{C}_i^{-1}\cdot\boldsymbol{1}_k}$，其中$\boldsymbol{C}_i$为$\{T_{j1},T_{j2},\cdots,T_{jk}\}$的协方差矩阵，$\boldsymbol{1}_k$为$k$维全1向量;
(6) end
(7) 计算矩阵$\boldsymbol{M}=(\boldsymbol{I}-\boldsymbol{W})(\boldsymbol{I}-\boldsymbol{W})^{\mathrm{T}}$;
(8) 设$\beta=\alpha/2$从矩阵$\boldsymbol{M}$中选择较小的β个特征值，记为$\boldsymbol{M}_\beta$，计算$T'_\alpha=T\cdot\boldsymbol{M}_\beta$;
(9) return $T_\alpha{}'$。

3.2 降维方法

经过对齐算法后，相对对齐的不同标签的能量迹在空间结构上保持相对位置，对此类的数据，通过转动坐标系进行线性投影降维，即可实现同标签数据的聚类。LDA算法的原理正是通过转换坐标系，进行低维映射的方法，将归属同类的数据映射到欧氏空间上较为接近的区域。LDA算法基于有监督学习的思路，通过调整转动坐标系方式，将同类数据映射到欧氏距离更为接近的局域，同时尽量保持不同类数据间的欧式距离。特别注意的是，PCA方法也是一种转换坐标系进行降维的线性降维方法，与LDA不同，它是一种无监督的降维方法，保证各数据间保持较大的距离。由于3.1节中的对

齐方法，不是通过平移能量数据而进行的对齐，因此，经过对齐处理后，不同标签的数据在欧氏空间中的距离的可能更小，在这种情况下，PCA算法难以区分原本欧氏距离较小的数据。因此，PCA方法不适用此处的降维。实验分析也表明，PCA方法不适用本文的场景。因此，选用LDA算法作为降低数据维度的方法。

经过对齐和降维的预处理过程后，将输出的特征值为经典模板攻击的输入数据，进行建模和匹配，以恢复目标密钥。

4　实验分析

为了验证第3节提出的预处理算法，本文针对部署了防御对策的AES算法公开数据集Panda 2018 challenge1进行了密钥恢复实验。Panda 2018 challenge1数据集[17]是采集AT89S52单片机软件实现的无掩码AES算法的能量数据，并添加了指令偏移和随机时延防护对策。该数据集是以明文和密文为文件名的二进制文件，共有1200条能量迹，数据维度为63325维，记录了AES算法第1轮全部S盒运算。其中前3条曲线如图1所示。由于该数据集的数量仅有1200条，在数据量上不能满足传统模板攻击的需求，因此本文提出的方法为建模样本较少情况下实现模板攻击提供了参考。

由于该数据集采用了指令偏移与随机时延的防御对策，基于数据特征的对齐和基于兴趣区间选择的降维手段难以奏效。基于数据特征的对齐方法是以数据的表现特征为标志，对数据进行平移对齐，随机时延防护能扰乱数据的外在表现特征，从而降低对齐效果。而基于兴趣区间选择的降维方法要求数据集本身是对齐的。因此，研究人员转而使用PCA和LDA等有学习的方法对数据进行预处理。在实验中，选择为S盒的输出作为关键中间值进行分析，并对本文提出的方法与PCA和LDA的效果进行对比。

4.1　对齐

采用改进后的方法对能量数据进行对齐，则前3条曲线对齐后，如图3所示。与通过平移曲线的方法进行数据对齐不同，经过该对齐方法处理后数据，在相同位置的会出现不同程度的数值跳变，大部分其他位置数值接近于0，如图中黑色标准线所示，相同位置的不同的跳变程度即为数据的标签特征。再经过降维算法进一步提取数据的特征值后，可以降低模板攻击建模时的计算复杂度，提高匹配成功率。

4.2　降维

使用LDA算法，将目标数据降至20维，数据表现如图4所示，其中，图4(a)为标签不同的3条曲线，图4(b)为标签相同的3条曲线。由图中可知，标签相同的曲线在提取的特征值上表现了良好的相似性，与之相对的，不同的标签的曲线提取的特征值则表现出较大的差异性。

如图5所示，仅采用了PCA方法或LDA方法，将能量数据降至20维后的数据表现，其中，图5(a)和5(c)为标签不同的3条曲线，图5(b)和5(d)为标签相同的3条曲线。

使用改进后的方法进行预处理后的数据，相比于目前常用的PCA和LDA，如图4(b)所示，相较

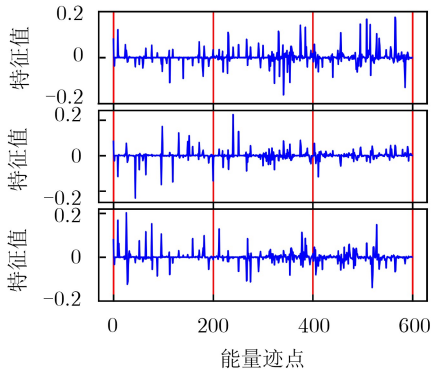
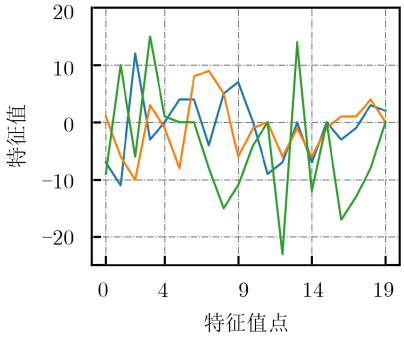
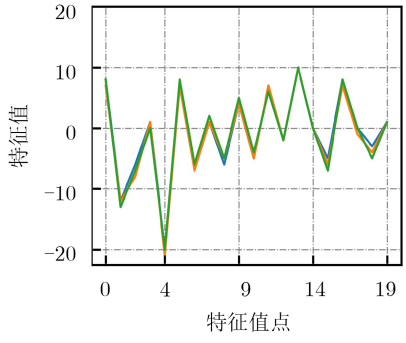


图 3 PANDA 2018 Challenge1能量数据对齐后



(a) 标签不同



(b) 标签相同

图 4 PANDA 2018 Challenge1 能量迹降维后

图5(b)和5(d)，具有更为良好的类内一致性，而如图4(a)所示，相较于图5(a)和5(c)，具备较高的类间差异性，表明本文提出的预处理方法的优越性。

4.3 数据分析

为了更加直观的描述本方法的类内一致性和类间差异，本文计算了处理后数据的类内方差和类间方差。方差是统计学中衡量数据的离散程度的度量。统计中的方差(样本方差)是每个样本值与全体样本值的平均数之差的平方值的平均数。以分类为目的进行的数据预处理，方差可以代表提取的特征向量的差异性，其中，类间方差代表各分类的特异程度，类内方差代表同类别的聚类效果。类间方差越大、类内方差越小，则预处理效果越好。由于本文研究256分类，全表过于庞大，现选取具有代表意义的类别进行对比说明，其中表2对标签汉明重量不同的9类进行对比说明，表3对标签汉明重量同为3的9类进行对比说明。AT89S52单片机的侧信息泄露符合汉明重量模型，同汉明重量的能量数据特征值相比不同汉明重量更加难以区分。

由表2和表3可知，在大部分情况下，经过预处理后的特征值的类内方差(对角线上的元素)明显小于类间方差(同行或同列其他数据)。PANDA 2018 Challenge1数据采集自AT89S52单片机实现的AES算法，其能量数据的表现特征符合汉明重量模型，在实际的实验过程中，相同汉明重量的几类标签分类时，容易出现分类错误的情况。在表3中，

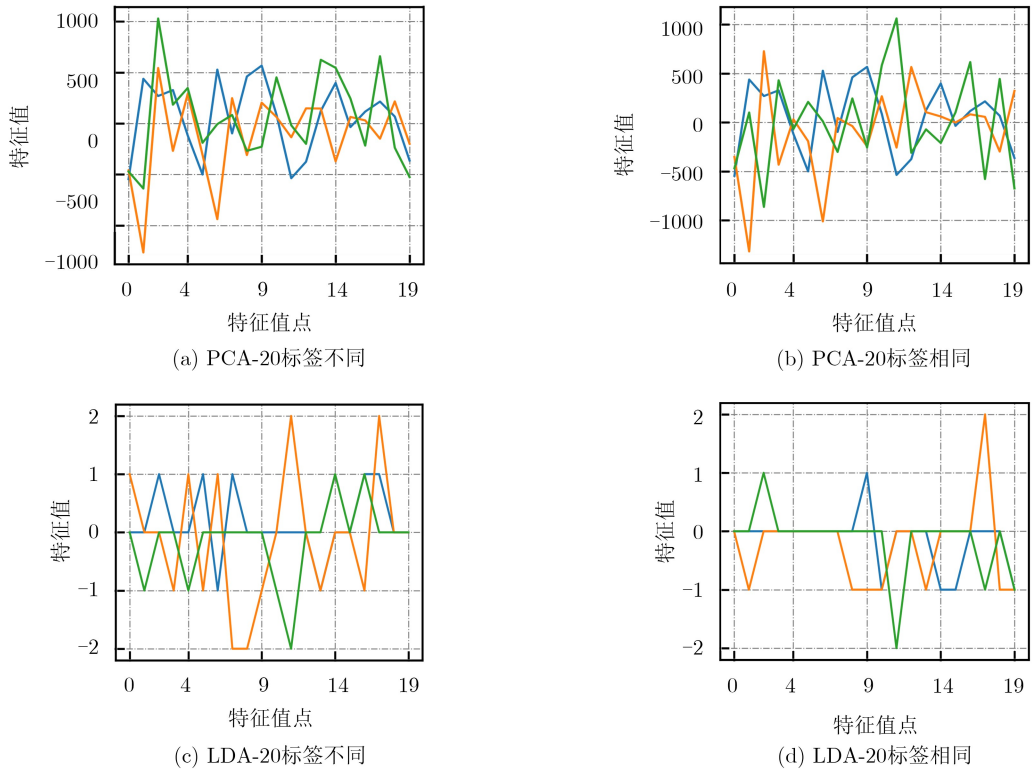


图 5 PANDA 2018 Challenge1 能量迹PCA-20和LDA-20降维后

表 2 PANDA 2018 Challenge1数据集预处理后方差($\times 10^4$)表(汉明重量不同)

方差	0	1	3	7	15	31	63	127	255
0	**4.08**	10.99	14.31	16.61	9.80	15.80	18.32	13.02	10.19
1	10.99	**2.67**	12.49	8.83	7.34	9.50	11.48	5.00	6.33
3	14.31	12.49	**8.53**	13.62	15.21	12.67	11.73	13.00	15.81
7	16.61	8.83	13.62	**3.62**	16.24	8.13	11.60	4.99	10.73
15	9.80	7.34	15.21	16.24	**4.23**	12.21	12.85	9.23	9.84
31	15.80	9.50	12.67	8.13	12.21	**4.17**	11.62	8.86	9.61
63	18.32	11.48	11.73	11.60	12.85	11.62	**4.54**	9.26	9.73
127	13.02	5.00	13.00	4.99	9.23	8.86	9.26	**1.97**	5.23
255	10.19	6.33	15.81	10.73	9.84	9.61	9.73	5.23	**4.26**

大部分标签的类间方差也同样小于类内方差。也就是说，经过特征提取后，能量数据已经进行了可区分的分类。特别注意的是，在标签为13和131时，类内方差大于部分类间方差，此时，即为特征提取算法提取的特征不明显，难以区分标签为13和131的分类。为了更加直观的对比预处理效果，如表4和表5所示，将使用PCA-20和LDA-20算法进行处理后的数据方差如下，由表中数据可知，在汉明重量不同的9类标签中，也出现了大量类内方差大于类间方差的情况，密钥区分的难度将大大提高。

随机选取两条非训练集的曲线，使用模板攻击方法进行密钥恢复，恢复成功率可达80%。与之相对的，使用LDA-20或PCA-20的方法处理能量数据并进行模板攻击时，使用两条曲线恢复成功率不高于5%。

5　结束语

本文提出的基于能量数据局部关系和线性投影

表 3　PANDA 2018 Challenge1数据集预处理后方差($\times 10^4$)表(汉明重量相同)

方差	7	11	13	14	19	35	67	131	224
7	**3.62**	11.23	23.70	12.19	13.35	13.52	11.55	14.04	9.86
11	11.23	**2.60**	18.80	11.73	12.07	11.85	12.43	10.97	10.21
13	23.70	18.80	**31.91**	23.04	27.09	22.52	23.58	56.33	19.22
14	12.19	11.73	23.04	**3.89**	12.54	9.52	14.47	14.96	12.70
19	13.35	12.07	27.09	12.54	**4.78**	13.86	15.33	17.68	11.98
35	13.52	11.85	22.52	9.52	13.86	**3.15**	15.07	15.10	10.67
67	11.55	12.43	23.58	14.47	15.33	15.07	**4.98**	17.73	9.50
131	14.04	10.97	56.33	14.96	17.68	15.10	17.73	**37.04**	20.31
224	9.86	10.21	19.22	12.70	11.98	10.67	9.50	20.31	**3.91**

表 4　PANDA 2018 Challenge1数据集PCA-20处理后方差($\times 10^4$)表(汉明重量不同)

方差	0	1	3	7	15	31	63	127	255
0	**33.00**	27.97	30.58	29.58	28.96	30.91	29.07	31.04	31.06
1	27.97	**13.72**	15.97	16.05	15.23	16.10	15.99	20.49	14.26
3	30.58	15.97	**13.79**	16.97	15.97	17.57	15.58	23.60	16.56
7	29.58	16.05	16.97	**17.04**	16.70	17.60	17.34	22.65	17.31
15	28.96	15.23	15.97	16.70	**14.53**	16.83	16.07	21.60	16.43
31	30.91	16.10	17.57	17.60	16.83	**16.64**	16.65	22.57	17.06
63	29.07	15.99	15.58	17.34	16.07	16.65	**15.41**	22.27	16.76
127	31.04	20.49	23.60	22.65	21.60	22.57	22.27	**24.36**	22.35
255	31.06	14.26	16.56	17.31	16.43	17.06	16.76	22.35	**13.91**

表 5　PANDA 2018 Challenge1数据集LDA-20处理后方差($\times 10^4$)表(汉明重量不同)

方差	0	1	3	7	15	31	63	127	255
0	**0.95**	1.21	0.93	0.99	1.07	1.09	1.08	1.12	1.13
1	1.21	**1.13**	1.07	1.17	1.20	1.11	1.24	1.15	1.20
3	0.93	1.07	**0.65**	0.90	0.99	0.93	1.00	1.05	1.01
7	0.99	1.17	0.90	**0.84**	0.97	1.02	1.10	1.09	1.06
15	1.07	1.20	0.99	0.97	**0.92**	1.08	1.17	1.16	1.11
31	1.09	1.11	0.93	1.02	1.08	**0.89**	1.10	1.10	1.02
63	1.08	1.24	1.00	1.10	1.17	1.10	**1.07**	1.18	1.15
127	1.12	1.15	1.05	1.09	1.16	1.10	1.18	**0.98**	1.15
255	1.13	1.20	1.01	1.06	1.11	1.02	1.15	1.15	**0.97**

进行预处理的方法，与传统方法，如PCA和LDA相比，特征选择的区分效果更为明显，提升了模板攻击的实现效率和恢复成功率，且无须使用深度学习或高阶攻击方法即可攻破有掩码防护机制的密码设备。

在密钥恢复阶段采用的经典模板攻击方法，是一种实现和使用简便的密钥恢复算法，其在恢复效率和成功率上不是与此类降维方法最配合的密钥恢复方法，在下一步工作中，课题组将实验SVM, SF, MLP和CNN等广泛应用的机器学习乃至深度学习方法进行密钥恢复。侧信道攻击是对物联网密码设备最有效的攻击方法之一，本文旨在研究现实可用的快速侧信道攻击技术，区别于在实验室环境下进行侧信道攻击的复杂苛刻前置条件和繁复的参数调整过程，课题组致力于采用尽可能简单的参数，在掌握尽可能少的目标相关信息条件下进行快速的密钥恢复，这也是课题组选择经典模板攻击进行密钥恢复的原因。简单有效的预处理技术是现实侧信道攻击的关键步骤，在后续工作中，将会调整预处理算法中采用的参数，对该方法进行效率优化，最终开发针对能量数据的专用预处理算法。

参 考 文 献

[1] KOCHER P, JAFFE J, and JUN B. Differential power analysis[C]. The 13th Annual International Cryptology Conference, Santa Barbara, USA, 1999: 388–397. doi: 10.1007/3-540-48405-1_25.

[2] ERNST D and MARTIN S. The common criteria for information technology security evaluation: Implications for China's policy on information security standards[R]. East-West Center Working Papers, No. 108, 2010. doi: 10.2139/ssrn.2770146.

[3] VAN TILBORG H C A and JAJODIA S. Encyclopedia of Cryptography and Security[M]. Boston: Springer, 2011: 468–471. doi: 10.1007/978-1-4419-5906-5.

[4] CHARI S, RAO J R, and ROHATGI P. Template attacks[C]. The 4th International Workshop on Cryptographic Hardware and Embedded Systems, Redwood Shores, USA, 2002: 13–28. doi: 10.1007/3-540-36400-5_3.

[5] BRIER E, CLAVIER C, and OLIVIER F. Correlation power analysis with a leakage model[C]. The 6th International Workshop on Cryptographic Hardware and Embedded Systems, Cambridge, USA, 2004: 16–29. doi: 10.1007/978-3-540-28632-5_2.

[6] BOGDANOV A. Improved side-channel collision attacks on AES[C]. The 14th International Workshop on Selected Areas in Cryptography, Ottawa, Canada, 2007: 84–95. doi: 10.1007/978-3-540-77360-3_6.

[7] RIVAIN M, PROUFF E, and DOGET J. Higher-order masking and shuffling for software implementations of block ciphers[C]. The 11th International Workshop on Cryptographic Hardware and Embedded Systems, Lausanne, Switzerland, 2009: 171–188. doi: 10.1007/978-3-642-04138-9_13.

[8] CORON J S and KIZHVATOV I. Analysis and improvement of the random delay countermeasure of CHES 2009[C]. The 12th International Workshop on Cryptographic Hardware and Embedded Systems, Santa Barbara, USA, 2010: 95–109. doi: 10.1007/978-3-642-15031-9_7.

[9] 黄海, 冯新新, 刘红雨, 等. 基于随机加法链的高级加密标准抗侧信道攻击对策[J]. 电子与信息学报, 2019, 41(2): 348–354. doi: 10.11999/JEIT171211.
HUANG Hai, FENG Xinxin, LIU Hongyu, *et al*. Random addition-chain based countermeasure against side-channel attack for advanced encryption standard[J]. *Journal of Electronics & Information Technology*, 2019, 41(2): 348–354. doi: 10.11999/JEIT171211.

[10] LERMAN L, BONTEMPI G, and MARKOWITCH O. Power analysis attack: An approach based on machine learning[J]. *International Journal of Applied Cryptography*, 2014, 3(2): 97–115. doi: 10.1504/IJACT.2014.062722.

[11] ARCHAMBEAU C, PEETERS E, STANDAERT F X, *et al*. Template attacks in principal subspaces[C]. The 8th International Workshop on Cryptographic Hardware and Embedded Systems, Yokohama, Japan, 2006: 1–14. doi: 10.1007/11894063_1.

[12] STANDAERT F X and ARCHAMBEAU C. Using subspace-based template attacks to compare and combine power and electromagnetic information leakages[C]. The 10th International Workshop on Cryptographic Hardware and Embedded Systems, Washington, USA, 2008: 411–425. doi: 10.1007/978-3-540-85053-3_26.

[13] HETTWER B, GEHRER S, and GÜNEYSU T. Applications of machine learning techniques in side-channel attacks: A survey[J]. *Journal of Cryptographic Engineering*, 2020(10): 85–95. doi: 10.1007/s13389-019-00212-8.

[14] 王燚, 吴震, 蔺冰. 对加掩加密算法的盲掩码模板攻击[J]. 通信学报, 2019, 40(1): 1–14. doi: 10.11959/j.issn.1000-436x.2019007.
WANG Yi, WU Zhen, and LIN Bing. Blind mask template attacks on masked cryptographic algorithm[J]. *Journal on Communications*, 2019, 40(1): 1–14. doi: 10.11959/j.issn.1000-436x.2019007.

[15] CAGLI E, DUMAS C, and PROUFF E. Convolutional neural networks with data augmentation against jitter-based countermeasures: Profiling attacks without pre-

processing[C]. The 19th International Conference on Cryptographic Hardware and Embedded Systems, Taipei, China, 2017: 45–68. doi: 10.1007/978-3-319-66787-4_3.

[16] ZHOU Yuanyuan and STANDAERT F X. Deep learning mitigates but does not annihilate the need of aligned traces and a generalized ResNet model for side-channel attacks[J]. *Journal of Cryptographic Engineering*, 2020(10): 135–162. doi: 10.1007/s13389-019-00209-3.

[17] WANG Z. The data of PANDA challeng1[EB/OL]. https://github.com/kistoday/Panda2018/tree/master/challeng1, 2019.

[18] CRIMINISI A, SHOTTON J, and KONUKOGLU E. Decision forests: A unified framework for classification, regression, density estimation, manifold learning and semi-supervised learning[J]. *Foundations and Trends® in Computer Graphics and Vision*, 2012, 7(2/3): 81–227. doi: 10.1561/0600000035.

[19] HOMMA N, NAGASHIMA S, IMAI Y, *et al*. High-resolution side-channel attack using phase-based waveform matching[C]. The 8th International Workshop on Cryptographic Hardware and Embedded Systems - CHES 2006, Yokohama, Japan, 2006: 187–200. doi: 10.1007/11894063_15.

[20] GUILLEY S, KHALFALLAH K, LOMNE V, *et al*. Formal framework for the evaluation of waveform resynchronization algorithms[C]. The 5th IFIP WG 11.2 International Workshop on Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication, Heraklion, Greece, 2011: 100–115. doi: 10.1007/978-3-642-21040-2_7.

[21] MATEOS E and GEBOTYS C H. A new correlation frequency analysis of the side channel[C]. The 5th Workshop on Embedded Systems Security, Scottsdale, USA, 2010: 4. doi: 10.1145/1873548.1873552.

[22] GIERLICHS B, LEMKE-RUST K, and PAAR C. Templates vs. stochastic methods: A performance analysis for side channel cryptanalysis[C]. The 8th International Workshop on Cryptographic Hardware and Embedded Systems, Yokohama, Japan, 2006: 15–29. doi: 10.1007/11894063_2.

[23] ZHANG Hailong and ZHOU Yongbin. Template attack vs. stochastic model: An empirical study on the performances of profiling attacks in real scenarios[J]. *Microprocessors and Microsystems*, 2019, 66: 43–54. doi: 10.1016/j.micpro.2019.02.010.

袁庆军：男，1993年生，讲师，研究方向为机器学习侧信道分析.

王　安：男，1983年生，副教授，研究方向为侧信道分析与防护技术.

王永娟：女，1982年生，研究员，研究方向为侧信道分析与密码系统安全.

王　涛：男，1995年生，硕士生，研究方向为机器学习侧信道分析.

责任编辑：马秀强