研究与开发

基于模板和 *K*NN 算法的能量分析攻击对比研究

靳济方，刘承远，范晓红，段晓毅，刘嘉瑜
（北京电子科技学院电子与通信工程系，北京 100070）

摘　要：能量分析攻击至今仍是针对密码芯片最具威胁的攻击方法之一，针对传统的模板分析攻击和 *K*NN 算法的攻击进行对比研究，对比模板攻击和机器学习中的 *K*NN 优缺点。首先对皮尔逊相关系数、互信息和最大信息系数、距离相关系数 3 种降维方法进行了研究；然后对比了相同数量功耗曲线下，特征点数量对两种能量分析的成功率等性能的影响；同时研究了不同降维技术在相同功耗曲线数量和不同功耗曲线数量时对两种能量分析攻击的影响。结果表明，模板攻击在运行速度、占用内存方面优于 *K*NN 算法攻击，而在攻击成功率和鲁棒性方面，*K*NN 算法攻击具有更好的表现。

关键词：能量分析攻击；模板攻击；*K*NN 算法；特征点
中图分类号：TM344.1
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2022080

Comparative study of power analysis attacks based on template and *K*NN algorithm

JIN Jifang, LIU Chengyuan, FAN Xiaohong, DUAN Xiaoyi, LIU Jiayu
Department of Electronics and Information Engineering, Beijing Electronic Science and Technology Institute, Beijing 100070, China

Abstract: Power analysis attack is still the most threatening type of side channel attack on cryptographic hardware. The template analysis attack with the attack of *K*NN algorithm was compared. Firstly, three dimensionality reduction methods of Pearson correlation coefficient, mutual information and maximum information coefficient and distance correlation coefficient were studied. Then, the effects of the number of feature points on the attack success rate of the two power analysis attacks under the same number of power consumption curves were compared. At the same time, the effects of different dimensionality reduction techniques on the two power analysis attacks when the number of power curves is the same and different. The results show that the template attack is better than the *K*NN algorithm attack in running speed, memory occupation and robustness, and the *K*NN algorithm attack has better performance in attack success rate.

Key words: power analysis attack, template attack, *K*NN algorithm, feature point

收稿日期：2021−11−22；**修回日期**：2022−03−03
通信作者：段晓毅，duanxiaoyi@besti.edu.cn
基金项目：北京市高精尖学科建设基金资助项目（No.20210032Z0401，No.20210033Z0402）
Foundation Items: The High-Tech Discipline Construction Funds of China (No.20210032Z0401, No.20210033Z0402)

0 引言

随着移动通信过程中对信息安全需求的提高，通信终端设备通常采用加密的安全芯片（如手机 SIM 卡等）保证用户身份认证信息的硬件安全。但随着技术的发展，密码芯片的安全性面临着威胁，其中最大的威胁来自功耗分析攻击。它通过采集密码芯片工作时的能量迹，利用统计分析等手段猜测密码算法的密钥，对终端密码设备的安全构成了极大的威胁。

1999 年，Paul 和 Joshua 等[1]提出了差分能量分析（differential power analysis，DPA）恢复 DES（data encryption standard）的密钥。2003 年，Chari 等[2]通过采集大量能量迹样本建立统计信息，利用模板攻击（template attack，TA）获取密钥。2004 年，Rechberger 和 Oswald 对模板攻击方法的实际问题进行讨论，并分析了特征点数量对攻击成功率的影响，提出使用差分能量分析攻击寻找特征点的方法[4]。2006 年，Archambeau 等[5]提出从侧信道信息中选取特征点构成样本的主子空间（principal subspace），以减少模板攻击的运算量。2011 年，Gabrielet 等[8]首次将机器学习技术应用到侧信道攻击中，利用具有明显汉明重量泄露的数据集进行功率分析攻击，利用最小二乘支持向量机（LS-SVM）成功攻击了一些高级加密标准（advanced encryption standard，AES）的软件实现。2013 年，Lerman 等[9]提出一种半监督的模板攻击方法，这一方法放松了模板攻击中必须完全掌握被攻击设备的限制。可见，模板攻击和基于机器学习的 *K*NN 算法的能量分析攻击日益成为能量分析攻击具有威胁的攻击手段。2019 年，Kim 等[10]介绍了一种使用卷积神经网络分析侧通道的方法。马向亮[11]使用基于能量分析技术分析芯片后门指令，Ryad 等[12]使用 CNN 攻击了有掩码、扰乱防御的基于单片机上的算法实现，文献[13]利用 CNN 对单片机上的算法实现进行了掩码和抗干扰攻击。2020 年，Cai 等[14]提出了差分功率分析攻击的能量曲线压缩方法，段晓毅等[15]使用数据增强技术解决了机器学习中 SBOX（substitution box）输出值的汉明重量不平衡问题。

本文对基于 TA 和 *K*NN 算法的能量分析攻击进行了对比研究。在对皮尔逊相关系数（Pearson correlation coefficient，PCC）、互信息和最大信息系数（maximal information coefficient，MIC）、距离相关系数（distance correlation coefficient，dcorr）3 种降维方法研究的基础上，选出适合两种能量分析攻击的特征点，进一步研究特征点数量 p 对两种能量分析方法的攻击成功率以及 3 种降维方法对两种能量分析方法的攻击成功率的影响等。

1 能量分析攻击

1.1 基于模板的能量分析攻击

TA 过程主要可以分为两个阶段：第一阶段为建立模板阶段，第二阶段为模板匹配阶段。最常用的模板攻击模型是多元高斯模型。

其中，建立模板阶段，构建的模板实际是一个二元组 $T=<\overline{t},\boldsymbol{C}>$，由同一时刻该点的电压均值 $\overline{t}$ 和计算不同点的协方差矩阵 $\boldsymbol{C}$ 组成。分为如下 3 步。

第一步：对 L 位密钥的 2^L 种可能密钥进行建模。

第二步：每一种可能密钥对同一个明文进行 m 次加密，得到 m 条能量/电磁曲线，然后在每条曲线上寻找 n 个与密钥相关的特征点。计算这 n 个点的平均值，得到 $\overline{t}$，如式（1）所示。

$$\begin{aligned}\overline{t} &=<\overline{t}_1,\overline{t}_2,\cdots,\overline{t}_n>\\ &=<\frac{1}{m}\sum_{i=1}^{m}t_{i1},\frac{1}{m}\sum_{i=1}^{m}t_{i2},\cdots,\frac{1}{m}\sum_{i=1}^{m}t_{in}>\end{aligned}\tag{1}$$

第三步：计算不同点的协方差。协方差是构建不同点的相关性，如式（2）所示。

$$\boldsymbol{C}_{n\times n}=\begin{bmatrix}\operatorname{cov}(N_1,N_1) & \operatorname{cov}(N_1,N_2) & \cdots & \operatorname{cov}(N_1,N_n)\\ \operatorname{cov}(N_2,N_1) & \operatorname{cov}(N_2,N_2) & \cdots & \operatorname{cov}(N_2,N_n)\\ \vdots & \vdots & \ddots & \vdots\\ \operatorname{cov}(N_n,N_1) & \operatorname{cov}(N_n,N_2) & \cdots & \operatorname{cov}(N_n,N_n)\end{bmatrix}\tag{2}$$

模板匹配阶段是利用极大似然法则，计算能量迹 t 与模板 $T=<\bar{t},\boldsymbol{C}>$ 匹配的概率，概率最大的是匹配最好的模板，对应的密钥是最可能的正确密钥。其概率计算式如式（3）所示。

$$p\left(t';\left\langle \bar{t},\boldsymbol{C}\right\rangle\right)=\frac{1}{\sqrt{(2\pi)^m|\boldsymbol{C}|}}\exp\left[-\frac{1}{2}(t'-\bar{t})^{\mathrm{T}}\boldsymbol{C}^{-1}(t'-\bar{t})\right] \tag{3}$$

1.2　基于 *K*NN 算法的能量分析攻击

*K*NN 作为监督学习中一种分类算法，该算法的中心思想为：若某样本在特征空间中的 k 个最近邻样本多数属于某一个类别，则该样本属于这个类别。*K*NN 算法原理如图 1 所示。

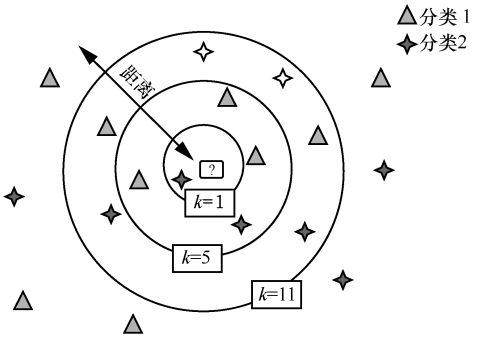

图 1　算法原理

*K*NN 算法的完整步骤如下：

- 计算测试数据与各个训练数据之间的距离；
- 按照距离的递增关系进行排序；
- 选取距离最小的 k 个点；
- 确定前 k 个点所在类别的出现频率；
- 返回前 k 个点中出现频率最高的类别作为测试数据的预测分类。

其中，k 值的选择对训练模型的拟合效果至关重要。k 值过大或过小会造成训练模型过拟合或欠拟合。因此，为了解决这个问题，一开始可以先选择一个较小的 k 值，然后再使用交叉验证的方法最终得到一个适合模型的终值。

*K*NN 在各类开发库中应用广泛。Python3.8 Scikit-Learn 机器学习库中的 *K*NN 算法函数是此类库函数中一个经典的例子。本文中，该函数输入为测试集功耗曲线以及对应的类标签（即 AES-256 算法的字节代替环节第一个 SBOX 输出汉明重量值），输出则为具有分类功能的模型（函数默认近邻数量 k=5，距离默认欧氏距离 p=2）。再将测试集功耗曲线给到该模型进行分类预测。在测试过程中，最后需要将上述得到的汉明重量值与测试集数据实际对应的标签值进行对比，以得到基于 *K*NN 算法进行能量分析攻击时的攻击成功率。

2　降维技术的原理及实现

进行能量分析攻击的第一步是将庞杂的能量数据进行降维，去除噪声，将攻击对象（密钥等敏感数据）有关的点保留，即进行特征点选择。

2.1　特征点选择

目前使用机器学习应用于能量分析攻击是能量分析攻击的一个研究热点，而特征点选择是影响机器学习模型的一个重要因素，当输入数据的特征点数较大时，数据的冗余会造成训练结果差；当输入数据特征点数较小时，小的特征子集不能满足训练算法的需求，从而引起过拟合现象，导致模型误差变大。因此，攻击者在进行模板攻击前，会对功耗曲线上的特征点进行筛选，选出与关键数据相关性高的点，把区分度不够的点排除，以此提高输入数据的优质程度。要评估相关性，需要引入统计学中的概念和统计量衡量。本文将分别使用 3 种常用的特征点选择方法：PCC、MIC 和 Dcorr 对输入数据进行优化。

2.2　3 种降维技术原理

2.2.1　皮尔逊相关系数

PCC 是实现分析特征以及响应变量间关系的一种方法，其实现简单且计算效率较高，能有效衡量各个变量间的线性相关性，结果的取值区间为[−1，1]，−1 表示完全的负相关，1 表示完全的正相关，0 表示没有线性相关。

PCC 计算式如式（4）所示。

$$\rho_{X,Y}=\frac{\sum XY-\frac{\sum X\sum Y}{\mathrm{N}}}{\sqrt{\left(\sum X^2-\frac{\left(\sum X\right)^2}{\mathrm{N}}\right)\left(\sum Y^2-\frac{\left(\sum Y\right)^2}{\mathrm{N}}\right)}} \quad (4)$$

其中，X、Y 是变量的值，N 为样本数。

2.2.2 互信息和最大信息系数

一般来说，互信息（MI）是指随机变量 X 与 Y 在计算时产生的交互信息，其中用 $I(X;Y)$ 表示各个事件间互信息，如式（5）所示。

$$I(X;YX;Y)=\sum_{x_i\in X}\sum_{y_j\in Y}p(x_i;y_j)\log\frac{p(x_i;y_j)}{p(x_i)p(y_j)} \quad (5)$$

可以通过分析互信息检测定性因变量与自变量间的相关性。但互信息在应用于特征选择时具有一定的缺陷。若计算一组连续的变量，就必须先将变量离散化，但将变量离散处理，互信息的结果就会受到一定影响，出现计算误差。

MIC 解决了互信息存在的以上缺陷。其在离散化变量之前挑选一个最优方案，再将互信息的取值方式变为统一化的标准度量方法，如式（6）所示。

$$\mathrm{MIC}[x;y]=\max_{|X||Y|<B}\frac{I[X;Y]}{\mathrm{lb}\left(\min\left(|\boldsymbol{X}|,|\boldsymbol{Y}|\right)\right)} \quad (6)$$

将取值区间定在[0,1]，相较于互信息而言，MIC 有更高的准确度。

2.2.3 距离相关系数

传统的 PCC 存在一定的缺陷，在实际计算过程中，即使 PCC 的值为 0，也不能证明计算变量是相互独立的。但距离相关系数有效克服了这一缺点，当计算的距离相关系为 0 时，可以完全证明两个计算变量是相互独立的。距离相关系数是基于距离的变量 u、v 间相对独立性的研究，其可以表示为 $\hat{\mathrm{d}}\mathrm{corr}(u,v)$，如式（7）所示。当 $\hat{\mathrm{d}}\mathrm{corr}(u,v)$ 为 0 时，则证明两变量是相互独立的；$\hat{\mathrm{d}}\mathrm{corr}(u,v)$ 的值越大，则证明两个变量间的相关性越强。

$$\hat{\mathrm{d}}\mathrm{corr}(u,v)=\frac{\hat{\mathrm{d}}\mathrm{cov}(u,v)}{\sqrt{\hat{\mathrm{d}}\mathrm{cov}(u,u)\hat{\mathrm{d}}\mathrm{cov}(v,v)}} \quad (7)$$

3 实验结果与分析

本实验将差分功耗分析（differential power analysis，DPA）国际学术大赛第四阶段（DPA contest v4）[16]的数据集作为实验对象，该数据集包含 10 000 条能量曲线，每条能量曲线包含 435 000 个特征值，本文实验攻击点为 S 盒输出，模型为汉明重量模型。对 TA 和基于 *K*NN 算法的能量攻击性能进行对比研究。

3.1 特征点选择

本文实验选用的数据集包含 10 000 条能量曲线，每条能量迹对应的时刻点是相同的，为了提高实验运算速度，本文仅选择前 r 条（r = 100、200、300、400）能量曲线分别采用 3 种降维技术实现特征点选择。

3.1.1 PCC 进行特征点选择

使用 PCC 进行特征点选择时，X 为一组能量曲线，Y 为这组能量曲线对应的 S 盒输出的汉明重量值，把 X 和 Y 代入式（4），得到曲线中与 Y 相关性较大的特征点（绝对值越接近 1 的点），选择这些特征点进行能量分析攻击。不同 r 值计算出 435 001 个特征点对应的 PCC 如图 2 所示。

3.1.2 MIC 进行特征点选择

使用 MIC 进行特征点选择时，X 为一组能量曲线，Y 为这组能量曲线对应的第一个 S 盒输出的汉明重量值，把 X 和 Y 代入式（6）中，即可以得到曲线中与 Y 相关性较大的特征点，选择这些特征点进行能量分析攻击。不同 r 值计算出 435 001 个特征点对应的 MIC 如图 3 所示。

3.1.3 Dcorr 特征点选择

使用 Dcorr 进行特征点选择时，u 为一组能量

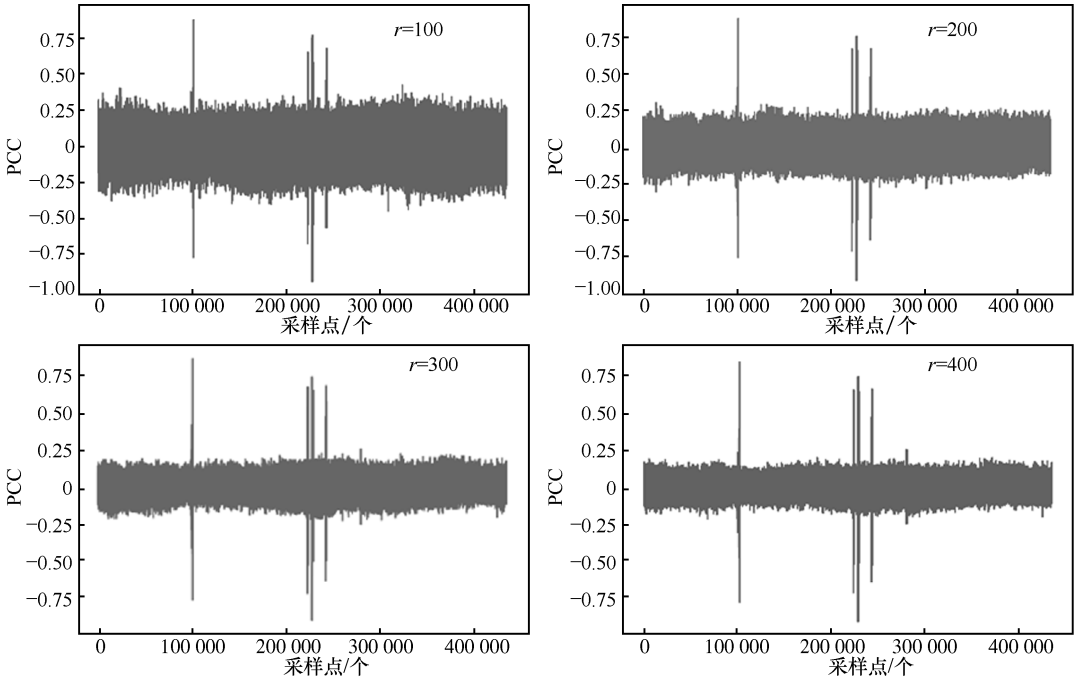

图 2　不同 r 值计算 435 001 个特征点对应的 PCC

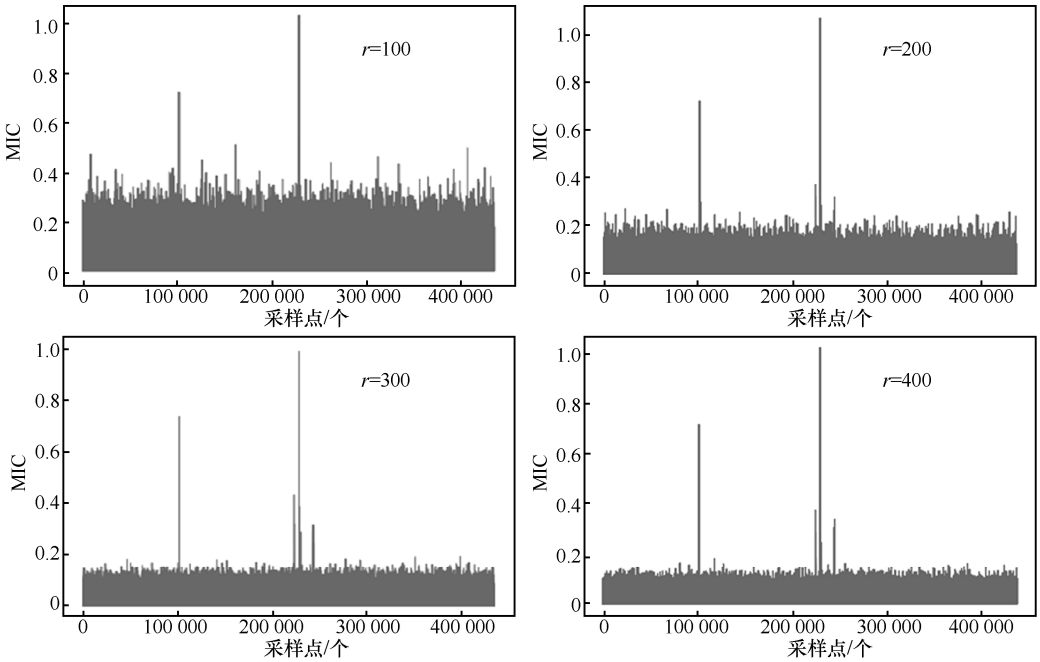

图 3　不同 r 值计算出 435 001 个特征点对应的 MIC

曲线，v 为这组能量曲线对应的第一个 S 盒输出的汉明重量值，把 u 和 v 代入式（7），即可以得到曲线中与 v 相关性较大的特征点，选择这些特征点进行能量分析攻击。不同 r 值计算出 435 001 个特征点对应的 Dcorr 相关系数如图 4 所示。

由图 2、图 3 和图 4 可知，3 种特征点选择方法

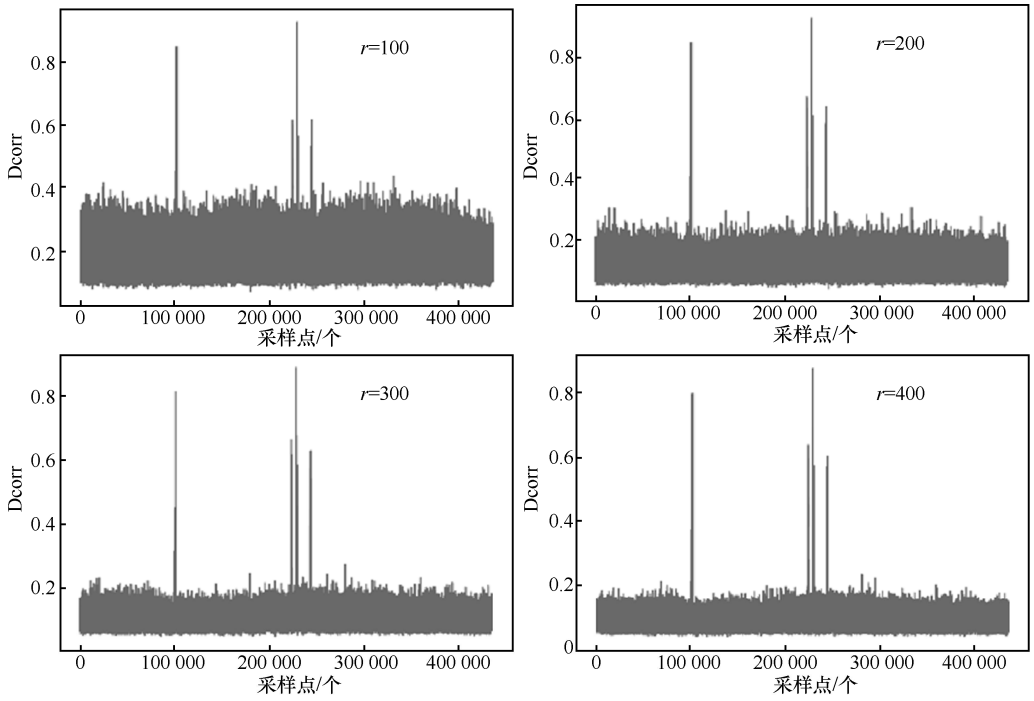

图 4　不同 r 值计算 435 001 个特征点对应的 Dcorr 相关系数

均适用于能量分析攻击，均可以很好地选择特征点。且不同的能量曲线条数对相关系数的结果是有影响的，可以看出当能量曲线条数 r =300、r =400 时的图像已经趋于相同，所以在统筹节约运算时间和效果的前提下，暂选定 r=300。

3.2　特征点数量 p 对攻击成功率的影响

3.2.1　特征点数量 p 对 TA 的影响

对于 TA 来说，每条功耗曲线选取特征点 p 不能过多。每个模板中的功耗曲线是对相同操作数的多次测量，所以具体功耗值都是十分接近的，当选取的特征点越多时，对应的协方差方阵 $\boldsymbol{C}$ 规模越大，矩阵的行列式 $|\boldsymbol{C}|$ 越接近于 0，即被看作一个奇异矩阵，没有逆矩阵。在模板匹配时采用多元高斯分布概率密度公式中需要用到协方差矩阵的逆矩阵 $\boldsymbol{C}^{-1}$，所以在 TA 的过程中每条曲线选取的特征点个数不能太多。经过实际测试，特征点个数 p 不能大于 27。采用 300 条能量曲线（r=300），基于 PCC 技术进行特征点选择后，对数据进行 p 值分析。p 值的选择对基于 TA 的能量分析攻击成功率影响如图 5 所示。

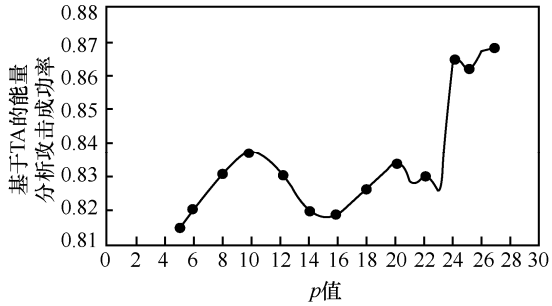

图 5　p 值的选择对基于 TA 的能量分析攻击成功率的影响

由图 5 可知，特征点个数 p 值对基于 TA 的能量分析攻击的影响较为明显。整体上看，当 p 值越大时，基于模板的能量分析攻击成功率越高（少数情况有小幅波动）。当 $p \leqslant 23$ 时，攻击成功率在 0.85 以下，相对较低；当 $p \geqslant 24$ 时，攻击成功率提高到 0.86~0.87；当 $p = 27$ 时，攻击成功率最高，达到 0.868 以上。

3.2.2　特征点数量 V 对 KNN 算法的影响

采用 300 条能量曲线（r=300），PCC 进行特征点选择后得到的数据进行 p 值分析。p 值的选择对于基于 KNN 算法的能量分析攻击成功率影响如图 6 所示。

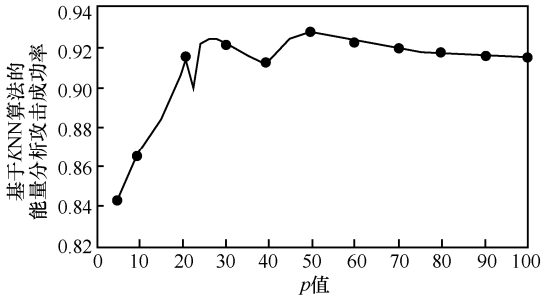

图 6　p 值的选择对基于 KNN 算法的能量分析攻击成功率的影响（k=7）

由图 6 可知，当 p 值逐渐增大，攻击成功率逐渐升高（少数情况有小幅波动），当 p 值超过某阈值后，攻击成功率转而逐渐降低。当 p =50 时，攻击成功率最高，达到 0.928。

3.3.3　特征点数量 p 对两种能量分析攻击的横向比较

由图 5 和图 6 可以看出，当 $p\in$[20,27]时，两种能量分析攻击方法的攻击成功率均很高，将 p 与两种能量分析攻击方法进行横向比较，分析 p 值的选择对两种能量分析算法的影响。p 值的选择对两种能量分析攻击方法的影响如图 7 所示，整体上看，基于 KNN 算法的能量分析攻击成功率明显高于基于能量分析攻击成功率，其平均成功率之差在 0.066 7 以上。

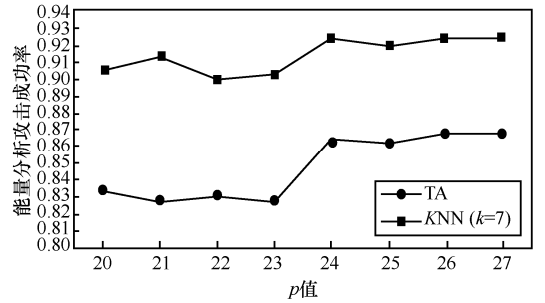

图 7　p 值的选择对两种能量分析攻击方法的影响

综上可得，针对 PCC 降维技术得到的数据集，当两个模型选取相同个数的特征点 p 时，明显看出结果基于 KNN 算法的能量分析攻击成功率更高，且 p 值的改变引起攻击成功率的波动幅度更小，即基于 KNN 算法的能量分析攻击的鲁棒性更强。

3.3　不同特征点选择方法对攻击成功率的影响

本节将分析 PCC、MIC 和 Dcorr 3 种特征点选择方法对模板攻击和 KNN 算法攻击成功率的影响。

3.3.1　能量曲线条数固定的影响

当能量曲线条数 r 为 300 时，经过 3 种特征点选择方法得到数据集，对两种能量分析攻击方法的攻击成功率见表 1。TA 表示基于模板的能量分析攻击，KNN 表示基于 KNN 算法的能量分析攻击，特征点个数 p 为 27。

表 1　3 种特征点选择方法对两种能量分析攻击成功率的影响（r=300）

	TA	KNN（k=7）
PCC	0.868	0.923
MIC	0.897	0.940
Dcorr	0.857	0.926

由表 1 可知，PCC、MIC 和 Dcorr 3 种特征点选择方法对两种能量分析攻击方法的影响程度不同，其中，对基于 TA 的能量分析攻击的整体影响范围在 0.04 内，对于基于 KNN 算法的能量分析攻击的整体影响范围在 0.02 以内。其中，MIC 特征点选择方法对两种能量分析攻击方法的成功率更高。

3.3.2　不同能量曲线条数的影响

控制变量保持不变：特征点个数 p=27，KNN 算法中近邻数量 k=7。分别对比经 3 种特征点选择方法得到的数据对两种能量分析攻击成功率的影响。其中，r 值的选择对 PCC 降维技术效果的影响如图 8 所示，r 值的选择对 MIC 降维技术效果的影响如图 9 所示，r 值的选择对 Dcorr 降维技术效果的影响如图 10 所示。

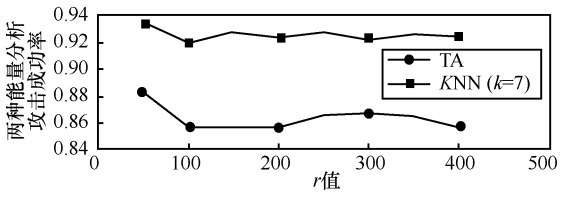

图 8　r 值的选择对于 PCC 降维技术效果的影响

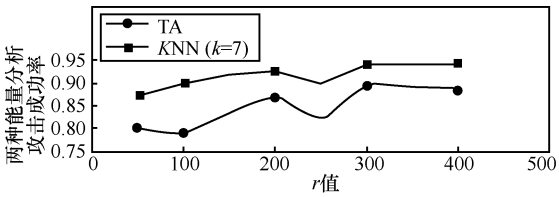

图 9　r 值的选择对于 MIC 降维技术效果的影响

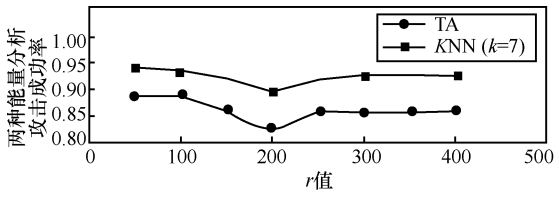

图 10　r 值的选择对于 Dcorr 降维技术效果的影响

由图 8 可看出，对 PCC 降维技术来说并非在计算相关系数时选择的功耗曲线的条数越多越好，在 $r=50$ 时，两种能量分析攻击的成功率最高。具体地，对基于高斯模板的能量分析攻击来说，在 $r=300$ 时攻击成功率优于除 $r=50$ 的其他情况，基于 *K*NN 算法的能量分析攻击来说，r 值在大于 50 之后攻击成功率没有很大波动，基本趋于稳定。

由图 9 可看出，对 MIC 降维技术来说计算相关系数时选择的功耗曲线条数越多越好，另外由曲线的波动幅度可以看出基于高斯模板的能量分析攻击对 r 值的改变反应更为敏感，而当 $r\geqslant 300$ 后，攻击成功率没有很大的波动，基本趋于稳定。

由图 10 可看出，对于 Dcorr 降维技术来说，当 $r\leqslant 300$ 时，r 值的增大会导致两种能量分析攻击成功率的降低；当 $r=200$ 时，两种能量分析攻击成功率最低；当 $r\geqslant 250$ 后，攻击成功率在一个较小的范围内变化（成功率不如 $r=50$ 时高），没有很大的波动，基本趋于稳定。

综上可以得出，为达到较理想的能量分析攻击效果，采用不同降维技术，应选择不同功耗曲线条数计算相关系数，即选择不同的 r 值。对于采用 PCC 降维技术，r=50 时，两种能量分析攻击的成功率最高，效果最理想；对于采用 MIC 降维技术，r=300 或 r=400 时，两种能量分析攻击的成功率最高，效果最理想；对于采用 Dcorr 降维技术，r=50 时，两种能量分析攻击的成功率最高，效果最理想。

3.4　两种能量分析攻击方法比较

由第 3.3 节可以看出，攻击成功率方面，*K*NN 算法的攻击成功率和鲁棒性明显优于模板攻击，从运算速度和内存使用情况看，基于模板的能量分析攻击训练模型的速度较快，内存使用空间较小，而基于 *K*NN 算法的能量分析攻击训练模型的运算速度较慢，内存使用空间较大。原因是 *K*NN 算法属于机器学习算法，模型训练时需要耗费大量内存空间完成计算。两种能量分析攻击在攻击成功率、鲁棒性、运行速度和占用内存 4 个方面的对比见表 2。

表 2　两种能量分析攻击方法的对比

	攻击成功率	鲁棒性	运行速度	占用内存
模板攻击	低	弱	快	小
*K*NN 算法攻击	高	强	慢	大

4　结束语

通过本文的对比研究，基于 PCC、MIC 和 Dcorr 的 3 种特征点选择方法均适用于能量分析攻击，均可以很好地选择特征点；特征点 p 的数量对两种攻击方法的攻击成功率都有一定的影响。不同的降维技术对模板攻击和基于 *K*NN 算法的攻击成功率有区别。MIC 特征点选择方法对两种能量分析攻击方法的成功率更高；为达到较理想的能量分析攻击效果，建议采用不同的降维技术时，应选择不同条功耗曲线计算相关系数。采用 PCC 降维技术时，r 值选择 50，可使两种能量分析攻击的成功率最高；采用 MIC 降维技术时，r 值选择 300 或 400，可使两种能量分析攻击的成功率最高；采用 Dcorr 降维技术时，r 值选择 50，可使两种能量分析攻击的成功率最高。

本文主要针对传统的模板分析攻击和 *K*NN 算法的攻击进行对比研究，实验结果表明模板攻击在运行速度、占用内存优于基于 *K*NN 算法的攻击，而在攻击成功率和鲁棒性方面，基于 *K*NN 算法的攻击具有更好的表现。当然，有很多方面仍可做进一步的研究和完善：进一步优化 *K*NN 算法，使其在运行速度、占用内存方面得到提升；采用多种特征点选择方法来对两种攻击方法进行探索。

参考文献：

[1] KOCHER P, JAFFE J AND JUN B. Differential power analysis[J]. Lecture Notes in Computer Science, 1999: 388-397.

[2] AO J R, ROHATGI P. Template attacks[J].International Workshop on Cryptographic Hardware and Embedded Systems, 2002: 13-28.

[3] BRIER E, CLAVIER C, OLIVIER F. Correlation power analysis with a leakage model[C]//Cryptographic Hardware and Embedded Systems. [S.l.:s.n.] , 2004.

[4] CHRISTIAN R, ELISABETH O. Practical template attacks[C]// Proceedings of the 5th international conference on Information Security Applications (WISA'04). [S.l.:s.n.], 2004: 440-456.

[5] ARCHAMBEAU C, PEETERS E, STANDAERT F X, et al. Template attacks in principal subspaces[C]//Cryptographic Hardware and Embedded Systems. [S.l.:s.n.], 2006.

[6] GIERLICHS B, LEMKE-RUST K, PAAR C. et al. Stochastic methods[C]//Cryptographic hardware and embedded systems. [S.l.:s.n.], 2006.

[7] STANDAERTF X, ARCHAMBEAU C. Using subspace-based template attacks to compare and combine power and electromagnetic information leakages[C]//Cryptographic Hardware and Embedded Systems. [S.l.:s.n.], 2008.

[8] HOSPODAR G, GIERLICHS B, DE MULDER E, et al. Machine learning in side-channel analysis: a first study[J]. Journal of Cryptographic Engineering, 2011, 1(4): 293-302.

[9] LERMAN L, MEDEIROS S F, VESHCHIKOV N, et al. Semi-supervised template attack[J]. IACR Cryptology EPrint Archive, 2012, 2012: 82.

[10] KIM J, PICEK S, HEUSER A, et al. Make some noise. unleashing the power of convolutional neural networks for profiled side-channel analysis[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019: 148-179.

[11] 马向亮, 王宏, 李冰, 等. 基于能量分析技术的芯片后门指令分析方法[J]. 电子学报, 2019, 47(3): 686-691.
MA X L, WANG H, LI B, et al. A power analysis method against backdoor instruction in chips[J]. Acta Electronica Sinica, 2019, 47(3): 686-691.

[12] BENADJILA R, PROUFF E, STRULLU R, et al. Deep learning for side-channel analysis and introduction to ASCAD database[J]. Journal of Cryptographic Engineering, 2020, 10(2): 163-188.

[13] BENADJILA R, PROUFF E, STRULLUR, et al. Deep learning for side-channel analysis and introduction to ASCAD database[J]. Journal of Cryptographic Engineering, 2020, 10(2): 163-188.

[14] CAI X M, LI R F, KUANG S J, et al. An energy trace compression method for differential power analysis attack[J]. IEEE Access, 2020(8): 89084-89092.

[15] DUAN X Y, CHEN D, FAN X H, et al. Research and implementation on power analysis attacks for unbalanced data[J]. Security and Communication Networks, 2020: 5695943.

[作者简介]

靳济方（1972− ），女，北京电子科技学院电子与通信工程系副教授，主要研究方向为电路与系统安全。

刘承远（1999− ）,男，北京电子科技学院硕士生，主要研究方向为信息安全。

范晓红（1979− ），女，北京电子科技学院电子与通信工程系讲师，主要研究方向为信息安全。

段晓毅（1979− ），男，北京电子科技学院电子与通信工程系副教授，主要研究方向为信息安全。

刘嘉瑜（1999− ），女，北京电子科技学院在读，主要研究方向为信息安全。