双重掩码的模幂算法聚类相关功耗分析攻击

万武南，陈　俊

(成都信息工程大学网络空间安全学院；成都信息工程大学计算机学院　成都　610225)

【摘要】相关功耗分析方法是模幂算法最常用的攻击方法之一，当设计中使用底数和指数双重掩码防护措施时，现有的相关功耗分析无法使用。采用高阶相关功耗分析可以对这类防护措施实施有效攻击，但会带来噪声、降低攻击准确率，并且攻击过程中分类方法采用人工观察设定阈值方式，攻击效果严重依赖于攻击者的经验。针对以上问题，提出了一种基于聚类相关功耗分析攻击方法，利用模乘之间功耗的相关性特征差异，评估功耗点有效度，提高有效信息利用率，降低噪声和人工参与过程。实验结果表明，针对双层掩码的模幂防范算法，聚类相关功耗分析与现有策略相比，攻击效率和算法通用性得到提升，400条功耗曲线攻击准确率收敛于1。

关　键　词　聚类算法；　相关功耗分析；　模幂运算；　RSA；　侧信道攻击

中图分类号　TP309.2　　**文献标志码**　A　　doi:10.3969/j.issn.1001-0548.2018.04.018

A Cluster Correlation Power Analysis Attack against Modular Exponentiation Algorithm Based on Double Masking Scheme

WAN Wu-nan and CHEN Jun

(School of Cybersecurity, Chengdu University of Information Technology;

School of Computer, Chengdu University of Information Technology　Chengdu　610225)

Abstract　Correlation power analysis (CPA) which is one of the most useful techniques for side channel attack can not implement a successful attack against the exponent and　the message blinding countermeasures on modular exponentiation algorithm. And a successful attack against these protected implementations is performed by the high order CPA. But a lot of noise caused by the high order CPA lead to the less attack accuracy of side channel attack. Moreover, the methods of artificial observation are currently used by setting the threshold in attack process, so the attack effect is heavily dependent on the attacker's experience. In order to solve these problems, a cluster CPA is proposed by utilizing correlation characteristics difference between power consumption of modular multiplication to evaluate the effectiveness of power points. The utilization of valid information is improved and the noise and artificial participation are reduced by using the new proposed method. Experiment results demonstrate that the proposed cluster CPA can enhance attack efficiency and attack algorithm generality by comparing with other CPA methods, and only 400 power traces are required to launch the attack with the attack accuracy of 100%.

Key words　cluster;　correlation power analysis (CPA);　module exponentiation;　RSA;　side channel attack

自文献[1]提出差分功耗分析(differential power analysis, DPA)方法以来，研究者提出了多种破解模幂运算法的功耗攻击方法，如简单功耗分析(simple power analysis, SPA)[1]、DPA[2-3]、相关功耗分析(CPA)[4-5]。为了防止侧信道攻击，目前模幂算法常采用指数和底数掩码进行有效防范[6]。针对底数掩码的抗功耗攻击算法，文献[7]提出一种互相关功耗分析方法(CCA)，通过模乘与模乘之间相关性差异破译指数；文献[8-9]则针对指数掩码，提出水平相关功耗分析方法。但一阶CPA方法对双重掩码的抗攻击算法无效，并且对功耗曲线采集设备噪声的前提非常严格。随后，文献[10]提出针对指数掩码防范算法的高阶CPA方法。文献[11]对HeeSeok方法进行改进，针对双重掩码的模幂防范算法，通过人工观测，阈值设定选择有效点，提出一种二阶CPA攻击算法。

收稿日期：2017－09－12；修回日期：2018－01－17

基金项目：国家自然科学基金面上项目(61572086)；四川省科技厅攻关项目(2017GZ0314)；四川省教育厅重点项目(16ZA0212)

作者简介：万武南(1978－)，女，博士，副教授，主要从事侧信道攻击、网络存储安全方面的研究.

随着机器学习技术的发展，文献[12]提出采用k均值聚类分析方法攻击模幂算法。文献[13]针对模幂算法，提出选择明文聚类功耗分析方法，通过选择输入特殊的两条明文，成功破解幂指数。文献[14]则采用k均值聚类方法，提出相关电磁攻击方法，能够有效攻击模幂算法，并且对采用Lopez-Dahab坐标系的二元有限域上实现的ECC算法进行了破译。文献[15]将模糊理论引入到k均值算法中，采用一条功耗曲线，针对指数掩码的抗攻击模幂算法，提出对RSA密码算法的一种无监督的电磁攻击。文献[16]对文献[14]提出算法进行改进，采用最大期望算法(expectation maximization algorithm)的聚类算法，并结合主成分分析(principal component analysis)特征提取方法，对模幂算法进行电磁攻击。

采用高阶相关功耗分析攻击，对双重掩码的模幂防范算法理论上被证明是有效的，但该攻击方法会带来有效信息损失，降低攻击效率。现有的高阶功耗分析法，分析攻击中分类阈值设定采用人工观察进行设定，阈值设定的主观性对攻击准确率影响较大。此外，国内外文献研究中没有针对双重掩码的模幂运算进行聚类功耗攻击分析的研究[17-19]。

本文考虑到实际应用，针对双重掩码模幂算法，利用模乘功耗之间相关性的特征差异，采用多重k均值聚类选择有效功耗操作点，提出了一种基于聚类的相关功耗分析攻击方法，该方法可以减少有效信息损失及攻击过程中的人工干预。最后搭建实验，对自制功耗采集设备运行双重掩码的模幂算法的智能卡实施攻击，实验结果表明，本文方法能有效提升攻击效率和攻击算法通用性。

1　双重掩码相关功耗分析模型

1.1　双重掩码的模幂算法

为了防止密码硬件设备中的模幂算法遭受SPA和DPA攻击，文献[7]提出了一种双重掩码的模幂防范方法，如算法1。算法1没有直接计算$m^d \bmod N$，通过随机数r对消息m进行掩码，并采用t和s对指数d进行重编码，重编码 $t=k\varphi(N)+d-2^n+1$，$s=\varphi(N)-d$，其中$\varphi(N)$为N的欧拉函数，k为整数。

算法1　抗SPA-DPA 双重掩码模幂算法

输入　$m,d=(d_{n-1},d_{n-1},\cdots,d_2,d_1,d_0),N,r$)，$r$是一个任意数。

输出　$C=m^d \bmod N$。

1) $t=k\varphi(N)+d-(2^n-1)$, $s=\varphi(N)-d$

2) $T[00]=m\times r \bmod N$; $T[01]=m\times r^2 \bmod N$;

$T[10]=m^2\times r^2 \bmod N$; $T[11]=m^2\times r^3 \bmod N$;

3) $C=T[t_{n-1}s_{n-1}]$；

4) for $i=(n-2)\sim 0$

① $C=C\times C \bmod N$　– 平方(squaring)

② $C=C\times T[t_i s_i] \bmod N$　– 乘(multiplication)

5) return (C)

1.2　双重掩码模幂算法相关功耗模型

密码设备运行密码操作所泄露的功耗信息依赖于所处理的数据和执行的操作，即：数据依赖性和操作依赖性。因此，这两种依赖分量是边信道攻击基础。除了这两种依赖分量之外，功耗数据还包含了大量噪声和直流分量。进行功耗曲线的采集要受到设备、环境等多方面的影响，为了便于描述，功耗曲线的总功耗组成为：

$$P_{\text{total}}=P_{\text{op}}+P_{\text{data}}+P_{\text{el.noise}}+P_{\text{const}} \tag{1}$$

式中，P_{total}为总功耗；P_{op}为操作依赖分量；P_{data}为数据依赖分量；$P_{\text{el.noise}}$为电子噪声；P_{const}为恒定分量。根据式(1)中功耗组成可知，模乘$a\times b(\bmod N)$和$cd(\bmod N)$的功耗，P_{op}分量主要依赖于模乘算法实现操作步骤，理论上来说，模乘操作P_{op}不变；P_{data}与模乘中操作数相关，根据汉明重量功耗模型可知，理论上来说操作数的汉明重量不同，P_{data}功耗也有高低之分。操作数汉明重量越相似，两模乘的P_{data}越相似，即功耗相关性越高。若模数N相同，模乘之间的功耗相关性与操作数关系如表1所示。

表1　两模乘运算的功耗相关性

a,c 的值	b,d 的值	对应功耗相关性 R
$a=c$	$b=d$	R_{High}
$a\neq c$	$b\neq d$	R_{Low}
$a=c$	$b\neq d$	R_{Medium}

因此根据模幂运算与操作数的相关功耗模型可知，通过模乘功耗相关性的不同，来判断区分模乘操作数之间关系。算法1中，步骤4)循环运算中包含两种模乘运算，其中步骤①的模乘称为“平方(S)”，步骤②的模乘称为“乘(M)”，功耗示意图如图1所示。图1中纵坐标表示各模乘的功耗电压值，横坐标则表示时间。白色为底的表示步骤①模乘功耗，带颜色为底是步骤②模乘功耗。

步骤②的模乘中，涉及到两操作数分别为C和$T[t_i s_i]$，其中C是动态变化的，$T[t_i s_i]$是固定值，4种取值分别为$T[00]$、$T[01]$、$T[10]$、$T[11]$。T值的下标取值是由幂指数d重编码t和s确定，因此可知步骤②模乘的运算与幂指数d值密切相关，是幂指数泄露点。根据模幂相关功耗模型，理论上来说，统

计步骤②中模乘之间的功耗的相关性，可以区分出操作数 $T[t_i s_i]$ 的不同。

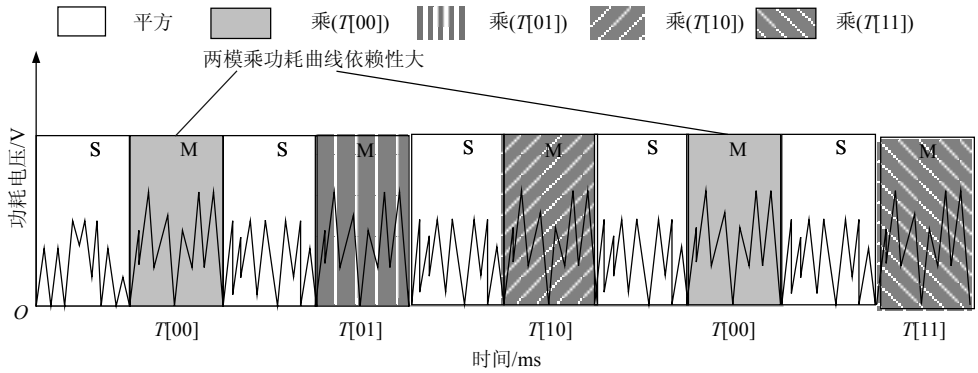

图1 算法1模乘功耗示意图

而在真实环境下，采集的模乘多个功耗点是由数据功耗与操作功耗，以及各种电路噪声混叠在一起，并不是每个功耗点都直接与模乘操作数相关，包含着与操作数不相关的功耗。因此除了通过滤波去除电路固有噪声，还选择与操作数数据依赖强的功耗点，提高攻击效率和准确率。分量 P_{data} 数据依赖功耗可以分为有效数据依赖功耗 $P_{\text{data\_valid}}$ 和较弱数据依赖功耗 $P_{\text{data\_lvalid}}$ 两部分，则功耗组成为：

$$P_{\text{total}} = P_{\text{op}} + P_{\text{data}} + P_{\text{el.noise}} + P_{\text{const}} \tag{2}$$

相关功耗分析模型中，模乘各功耗点相关性包含了较弱数据依赖相关性。根据信噪比理论可知，信号之间的方差越大，信噪比越高；方差越小，噪声越大。为了去除较弱数据依赖功耗，把模乘各点相关性作为“信号”，通过方差对模乘相关性二次处理，提取出有效数据依赖功耗 $P_{\text{data\_lvalid}}$ 的有效点，利用聚类k均值相关功耗算法，提高攻击效率和准确率。

2 聚类k均值相关功耗算法

1) 首先输入相同幂底数和幂指数，将算法1采集功耗曲线进行滤波、对齐，然后截取算法1中步骤②$C = C \times T[t_i s_i] (\bmod N)$ 的功耗曲线，组成如下分块矩阵：

$$\boldsymbol{Z} = \begin{bmatrix} \boldsymbol{M}_{0,0} & \boldsymbol{M}_{0,1} & \cdots & \boldsymbol{M}_{0,n-3} & \boldsymbol{M}_{0,n-2} \\ \boldsymbol{M}_{1,0} & \boldsymbol{M}_{1,1} & \cdots & \boldsymbol{M}_{1,n-3} & \boldsymbol{M}_{1,n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \boldsymbol{M}_{r-2,0} & \boldsymbol{M}_{r-2,1} & \cdots & \boldsymbol{M}_{r-2,n-3} & \boldsymbol{M}_{r-2,n-2} \\ \boldsymbol{M}_{r-1,0} & \boldsymbol{M}_{r-1,1} & \cdots & \boldsymbol{M}_{r-1,n-3} & \boldsymbol{M}_{r-1,n-2} \end{bmatrix} \tag{3}$$

式中，每个分块矩阵 $\boldsymbol{M}_{i,j}$ 代表第i条功耗曲线第j个模乘；n代表曲线中模乘的数量；r代表曲线条数。而每个分块矩阵为：

$$\boldsymbol{M}_{i,j} = [\boldsymbol{m}_{i,j*p}, \boldsymbol{m}_{i,j*p+1}, \cdots, \boldsymbol{m}_{i,j*p+p-1}]$$

式中，p代表每个模乘功耗的点数。矩阵$\boldsymbol{Z}$中的列向量 $\boldsymbol{m}_{j*p+k} = [m_{0,j*p+k}, m_{1,j*p+k}, \cdots, m_{r-1,j*p+k}]$，其中 $0 \leqslant j < n-1$，$0 \leqslant k < p$。

2) 由矩阵$\boldsymbol{Z}$，计算模乘与第s模乘之间功耗相关系数，得到模乘之间相关系数矩阵为：

$$\boldsymbol{C}_S = \begin{bmatrix} C_{0,0}^S & C_{0,1}^S & \cdots & C_{0,l-2}^S & C_{0,l-1}^S \\ C_{1,0}^S & C_{1,1}^S & \cdots & C_{1,l-2}^S & C_{1,l-1}^S \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ C_{n-3,0}^S & C_{n-3,1}^S & \cdots & C_{n-3,l-2}^S & C_{n-3,l-1}^S \\ C_{n-2,0}^S & C_{n-2,1}^S & \cdots & C_{n-2,l-2}^S & C_{n-2,l-1}^S \end{bmatrix} \tag{4}$$

式中，$C_{i,j}^S$ 代表第i模乘与固定第s模乘中，第j个功耗点之间的相关系数，其中 $0 \leqslant i < n-1$，$0 \leqslant j < p$，$0 \leqslant S < n-1$。即 $C_{i,j}^S$ 相关系数计算公式为：

$$C_{i,j}^S = \rho(m_{s*p+j}, m_{i*p+j}) = \frac{\sum_{t=0}^{r-1}(m_{t,s*p+j} * m_{t,i*p+j}) - \frac{\sum_{t=0}^{r-1} m_{t,s*p+j} \sum_{t=0}^{r-1} m_{t,i*p+j}}{r}}{\sqrt{\left(\sum_{t=0}^{r-1} m_{t,s*p+j}^2 - \frac{\left(\sum_{t=0}^{r-1} m_{t,s*p+j}\right)^2}{r}\right)}\sqrt{\left(\sum_{t=0}^{r-1} m_{t,i*p+j}^2 - \frac{\left(\sum_{t=0}^{r-1} m_{t,i*p+j}\right)^2}{r}\right)}} \tag{5}$$

3) 计算 $\boldsymbol{C}_S$ 每列的方差，v_i 代表矩阵 $\boldsymbol{C}_S$ 的每列方差值，得到方差向量值为：

$$\boldsymbol{V}^S=[v_0,v_1,v_2,\cdots,v_{p-2},v_{p-1}] \tag{6}$$

4) 计算方差向量与向量均值的欧式距离，得到欧式距离向量为：

$$\boldsymbol{D}^S=[d_0,d_1,d_2,\cdots,d_{p-2},d_{p-1}] \tag{7}$$

5) 采用k均值聚类方法，将方差欧式距离 $\boldsymbol{D}^S$ 进行聚类，聚类数目为 δ，选择聚类中心点最大的簇的集合作为功耗有效点选择集 G^S_{valide}。

输入：数据集 $\boldsymbol{D}^S$，聚类数目为 δ。

输出：聚类中心点最大的簇的集合 G^S_{valide}。

① 初始化，随机指定 δ 个聚类中心点 μ_1、μ_2、$\cdots$、μ_δ。② $\forall i\in(0,1,2,\cdots,l-1)$，计算距离值$d_i$到各聚类中心 μ_j 的距离 $D(d_i,u_j)$，$j=1,2,\cdots,\delta$，判断 d_i 与 μ_j 之间距离的函数 $D(d_i,u_j)=\min\{D(d_i,u_j),j=1,2,\cdots,\delta\}$，则 $d_i\in G^S_j$，i值为 d_i 在数据集 $\boldsymbol{D}^S$ 中原编号。③ 重新计算各簇中心点，对每个簇 G^S_j 计算 $\mu_j=\frac{1}{N_j}\sum_{t=1}^{N_j}d_{jt},j=1,2,\cdots,\delta$，$d_{jt}$ 为每个簇中的数据值，t为距离值在新簇中的新编号，N_j 为第j个簇中变量的个数。④ 计算偏差 $J=\sum_{j=1}^{\delta}\sum_{t=1}^{N_j}\left\|d_{jt}-u_j\right\|$。⑤ 收敛判断，如果$J$值收敛，则转步骤⑥；否则转步骤②。⑥ 对每个簇 G^S_j，计算 $\mu_j=\frac{1}{N_j}\sum_{t=1}^{N_j}d_{jt}$ 和 $\mu_{\max}=\max\{u_j,j=1,2,\cdots,\delta\}$，则 $\mu_{\max}$ 聚类中心所属的簇为选择集 $G^S_{\text{valide}}=(\gamma_1,\gamma_2,\cdots,\gamma_{x-1})$。

6) 根据 G^S_{valide}，选取相关系数 $\boldsymbol{C}_S$ 中每行对应位置相加，相关系数和组成集合 $\text{cof}_S=(\lambda_1,\lambda_2,\cdots,\lambda_{n-2})$，则 $\lambda_i=\sum_{t=0}^{x-1}c^S_{i,\gamma_t},\gamma_t\in G^S_{\text{valide}}$。

7) 采用类似步骤4)的k均值聚类方法，将 cof_S 再次进行聚类，聚类数目为2，输出聚类中心点最大的簇的集合 $\text{cof}_{\text{valid}}$，则簇中位置编号对应的模乘与固定模乘$s$的依赖关系强，即判断为与模乘$s$的操作数一致。

8) 返回步骤2)，依次将n–1个模乘分成4类，每类可猜测为T[00]、T[01]、T[10]、T[11]，重组编码出t和s的16种取值，然后推算出正确的幂指数d值。

3　实验结果

3.1　功耗采集环境

功耗采集的实验设备有PC工作站、数字采样示波器(Tektronix PPO4032)、自制功耗采集板，如图2所示。实验PC工作站与示波器通过网线相连，示波器与自制功耗采集板相连，自制功耗采集板通过USB串口通信与PC机相连。示波器主要是接收自制功耗采集板的触发信号指令和采集功耗曲线，自制功耗采集板集成了智能卡读卡器、STM32开发板等多种功能。

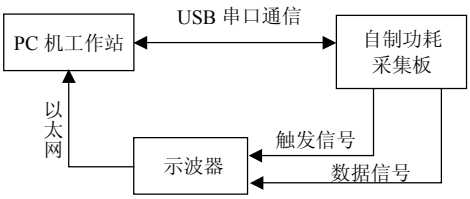

图2　功耗采集实验硬件环境

3.2　实验数据处理

在图2所示功耗采集平台上，采集智能卡算法1的功耗曲线，将采集原始功耗曲线进行滤波，去除固有噪声；再对功耗曲线进行切割和重组，构成只由算法1中步骤4)的步骤②功耗构成的新的模乘曲线，数据存放在矩阵$\boldsymbol{M}$中。然后对功耗矩阵$\boldsymbol{M}$进行聚类相关功耗分析：计算模乘与固定模乘之间的相关性；通过对相关系数计算方差和方差欧式距离；对方差欧式距离聚类处理进行分类，如图3所示，图中聚类数目C=3，选取聚类中心最大值的簇类作为有效功耗点。

根据聚类选取的有效功耗点，对模乘与模乘之间相关系数进行再次处理，选择有效点位置的相关系数相加，然后再采用聚类，如图4所示。图中，聚类数目C=2，分别为与固定模乘相关性强的簇类及与固定模乘相关性弱的簇类，选取聚类中心最大值的簇类的编号对应模乘为固定模乘相关性强，即数据操作数相同。

实验对幂指数长度1 024 bit的双重掩码模幂算法攻击，示波器采样频率1 MHz，采集功耗曲线为450条进行了攻击实验。并与文献[5,10-11]中提出的算法攻击准确率进行对比，实验结果如图5所示。从图5可以看出，文献[5]提出的一阶CPA对双重掩码的模幂算法攻击准确率低于0.5，无效。而文献[10-11]提出基于阈值设定的二阶CPA攻击方法，在阈值设定最优情况下，文献[11]攻击准确率在曲线达到400条左右，攻击准确率最高接近99%左右，文献[10]的攻击准确率最高70%左右。但是两种算法攻击准确率与攻击者阈值的设定直接相关，攻击准确率依赖攻击者的经验。

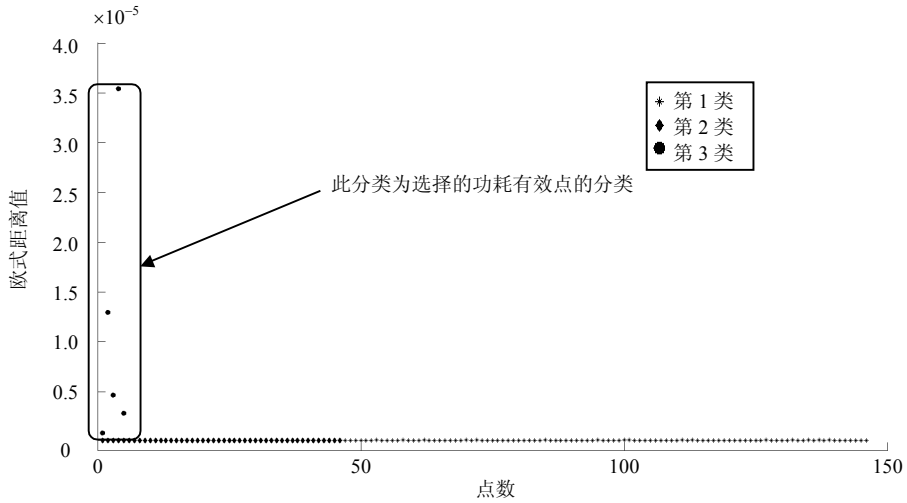

图3 方差欧式聚类分类

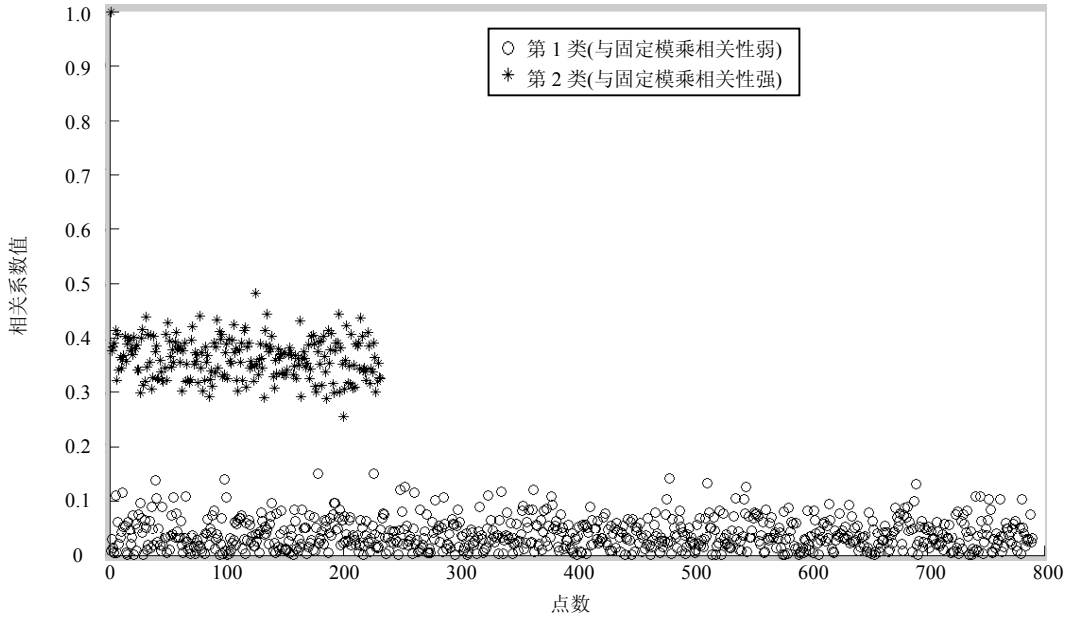

图4 有效功耗点相关系数聚类分类

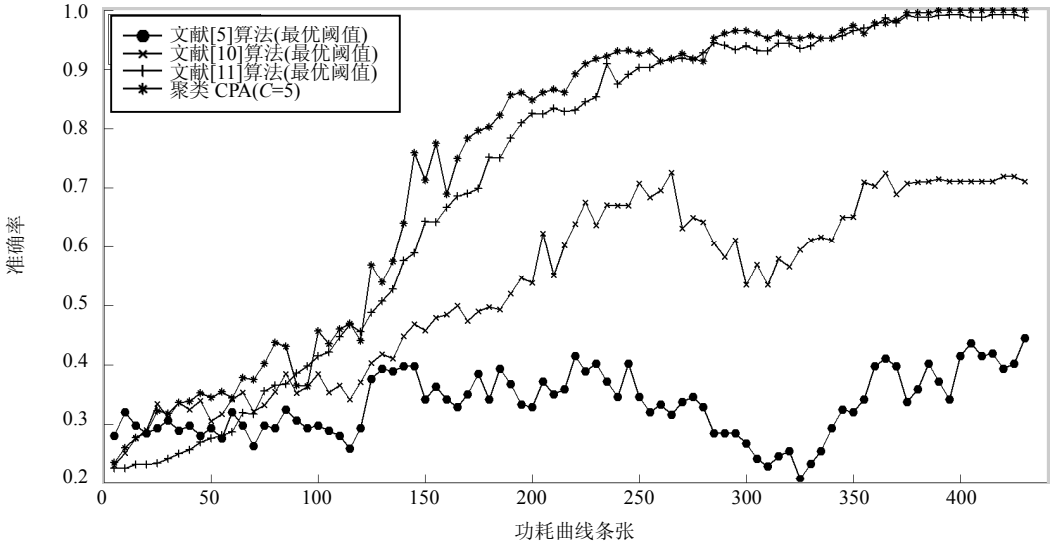

图5 不同CPA攻击算法准确率图

图6给出了4种攻击方法在实验中对阈值调整，3种不同阈值设置攻击结果，从图中可以看出不同阈值攻击准确率差异明显。本文提出的聚类CPA方法，在曲线条数大于400条左右时，攻击准确率收敛于100%。从图6也可以看出，功耗曲线条数接近200，不同聚类数目的攻击准确率接近，当功耗曲线小于200时，聚类数目对攻击准确率有影响，这主要是因为曲线数目小，模乘之间相关性差异小。而k均值聚类算法的分类受聚类数目和聚类中心初始值影响，因而攻击准确率不随曲线条数递增而有波动。另外3种攻击算法总体趋势也是往上增加，功耗曲线达到400条左右，攻击准确率趋于稳定。

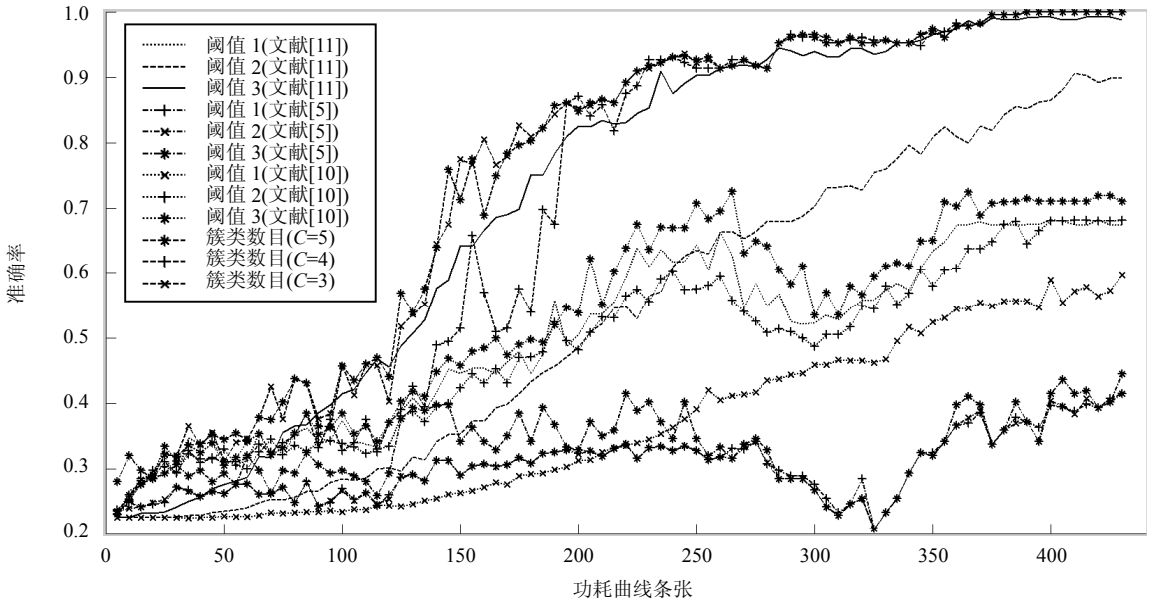

图6　4种CPA攻击算法不同阈值准确率图

4　结 束 语

本文针对真实环境中双重掩码的模幂防范算法的功耗分析攻击问题，在高阶互相关功耗分析算法基础上，提出聚类高阶相关功耗分析改进方法，通过对模乘之间相关系数采用聚类再处理，选取有效功耗点，去除模乘数据有效性低的功耗点，提高双重掩码的模幂算法准确率和智能性。在真实环境下，应用本文的方法，400条功耗曲线以后，攻击准确率稳定在100%。

本文的研究工作得到了成都市科技局惠民研发项目(2016-HM01-00217-SF)的资助，在此表示感谢！

参 考 文 献

[1] KOCHER P, JAFFE J, JUN B. Differential power analysis[C]//Advances in Cryptology-CRYPTO'99. Boston, MA, USA: Springer, 1999: 789-789.

[2] FOUQUE A P, VALETTE F. The doubling attack-why upwards is better than downwards[C]//Proc Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES '03). Berlin, Heidelberg: Springer, 2003: 269-280.

[3] YEN S M, LIEN W C, MOON S J, et al. Power analysis by exploiting chosen message and internal collisions vulnerability of checking mechanism for RSA decryption [C]//Proc Mycrypt'05. Berlin, Heidelberg: Springer, 2005: 183-195.

[4] HOMMA N, MIYAMOTO A, AOKI T, et al. Comparative power analysis of modular exponentiation algorithms[J]. IEEE Transactions on Computer, 2010, 59(6): 795-807.

[5] KOCHER P. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems[C]//Advances in Cryptology-CRYPTO'96. Berlin, Heidelberg: Springer, 1996: 104-113.

[6] WITTEMAN M F, JASPER G J, MENARINI F, et al. Defeating RSA multiply-always and message blinding countermeasures[C]//The Cryptographers' Track at the RSA Conference 2011. San Francisco, CA, USA: [s.n.], 14-18.

[7] HA J C, JUN Chu-hun , PARK J H, et al. A new CRT-RST scheme resistant to power analysis and fault attack[C]// The Third 2008 ICCHIT. [S.l.]: [s.n.], 2008: 351-356.

[8] CLAVIER C, FEIX B, GAGNEROT G, et al. Horizontal correlation analysis on exponentiation[C]//Proc ICICS, Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2010, 6476: 46-61.

[9] BAUER A, JAULMES E, PROUFF E, et al. Horizontal and vertical side channel attacks against secure RSA iImplementations[C]//Proc CT-RSA, Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2013, 7779: 1-17.

[10] KIM H S, KIM T H, YOON J C, et al. Practical second-order correlation power analysis on the message blinding method and its novel countermeasure for RSA[J].

ETRI Journal, 2010, 32(11): 1-4.

[11] WAN Wu-nan, YANG Wei, CHEN Jun. An optimized cross correlation power attack of message blinding exponentiation algorithms[J]. China Communication, 2015, 12(6): 22-32.

[12] BATINA L, GIERLICHS B, LEMKE-RUST K. Differential cluster analysis[C]//CHES, Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2009, 5747: 112-127.

[13] CHEN Ai-dong, XU Son, CHEN Yun, et al. Collision based on chosen message sample power clustering attack algorithm[J]. China Communications, 2013(5): 114-119.

[14] HEYSZL J, IBING A, MANGARD S, et al. Clustering algorithms for non-profiled single-execution attacks on Exponentiations[C]//Smart Card Research and Advanced Applications, Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2014, 8419: 79-93.

[15] PERIN G, IMBERT L, TORRES L, et al. Attacking randomized exponentiations using unsupervised Learning [C]//COSADE. [S.l.]: Springer, 2014, 8622: 144-160.

[16] SPECHT R, HEYSZL J, KLEINSTEUBER M, et al. Improving non-profiled attacks on exponentiations based on clustering and extracting leakage from multi-channel high-resolution EM measurements[C]//The International Workshop on Constructive Side-channel Analysis & Secure Design. [S.l.]: Springer, 2015: 3-19.

[17] BAUER A, JAULMES E. Correlation analysis against protected SFM implementations of RSA[C]//Proc INDOCRYPT, Lecture Notes in Computer Science. [S.l.]: Springer, 2013, 8520: 98-115.

[18] BAUER S. Attacking exponent blinding in RSA without CRT[C]//COSADE, Lecture Notes in Computer Science. [S.l.]: Springer, 2012, 7275: 82-88.

[19] SCHINDLER W. Exclusive exponent blinding may not suffice to prevent timing attacks on RSA[C]// Cryptographic Hardware and Embedded Systems–CHES 2015, Lecture Notes in Computer Science. [S.l.]: Springer, 2015, 9293: 229-247.

编 辑 漆 蓉