文章编号：2096-1618(2016)04-0353-05

针对双重掩码模幂算法的二阶互相关功耗分析攻击

万武南[1]， 陈 俊[2]

(1. 成都信息工程大学信息安全工程学院，四川 成都 610225；2. 成都信息工程大学计算机学院，四川 成都 610225)

摘要：针对一阶互相关功耗分析(cross correlation power analysis，CCPA)攻击方法无法攻击基于底数和指数的模幂算法，提出一种基于方差的二阶互相关功耗分析攻击改进算法。在一阶CCPA算法基础上，对功耗曲线的相关系数进行二次处理，对模乘操作的每个功耗点的相关系数计算方差，然后挑选方差偏差大的功耗点作为有效攻击点，去除掉方差小的功耗点；然后有效攻击点的相关系数相加和分类，有效区分不同指数，实现对底数掩码和指数重编码的模幂防御算法的指数提取。根据实验结果，100条功耗曲线攻击准确率达到99 %。

关 键 词：侧信道攻击；相关功耗分析；方差；模幂运算

中图分类号：TN918.4 **文献标志码**：A

0 引言

模幂算法是大多数公钥密码体制(RSA、ECC(椭圆曲线密码算法)、DH密钥交换等)最重要的运算，并且与密码算法的密钥密切相关，因而模幂算法的安全非常重要。然而，自Kocher等提出的差分功耗分析(differential power analysis，DPA)方法以来，针对密码芯片进行模幂运算泄露的功耗信息，提出了多种破解RSA、ECC等公钥密码算法密钥的信道攻击方法，例如简单功耗分析(simple power analysis，SPA)[1]，DPA[2-3]，相关功耗分析(correlation power analysis，CPA)[4-5]。

目前模幂算法的实现广泛采用的一种称为二元表示法(binary representations，BR)的迭代算法，即所谓的平方-乘积算法，将模幂分解成一系列的平方乘积运算，对于基本的平方和乘积运算，一般采用蒙哥马利(Montgomery)模乘算法实现。为防止密码芯片模幂运算泄露密钥信息，针对模幂运算实现方法提出了静态掩盖、随机掩盖、伪指令、随机伪操作、底数掩码、指数重编码、指数掩码、随机指数RAD(randomized exponentiation)、随机时钟等防范算法。而针对模幂底数的抗功耗攻击算法，M. F. Witteman等[6]提出一种互相关功耗分析方法(CCAs)，通过模乘与模乘之间相关性差异，破译指数。HeeSeok等[7]提出一种二阶相关功耗分析攻击方法，针对底数掩码抵抗功耗攻击模幂算法进行了有效攻击。Akalp Kuzu等[8-10]，则采用互相关功耗分析方法，对Montgomery阶梯实现方法的模幂算法进行攻击。C. Clavier等[11-15]则针对指数掩码，对互相关功耗进行改进，根据底数的汉明重量的相关性，选择攻击点，提出水平相关功耗分析方法。

互相关功耗攻击方法虽然在理论上被证明有效。但在实际的硬件环境下，由于硬件设备噪声，随机延迟，随机时钟的影响，自相关功耗分析方法不能对底数掩码和幂指数重编码的模幂防范方法进行有效攻击[6-14]。因此，在一阶互相关功耗分析攻击基础上，采用方差对功耗曲线相关系数进行二次处理，提出一种二阶互相关功耗攻击方法，实现基于的底数掩码和幂指数重编码的模幂防范算法的幂指数的提取。在搭建真实的8051芯片攻击环境下，验证算法通过不到100条功耗曲线，就能99 %提取幂指数。

1 基于底数和幂指数掩码的模幂算法与相关功耗分析模型

1.1 基于明文掩码的模幂算法

为防止密码硬件设备中的模幂算法遭受SPA和DPA攻击，提出对模幂运算的底数和指数进行随机化的掩码防御方法。在文献[16]中JaeCHeol Ha和ChuHyun Jun.提出一种底数和指数同时掩码的防御方法，如算法1。

Algorithm1 SPA-DPA resistant binary modular exponentiation algorithm of the blinding message

Input $m, d=(d_{n-1}, d_{t-2}, \cdots d_2, d_1, d_0), N, r$
where r is a random number
Output $C=m^d \bmod N$

收稿日期：2016-07-06
基金项目：国家自然科学基金面上资助项目(61572086)；四川省大数据与智慧城市创新开放基金资助项目(RWS-CYHKF-01-20150003)；四川省教育厅重点资助项目(16ZA0212)

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

(2) $T[00]=m\cdot r \bmod N$; $T[01]=m\cdot r^2 \bmod N$;
$T[10]=m^2\cdot r^2 \bmod N$; $T[11]=m^2\cdot r^3 \bmod N$;

(3) $C=T[t_{n-1}s_{n-1}]$;

(4) for $i=n-2$ down to 0

4.1 $C=C\cdot C \bmod N$ —squaring(平方)

4.2 $C=C\cdot T[t_i\ s_i] \bmod N$ —multiplication(乘)

(5) return (C)

在算法 1 中没有直接计算 $m^d \bmod N$,通过采用随机数 r,用于对消息 m 进行掩码。k 为整数,$t=k\cdot\Phi(N)+d-(2^n-1)$,$s=\Phi(N)-d$,$t$ 和 s 对指数 d 进行重编码,其中 $\Phi(N)$ 为 N 的欧拉函数。

1.2 互相关功耗分析攻击模型

在真实环境下,进行功耗曲线的采集要受到设备、环境等多方面的影响,具体的功耗的组成如下:

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

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。

根据公式(1)可知,$a\times b \bmod N$ 和 $c\times d \bmod N$ 的功耗,理论上其中操作 P_{op}不变;P_{data}则跟模乘的两操作数直接相关,若操作数 $a=b$ 和 $c=d$,将产生相似的功耗,P_{data}基本相近,进而使总体的功耗 P_{total}也相近。若输入不相同的操作数(如 $a\neq b$,且 $c\neq d$),根据汉明重量模型,其不同输入的功耗曲线之间没有数据相关性小;若输入两操作数某一操作数相同(如 $a=b$,且 $c\neq d$),则两模乘的 P_{data}之间有较大数据相关性。因此根据汉明重量模型,理论上可通过每个模乘操作的功耗曲线相互之间相关性判断不同模乘之间操作数的特性,即两模乘操作功耗曲线相关系性大,则两模乘操作数据依赖性大;相关性小,则模乘操作数据依赖性小。

算法 1 中,模 4.1 操作为平方,4.2 操作为乘。在 4.2 步模乘操作中,两操作数 C 和 $T[tisi]$,其中操作数 C 一直在动态变化,而另外一个操作数 $T[tisi]$则固定为 4 种值,分别为 $T[00]$、$T[01]$、$T[10]$、$T[11]$。根据相关功耗模型理论可知,模乘数的特性,理论上 4.2 步产生的各模乘功耗曲线可以分成 4 类,可以通过计算 4.2 步各模乘之间相关相关系数不同进行分类。

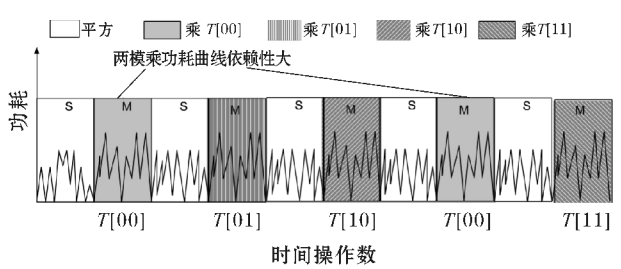

图 1 算法 1 模乘功耗示意图

如图 1 给出算法 1 中 4.1 和 4.2 模乘功耗曲线示意图。其中纵坐标表示各模乘的功耗曲线值,横坐标则表示时间。白色为底的则表示 4.1 步模乘功耗曲线图。带颜色为底则是 4.2 步产生功耗曲线图。

2 基于方差的二阶自相关功耗分析攻击算法

根据互相关功耗模型,理论上来说算法 1 中 4.2 步功耗曲线特性而区分出 4 类不同的操作数 $T[t_is_i]$,从而分析出重编码指数 s 和 t 的值,最终获得幂指数 d。但是在真实环境下,每个模乘操作 $C=C\cdot T[t_is_i] \bmod N$ 是由多个功耗曲线点构成,这些功耗曲线包括了模乘运算的移位,取数等多种操作,并不是每个点的功耗都与模乘运算的两操作数相关。并且由于噪声和功耗曲线对齐问题的干扰,难以细分出跟操作数 $T[t_is_i]$数据直接相关的功耗点。因此,有效挑选与操作数 $T[t_is_i]$相关的功耗点,是算法 1 互相关功耗攻击的成功的关键。根据信噪比理论可知,信号之间的方差越大,则信噪比越高;方差越小的变化,则噪声越大。因此在一阶互相关功耗分析攻击基础上,对各模乘各个点的相关系数求方差,挑选方差值大所对应的相关系数,作为有效攻击点,进行二阶互相关功耗分析,具体处理方法如下。

2.1 功耗曲线预处理

首先输入相同的幂底数和幂指数,获取 r 条功耗曲线,然后对 r 条功耗曲线进行预处理,滤波和对齐,然后截取算法 1 中 4.2 步 $C=C\cdot T[t_is_i] \bmod N$ 的功耗曲线组成 r 条新的功耗曲线,则一条新的功耗曲线则记为

$$T_i=M_{i,0}\,||\,M_{i,1}\,||\,\cdots\,||\,M_{i,n-2}\,||\,M_{i,n-1}$$

每个模乘 $M_{i,j}$ 的功耗曲线有 l 个功耗点,每个模乘记为 $M_{i,j}=[m_{i,j\cdot l},m_{i,j\cdot l+1},\cdots,m_{i,j\cdot l+l-1}]$,因此 r 条新的功耗曲线分块矩阵 $\boldsymbol{Z}$ 定义如下:

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

2.2 二阶互相关功耗分析方法改进

若功耗曲线分块矩阵 $\boldsymbol{Z}$ 中每列的列向量可以用

$\boldsymbol{V}_{j\cdot l+k}$表示:

$$\boldsymbol{V}_{j\cdot l+k}=(m_{0,j\cdot l+k},m_{1,j\cdot l+k},m_{2,j\cdot l+k},\cdots,m_{m-1,j\cdot l+k})^{\mathrm{T}}$$

其中$0\le j<n-1$, $0\le k<l$

则每个模乘对应相同操作点 k 的相关系,可通过公式(2)计算:

$$\rho(\boldsymbol{V}_{j_1\cdot l+k},\boldsymbol{V}_{j_2\cdot l+k})=\frac{\sum_{i=0}^{r-1}(\boldsymbol{V}_{j_1\cdot l+k}\boldsymbol{V}_{j_2\cdot l+k})-\frac{\sum_{i=0}^{r-1}\boldsymbol{V}_{j_1\cdot l+k}\sum_{i=0}^{r-1}\boldsymbol{V}_{j_2\cdot l+k}}{r}}{\sqrt{\left(\sum_{i=0}^{r-1}(\boldsymbol{V}_{j_1\cdot l+k}^2)-\frac{\left(\sum_{i=0}^{n-1}\boldsymbol{V}_{j_1\cdot l+k}\right)^2}{n}\right)\left(\sum_{i=0}^{r-1}(\boldsymbol{V}_{j_2\cdot l+k}^2)-\frac{\left(\sum_{i=0}^{r-1}\boldsymbol{V}_{j_2\cdot l+k}\right)^2}{r}\right)}}\tag{2}$$

二阶互相关功耗分析算法具体如下:

(1)首先根据公式(2),对功耗曲线分块矩阵 $\boldsymbol{Z}$ 的第一个模乘功耗曲线每 1 列与其他模乘功耗曲线每 1 列相系数,即 $\rho(\boldsymbol{V}_{j_1\cdot l+k},\boldsymbol{V}_{j_2\cdot l+k})$,其中 $j_1=0$, $0<j_2<n-1$,则两模乘之间求解相关系数为行向量为

$$[\delta_{j_2\cdot l},\delta_{j_2\cdot l+1},\cdots,\delta_{j_2\cdot l+l-1}]$$

因此功耗曲线分块矩阵 $\boldsymbol{Z}$ 的第一个模乘功耗曲线与其他模乘功耗曲线相关系数相关系数矩阵记为 *Cof_M*:

$$Cof\_M=\begin{bmatrix}\delta_0 & \delta_1 & \cdots & \delta_{l-2} & \delta_{l-1}\\ \delta_l & \delta_{l+1} & \cdots & \delta_{2l-2} & \delta_{2l-1}\\ \vdots & \vdots & \cdots & \vdots & \vdots\\ \delta_{(n-3)l} & \delta_{(n-3)l+1} & \cdots & \delta_{(n-3)l+l-2} & \delta_{(n-3)l+l-1}\\ \delta_{(n-2)l} & \delta_{(n-2)l+1} & \cdots & \delta_{(n-2)l+l-2} & \delta_{(n-2)l+l-1}\end{bmatrix}$$

(2) 然后计算相关系数矩阵 *Cof_M* 中每列的方差值,每列方差值记为 v_i, $0\le i\le l-1$,则矩阵 *Cof_M* 中 l 列求方差值记为: $\boldsymbol{V}=[v_0,v_1,\cdots,v_{l-2},v_{l-1}]$。

(3)根据信噪比原理,方差大,则模乘操作的功耗点处信噪比高;方差小,则功耗点为噪声。因此选取 v_i 中方差值明显较大的值 x 个点作为有效功耗点,选取点的位置记为 $S=[u_0,u_1,\cdots,u_{x-2},u_{x-1}]$

(4)根据选取有效点,然后矩阵 *Cof_M* 中每一行选取点的和,即

$$s_j=\sum_{i=0}^{x-1}\delta_{u_i}\quad \text{其中}\ 0\le j\le n-2$$

(5)然后根据阈值 s_j 分成两类,即把 $n-1$ 模乘分成不同两类, s_j 大于阈值,对应模乘则假定操作数 $T[t_i\ s_i]$是相同。则 s_j 小于阈值的其余模乘重新构成新的 $\boldsymbol{M}$ 矩阵,则返回步骤(1),重新进行分类,直到分成 4 类为止。

根据上述步骤,$n-1$ 个模乘分乘 4 类,每类可猜测为 $T[00]$、$T[01]$、$T[10]$、$T[11]$,t 和 s 经过自相关功耗分析总共有 16 种取值,后续攻击则可以 16 种取值分别代入模幂运算,得到重编码 t 和 s 的值,然后推算出幂指数 d 值。

3　模幂二阶相关功耗分析实验结果

3.1　功耗测试环境

实验是在自主开发的功耗采集和分析平台上对 8051 芯片进行测试,整个功耗分析攻击平台的硬件配置主要有:工作站、数字采样示波器(Tektronix PPO4032)、直流电源、接口板及读卡器。

功耗采集和分析平台中,工作站与示波器网线相连,对示波器与接口板进行设置。发送指令或者数据到接口板,然后发送给读卡器,读卡器驱动智能卡工作,接口板接收返回数据。示波器采用 Tektronix PPO4032,接收指令采集功耗曲线和触发信号。功耗分析攻击实验平台的抽象框图如图 2 所示。算法 1 功耗采集中示波器采用频率通常设置为1 M,并在算法 1 的开始和结束设置示波器采取触发点,示波器采集算法 1 完整的功耗曲线, 4.1 和 4.2 两步的模乘运算通过曲线预处理进行截取并进行分析。

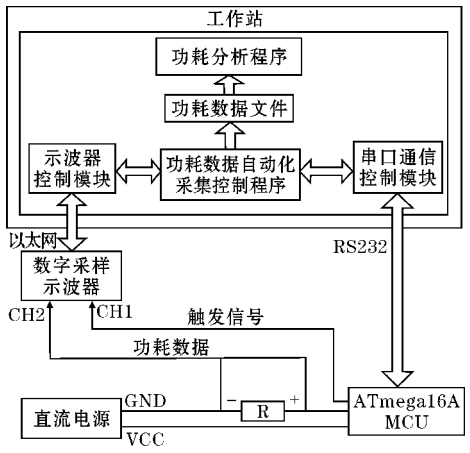

图 2　功耗采集平台

3.2 实验数据处理

在图 2 的功耗采集平台上,示波器采样频率设置 1 M,采集智能卡上算法 1 的功耗曲线如图 3 所示。

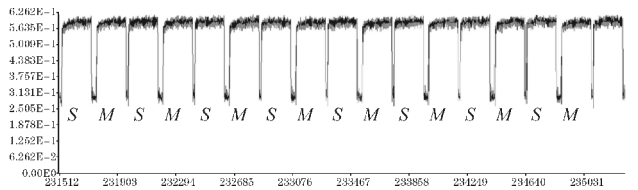

图 3 算法 1 模乘功耗曲线波形图

图 3 是算法 1 中 8 bits 的模乘功耗曲线波形图,其中 4.1 步为平方运算(S),4.2 步为模乘运算(M)。首先对功耗曲线进行预处理,把算法 1 中的4.2步的模乘运算的功耗曲线进行截取,重新构造,构成出功耗曲线分块矩阵 $\boldsymbol{Z}$。然后再根据 1.2 小节,求解相关系数 Cof_M,第一个模乘的相关系数如图 4 所示。

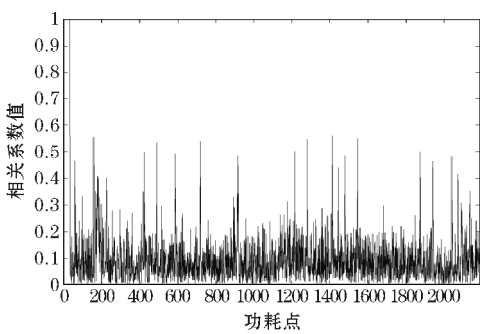

图 4 与第一个模乘的相关系数图

计算各模乘对应点的方差,如图 5 所示。图中横坐标表示单个模乘操作点数,即 l=33,纵坐标为方差值。

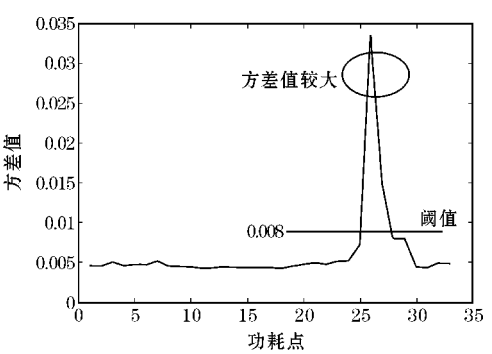

图 5 各模乘操作点相关系数方差

根据信噪比原理,功耗点方差大,则模乘操作的功耗点处信噪比高;方差小,则功耗点可看作为噪声。因此,从图 5 可以看出,在功耗点为 26,27,28 三处方差值明显增大,因此方差阈值可设置大约为 0.008,选取 26,27,28 功耗点为有效功耗点。然后对各模乘相应 3 点对应的相关系数相加,得到各模乘有效功耗点的相关系数值和,如图 6 所示。

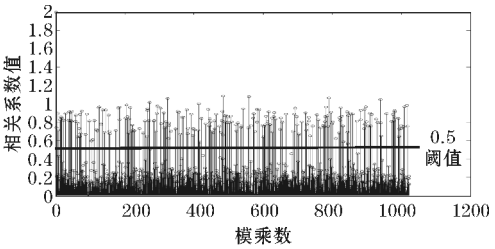

图 6 有效点模乘相关系数值和

图 6 中,根据 1.2 小节可知,根据相关系数和值的大小可分为两类:一类模乘功耗点相关系数高,模乘与第一个模乘的操作数 $T[t_i s_i]$ 是相同;模乘功耗点相关系数低,则第一个模乘的操作数 $T[t_i s_i]$ 是不同。阈值设定大于0.5分为 2 类,推出重编码 s 和 t,然后由 t 和 s 由此推出幂指数 d。

依照上述实验步骤,对长度 1024 比特的 1000 个不同幂指数 d 进行了攻击,分成采用示波器采频率 1 MHz,2.5 MHz,采集功耗曲线为 50 条、100 条、300 条进行了攻击实验,并与模乘所有功耗点相关系数和方法[8]准确率进行对比,实验结果如表 1。

表 1 实验结果

采样频率/MHz	曲线条数	文献[8]算法准确率/%	新攻击准确率/%
1	50	78	96.3
2	50	80	97
1	100	85.3	99
2.5	100	86	99.79
1	300	88	99.3
2.5	300	93.2	99.9

从表 1 可以看出,在相同采样频率和功耗曲线样本条数下,与文献[8]攻击方法相比,提出基于方差的二阶互相关功耗分析攻击改进算法攻击准确率更高。而采样频率和功耗曲线条数增加,可以提高攻击准确率。

4 结束语

针对真实环境中底数和指数同时防御的模幂算法功耗分析攻击问题,在一阶互相关功耗分析算法基础上,提出基于方差的二阶功耗自相关功耗分析改进方法,通过对模乘之间相关系数采用方差,选取有效功耗点,去除模乘功耗曲线噪声大的点,提高对底数和指数同时防御的模幂算法攻击效率。在真实环境下,应用文中方法,100 条功耗曲线,可以小样本99.9 % 准确率。

致谢:感谢中央高校基本科研业务费项目对本文的支持

参考文献:

[1] Kocher P, Jaffe J, Jun B. Differential power analysis[C]. Advances in Cryptology-CRYPTO´99, California, USA: Springer, 1999: 789-789.

[2] A P Fouque, F Valette, The Doubling Attack—WhyUpwards is Better Than Down wards, Proc. Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES '03), 2003: 269-280.

[3] S M Yen, W C Lien, S. J. Moon, et al. Power Analysis by Exploiting Chosen Message and Internal Collisions-Vulnerability of Checking Mechanism for RSA-Decryption[C], Proc. Mycrypt '05, 2005: 183-195.

[4] Naofumi Homma, Atsushi Miyamoto, Takafumi Aoki, et al. Comparative power analysis of modular exponentiation algorithms[J]. IEEE Transations 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, California, USA: Springer, 1996: 104-113.

[6] M F Witteman, Jasper G J van Woudenberg, Federico Menarini. Defeating RSAMultiply-Always and Message Blinding Countermeasures[C]. The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, 2011, 14-18.

[7] HeeSeok Kim, Tae Hyun Kim, Joong Chul Yoon, et al. Practical Second-Order Correlation Power Analysis on the Message Blinding Method and Its Novel Countermeasure for RSA[J]. ETRI Journal, 2010, 32(1).

[8] E Akalp Kuzu, B Soysal, M Sahinoglu, et al. New cross correlation attack methods on the Montgomery Ladder implementation of RSA [C]. Advance Computing Conference (IACC), 2013 IEEE 3rd International, 2013: 138-142.

[9] E Akalp Kuzu, A Tangel. All bits cross correlation attack on the Montgomery Ladder implementation of RSA[C]. 18th International Conference on Digital Signal Processing(DSP), 2013.

[10] E Akalp Kuzu, A Tangel. A new style CPA attack on the ML implementation of RSA[C]. Computer Science and Engineering Conference (ICSEC), 2014.

[11] C Clavier, B Feix, G Gagnerot, et al. Horizontal Correlation Analysis on Exponentiation [C]. Proc. ICICS, ser. Lecture Notes in Computer Science, 2010, 6476: 46-61.

[12] A Bauer, E Jaulmes, E Prouff J Wild, et al. Side-Channel Attacksagainst Secure RSA Implementations[C]. Proc. CT-RSA, ser. Lecture Notes in Computer Science, 2013, 7779: 1-17.

[13] A Bauer, E Jaulmes. Correlation Analysis against Protected SFM Implementations of RSA [C], Proc. INDOCRYPT, ser. Lecture Notes in Computer Science, 2013, 8520: 98-115.

[14] S Bauer. Attacking Exponent Blinding in RSA without CRT[C]. COSADE, ser. Lecture Notes in Computer Science, 2012, 7275: 82-88.

[15] Werner Schindler. 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, 2015, 2523: 229-247.

[16] JaeCheol Ha, ChuHun Jun, JeaHoon Park, et al. A new CRT-RST Scheme Resistant to Power Analysis and Fault Attack[C]. InThe third 2008 ICCHIT, 2008: 351-356.

A Second Order Cross Correlation Power Analysis Attack on Double Blinding Exponentiation Algorithms

WAN Wu-nan[1], CHEN Jun[2]

(1. College of Information Security Engineering, Chengdu University of Information Technology, Chengdu 610225, China; 2. College of Computer Science, Chengdu University of Information Technology, Chengdu 610225, China)

Abstract: According to the fact that the countermeasures for modular exponentiation algorithms based on the message blinding methods and the exponent blinding methods secure against the first order cross correlation power analysis (CCPA) attacks. An improved algorithm of a second order cross correlation power attacks based on variance is proposed in the paper, and the bits of the secret exponent of the message blinding methods and the exponent blinding methods can be defeated. On the basis of CCPA, we use the variation of correlation coefficients for each power point of every modular multiplication for the improved algorithm. Then the power points are selected as effective attack points, while the variance value is a bigger value in the power points, and other power points of the smaller variance value are discarded for reducing the noise. We can effectively distinguish the exponent bit through summing the value of correlation coefficients and classifying. The results of experiments show that recognition rate increases to 99 % with 100 power traces.

Key words: side channel attack; correlation power analysis; variance; module exponentiation