doi:10.3969/j.issn.1000-436x.2013.z1.020

基于 Montgomery 算法安全漏洞的 SPA 攻击算法

甘刚，王敏，杜之波，吴震
（成都信息工程学院 网络工程学院，四川 成都 610225）

摘 要：公钥密码体制的算法大多基于有限域的幂指数运算或者离散对数运算。而这些运算一般会采用 Montgomery 算法来降低运算的复杂度。针对 Montgomery 算法本身存在可被侧信道攻击利用的信息泄露问题，从理论和实际功耗数据 2 方面分析了 Montgomery 算法存在的安全漏洞，并基于该漏洞提出了对使用 Montgomery 算法实现的模幂运算进行简单能量分析（SPA, simple power analysis）攻击算法。利用该算法对实际模幂运算的能量曲线进行了功耗分析攻击。实验表明该攻击算法是行之有效的。
关键词：模幂运算；侧信道攻击；简单能量分析攻击；Montgomery 算法
中图分类号：TP309.1,TN492 **文献标识码**：A **文章编号**：1000-436X(2013)Z1-0156-06

Simple power analysis attack against cryptosystems based on Montgomery algorithm

GAN Gang, WANG Min, DU Zhi-bo, WU Zhen
(Network Engineering Department, Chengdu University of Information Technology, Chengdu 610225, China)

Abstract: The Montgomery algorithm is widely used to reduce the computational complexity of large integer modular exponentiation. The SPA (simple power analysis) attacks against public-key cryptosystems based on Montgomery algorithm implementation were presented by exploitation of the inherent security vulnerability which that sensitive information leakage could be used by side-channel attack. The chosen-message SPA attacks were focused on, which enhance the differences of operating wave-forms between multiplication and squaring correlated to the secret key by using the input of particular messages. In particular, a SPA attack against RSA cryptosystem was showed based on large integer modular exponentiation. The results show that the attack algorithm is correct and effective.
Key words: modular exponentiation; side-channel attack; simple power analysis; Montgomery algorithm

1 引言

随着电路等分析技术的发展，对于密码破解不再单纯地停留在数学手段，其中利用硬件密码设备在运行密码算法时产生的能量波形，结合密码学和统计学原理等，分析和破译密钥信息的攻击方式[1,2]就是所谓的能量分析攻击，能量分析攻击分为简单能量分析攻击和差分能量分析攻击（DPA, differential power analysis）2 类，自从能量分析攻击方法提出后，看似牢不可破的密码算法表现出其脆弱的一面，成为当今密码学领域研究的重点。

目前国内外针对有限域上幂指数和离散对数的公钥密码体制的能量分析攻击大都基于模幂运算进行研究[3~7]，主要研究模幂运算存在的信息泄露，以及对模幂运算的能量分析攻击[1,4~6,9,10]和防范能量分析攻击的改进[3,7,11]，而对模乘运算的信息泄

收稿日期：2013-06-14
基金项目：“十二五”国家密码发展基金资助项目（MMJJ201101022)；四川省科技支撑计划基金资助项目（2011GZ0170)；四川省教育厅重点科研基金资助项目（13ZA0091）
Foundation Items: “The 12th Five-Years” National Cryptogram Development Fund(MMJJ201101022); The Science and Technology Support Program of Sichuan Province(2011GZ0170); Education Department Key Scientific Research Projects of Sichuan Province(13ZA0091)

露以及模乘运算导致模幂运算信息泄露的研究较少。在实际应用中，模乘运算是模幂运算的基础，模乘运算的安全性在一定程度上也是模幂运算的安全性，因此为研究模幂运算的安全性，有必要研究模乘运算的安全性。

本文从模幂运算和 Montgomery 算法原理入手，具体分析了硬件实现的 Montgomery 算法存在信息泄露的问题，提出了基于 Montgomery 算法安全漏洞的 SPA 攻击算法，并给出实测分析攻击结果，对比验证了该方法在本文提到的 Montgomery 算法安全漏洞存在的前提条件下，对任意底数的 SPA 和 DPA 更有效。

2　模幂算法的快速 BR 算法

2.1　模幂运算简介

基于大整数难分解和离散对数的公钥密码体制，其核心运算都是模幂运算，其数学形式如式（1）所示。

$$C = M^k \bmod N \tag{1}$$

模幂运算的实现。目前广泛采用一种称为二元表示法(BR, binary representations)[7]的迭代算法，该算法又被称为“平方和乘积(square and multiply)”算法[12]，即将模幂运算分解成一系列的平方剩余和模乘运算。

BR 算法的具体实现形式。根据对指数 e 不同的扫描方向，分为从左至右(L-R)、从右至左(R-L)等多种[7]，而事实上它们并没有本质的区别，这里只介绍从右至左和从左至右 2 种扫描方式。

令

$$k = [k_{n-1}, k_{n-2}, \cdots, k_0] \tag{2}$$

其中，n 为 k 的二进制长度。

从左到右的 BR 算法如图 1 所示。

算法 1　LR-BR 算法
输入：正整数 M，e，N
输出：$C = M^k \bmod N$
1)　$C \leftarrow 1$
2) For i from $n-1$ downto 0 do
①　$C \leftarrow C^2 (\bmod N)$
②　If $k_i = 1$, then $C \leftarrow C*M (\bmod N)$
3) Return C

图 1　LR-BR 算法步骤

从右到左的 BR 算法如图 2 所示。

算法 2　RL-BR 算法
输入：正整数 P，K，N
输出：$C = M^k \bmod N$
1)　$C \leftarrow 1$
2)For i from 0 upto $n-1$ do
①　If k_i =1, then $C \leftarrow C*M (\bmod N)$
②　$M \leftarrow M^2 (\bmod N)$
3) Return C

图 2　RL-BR 算法步骤

2.2　基于 Montgomery 模乘的 BR 算法快速实现

从 BR 算法中可看出，模幂运算中的主要开销在于大数模乘运算，因此在实际应用中，经常利用 Montgomery 模乘器[13]来提高模幂运算的效率。

二进制 Montgomery 模乘算法步骤如图 3 所示。

算法 3　二进制 Montgomery 模乘算法
输入：正整数　$A, B, N, R = 2^k, N' = -N^{-1} \bmod R$
输出：$MM(A, B, N) = A \cdot B \cdot R^{-1} \bmod N$
1)　$T \leftarrow A \cdot B$
2)　$U \leftarrow (T + ((T \cdot N') \bmod R)) / R$
3) if　$(U \geqslant N)$, then　$U \leftarrow U - N$
4) Return U

图 3　二进制 Montgomery 模乘算法步骤

使用 Montgomery 实现的 L-R 算法如图 4 所示。

算法 4　使用 Montgomery 实现的 L-R 算法
输入：正整数 M，e，N
输出：$C = M^k \bmod N$
1)　$C \leftarrow 1$
2)　$C' \leftarrow MM(C', R^2, N); M' \leftarrow MM(M, R^2, N)$
3) For i from $n-1$ downto 0 do
①　$C' \leftarrow MM(C', C', N)$
②If $k_i = 1$, then　$C' \leftarrow MM(C', M', N)$
4)　$C \leftarrow MM(C', 1, N)$
5) Return C

图 4　使用 Montgomery 实现的 L-R 算法步

使用 Montgomery 实现的快速 R-L 算法如图 5 所示。

算法 5　使用 Montgomery 实现的 R-L 算法
输入：正整数 P，K，N
输出：$C = M^k \bmod N$
1)　$C \leftarrow 1$
2)　$M' \leftarrow MM(M, R^2, N)$
3) For i from 0 upto $n-1$ do
①　If $k_i = 1$ then $C \leftarrow MM(C, M', N)$
②　$M' \leftarrow MM(M', M', N)$
4) Return C

图 5　使用 Montgomery 实现的 R-L 算法步骤

3 Montgomery 实现漏洞分析和基于该漏洞对 BR 算法的 SPA 攻击算法

3.1 对 Montgomery 算法的漏洞分析

图 3 算法主要用来解决公钥密码体制中大整数运算问题，因此，算法中的乘法、加法和减法等运算均需要大整数的算法完成操作，所以算法 3 由硬件实现时，各种运算均需要一定数量的 clock 才能完成相应的运算操作，因此在采集的 BR 算法能量波形上，从波形长度（时间）上可以清晰地看到 Montgomery 模乘的能量轮廓，以 1 024 bit（字长为 32 bit）的 LR-BR 算法为例，其模幂运算能量波形如图 6 所示，下文中所有能量波形均采用相同的坐标系，从图 6 中可以清晰地看出 Montgomery 模乘的能量轮廓。

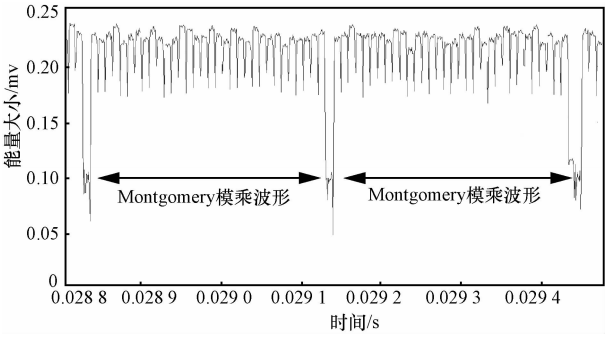

图 6 LR-BR 算法能量波形

从运算操作的执行过程来看，无论 A、B 和 N 为怎样的数据，算法 3 中的第 1）步和第 2）步都是必须要执行的，但是算法 3 中的第 3）步则存在例外，这是因为：

1) 当 $U < N$ 时，算法不执行 $U \leftarrow U - N$ 操作；

2) 当 $U > N$ 时，算法必须执行 $U \leftarrow U - N$ 操作。

所以，不同的数据 A、B 和 N 就会导致算法 3 第 3)步不同的操作，此外由于 $U \leftarrow U - N$ 是大整数运算，需大整数的减法算法才能完成运算。因此当选择不同的数据 A、B 和 N 时，有无 $U \leftarrow U - N$ 运算操作，就会导致硬件实现的 Montgomery 模乘产生不同的能量波形，如果选择的数据 A、B 和 N 使 Montgomery 模乘算法退出时进行 $U \leftarrow U - N$ 操作，就会导致能量波形含有一个台阶状拖尾波形，如图 7 所示，反之则无，如图 8 所示。

从图 7 和图 8 的波形对比不难看出，不同的 Montgomery 运算数据将导致硬件实现的蒙哥马利算法产生不同的能量波形有无台阶状拖尾波形，因此通过选择特殊的运算数据可以人为控制硬件实现的蒙哥马利算法产生不同的能量波形。

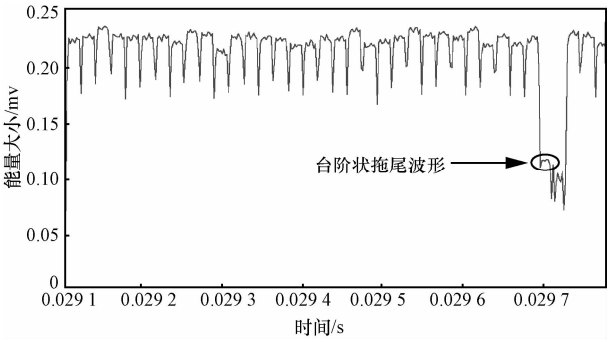

图 7 含有台阶状拖尾波形的 Montgomery 能量波形

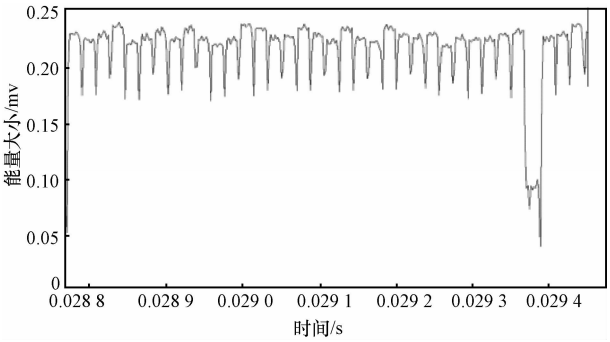

图 8 不含台阶状拖尾波形的 Montgomery 能量波形

3.2 基于 Montgomery 算法漏洞的 SPA 攻击实现算法

正如上文所述，既然硬件实现的 Montgomery 算法存在信息泄露的问题，那么就可以利用该问题对使用 Montgomery 实现的 BR 算法进行 SPA 攻击。通过选择特殊的运算数据，使 BR 算法在计算幂指数“1”和幂指数“0”时，模乘运算产生不同的能量，即当 BR 算法在计算幂指数“1”时，由 Montgomery 算法实现的模乘运算含有最后一步的 $U \leftarrow U - N$ 操作，产生的能量波形如图 7 所示，当 BR 算法在计算幂指数“0”时，由 Montgomery 算法实现的模乘运算无最后一步的 $U \leftarrow U - N$ 操作，产生的能量波形如图 8 所示，根据这 2 种波形的差异（有无台阶状拖尾波形），即可判断当前 BR 算法进行运算的幂指数数据，进而可以得出以模幂运算为核心的公钥密码算法的密钥。

实施 SPA 的关键点为需要选择特殊的 Montgomery 运算数据，由算法 4 和算法 5 可知，该数据即为 M，使 BR 算法在计算幂指数“0”和幂指数“1”时，导致 Montgomery 运算的最后一步运算（if 条件分支）进行不同的操作，所以构造 Montgomery 模乘

测试例生成器算法，该算法如图 9 所示，产生特殊的 M。

算法 6　Montgomery 模乘测试例生成器算法

（U, $Flag$）=$TMM(A, B, N)$

输入：（A, B, N）

输出：（U, $Flag$）

U 返回 Montgomery 模乘结果，$Flag$ 返回是否进行减操作

步骤：

1) $Flag$=0;T=A×B

2) U= [T+(T×N' mod R)×N]/R

3) if (U≥N) U=U−N; $Flag$=1

4) Return U, $Flag$

图 9　LR-BR 算法步骤

通过选择特殊的 M 便可以对使用 Montgomery 实现的 LR-BR 算法进行 SPA 攻击，具体攻击算法如图 10 所示。

算法 7　对使用 Montgomery 实现的 LR-BR 算法进行 SPA 的攻击算法

输入：（K_{s-1}, K_{s-2},…, K_{s-l})

输出：K_{s-l-1}

1) 随机生成一个 M

2) 计算前 l 轮结束后 C_l'的值

3) 计算 X=$MM(C_l', C_l', N)$; //得到循环体内第一个 Montgomery 模乘结果

4) 计算(X_1, $Flag_1$)=$TMM(X, M', N)$; //密钥为 1 时的计算

5) 计算(X_0, $Flag_0$)=$TMM(X, X, N)$; //密钥为 0 时的计算

6) 如果 $Flag_1$==$Flag_0$ 则回到步骤 1)

7) 用 M 作为测试输入，获得波形

8) 找到对应位置，观察波形

9) 如果波形中有拖尾部分，则 W=1，否则 W=0

10) 如果 W==$Flag_1$, 则对应位置的密钥 K_{s-l-1}=1;
否则对应位置的密钥 K_{s-l-1}=0

11) 返回 K_{s-l-1}

图 10　LR-BR 算法步骤

已知从高到低的前 l bit 密钥序列（K_{s-1}, K_{s-2},…, K_{s-l}），攻击第 l+1 位 K_{s-l-1} 的值。

对使用 Montgomery 实现的 RL-BR 算法进行 SPA 攻击，具体的攻击算法如图 11 所示。

已知从高到低的前 l bit 密钥序列（K_{s-1}, K_{s-2},… K_{s-l}），攻击第 l+1 位 K_{s-l-1} 的值。

算法 8　对使用 Montgomery 实现的 RL-BR 算法进行 SPA 的攻击算法

输入：（K_{l-1}, K_{l-2},…,K_0), N

输出：K_l

1) 随机生成一个 M

2) 计算前 l 轮结束后 C_l'、M_l'的值

3) 计算(X_1, $Flag_1$)=$TMM(C_l', M_l', N)$; //密钥为 1 时的计算

4) 计算(X_0, $Flag_0$)=$TMM(M_l', M_l', N)$; //密钥为 0 时的计算

5) 如果 $Flag_1$==$Flag_0$ 则回到步骤 1)

6) 用 M 作为测试输入，获取波形

7) 找到对应位置，观察波形

8) 如果波形中有拖尾，则 W=1，否则 W=0

9) 如果 W==$Flag_1$, 则对应位置的密钥 K_l=1;
否则对应位置的密钥 K_l=0;

10) 返回 K_l

图 11　RL-BR 算法步骤

4　对由 Montgomery 实现的 BR 算法的实测能量分析攻击

以 SPA 攻击使用 Montgomery 实现的 LR-BR 算法为例，详述攻击过程，SPA 攻击使用 Montgomery 实现的 RL-BR 算法和该过程类似，本实验采用的硬件密码设备为 Infineon 智能卡。智能卡上运行的 BR 算法为算法 4，被攻击的幂指数为 k=[1011]$_2$，k 的长度 s=4。

4.1　对任意底数 M 的 SPA

在底数 M 无约束的情况下，存在无台阶状拖尾波形的情况，如图 12 所示，由于智能卡运行的是算法 4，所以应根据左边第 2 个模乘来判断当前运行的幂指数，第 2 个模乘放大后的图形如图 13 所示，该波形无图 7 中所指的台阶状拖尾波形，因此在该情况下，使用 SPA 无法攻击出指数比特信息，且无法对结果做定性和定量分析。

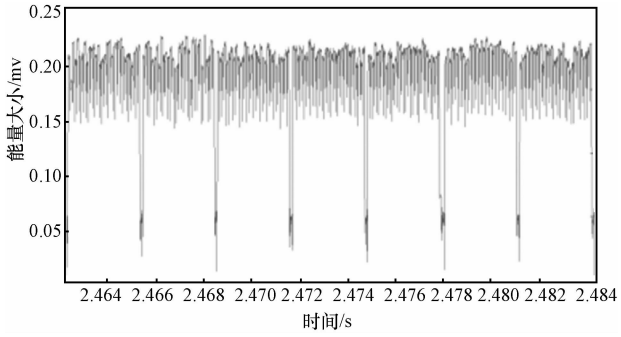

图 12　任意底数 M 的 RL-BR 算法能量波形

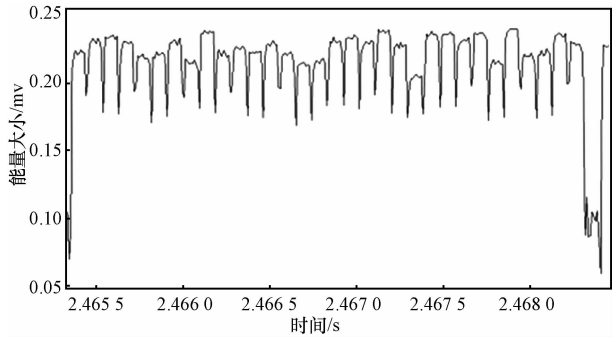

图 13 任意底数 MRL-BR 算法中第 2 个模乘放大后的能量波形

4.2 对选择底数 *M* 的 SPA

根据算法 7 产生特殊的数据 M_1，使 $Flag_1$=True 且 $Flag_0$=False，用 M_1 作为测试输入，采集能量波形数据，幂指数 k 运行时对应的能量波形如图 14 所示。

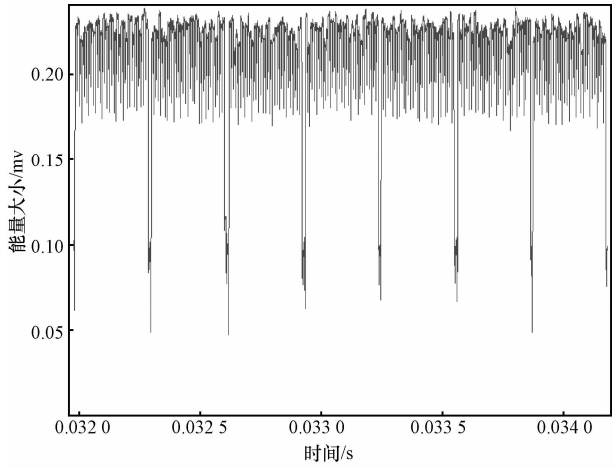

图 14 RL-BR 算法能量波形

由于智能卡运行的是算法 4，所以在图 14 中，左边第 2 个模乘即为算法 7 中第 8)步所指的观察波形，如图 15 所示。

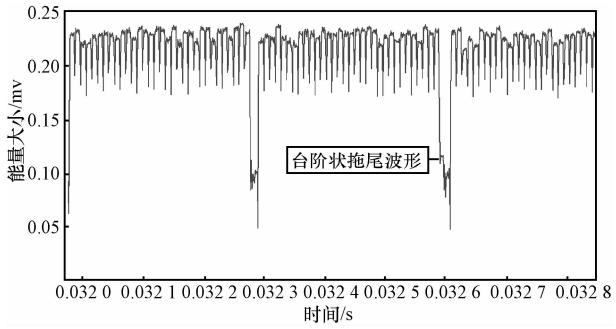

图 15 被攻击幂指数对应的 Montgomery 算法能量波形

从图 15 中可以观察出，该波形中存在图 7 中所指的台阶状拖尾波形，故猜测当前被攻击的幂指数为 1，即 $k_1=[1]_2$。

按照算法 7 所述，依次类推，就可以攻击出 k 的剩余比特位的信息，且攻击出完整幂指数所需要的曲线条数是由幂指数二进制长度决定的，因此攻击出完整的 k 共需能量波形曲线条数为 4。

4.3 DPA

根据 DPA 原理[1]，对智能卡实施 DPA，底数 M 随机选择，能量波形曲线条数和对选择底数 M 的 SPA 曲线条数一样为 4，对曲线不做任何处理。由算法 4 可知，当幂指数为 0 时，智能卡进行 $C' \leftarrow MM(C',C',N)$ 模乘，当幂指数为 1 时，智能卡要进行 $C' \leftarrow MM(C',C',N)$ 和 $C' \leftarrow MM(C',M',N)$ 2 个模乘，根据二者不同操作的差异，选择 DPA 攻击波形，例如攻击 k 的首比特，应选择图 12 中的左边第 2 个波形，攻击结果如图 16 所示，图中无明显的尖峰波形，因此在这种情况下，DPA 无法攻击出幂指数信息。

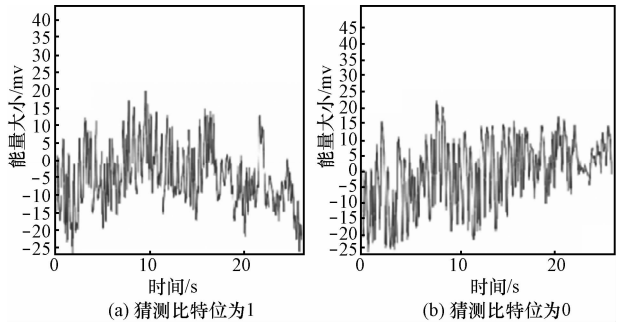

图 16 DPA k 首比特结果

增加曲线条数，采集智能卡上运行的能量波形曲线 8 000 条[11]，且对曲线做低通滤波和对齐处理，仍然攻击 k 的第一位比特，其攻击结果如图 17 所示。

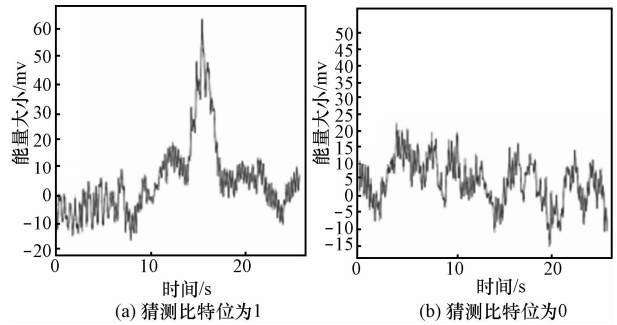

图 17 DPA k 首比特结果

从图 16 中可以看出，当猜测比特位为 1 时，功耗曲线尖峰非常明显，因此 k 首比特为 1。

4.4 性能对比

3 种攻击方法的性能对比如表 1 所示。

表 1　　3 种攻击方法的性能对比

攻击方法	曲线条数	成功率	其他操作
对任意底数 M 的 SPA	无法定量分析	无法保证 100%	无
对选择底数 M 的 SPA	幂指数二进制长度	100%	无
DPA	>8 000	100%	虑波处理，对齐操作

由表 1 可知，在对曲线的数量和其他操作要求上，对选择底数 M 的 SPA 要优于 DPA，成功率上要优于对任意底数 M 的 SPA。

5　结束语

本文对 Montgomery 算法存在的信息泄露问题进行了详细的分析，并通过采集实际的 Montgomery 算法的能量波形验证了该安全问题的存在。

基于该问题，本文提出了对使用 Montgomery 实现的 BR 算法的 SPA 攻击算法，并通过实验验证了该攻击算法对基于 Montgomery 算法的模幂运算进行 SPA 攻击的可行性，同时验证了该方法优于对任意底数 M 的 SPA 和 DPA。

参考文献：

[1] KOCHER P, JAFFE J, JUN B. Differential power analysis[A]. Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology[C]. 1999. 388-397.

[2] P KOCHER C. Timing attacks on implementations of diffie-hellman, RSA, DSS, and other systems[A]. Advances in Cryptology-CRYPTO' 96, Lecture Notes in Computer Science[C]. 1996. 104-113.

[3] 韩军, 曾晓洋, 汤庭鳌. 基于时间随机化的密码芯片防攻击方法[J]. 计算机工程, 2007, 33(2):6-8.
HAN J,ZENG X Y,TANG T A. Modeling timing randomization in cryptographic chip against power analysis attack[J]. Computer Engineering, 2007, 33(2):6-8.

[4] 成为, 谷大武, 郭筝等. 一种针对 RSA-CRT 的功耗分析攻击方法[J]. 通信技术, 2011, 6(44):123-125.
CHENG W, GU D W, GUO Z, *et al*. A power analysis attack against RSA-CRT[J]. Communications Technology,2011, 6(44):123-125.

[5] 吴震, 陈运, 陈俊等. 真实硬件环境下幂剩余功耗轨迹指数信息提取[J]. 通信学报, 2010, 31(2):17-21.
WU Z, CHEN Y, CHEN J, *et al*. Exponential information's extraction from power traces of modulo exponentiation implemented on FPGA[J]. Journal on Communications, 2010, 31(2):17-21.

[6] ACICMEZ O, SEIFERT J P, KOC C K. Predicting Secret Keys Via Branch Prediction[R]. Topics in Cryptology-CT-RSA, 2007.

[7] ACIICMEZ O, KOC C K, SEIFERT J P. On the Power of Simple-Branch Prediction Analysis[R]. Cryptology ePrint Archive, 2006.

[8] 李志强, 严迎建, 段二鹏. 差分能量攻击所需样本数量研究[J]. 计算机工程, 2013, 38(24):128-132.
LI Z Q, YAN Y J, DUAN E P. Research on sample amounts needed by differential power attack[J]. Computer Engineering, 2013, 38(24):128-132.

[9] KADLOOR S, KIYAVASH N, VENKITASUBRAMANIAM P. Mitigating timing side channel in shared schedulers[J]. arXiv preprint arXiv:1302.6123, 2013,

[10] BAUER A, JAULMES E, PROUFF E, *et al*. Horizontal and vertical side-channel attacks against secure RSA implementations[A]. Topics in Cryptology-CT-RSA 2013 Springer Berlin Heidelberg[C]. 2013. 1-17.

[11] PROUFF E, RIVAIN M. Masking against side-channel attacks: a formal security proof[A]. Advances in Cryptology-EUROCRYPT 2013 Springer Berlin Heidelberg[C]. 2013. 142-159.

[12] 杜之波, 陈运. 防范边信道攻击的逆伪操作实现算法[J]. 计算机工程, 2010, 36(3):131-133.
DU Z B, CHEN Y. Implementation algorithm of pseudo modular inversion secure against side channel attack[J].Computer Engineering, 2010, 36(3):131-133.

[13] BRICKEL E F. A survey of hardware implementations of RSA[A]. Proceedings of the Advances in Cryptology(CRYP TO'89)[C]. Santa Barbara, USA, 1990. 368-370.

[14] MARCELO E K, NAOFUMI T. A hardware algorithm for modular multiplication division based on the extended Euclidean algorithm[A]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences[C]. 2005. 3610-3617.

作者简介：

甘刚（1974-），男，四川茂县人，硕士，成都信息工程学院副教授，主要研究方向为网络攻防、侧信道攻击与防御等。

王敏（1977-），女，四川资阳人，硕士，成都信息工程学院讲师，主要研究方向为网络攻防、侧信道攻击与防御。

杜之波（1982-），男，山东冠县人，硕士，成都信息工程学院讲师，主要研究方向为信息安全、侧信道攻击与防御、天线应用和物联网安全。

吴震（1975-），男，江苏苏州人，硕士，成都信息工程学院副教授，主要研究方向为信息安全、密码学、侧信道攻击与防御、信息安全设备设计。