

一种针对 SM2 规整点乘算法的新型 SPA 攻击

王立辉¹, 赵 兵², 李 清¹, 梁晓兵², 刘 静³

(1 上海复旦微电子集团股份有限公司, 上海 200433; 2 中国电力科学研究院, 北京 100192;
3 国网宁夏电力公司电力科学研究院, 宁夏 银川 750002)

摘 要: 相比于 RSA 密码算法, SM2 在同样的安全强度下需要更短的密钥长度, 因此更适合于应用到资源受限的智能卡中. 为了 SM2 应用的安全性, 人们研究出多种具有抗侧道攻击能力的 SM2 点乘算法. 本文提出了一种基于条件减法的新简单功耗分析方法, 可以对常用的两种防护实现进行密钥的破解. 实验结果表明, 该方法只需要一条功耗曲线, 即可在几秒钟内破解出 SM2 密钥. 同时本文也给出了几种可以抵御该攻击的防护方法.

关键词: SM2; SPA; 蒙哥马利模乘; 条件减法

中图分类号: TP393.08

文献标识码: A

文章编号: 1000-7180(2018)08-0026-05

A Novel SPA Attack on SM2 with Regular Point Multiplication

WANG Li-hui¹, ZHAO Bing², Li Qing¹, LIANG Xiao-bing², LIU Jing³

(1 Shanghai Fudan Microelectronics Group Company Limited, Shanghai 200433, China;
2 China Electric Power Research Institute, Beijing 100192, China;
3 Power Research Institute of State Grid Ningxia Power Co., Yinchuan 750002, China)

Abstract: Compared with the RSA, the shorter key length is needed in the same security strength, so SM2 is more suitable for the application to the resource limited smart card. For the security of application of SM2, people study the variety point multiplication algorithms with countermeasures to resist the side channel attacks. This paper proposes a new simple side-channel analysis (SPA) method based conditional subtraction to attack two usual SM2 algorithms with countermeasures. Experimental results show that this method only needs a power trace, which can be used to break the SM2 key in a few seconds. At the same time, this paper also demonstrates some countermeasures to resist the attack.

Key words: SM2; SPA; montgomery modular multiplication; conditional subtraction

1 引言

自 1985 年 N. Koblitz^[1]和 V. Miller^[2]各自独立地提出椭圆曲线密码体制(ECC)以来, ECC 就以特有的短密钥、安全性高等魅力吸引着广大密码专家和学者对它进行广泛深入的研究, 人们发现 ECC 完全可以替代 RSA, 有些方面还大大优于 RSA, 这在限制资源的系统中尤为突出. 经过 20 多年的研究, ECC 逐步走向成熟, 将逐步取代 RSA 密码体制成为公钥密码算法的主流算法.

在商用密码领域, 中国使用国际标准密码算法和自主定义的密码算法. 2010 年 12 月 17 日, 为满足电子认证服务系统等应用需求, 国家密码管理局发布了 SM2 椭圆曲线公钥密码算法^[3]. 其算法文本包含数字签名算法, 密钥交换协议, 公钥加密算法三部分. 未来 SM2 算法在金融应用领域的场景会越来越广.

然而近年出现了一种侧信道攻击手段^[4], 对智能卡芯片安全性构成很大的威胁. 侧信道攻击中最常用的是功耗分析, 主要包括两类分析: 简单功耗分

析(simple power analysis ,SPA)和差分功耗分析(differential power analysis ,DPA).

对于 ECC,SM2 等公钥密码算法来说,最具威胁性的侧信道攻击是 SPA. 目前,国内外针对 ECC 已有多种侧信道攻击与防御对策^[5-6],为了防护 SPA,主要采用总是倍点点加算法^[5]和蒙哥马利梯子算法^[7]等规整的点乘算法,点加和倍点的运算顺序和密钥无关.然而,以上的防护手段并不能保证点乘的绝对安全,本文提出了一种新的更加强大的 SPA 攻击方法,可以对以上的规整点乘算法进行攻击.

2 相关技术

2.1 M2 算法及实现

和 ECC 类似,SM2 算法也是一种基于椭圆曲线的公钥密码算法,椭圆曲线即是在有限域上的满足 Weierstrass 方程的所有点,以及无穷远点的集合.

SM2 国密标准明确规定了 SM2 签名、验签、加密、解密和密钥交换流程^[3]. 由于签名,解密与密钥交换中含有用户私钥信息,通常对其进行抗攻击性研究.在以上运算中,最核心的运算是点乘运算.而点乘算法又包含了点加和倍点运算,执行顺序取决于密钥 d :如果当前的密钥比特位是 0,只做一次倍点运算;否则做完倍点运算后,还要做一次点加运算.

无论点加还是倍点,都可以用最基本的模加,模减和模乘来实现.和模加模减相比,模乘实现起来相对困难,虽然目前有多种模乘实现方法,但目前最常用的还是蒙哥马利模乘(Montgomery Modular Multiplication ,MMM),它非常适合于公钥加密算法,基本实现方式如算法 1 所示^[7]:

算法 1(蒙哥马利模乘算法)

Input: A 和 B ,满足: $A, B < R = r^n$ 并且 P 和 r 互质

Output: C ,满足 $C = AB r^{-n} \bmod P$ 并且 $C < R$

1. $C \leftarrow 0$

2. for $i=0$ to $n-1$

$$q_i = -(c_0 + a_i b_0) p_{0-1} \bmod r$$

$$C = (C + a_i B + q_i P) / r \leftarrow (C + a_i B + q_i P) \text{ div } r$$

3. if $C \geq PC \geq R$ then $C = C - PC \leftarrow C - P$

4. output C

可以看出在蒙哥马利模乘的结尾有一个条件减法,我们可以计算出该条件减法在模乘运算分别是

平方和乘法时出现的概率^[8].

如果是平方运算 X^2 ,条件减法出现概率相当于 $\text{prob}(X^2 r^{-n} + Z > P) \text{prob}(X^2 r^{-n} + Z > P)$,其中 Z 在 $[0, P]$ 区间内均匀分布.因此:

$$p_S = \int_0^P P^{-1} f(x) x^2 r^{-n} dx = \frac{1}{3} P r^{-n} \quad (1)$$

如果是乘法运算 XY ,其中 X 和 Y 是分别独立均匀分布的,则条件减法出现概率相当于 $\text{prob}(XY r^{-n} + Z > P) \text{prob}(XY r^{-n} + Z > P)$,其中 Z 在 $[0, P]$ 区间内均匀分布.因此:

$$p_M = \int_0^P \int_0^P P^{-1} f(x) f(y) xy r^{-n} dx dy = \frac{1}{4} P r^{-n} \quad (2)$$

对于 SM2, $P \approx r^n$,因此 $p_S \approx 1/3$, $p_M \approx 1/4$.

2.2 SPA 攻击及防护

本文只考虑针对点乘的 SPA,因为点乘算法执行时,不同的密钥会产生不同的操作指令,条件分支语句的执行依赖于当前的密钥比特位,如果点加和倍点运算可以通过功耗来区分,那么攻击者就可以推断出密钥 d .

倍点和点加运算通常按照文献^[9]中的流程来执行.当 $a = p-3$ 且 $Z=1$ 时,倍点运算需要 8 个模乘,而点加运算需要 11 个模乘.由于模乘的功耗较大,在功耗曲线上非常容易区分出哪些是点加和倍点,从而分析出密钥.

为了防护 SPA,点乘算法中不应该出现任何依赖于密钥的不同分支操作.其中应用最广泛的是总是倍点点加算法和蒙哥马利梯子算法.分别如算法 2 和算法 3 所述.无论当前的密钥比特位是 1 还是 0,总是执行一次倍点和一次点加,因此攻击者即使通过测量功耗曲线识别出倍点和点加运算,也无法推导出密钥.

算法 2 (总是倍点点加算法)

Input: d, P

Output: dP

1. $T_0 = P$ $T_0 = P$

2. for $i=n-2$ to 0

$$T_0 = 2T_0$$

$$\text{if } d_i = 1 \text{ then } T_0 = T_0 + P$$

$$\text{else } T_1 = T_0 + P$$

3. output T_0

算法 3(蒙哥马利梯子算法)

Input: d, P

Output: dP

- 1. $T_0 = P, T_1 = 2P$
- 2. for $i = n - 2$ to 0
 - $T_{1-di} = T_0 + T_1$
 - $T_{di} = 2 T_{di}$
- 3. output T_0

3 新型 SPA 攻击及防护

3.1 攻击方法原理

为了简便起见,假设该攻击所利用的主要泄露信息为会在功耗曲线上观察到蒙哥马利模乘执行时是否会有条件减法. 对于利用其它原理实现的模乘,只要存在和数据相关的侧信道泄露,也可以使用类似的攻击方法.

如前所述,蒙哥马利模乘中是否会出现条件减法,完全取决于输入的两个乘数,而依据算法 1,这两个乘数又是由输入点和计算该模乘时之前所使用的部分密钥来决定的. 换言之,可以通过已知的输入点和某时刻之前使用的密钥比特位来计算出该时刻的模乘是否会出现条件减法.

本文的攻击方法就是利用以上原理:利用已知的输入点和猜测的部分密钥,攻击者可以计算出中间多个模乘出现条件减法的位置,如果和实际功耗曲线中出现的位置相符,则认为猜测的密钥是正确的,否则换一组猜测值重新计算,直到获得正确的密钥. 下面我们以最标准的总是倍点点加算法为例,如图 1 所示,描述针对点乘的具体攻击流程.

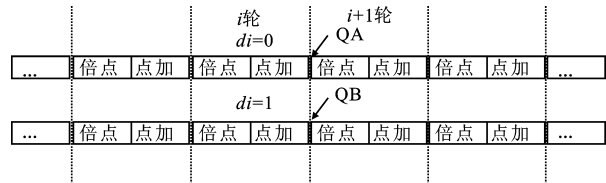


图 1 总是倍点点加算法的攻击方法

假设攻击者已知前 $i - 1$ 个密钥比特位,那么他可以猜测第 i 个密钥位 $d_i = 0$ 和 $d_i = 1$,分别计算出第 i 轮的输出,也就是第 $i + 1$ 轮的输入 QA 和 QB. 通常情况下计算点乘时使用的坐标系为雅克比坐标,所以倍点是 8 个模乘,点加是 11 个模乘,即每轮共有 19 个模乘. 这样第 $i + 1$ 轮的 19 个模乘出现条件减法的位置就可以计算了,如果由 QA 计算出的条件减法和实际情况相符并且由 QB 计算出的条件减法和实际情况不符,则 $d_i = 0$,反之则 $d_i = 1$. 我

们可以重复以上流程,直到获得倒数第二轮的密钥. 最后一轮的密钥由于无法用以上方法来确认,只能通过穷举来破解.

以上方法能够成功的前提条件是:当 $d_i = 0$ 和 $d_i = 1$ 时,19 个模乘出现条件减法的位置是不完全相同的. 根据第二节分析,可以得出两个平方运算的条件减法一致的概率是:

$$p_S^2 + (1 - p_S)^2 = 5/9$$

同样地,两个乘法运算的条件减法一致的概率是:

$$p_M^2 + (1 - p_M)^2 = 5/8$$

由于 19 个模乘里面有 7 个平方运算和 12 个乘法运算,因此我们可以计算出这 19 个模乘的条件减法出现位置完全相同的概率是: $(5/9)^7 \times (5/8)^{12} \approx 2^{-14}$. 这个概率小到可以忽略,对于 SM2 来说,一条功耗曲线就可以获得密钥的成功率为: $(1 - 2^{-14})^{255} \approx 98.5\%$.

对于蒙哥马利梯子算法实现的 SM2,也可以使用类似的方法进行攻击. 如图 2 所示.

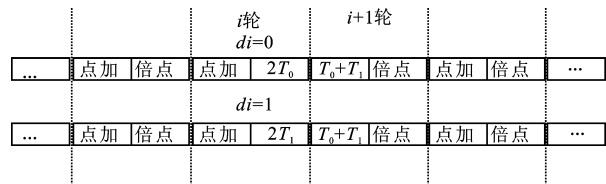


图 2 蒙哥马利梯子算法的攻击方法

假设攻击者已知前 $i - 1$ 个密钥比特位,那么他可以猜测第 i 个密钥位 $d_i = 0$ 和 $d_i = 1$,从而计算出第 i 轮的倍点运算和第 $i + 1$ 轮的点加运算. 这两组运算共有 24 个模乘,其中 8 个平方,16 个乘法. 因此这 24 个模乘的条件减法出现位置完全相同的概率是: $(5/9)^8 \times (5/8)^{16} \approx 2^{-18}$. 这个概率同样很小,对于 SM2 来说,一条功耗曲线就可以获得密钥的成功率为: $(1 - 2^{-18})^{255} \approx 99.9\%$.

实际攻击时如果出现当 $d_i = 0$ 和 $d_i = 1$ 时模乘出现条件减法的位置完全相同的这种情况,还可以借助于猜测下一轮的密钥来判断,仍然可以通过一条功耗曲线来破解出整个密钥.

3.2 防护方法

由于该方法只需要一条点乘的功耗曲线就可以破解出整个密钥,像常用的指数随机化等防护方法是无效的,因为通过随机化后的密钥完全可以恢复出真实密钥.

很明显,攻击者需要知道输入点并且要求可以从功耗曲线中分辨出模乘的条件减法,因此输入点随机化,坐标随机化^[5],去除条件减法等防护都可以达到防护的目的.但是如果攻击者引入故障注入等联合攻击手段,则可以通过跳过随机化等步骤的方式,依然实现该攻击,因此去除条件减法才是最根本的防护手段.

4 实验结果

为了验证上一节所述攻击方法的有效性,本文对智能卡中硬件实现的 SM2 进行实验攻击.实验设备包括 PC,功耗采集设备,智能卡和 LeCroy 示波器.智能卡利用 PAE 协处理器来实现模乘,模加等底层硬件操作,利用算法库来实现可以防护 SPA 和 DPA 攻击的 SM2 点乘算法.

在实际的攻击中,该方法要求对功耗曲线上条件减法的判断不能出错.有多种方法可以区分出模乘是否带有条件减法,例如测量模乘的执行时间,模式匹配等.本文选择后者,因为更加地简便易行.具体步骤如下:

(1)首先采集 SM2 点乘运行时的一条功耗曲线,并不限于采用总是倍点点加算法或蒙哥马利梯子算法,选取一个带有条件减法的模乘作为模式,然后逐个计算该模式和功耗曲线所有等长区间的相关系数,如果该区间也是带有条件减法的模乘,则相关系数会较高.再挑选出相关系数满足一定阈值(例如 0.9)的所有区间,把这些区间对齐后再做平均,作为标准模式,代表一个带有条件减法的模乘,如图 3 所示.

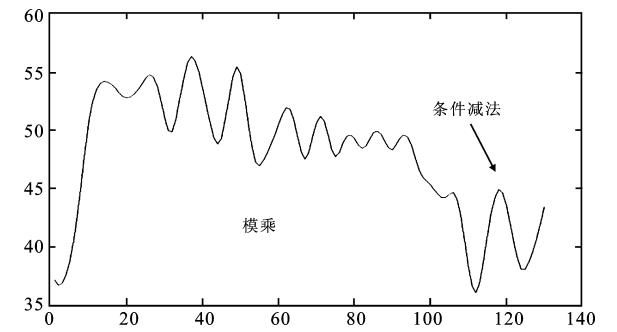


图 3 带有条件减法模乘的标准模式

(2)重新计算标准模式和功耗曲线所有等长区间的相关系数,部分结果如图 4 所示.

根据图 4 的结果,明显可以把相关系数分为 3

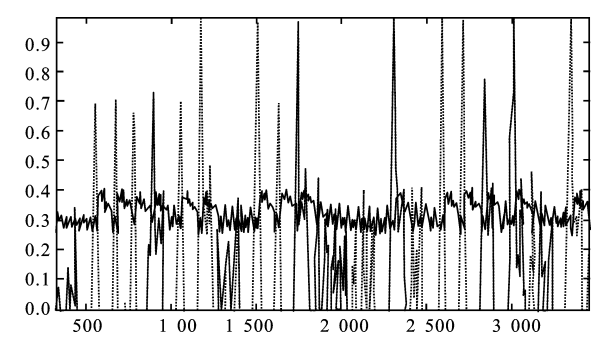


图 4 标准模式和功耗曲线所有等长区间的相关系数

类:第一类大于 0.9,说明匹配得很好,对应区间是带有条件减法的模乘,第二类介于 0.6 和 0.9 之间,意味着和标准模式有些区别,对应区间应该还是没有条件减法的普通模乘,第三类小于 0.6,和标准模式差别较大,说明对应的区间并不是模乘.根据相关系数曲线从左到右进行扫描,如果出现第一类的尖峰,则记为 1,出现第二类的尖峰,则记为 0,最终得到一个代表额外减法出现情况的模乘序列.

(3)把以上识别结果输入到依据上一节所描述方法开发的分析程序中,应用到总是倍点点加算法或蒙哥马利梯子算法中,实验结果表明:只需要一条功耗曲线,在几秒钟内就可以准确地恢复出整个密钥.

分别对两种点乘算法的签名和解密各采集 10 000 条功耗曲线进行攻击,成功率如表 1 所示.

表 1 实际攻击的成功率

点乘算法	应用协议	成功率 1/ %	成功率 2/ %
总是倍点点加	签名	98.05	99.09
总是倍点点加	解密	97.73	98.84
蒙哥马利梯子	签名	99.79	99.90
蒙哥马利梯子	解密	99.79	99.89

在攻击过程中,如果无论猜测密钥比特位为 0 和 1,和实际的额外减法都相符或都不相符,即认为攻击失败,只和一种猜测值完全相符才继续进行攻击,那么这种情况下获得的密钥一定是正确密钥,对应成功率 1(应和 3.1 节计算的理论值相符);如果实际的额外减法和猜测密钥比特位为 0 的时候相符即认为是 0,不符便是 1,不做更多的判断,那么这种假设没有考虑到 0 和 1 无法区分的情况,获得的密钥不一定是正确密钥,还需要进一步验证正确性,此时对应成功率 2(攻击速度更快,成功率更高).签名和解密的区别是:签名时所用的输入点固定为 SM2

的基点,而解密时输入点和密钥都是随机的.

从表 1 中实际攻击的成功率来看,和理论计算值非常接近,而且不同的应用协议对破解影响不大,实际成功率完全可以满足各种不同点乘算法在同应用协议下的攻击需求.

5 结束语

本文提出了一种针对 SM2 规整点乘算法的新型 SPA 攻击方法,主要利用了蒙哥马利模乘的条件减法所泄露的信息,通过观察点乘的功耗曲线来获取密钥信息.从实验结果至少可以得到以下两点:首先,总是倍点点加和蒙哥马利梯子等规整的点乘算法并不是总能防护所有的 SPA 攻击;其次,对于某些攻击,指数随机化等经典方法不能起到任何的防护作用.

本文方法可以看成是对普通 SPA 的增强,和普通的 SPA 攻击相比,对于一些特定算法及实现,例如采用了蒙哥马利模乘的规整点乘算法等具有很大的威胁,因此需要考虑更多的防护手段.由于仅对点乘部分进行攻击,该方法同样适用于梳状点乘,ECC,RSA 等算法.

参考文献:

[1] Koblitz N. Elliptic curve cryptosystems [J]. Mathematics of Computation, 1987, 177(48):203-209.

[2] Miller V S. Use of elliptic curves in cryptography [J]. Proceedings of Crypto 85, LNCS 218, Springer, 1986, 19 (3) :173-193.

[3] GM/T 0003-2012. SM2 elliptic curve public key cryp-

tographic algorithms [S]. China:Chinese Cryptograpy Administration,2010.

[4] Kocher P. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems [M]. Springer Berlin Heidelberg, 1996(1109) :104-113.

[5] Coron J S. Resistance against differential power analysis for elliptic curvecryptosystems [C] // CHES99, LNCS 1717. Berlin, Springer Verlag, 1999:292-302.

[6] Lopez J, Dahab R. Fast multiplication on elliptic curves overGF(2m) without precomputation [C] // CHES99 LNCS 1717. Berlin, Springer Verlag, 1999: 316-327.

[7] Montgomery P L. Speeding the pollard and elliptic curve methodsfor factorizations [J]. Mathematics of Computation, 1987, 177(48):243-264.

[8] Walter C D. Simple power analysis of unified code for ECC double and Add [C] // CHES 2004. Springer, Berlin, Heidelberg,2004(3156): 86-115.

[9] IEEE Std-1363-2000: Standard Specifications for Public KeyCryptography [S]. IEEE, DOI: 10. 1109/ IEEESTD. 2004. 94612, 2000.

作者简介:

王立辉 男,(1982-),博士,工程师.研究方向为密码芯片安全. E-mail:wanglihui@fmsh. com. cn.

赵 兵 男,(1971-),硕士,高级工程师.研究方向为信息学.

李 清 女,(1968-),硕士,高级工程师.研究方向为集成电路设计开发.

梁晓兵 男,(1978-),博士,高级工程师.研究方向为信息学.