针对随机伪操作的简单功耗分析攻击

王敏，吴震
（成都信息工程学院 网络工程学院，四川 成都 610225）

摘 要：讨论针对随机伪操作椭圆曲线密码标量乘算法的 SPA 攻击，理论推导和实测结果均表明，在单样本 SPA 攻击下，即可在功耗曲线中获取大量的密钥信息；而在针对算法中随机操作漏洞的一种新型多样本 SPA 攻击—多样本递推逼近攻击下，用极小样本量就可完整破译密钥。当密钥长度为 n 时，该攻击方法完整破译密钥所需的样本数仅为 $O(\mathrm{lb}\ n)$。

关键词：信息安全；边信道攻击；简单功耗分析攻击；随机伪操作；多样本递推逼近攻击
中图分类号：TN918.1; TP309.1 **文献标识码**：B **文章编号**：1000-436X(2012)05-0138-05

Simple power analysis attack on random pseudo operations

WANG Min, WU Zhen
(Network Engineering Department, Chengdu University of Information Technology, Chengdu 610225, China)

Abstract: Random pseudo-operations on elliptic curve scalar multiplication algorithm, less secure than it claimed by simple power analysis (SPA) attacks. Even in the single curve SPA, it leaks lots of useful key information. Multiple curve recursive approximation attack (MCRAA), a new multiple curve SPA attack, was proposed to get all of the key information with a small curve set. When the length of the key is n, the size of the set is $O(\mathrm{lb}n)$ which was confirmed by experiment.

Key words: information security; side-channel attack; simple power analysis; random pseudo operation; multiple curve recursive approximation attack

1 引言

功耗分析攻击是利用运算电路的功耗信息泄露，对密码芯片加解密过程的功耗进行分析，猜测出密码芯片加解密所使用密钥的一种攻击手段[1,2]。

在抵抗功耗分析攻击的各种策略中，使用随机动作来破坏功耗和密钥间的相关性是一种重要的方法，正确的使用这种技术确实能很好地达到抗功耗分析攻击目的。然而，错误的使用方式反而会使算法安全性大大下降。随机伪操作椭圆曲线密码标量乘算法就是这样的一个实例。

椭圆曲线密码（ECC, elliptic curve cryptography）是基于椭圆曲线数学的一种公钥密码。该算法与其他公钥密码算法相比具有比特强度高，计算速度快，存储空间小等特点，在资源受限的嵌入式系统（如智能卡）等安全领域广泛应用。

自从功耗分析攻击提出以后，公钥算法实现如何在兼顾效率的同时抵抗功耗分析攻击，成为密码学研究的一个重点。随机伪操作椭圆曲线标量乘算法[3]是在固定添加伪点加法算法（又称 double and add always 算法）[4,5]基础上引入随机机制而形成的一种提高效率的改进型算法，该算法试图用随机性

收稿日期：2011-07-01；**修回日期**：2011-10-05
基金项目：国家自然科学基金资助项目(60873216)；四川省科技支撑计划基金资助项目（2011GZ0170）
Foundation Items: The National Natural Science Foundation of China(60873216); Sichuan Science and Technology Support Programme (2011GZ0170)

保持其抗简单功耗分析（SPA, simple power analysis）攻击能力的同时提高运算效率。但该类算法在设计实现中对随机性的使用存在一定缺陷，为提高效率而引入的随机伪操作反而可能成为 SPA 攻击成功的决定因素。

下面从添加伪点加法算法的抗 SPA 攻击原理入手，具体分析添加随机伪操作的椭圆曲线标量乘算法的缺陷及其多样本 SPA 攻击实现方法，并给出实测结果，最后给出抗多样本 SPA 攻击的改进建议。

2　椭圆曲线密码算法的随机伪操作标量乘法

2.1　椭圆曲线密码算法的标量乘法

椭圆曲线密码算法的核心运算为标量乘 kP 的计算，而标量乘法运算过程中包含有密钥 k 的信息，因此对于标量乘法的功耗分析攻击成为了椭圆曲线密码算法重要的攻击点。

在标量乘实现算法中主要使用点加（$Q = Q + P$）和倍点（$P = 2P$）2 种定义在椭圆曲线上的运算[6,7]，SPA 攻击可利用这 2 种运算在功耗曲线上的不同形状，直接恢复出 K 值[3]。

2.2　添加伪点加法

针对标量乘的添加伪点加法是根据 SPA 攻击原理，为了掩盖密钥 k 与运算间的操作相关性，对标量乘实现算法进行修改，使得当密钥 k 对应比特是“0”或“1”时，都进行点加和倍点 2 种运算，来达到掩盖密钥与运算间的操作相关性的目的，其具体实现算法、抗 SPA 攻击能力和算法效率见文献[3]。

2.3　随机伪操作法实现原理

文献[3]提出的随机伪操作法是将上述添加伪点加实现算法进行的修改，当密钥 k 对应比特为 0 时不再单纯地添加一次伪点加操作，而是随机添加一次伪操作，该伪操作为点加、倍点、无操作三者之一，并且为了既能提高抵抗 SPA 攻击能力，又能尽可能地减少效率损失，对添加伪操作各类型概率进行控制，将添加无操作的概率控制在 50%左右，添加点加和倍点的概率总和控制在 50%左右，随机伪操作法程序流程如图 1 所示。

算法原意是想利用随机伪操作来掩盖功耗曲线与密钥 K 之间的相关性，同时对固定添加伪点加的算法加以效率上的改进，详见文献[3]。然而，在下面的分析中可以看到，这种添加伪操作的方法如果没有其他防护措施的配合，实际上破坏了原固定添加伪点法的安全性，仅使用 SPA 攻击便可获取密钥。

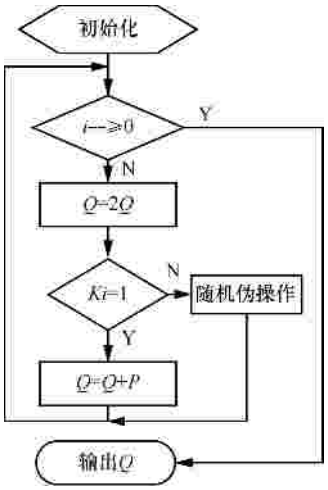

图 1　随机伪操作法程序流程

3　针对随机伪操作的 SPA 攻击分析

3.1　单样本 SPA 攻击分析

根据随机伪操作算法可知，当密钥比特为 0 时，随机添加伪点加、伪倍点运算或无操作。当添加伪点加运算时，则该比特使真“0”变为假“1”，从波形上看无法区分；当添加伪倍点时，该比特会使单比特的“0”变为双比特的“00”；但当无操作时，真“0”将真实地表现出来。

首先，根据文献[2,8,9]以及实测数据发现，如图 1 所示的算法中，每个循环内部 2 个运算之间的时间间隔较小，而循环之间的时间间隔比较大。用时间间隔的差别，可以在单样本中定位各个不同循环轮数，这就是利用计时攻击（TA, timing attack）在单样本中获取定位信息。由于每轮循环均可被定位，而每轮循环只会对应单比特二进制数“0”或“1”。则填加的伪倍点运算会被识别出来，这是因为该运算对应的双比特“00”不可能存在于同一个轮循环中。由此可知，单样本下，每轮中观测到的“00”波形均可被还原为真实值“0”。与之相对应，固定添加伪操作算法每轮边界被区分出来也得不到对 K 有用的 SPA 攻击信息。

其次，在单样本中，还可提取密钥 K 汉明重量的上限。令 HW（C）为二进制序列 C 的汉明重量（即二进制序列 C 中“1”的个数），K 为 $n$bit 的真实密钥值，其汉明重量 HW（K）为 n_k，K_e 为单样

本 SPA 攻击下获取 K 的估计值，其汉明重量 HW（K_e）为 n_e，则有

$$n_k \le n_e \le n \tag{1}$$

通过计算 K_e 的汉明重量，可获得 K 的汉明重量上限。即可确定在 K 中最多有 n_k 个“1”，至少存在 $n-n_e$ 个“0”。从暴力破解的难度上看，只需对 $n_k$bit 的“1”进行真假猜测，最坏情况计算复杂度从原来的 2^n 降到 2^{n_e}。若 K 为真随机数，在大数情况下，$n_k=[0.5n]$ 的概率趋近 1，这意味着在 n_e 中猜测有 $[0.5n]$ 个“1”的猜中几率最大，即进行 $\binom{n_e}{0.5n}$ 次猜中的几率最大。根据式（1），有

$$\binom{n_e}{0.5n} \le \binom{n}{0.5n} \tag{2}$$

可知单样本 SPA 攻击可使基于概率最大化暴力破解法的复杂度也大幅减小。由于“0”的个数下限及其位置信息的暴露，还可综合使用其他方法进行更有力、快速的密钥破解。而固定添加伪操作算法也不存在这样的缺陷。

3.2 基于 SPA 的多样本递推逼近攻击

由上述分析可知，想让破解复杂度降低，在 n 不变的情况下，应尽量使 n_e 的值接近 n_k。进行 SPA 攻击时，可先进行 L 个样本获取，然后对每个样本进行 SPA 攻击，获取不同 $K_{ei}(1\le i\le L)$，选取其中汉明重量最小的猜测值 $K_{ej}(1\le j\le L)$，再进行其他类型攻击。事实上，在多样本条件下，还存在更有效的分析攻击方法。

3.2.1 随机伪操作的分析模型

从密码分析和波形分析的角度看，随机伪操作法可看作将 K 中的“0”进行掩码保护，随机编码成“0”、“00”或“1”，而对 K 中的“1”并未进行掩码，仅编码成“1”。由于单样本 TA 攻击在可直接将“00”反推成“0”，故“00”这种情况在下面的分析中将归结于“0”中而不单独讨论。

根据这种规则，可得如下密码分析模型：

$$K_e = K + R \tag{3}$$

其中，K 为 n bit 的真实密钥，R 为 n bit 的真随机数，K_e 为单样本 SPA 攻击后猜测值，运算符“+”为按比特做逻辑“或”运算。易验证该模型完全符合以上编码规则。

3.2.2 多样本递推逼近 SPA 攻击的原理

在多样本条件下，令 L 为采集的样本次数，则第 i 个样本利用真随机数 R_i 形成的猜测值 K_{ei} 为

$$K_{ei} = K + R_i \ (1 \le i \le L) \tag{4}$$

其中，当 $i \ne j$ 时，$R_i \ne R_j$。

令 K_L' 为多样本综合猜测值，构造以下运算：

$$K_L' = (K_{e1} \bullet K_{e2} \bullet \cdots \bullet K_{ei} \bullet \cdots \bullet K_{e(L-1)} \bullet K_{eL}) \tag{5}$$

其中，运算符“$\bullet$”为按比特做逻辑“与”运算。

将式（4）代入式（5），根据逻辑运算规则，有：

$$K_L' = K + (R_1 \bullet R_2 \cdots \bullet R_i \bullet \cdots \bullet R_{(L-1)} \bullet R_L) \tag{6}$$

令 $R_L' = (R_1 \bullet R_2 \cdots \bullet R_i \bullet \cdots \bullet R_{(L-1)} \bullet R_L)$，则 K_L' 即为 K 在 R_L' 掩码下的猜测值。

$$K_L' = K + R_L' \tag{7}$$

从密码破译的角度看，K_L' 和真实值 K 两者的差值正是随机数 R_L'，该随机数中“1”的个数越少，则猜测值越接近于真实值。

根据随机数性质，当 L 充分大的时候，有

$$R_L' = (R_1 \bullet R_2 \cdots \bullet R_i \bullet \cdots \bullet R_{(L-1)} \bullet R_L) \approx 0 \tag{8}$$

则当 L 充分大时：

$$K_L' = K + R_L' \approx K \tag{9}$$

另外，当在原样本集合中再增加一条新样本时，有

$$HW(R_L') \ge HW(R_{L+1}') \tag{10}$$

$$HW(K_L') \ge HW(K_{L+1}') \tag{11}$$

这说明每增加一条新样本，K_{L+1}' 将越接近于真实值 K。

3.2.3 多样本递推逼近 SPA 攻击的实现算法

根据以上性质，构造新型多样本攻击算法如下。

算法1 多样本递推逼近SPA攻击算法

输入： $C=[K]P$

输出： $K_i'=K$

1) **初始化：** K_0' 为全1的比特序列，i=0

2) $i=i+1$，单样本SPA攻击出猜测值 K_{ei}

3) $K_i'=K_{i-1}' \bullet K_{ei}$

4) $C_i=[K_i']P$

5) **若** $C_i \ne C$，**则转至2）继续**

6) **返回** K_i'

在真随机数条件下，根据其均匀性有

$$P(HW(R_L')=\left[2^{-L}HW(R)\right]$$
$$=\left[2^{-L}2^{-1}n\right]=\left[2^{-L-1}n\right])=\max \quad (12)$$

根据上面的讨论可知，L 个样本猜测后得到的猜测值 K_L' 正确猜出 $n-\left[2^{-L-1}n\right]$bit 密钥的概率最高，当 $L=\mathrm{lb}\,n-1$ 时，有

$$P(K_L'=K)=\max \quad (13)$$

由信息熵理论也可得到类似的结果。

如此可见，攻击样本数 L 与受攻击 K 的比特数 n 之间呈对数关系，计算复杂度极小，攻击效率比一般的多样本攻击高得多。例如一个 n=256 的 K 在 7 个样本下就有极高的几率被完全攻破。

3.2.4　多样本递推逼近攻击实测实验结果分析

实验 1　在 n=256bit 时，对一个汉明重量为 130 的密钥 K，实施多样本递推逼近攻击，共独立测试 10 000 组，每组均用不同的随机数进行伪随机操作。测试结果频数直方图如图 2 所示，7 个样本攻击成功的频数最高，为 2 401 次，占总次数的 24.01%。其次是 6 个样本攻击成功，频数为 2 336 次，占总次数 23.36%。攻击成功所花样本数 $L\leq 11$ 的百分比为 97.03%，$L\leq 13$ 的百分比是 99.25%

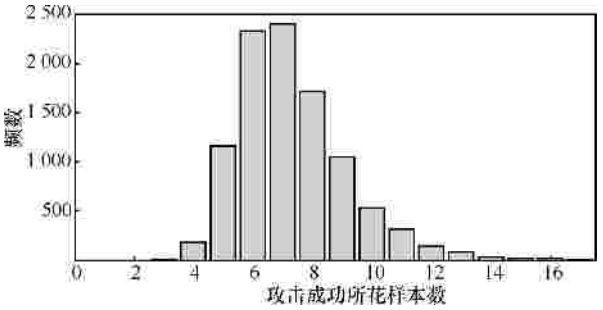

图 2　n=256bit 密钥 K 的 10 000 组攻击成功样本数频数直方图

实验 2　对 n=1 024bit，汉明重量为 541 的密钥 K，对其实施多样本递推逼近攻击。10 000 组测试后，测试结果频数直方图如图 3 所示。

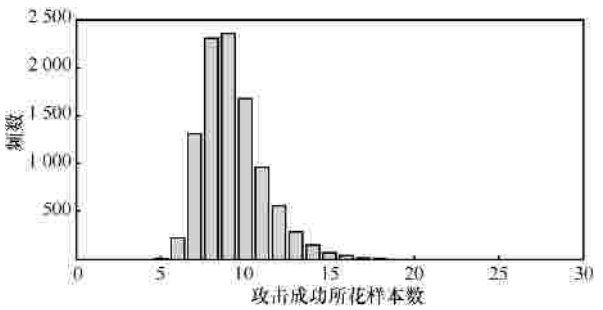

图 3　n=1 024bit 密钥 K 的 10 000 组攻击成功样本数频数直方图

由图 3 可知，当成功攻击样本 L=9 时的频数最高，为 2362 次，占 23.62%；其次为 L=8，为 2 313 次，占 23.13%，攻击成功所花样本数 $L\leq 13$ 的百分比为 97.09%, $L\leq 15$ 的百分比是 99.28%。

经过大量实验统计分析得到，对于 n bit 的密钥 K，成功攻击所花样本数 $L\leq \mathrm{lb}\,n+3$ 的概率大于 97%，$L\leq \mathrm{lb}\,n+5$ 的概率大于 99%。这说明只需小于等于 lb$n$+3 个样本，就有 97%的概率破解出完整的 n bit 密钥，在此基础上再增加 2 个样本则有大于 99%的概率成功破解。

4　随机伪操作算法抗 SPA 攻击可能的改进措施

随机伪操作算法中存在的多样本递推逼近攻击缺陷主要由以下原因造成。

1) 由于轮与轮之间的时间间隔与循环体内的时间间隔不同，可获得定位信息。

2) 由于运算的不同，倍点和点加运算在功耗曲线上很容易被辨识出来。结合随机伪操作算法，可获得每轮 K 的信息。

3) 掩码采用真随机数，对于相同的 K 每次都用不同的随机数进行掩码，而多样本递推逼近攻击正是针对这种随机机制实施的攻击。

针对第 1 个缺陷，需在精确测量的基础上，加入适当的延时机制，使得各运算之间的时间间隔相等，消除 TA 攻击的隐患。

针对第 2 种缺陷，需要在倍点和点加运算算法中加以改进，使得 2 种运算的操作相等，这样在功耗曲线上无法区分 2 种不同运算，给 SPA 攻击识别“0”、“1”增加难度。

针对第 3 种缺陷，则需规定随机数生成算法的规则，对相同的 K 生成相同的随机数 R，不同的 K 生成不同的随机数 R。固定添加伪点加算法是该改进的一个特例，其添加的随机数 R 为 K 的反码，这样可使得任意 K 对应的 K_e 均为固定值：全“1”。值得指出的是，该随机数产生算法最好能保证其单向性，即使在获得随机数 R 信息的条件下，仍无法逆推出 K 的值。其实现方案可使用散列技术或将 K 作为随机数发生器的种子，其破解的复杂度就等价于破解散列算法或随机数发生器。

特别要指出的是，修正以后的算法，其安全性仍然低于固定添加伪点加算法。首先，攻击者仍可获得 K 序列汉明重量的上限，其次，虽然不能确定

“0”的绝对位置，但可确定“0”和“1”的相对前后位置，最后，还可通过观察“0”和“1”的行程来确定子序列中“0”的最少个数和“1”的最多个数，这些信息均可使攻击难度大大下降，由此可见，消除倍点和点加运算之间的差别也非常重要，具体攻击过程另文撰述。

5 结束语

随机伪操作椭圆曲线标量乘算法虽然将运算效率提高，但本文证明，其抗 SPA 攻击能力大大降低。本文提出的多样本递推逼近攻击，利用在多样本中消除随机数的方法，实测结果表明只需小于等于 $\mathrm{lb}n+3$ 个样本，就有 97%的概率破解出完整密钥。该类攻击的存在证明，不恰当的应用随机性，不但不能增加安全性，反而会产生极大的安全缺陷。

在改进措施中，将随机数生成算法进行改进，有效抵抗了多样本递推逼近攻击；同时平衡了运算之间的时间间隔。但必须认识到，由于随机添加伪操作算法本身的缺陷，其安全性仍弱于固定添加伪点加算法，建议不使用该类算法。

参考文献：

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

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

[3] **朱冰**, **陈运**, **吴震等**. **一种抗简单功耗分析攻击的椭圆曲线标量乘快速实现算法**[J]. **成都信息工程学院学报**. 2011, 28(1):5-10.
ZHU B, CHEN Y, WU Z, *et al*. A fast algorithm of scalar multiplication on ECC resistant against SPA[J]. Journal of Chengdu University of Information Technology, 2011, 28(1):5-10.

[4] **廖嘉**, **夏国坤**, **王立鹏等**. **抵抗 SPA 和 DPA 的椭圆曲线上点的标量乘法**[J]. **天津科技大学学报**, 2009, 24(2):67-70.
LIAO J, XIA G K, WANG L P, *et al*. Scalar multiplication on ECC resistant against SPA and DPA[J]. Journal of Tianjin University of Science and Technology,2009,24(2): 67-70

[5] TETSUYA I, BODO M, TSUYOSH T. Improved elliptic curve multiplication methods resistant against side channel attacks[A]. Progress in Cryptology, LNCS 2551[C]. Springer-Verlag, 2002. 295-313.

[6] MILLER V S. Use of elliptic curves in cryptography[A]. Proceedings of Crypto 85 LNCS 218[C]. Springer, 1986. 417-426.

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

[8] ACICMEZ O, SEIFERT J P, KOC C K. Predicting secret keys via branch prediction[A]. Topics in Cryptology-CT-RSA 2007, Leture Notes in Computer Science[C]. 2006.225-242.

[9] ACIICMEZ O, KOC C K, SEIFERT J P. On the Power of Simple Branch Prediction Analysis[R]. Cryptology ePrint Archive, 2006. 312-320.

作者简介：

王敏（1977-），**女，四川资阳人，成都信息工程学院讲师，主要研究方向为信息安全、密码学、网络攻击与防御。**

吴震(1975-)，**男，江苏苏州人，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、边信道攻击与防御、信号分析处理、嵌入式系统设计。**