第 24 卷 第 2 期
2009 年 4 月

天津科技大学学报
Journal of Tianjin University of Science & Technology

Vol.24 No. 2
Apr. 2009

抵抗 SPA 和 DPA 的椭圆曲线上点的标量乘法

廖 嘉[1]，夏国坤[1]，王立鹏[2]，刘寅立[1]
（1. 天津科技大学理学院，天津 300457；2. 河北工业大学计算机科学与软件学院，天津 300130）

摘 要：标量乘法是椭圆曲线密码体制中的一种基本算法. 针对二进制方法和抵抗 SPA 的二进制方法无法抵抗倍点攻击和差分攻击的缺点,提出了两种改进方法. 方法一给出了区分奇数和偶数的标量乘法,计算标量乘法时完全对奇数进行操作,从而能够抵抗倍点攻击. 方法二采用同时随机化标量和随机化基点的方法,从而达到更好的随机性. 这两种方法计算量不大且简单易行.

关键词：椭圆曲线；标量乘法；简单能量分析；差分能量分析
中图分类号：TN918.4 **文献标志码**：A **文章编号**：1672-6510(2009)02-0067-03

Scalar Multiplication on ECC Resistant Against SPA and DPA

LIAO Jia [1]，XIA Guo-kun [1]，WANG Li-peng [2]，LIU Yin-li [1]
(1. College of Science,Tianjin University of Science & Technology,Tianjin 300457,China;
2. School of Computer Science and Engineering,Hebei University of Technology,Tianjin 300130,China)

Abstract: Two commonly used methods of scalar multiplication,binary methods and SPA-resistant binary methods were analyzed. To against doubling attack and DPA attack,the methods were improved. First,even numbers were turned to odd numbers by add 1,then '0' will not be handled,so doubling attack can be resisted. Second,the effect of random scalar and random point is proved. The quantity of computations is not large and it's easy to be realized.

Keywords: elliptic curve; scalar multiplication; SPA; DPA

椭圆曲线密码体制(ECC,elliptic curve cryptography)的安全性依赖于椭圆曲线离散对数问题的难解性. ECC 使用较短的密钥长度就能达到和 RSA 相同的安全性. 因此,它适用于像智能卡这样资源有限的便携设备. 这使得 ECC 的应用越来越广泛.

ECC的有效、安全实现是ECC研究的主要内容之一,其中ECC的基本算法 —— 标量乘法最易受到边信道攻击(SCA,side channel attack). SCA是在 1996 年由P.Kocher提出的一种利用加密过程中的计算时间或能量消耗来分析秘密消息的攻击方法,基本上分为两类,简单能量分析(SPA,simple power analysis)和差分能量分析(DPA,differential power analysis)[1]. 所谓简单能量分析是指分析一个设备上一次密码操作所消耗的能量. 因为对不同的操作有不同能量消耗,这样对应不同的能量消耗,攻击者可以判断以什么样的顺序进行了什么样的操作. 当将多种监听数据与概率的分析工具结合在一起时,攻击的成功率更高,即为差分能量分析.

目前,抵抗SPA的方法可以加入"虚"点加运算,使用归一化的标量乘法,或者使用"统一"过的点加和倍点运算公式[2]. 抵抗DPA的方法主要是随机化椭圆曲线、基点和标量. 随机化的方法有很多,一般采用"盲化",点的同态映射,投影坐标[3].

本文介绍并分析了常见的椭圆曲线上的标量乘法. 并根据目前抵抗 SPA 和 DPA 方法的思想,改进了已有的标量乘法的典型算法. 在基本不增加运算量的基础上,给出了抵抗 SPA 和 DPA 的标量乘法算法.

收稿日期：2008–08–22；**修回日期**：2008–11–04
基金项目：天津科技大学科研基金资助项目（20060227）
作者简介：廖 嘉（1978—），女，天津人，讲师.

1　椭圆曲上点的标量乘法

ECC 的加密、解密过程，公钥协议等的执行都要求计算椭圆曲线上点的标量乘法，即求

$$Q = kP = \underbrace{P + P + \cdots + P}_{k次}$$

其中：P 是椭圆曲线上的点；k（$0 \leqslant k \leqslant m$，$m$ 是点 P 的阶）是正整数. 点 P 或者是固定的，可产生 $E(GF(q))$ 素阶子群的点，或者是这样一个子群中的任意一个点.

1.1　二制方法(binary methods)[4]

标量乘法是 ECC 中的基本运算，通常使用 k 的二进制形式从左到右进行计算. 二进制算法如下：

输入：P，$k = (k_{l-1}, k_{l-2}, \cdots, k_0)_2$

输出：$Q = kP$

$Q \leftarrow O$

For　$i = l-1$　downto 0 do

　$Q \leftarrow 2Q$

　If　$k_i = 1$　then　$Q \leftarrow Q + P$

Return　Q

一般二进制表示的标量中，“1”和“0”出现的概率都是 1/2，因此该算法的计算量为 $(l-1)M + Al/2$（其中 M 表示倍点运算，A 表示点加运算），即 $l-1$ 次倍点运算，$l/2$ 次点加运算. 在这种算法中有两种不同的运算：倍乘和点加，它们在运算上消耗的能量是不同的，每轮循环中可根据是否进行了点加运算来判断出 k 的当前位是“0”或“1”，这样就可以分析出 k 的值. 因此，二进制方法很容易受到简单能量分析的攻击.

1.2　抵抗 SPA 的二进制方法(SPA-resistant binary methods)[4]

若要抵抗 SPA，则需要标量乘法的运算过程不依赖于数据 k. 抵抗 SPA 的二进制算法如下：

输入：P，$k = (k_{l-1}, k_{l-2}, \cdots, k_0)_2$

输出：$Q = kP$

$Q_0 \leftarrow O$

For　$i = l-1$　downto 0 do

　$Q_0 \leftarrow 2Q_0$

　$Q_1 \leftarrow Q_0 + P$

　$Q_0 \leftarrow Q_{k_i}$

Return　Q_0

在该算法中，无论 k 的当前位是“0”或“1”，均要进行点加运算，即加入了“虚”点加，每一轮进行相同的操作就避免了不同的能量消耗. 总计算量为 $(l-1)M + lA$.

但是以上两种算法仍不能抵抗SPA中的倍点攻击[5]和DPA[3]. 抵抗倍点攻击的主要方法是在标量乘法过程中完全避免对“0”位的操作；抵抗DPA的主要方法是随机化方法，随机化曲线、基点或标量. 本文在第二部分给出一种避免“0”位的操作的方法，在第三部分考虑同时采用随机化基点和随机化标量的方法来抵抗SPA和DPA.

2　避免“0”位操作的算法

任意给出一个正整数 k 的二进制表示 $k = \sum_{j=0}^{l-1} k_j 2^j$，$k_j \in \{0,1\}$，总可以对其中的二进制串“0，1”编码为“1，−1”. 如：

$$k = (1,0,1,0,0,1,0,1) = (1,1,-1,1,-1,-1,1,-1)$$

下面给出将二进制串“0，1”编码为“1，−1”的算法 $N0(k,l)$.

输入：$k = (k_{l-1}, k_{l-2}, \cdots, k_0), k_i \in \{0,1\}$

输出：$k = (k_{l-1}, k_{l-2}, \cdots, k_0), k_i \in \{-1,1\}$

　For　$i = 0$　to　$l-1$　do

　　If　$k_i = 1$　and　$k_{i+1} = 0$

　　then　$k_i \leftarrow -1$　and　$k_{i+1} \leftarrow 1$

　Return　k

因此对于一个奇数 k，总可通过 $N0(k,l)$ 表示为 $k = \sum_{j=0}^{l-1} k_j 2^j$，$k_j \in \{-1,1\}$. 这样对奇数 k 编码后就不再包含“0”位，可完全避免对“0”位的操作；当 k 为偶数时，考虑计算 $kP = (k+1)P - P$，则 $k+1$ 为奇数，也可完全避免对“0”位的操作. 但是 k 为偶数时多一步点加运算 $Q - P$，会泄露 k 为偶数的信息. 为了避免这种情况，k 为奇数时，考虑计算 $kP = (k+2)P - 2P$. 避免“0”位操作的算法如下：

输入：P，$k = (k_{l-1}, k_{l-2}, \cdots, k_0)_2$

输出：$Q = kP$

If　$k \bmod 2 = 0$　then　$k' = k+1$

　else　$k' = k+2$

$k = N0(k', l)$

Precompute

　$Q_0 \leftarrow O$

　$Q_1 = P, Q_{-1} = -P, Q_{-2} = -2P$

For　$i = l-1$　downto 0 do

　$Q_0 \leftarrow 2Q_0$

　$Q_0 \leftarrow Q_0 + Q_{k_i'}$

If　$k \bmod 2 = 0$　then　$Q_0 \leftarrow Q_0 + Q_{-1}$

　else　$Q_0 \leftarrow Q_0 + Q_{-2}$

Return　Q_0

该算法简单易行，除预计算外，总计算量为 $(l-1)M+(l+1)A$，仅比抵抗 SPA 的二进制方法多一次点加运算. 预计算的计算量仅为 M，占用三个静态计算器.

3　抵抗 DPA 的标量乘法

随机化基点 P 的主要方法是：在椭圆曲线上随机选择一点 $R \neq P$，计算 $kP=k(P+R)-kR$；随机化标量的常见方法是：计算 $kP=(k+nl)P$，其中 $n=ordE(P)$ 为椭圆曲线的阶，l 为一随机整数[3].

我们在随机化标量时采用 $kP=(k-h)P+hP$ 的方法，其中 h 为与 k 具有相同长度的随机整数；在随机化基点时选用点 $R=dP$，其中 d 为一随机整数. 将这两种方法结合起来，我们得到 $kP=(k-h)dP+[dh-(d-1)k]P$. 抵抗 DPA 的算法如下：

输入：P，$k=(k_{l-1},k_{l-2},\cdots,k_0)_2$

输出：$Q=kP$

$Q \leftarrow O$

$h \leftarrow random\ integer(\cdot), d \leftarrow random\ integer(\cdot)$

$a=(a_1,\cdots,a_l) \leftarrow k-h$

$b=(b_1,\cdots,b_l) \leftarrow dh-(d-1)k$

Precompute

$Q_d \leftarrow dP, Q_{-d} \leftarrow -dP$

$Q_2 \leftarrow Q_1+P, Q_{-2} \leftarrow Q_{-1}+P$

For $i=l-1$ downto 0 do

$Q \leftarrow 2Q$

$c \leftarrow a_i d+b_i$

$Q \leftarrow Q+Q_c$

Return Q

该算法仅通过两个随机数达到同时随机化基点和标量的目的，简单且随机性强，除预计算外，总计算量为 $(l-1)M+lA$，与抵抗 SPA 的二进制方法的运算量基本相同. 预计算占用了四个静态存储器. 预计算的计算量较大，但选用长度较小的 d 可以减少计算量.

4　结　语

本文针对二进制方法和抵抗 SPA 的二进制方法无法抵抗倍点攻击和差分攻击的缺点，提出了两种改进方法. 第一种方法将偶数转化为奇数进行处理，这样通过三进制编码可以完全避免对“0”位的操作，从而能够抵抗倍点攻击. 抵抗差分攻击的方法主要是随机化，第二种方法采用同时随机化标量和随机化基点的方法，从而达到更好的随机性，保证了对 DPA 的安全性. 这两种方法计算量不大且简单易行，比起原来的方法只多了三到四个静态寄存器.

参考文献：

[1] 张宁. 椭圆曲线上点的标量乘法[D]. 西安：西安电子科技大学，2005.

[2] Joye Marc. Elliptic curves and side-channel analysis[J]. ST Journal of System Research，2003，4(1)：283–306.

[3] Coron Jean-Sebastiem. Resistance against differential power analysis for elliptic curve cryptosystems[J]. Cryptographic Hardware and Embedded Systems，1999，1717：292–302.

[4] Izu Tetsuya，Möller Bodo，Takagi Tsuyoshi. Improved elliptic curve multiplication methods resistant against side channel attacks[C]//Progress in Cryptology，Springer-Verlag LNCS 2551，2002：296–313.

[5] Fouque P-A，Valette F. The doubling attack-why upwards is better than downwards[J]. Cryptographic Hardware and Embedded Systems，2003，2779：269–280.

[6] Brier E，Joye M，Weierstrass elliptic curves and side-channel attacks[J]. Public Key Cryptography，2002，2274：335–345.

（上接第 37 页）

[4] 赵冬至，杜飞，赵玲，等. 基于表面反射率的赤潮卫星荧光线高度算法比较[J]. 高技术通讯，2004，14(11)：93–97.

[5] 高中灵，汪小钦，陈云芝. MERIS 遥感数据特性及应用[J]. 海洋技术，2006，25(3)：61–65.

[6] Fell Frank，Fischer Jürgen，Schaale Michael，et al. Retrieval of chlorophyll concentration from MERIS measurements in the spectral range of the sun-induced chlorophyll fluorescence [C]//Conference on Ocean Remote Sensing and Applications. 2002.