

Koblitz 曲线密码体制中一种可抵抗边带信道攻击的标量乘算法

李 明, 秦宝东, 李大兴

(山东大学 网络信息安全研究所, 济南 250100)

(sdu_lm@yahoo.com)

摘 要: 分析了如何改造 Doubling 攻击来攻击 Koblitz 曲线上的标量乘算法, 提出了一种利用半点操作对输入的点进行随机化的方法, 并将其与 Koblitz 曲线上的固定窗口算法结合起来, 以抵抗边带信道攻击。分析表明, 该算法不仅具备了可以抵抗简单功耗分析、差分功耗分析、改进的差分功耗分析、零值攻击和 Doubling 攻击的性质, 而且保持了运算的高效, 具有实际意义。

关键词: 椭圆曲线密码体制; 标量乘; 边带信道攻击; Koblitz 曲线

中图分类号: TP309 **文献标志码:** A

Efficient scalar multiplication algorithm against SCA for Koblitz curve cryptosystems

LI Ming, QIN Bao-dong, LI Da-xing

(Institute of Network Security, Shandong University, Jinan Shandong 250100, China)

Abstract: Analysis of how to transform Doubling attack to attack Koblitz curve of the scalar multiplication was given. A randomized method for input points by using point halving was proposed, which was integrated with Koblitz curve of fixed window algorithm, to resist the side channel attack. The analysis demonstrates that the method can not only resist Simple Power Analysis (SPA), Differential Power Analysis (DPA), Refined Differential Power Analysis (RPA), Zero-value Power Attack (ZPA) and Doubling attack, but also has efficient and practical significance.

Key words: Elliptic Curve Cryptosystem (ECC); scalar multiplication; Side Channel Attack (SCA); Koblitz curves

0 引言

标量乘^[1] (点乘) dP 的计算是椭圆曲线密码体制 (Elliptic Curve Cryptosystem, ECC) 中最基本的运算, 通常用“倍点一点加”的方法来进行, 其中 d 表示一个整数标量而 P 是椭圆曲线上的一个点。文献[2]提出了在特征为 2 的子域曲线上实现 ECC, 通过利用 Frobenius 映射代替倍点操作, 大大提高了标量乘算法的运算效率。而后, 文献[3]提出了 Koblitz 曲线上的 τ -NAF 算法, 使在有限域 F_2^m 上进行的标量乘运算只需要 $m/3$ 次点加操作。

但在某些密码设备上实现基于离散对数问题的公钥密码算法时, 比如在智能卡上, 边带信道攻击 (Side Channel Attack, SCA)^[4,5] 会成为一种特别有效和方便的攻击。它通过分析密码设备的功耗及其相关信息来得到密钥的值。如果只是在设备上增加“干扰源”来抵抗这种攻击, 那么使用差分分析仍然是非常有效的。所以, 设计可以抵抗边带信道攻击的高效算法, 成为当务之急, 各种抵抗算法也曾出不穷^[6]。

简单功耗分析 (Simple Power Analysis, SPA)^[4] 和差分功耗分析 (Differential Power Analysis, DPA)^[5] 是边带信道攻击中最典型的两种方法, 很多其他方法都可以看作这两种方法的扩展。Doubling 攻击^[8] 针对从“左到右”的模指数计算, 也被扩展到了多种情况下。由于在 Koblitz 曲线上的标量乘算法有其特殊性, 所以对于边带信道攻击的分析和抵抗方法也会有所不同^[7]。

本文分析了 Koblitz 曲线上的边带信道攻击, 将一般曲线上的 Doubling 攻击扩展到了 Koblitz 曲线上。通过利用半点运算, 提出一种 Koblitz 曲线上的随机化方法, 构造了一个高效的标量乘算法。分析表明, 这种算法可以有效抵抗各种边带信道攻击。

1 基础知识

1.1 Koblitz 曲线及其上的运算

在域 F_2^m 上, Koblitz 曲线定义如下: $E_a = y^2 + xy = x^3 + ax^2 + 1$, 其中 $a \in \{0, 1\}$ 。这样, 曲线上所有的点再加上无穷远点 O , 在点加运算下构成一个加法群。用 τ 表示 Koblitz 曲线上的 Frobenius 映射, 于是有 $(x^4, y^4) + 2(x, y) = \mu(x^2, y^2)$, 其中 $\mu = (-1)^{1-a}$, 用点加公式可以验证这一点。这样, 推出 $\tau^2 + 2 = \mu\tau$, 解得 $\tau = ((-1)^{1-a} + \sqrt{-7})/2$, 而 τP 称为椭圆曲线上的复乘。用 $\bar{\tau}$ 来表示 τ 的共轭, 于是有 $\tau \cdot \bar{\tau} = 2$ 和 $\bar{\tau} + \tau = \mu$ 。如果用正规基来表示 F_2^m 上的元素, 那么 τP 运算只是分别对 (x, y) 进行一个移位操作。

在 $E(F_2^m)$ 上, 半点操作就是已知点 P , 求点 Q , 并且满足 $2Q = P$, 可以用 $Q = P/2$ 来表示。分析表明, 半点运算比点加操作要快 2 ~ 3 倍^[11]。

1.2 边带信道攻击及其抵抗算法

算法 1 最简单的标量乘算法

Input: a scalar d , base point P ;

Output: multiplied point $Q = dP$;

1) $Q \leftarrow O$;

收稿日期: 2007-02-06; 修回日期: 2007-04-22。 基金项目: 国家 863 计划资助项目 (2003AA141120)。

作者简介: 李明 (1982-), 男, 山东泰安人, 硕士研究生, 主要研究方向: 网络信息安全; 秦宝东 (1982-), 男, 江苏徐州人, 硕士研究生, 主要研究方向: 网络信息安全; 李大兴 (1963-), 男, 辽宁建昌人, 教授, 博士生导师, 主要研究方向: 网络信息安全。

- 2) for i from l down to 0 do
 - (1) $Q \leftarrow 2Q$;
 - (2) if $d_i = 1$ then $Q \leftarrow Q + P$;
- 3) return Q ;

在常用的模幂算法中,包含有程序分支,使硬件在处理不同数据时会消耗不同的时间和功耗,SPA 利用这种信息来分析得到密钥的信息。算法 1 是最简单的标量乘算法,与模幂算法有类似之处。算法 1 中的程序分支与密钥 d 有关,且不同情况下的运算所消耗功率不同,这样通过观察设备的功耗曲线,就可以揭示密钥 d 的信息。为了抵抗 SPA,出现了“总是点加一倍点”算法,通过加入冗余运算,将算法 1 中第(2)步改为不管 d_i 的值是什么,总是做一次点加操作。但这种改变使标量乘运算的效率大为降低。

多次输入不同的点,运行算法就会得到不同的功耗曲线。DPA 就是通过分析这些功耗曲线之间的相关性来得到密钥的信息。由于每次运行中 d 值不变,功耗曲线就会有所偏向,而这种非随机化的信息,正是可以用来分析密钥的工具。针对 DPA,很多随机化方法^[12]被提出,典型的有:密钥随机化、椭圆曲线参数随机化和投影坐标的随机化。然而,后两种方法随着 DPA 的发展被证明了不安全。比如从 DPA 发展而来的改进的差分功耗分析(Refined Differential Power Analysis, RPA)^[9]通过利用特殊的点 $(x, 0)$ 或者 $(0, y)$,使得随机化坐标系的方法变得脆弱。后来, RPA 又进一步发展成为零值攻击(Zero-value Power Attack, ZPA)^[10]:只要在标量乘的运算过程中会出现“0”值的寄存器,就能得到有用的功耗曲线来区分点加和倍点运算,从而进一步揭示密钥 d 中的相关信息。随机化坐标系的方法和随机化曲线参数的方法对于 ZPA 来说都是脆弱的。

1.3 Koblitz 曲线上的 Doubling 攻击

在 Koblitz 曲线上的标量乘算法,同样也有是否抵抗边带信道攻击的问题。由于 Koblitz 曲线上的标量乘算法的特殊性,其抵抗攻击的方法也不同于一般曲线。Koblitz 曲线上的各种抵抗算法也陆续被提出^[7,8]。但是,随着各种攻击分析方法的发展,其中一些方法也已经不再适用和安全。

Koblitz 曲线上实现 Doubling 攻击也有其特殊之处。在 Koblitz 曲线上的标量乘算法用的是“ τ -点加”方法,所以在攻击中,点加操作也要相应地变为 Frobenius 映射操作。Doubling 攻击适用于从左到右的标量乘算法。选择 P 和 τP , 分别输入算法进行运算,得到两条功耗曲线,观察其中功耗完全一样的片段。在 τP_1 和 τP_2 的计算过程中,如果 $P_1 = P_2$, 那么其此处的功耗曲线将完全一样。为了抵抗这种攻击,可以将输入的点随机化,使得每次运算的功耗曲线是随机的。

2 Koblitz 曲线上可以抵御 SCA 的标量乘算法

2.1 可抵抗 SPA 的一种标量乘算法

为了抵抗 SPA,所设计的标量乘算法中,主循环体中每次循环的运算量应该一致,同时考虑到尽量提高运算效率。利用如下定理可以得到一个高效且抵抗 SPA 的标量乘算法。

算法 2 Conversion to SPA-resistant τ NAFw

- Input: $\rho = r_0 + r_1 \tau \in ZZ[\tau]$ with r_0 odd, width w ;
 Output: $(d_i^{(w)}, \dots, d_0^{(w)}) = \tau\text{NAFw}(\rho)$;
- 1) $c_0 \leftarrow r_0$; $c_1 \leftarrow r_1$, $r \leftarrow 0$; $l \leftarrow \lceil m/w \rceil$;
 - 2) while $c_1 \neq 0$ or $c_0 > 2^w$ do
 - (1) $u \leftarrow \Psi_w(c_0 + c_1 \cdot \tau)$; $d_i^{(w)} \leftarrow u$; $c_0 \leftarrow c_0 - u$; $r \leftarrow r + 1$;
 - (2) for j from 1 to w do $(c_0, c_1) \leftarrow (c_1 + \mu c_0/2, -c_0/2)$;

- 3) $d_i^{(w)} \leftarrow \Psi_w(c_0 + c_1 \cdot \tau)$;
- 4) if $r < l$ then for i from $r + 1$ to l do $d_i^{(w)} \leftarrow 0$;
- 5) return $(d_i^{(w)}, \dots, d_0^{(w)})$;

定理 1^[11] 映射 Ψ_w 定义如下:

$$\Psi_w: d_0 + d_1 \cdot \tau \in ZZ[\tau] \rightarrow (d_0 + d_1 \cdot t_{w+1} \bmod 2^{w+1}) - 2^w \in ZZ/2^w ZZ$$

其中 $t_w = 2U_{w-1}U_{w-1} \bmod 2^w$, 则对任意 $d \in ZZ[\tau]$, 有 $d - \Psi_w(d)$ 可以被 τ^w 整除,但是不能被 τ^{w+1} 整除。

这样,可以利用 Ψ_w 来构造一个可以抵抗 SPA 的标量乘算法。注意,在计算 $Q = dP$ 之前,要先计算复数上的模运算 $\rho = r_0 + r_1 \cdot \tau = d \bmod \delta$, 其中 $\delta = (\tau^m - 1)/(\tau - 1)$, $\rho \in ZZ[\tau]$ 。这样使用 ρ 对标量进行重新编码,可以得到一个长度最大为 $m + a$ bit 的表示,其中平均有 $\lceil (m + a)/w \rceil$ 个非零比特。编码算法如算法 2 所示,标量乘算法如算法 3 所示。

算法 3 Scalar multiplication against SPA

- Input: a scalar d , base point P , width w ;
 Output: multiplied point $Q = dP$;
- 1) pre-compute $3P, 5P, \dots, (2^w - 1)P$; $\rho \leftarrow d \bmod \delta$;
 - 2) if $\tau \mid \rho$ then $\rho' \leftarrow \rho + 1$; else $\rho' \leftarrow \rho + \tau$;
 - 3) compute $(d_i^{(w)}, \dots, d_0^{(w)})$, from ρ' with Algorithm1;
 - 4) $Q \leftarrow O$;
 - 5) for i from l down to 0 do
 - (1) for j from 1 to w do $Q \leftarrow \tau Q$;
 - (2) if $d_i^{(w)} > 0$ then $Q \leftarrow Q + d_i^{(w)}P$;
 else $Q \leftarrow Q - (-d_i^{(w)})P$;
 - 6) if $\tau \mid \rho$ then $Q \leftarrow Q - P$; else $Q \leftarrow Q - \tau P$;
 - 7) return Q ;

算法 2 实际上是 Koblitz 曲线上的固定窗口算法^[11]。 τ 展开上的滑动窗口算法^[4]当然比固定窗口算法效率要高,但是固定窗口算法有抵抗 SPA 的特性。在算法 3 中,预计算里进行点加的次数是 2^{w-1} , 而 $l = \lceil m/w \rceil$, 所以点加的个数是 $2^{w-1} + (m + a)/w$ 。运算 τQ 只是进行了两次移位操作,所以算法的运算量是 $(2^{w-1} + (m + a)/w)$ ECADD, 其中 ECADD 表示点加操作。

2.2 DPA 和 Doubling 攻击及其抵抗算法

在一般椭圆曲线密码体制中,常见的抵抗 DPA 的方法有:密钥随机化、椭圆曲线参数随机化和投影坐标的随机化。由于 Koblitz 曲线方程是确定的,所以曲线参数随机化在这儿并不适用;而要求抵抗 RPA 和 ZPA,投影坐标的随机化也无法使用。因此我们选用密钥随机化的方法。要计算 dP , 先选取一随机数 r , 计算 $d + r \cdot \#E$, 其中 $\#E$ 表示点阶。由于 $\#E \cdot P = O$, 所以有 $(d + r \cdot \#E)P = dP$ 。

为了抵抗 RPA、ZPA 和 Doubling 攻击,选用对输入的点进行随机化处理的方法。定理 2 提供了一种高效的随机化的方法。

定理 2 在 F_m^m 上,有 $dP + (\tau - 1)(\sum_{i=0}^m \tau^i)R = dP$, 并且 $P/(\tau - 1) = ((\tau - 1)/(3 - \mu))P$, 其中 $\tau P = \tau P/2$ 。

算法 4 Scalar multiplication against SCA

- Input: a scalar d , base point P , width w ;
 Output: multiplied point $Q = dP$;
- 1) $R \leftarrow \text{Randompoint}() (R \in E(F_2^m) \setminus E(F_2))$,
 $r \leftarrow \text{Randominteger}(); R' \leftarrow ((\tau - 1)(\tau^w - 1)/(3 - \mu))R$.
 - 2) pre-compute $-P_{-}(2^w - 1) \leftarrow -(2^w - 1)P + R'$, \dots , $P_{-0} \leftarrow R'$,
 \dots , $P_{-}(2^w - 1) \leftarrow (2^w - 1)P + R'$;
 - 3) $\rho \leftarrow d + r \cdot \#E \bmod \delta$;

if $\tau \mid \rho$ then $\rho' \leftarrow \rho + 1$; else $\rho' \leftarrow \rho + \tau$;
 4) compute $(d_i^{(w)}, \dots, d_0^{(w)})$ from ρ' with Algorithm 1;
 5) $Q \leftarrow d_i^{(w)} P$; $r \leftarrow m - (l - 1) * w$
 6) for i from $r - 1$ down to 0 do $Q \leftarrow Q + \tau^i R$;
 7) for i from $l - 1$ down to 0 do
 (1) for j from 1 to w do $Q \leftarrow \tau Q$;
 (2) $Q \leftarrow Q + P_- d_i^{(w)}$;
 8) $Q \leftarrow (\tau - 1)Q$; $Q \leftarrow ((\tau - 1)/(3 - \mu))Q$;
 9) if $\tau \mid \rho$ then $Q \leftarrow Q - P$; else $Q \leftarrow Q - \tau P$;
 10) return Q ;

证明 容易验证:

$$(\tau - 1) \left(\sum_{i=0}^m \tau_i \right) R = \tau^{m+1} - \tau^m + \tau^m - \dots + \tau - 1 = \tau^{m+1} - 1$$

而由于 $(\tau^{m+1} - 1)P = O$, 所以 $dP + (\tau - 1) \left(\sum_{i=0}^m \tau_i \right) R = dP$ 。这样可以先计算 $P_1 = dP + \left(\sum_{i=0}^m \tau_i \right) R$, 然后计算 $P_2 = (\tau - 1)Q$, 于是 $dP = P_2/(\tau - 1)$ 。由于 $(\tau - 1)(\tau - 1) = 3 - \mu$, 故 $P_2/(\tau - 1) = ((\tau - 1)/(3 - \mu))P_2$ 。其中 $P_2/(3 - \mu) = P/2$ 或者 $P/4$, 可以用一次或者两次半点操作来计算。

这样, 利用随机化密钥 d 抵抗 DPA, 用随机化点的方法抵抗 RPA、ZPA 和 Doubling 攻击, 从而得到了算法 4。

算法 4 是在算法 3 的基础上修改得来的。与算法 3 相比, 算法 4 多做了第 1 行和第 8 行, 并且第 2 行的点加操作增加了 2^{w-1} 个。所以, 算法 3 的运算量是 $(2^w + 6 + w + (m + a)/w)$ ECADD。而算法 4 预计算里需要的存储量比算法 3 多了 2^{w-1} 个点。

3 分析和比较

通过在 Koblitz 曲线上应用 τ 展开的固定窗口方法和一种随机化方法, 构造了一个快速标量乘算法而几乎没有使用冗余运算。该算法与以往几个 Koblitz 曲线上标量乘算法的比较见表 1。

从表 1 可以看出, 算法 3 比算法 2 只增加了 $2^{w-1} + 6 + w$ 个点加运算。由于 w 取值很小, 通常取 $w = 2, 3, 4$, 所以 $2^{w-1} + 6 + w$ 个点加运算最多也就是 18 个点加运算, 但是却取得了可以抵抗 DPA、RPA、ZPA 和 Doubling 攻击的性质。在有限域 F_2^m 上, 当 $m \geq 160$ 并且取 $w = 4$ 时, 算法 4 的运行效率至少比 Hasan 的算法快 60%。

表 1 各种已有算法的运算量比较

方法名称	是否抵抗 SCA	预计算要求的存储空间/Points	总运算量/ECADD
τ -NAF ^[3]	否	0	$(m + a)/3$
τ 滑动窗口算法 ^[4]	否	$2^{w-2} - 1$	$2^{w-2} - 1 + (m + a)/(w + 1)$
Hasan 的算法 ^[7]	抵抗 SPA 和 DPA	2^{w-1}	$m + 2^{w-1} - 1$
算法 3	抵抗 SPA	$2^{w-1} - 1$	$2^{w-1} + (m + a)/w$
算法 4	抵抗已知常见的 SCA	2^{w-1}	$2^w + 6 + w + (m + a)/w$

4 结语

本文通过在 Koblitz 曲线上应用 τ 展开的窗口方法和一种随机化方法, 构造了一个快速标量乘算法而没有使用冗余运算。分析表明, 这种算法不仅高效, 而且可以有效抵抗各种已知边带信道攻击, 如: SPA、RPA、ZPA、DPA 和 Doubling 攻击。通过与已有算法的比较, 显示出该算法具有高效、安全等优点, 非常适合实际应用, 特别是适于在 IC 卡和 DSP 上的应用实现。

参考文献:

- [1] BLAKE I, SEROUSSI G, SMART N P. Elliptic curves in cryptography[M]. Cambridge: Cambridge University Press, 1999.
- [2] KOBLITZ N. CM-curves with good cryptographic properties[C]// Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology, LNCS 576. London: Springer-Verlag, 1991: 279 - 287.
- [3] SOLINAS J A. Efficient arithmetic on Koblitz curves[J]. Designs, Codes and Cryptography, 2000, 19(2/3): 125 - 179.
- [4] KOCHER C P. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other system[C]// Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology, LNCS 1109. London: Springer-Verlag, 1996: 104 - 113.
- [5] KOCHER C P, JAFFE J, JUN B. Differential power analysis[C]// Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology, LNCS 1666. London: Springer-Verlag, 1999: 388 - 397.
- [6] CORON J-S. Resistance against differential power analysis for elliptic curve cryptosystems[C]// Proceedings of the First International

Workshop on Cryptographic Hardware and Embedded Systems, LNCS 1717. London: Springer-Verlag, 1999: 292 - 302.

- [7] HASAN M A. Power analysis attacks and algorithmic approaches to their countermeasures for Koblitz curve cryptosystems[J]. IEEE Transactions on Computers, 2001, 50(10): 1071 - 1083.
- [8] FOUQUE P A, VALETTE F. The doubling attack-why upwards is better than downwards[C]// Proceedings of Cryptographic Hardware and Embedded Systems (CHES 2003), LNCS 2779. Berlin: Springer-Verlag, 2003: 269 - 280.
- [9] GOUBIN L. A refined power-analysis attack on elliptic curve cryptosystems[C]// Proceedings of 6th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2003), January 6 - 8, 2003, Miami, FL, USA, LNCS 2567. Berlin: Springer-Verlag, 2003: 199 - 210.
- [10] AKISHITA T, TAKAGI T. Zero-value point attacks on elliptic curve cryptosystem[C]// Information Security Conference (ISC '03), LNCS 2851. Berlin: Springer-Verlag, 2003: 218 - 233.
- [11] FONG K, HANKERSON D, LOPEZ J, et al. Field inversion and point halving revisited[J]. IEEE Transactions on Computers, 2004, 53(8): 1047 - 1059.
- [12] HAJ-C, MOON S-J. Randomized signed-scalar multiplication of ECC to resist power attacks[C]// 4th International Workshop on Cryptographic Hardware and Embedded Systems, LNCS 2523. London: Springer-Verlag, 2002: 551 - 563.
- [13] OKEYA K, TAKAGI T, VUILLAUME C. Efficient representations on Koblitz curves with resistance to side channel attacks[C]// Information Security and Privacy (ACISP 2005), LNCS 3574. Berlin: Springer-Verlag, 2005: 218 - 229.