

## 抗边信道攻击的高效多基标量乘算法

尹恒<sup>1\*</sup>, 蒋朝惠<sup>2</sup>, 付威<sup>3</sup>

(1. 贵州大学 大数据与信息工程学院, 贵阳 550025; 2. 贵州大学 计算机科学与技术学院, 贵阳 550025;

3. 国网湖北省电力公司 电力科学研究院, 武汉 430077)

(\* 通信作者电子邮箱 yinheng01988@163.com)

**摘要:**为提高椭圆曲线密码算法的安全性和效率,在现有的边信道攻击和标量乘算法的基础上,提出了一种新的多基标量乘算法。通过引入随机数和基点掩码技术来隐藏算法的相关边信道信息,从而增强算法的安全性;同时,结合快速的半点运算和多基表示标量,提高算法的运行效率。经安全性分析,该算法能较好地抵抗多种边信道攻击。实际实验结果也表明,在美国国家标准技术研究所(NIST)推荐的椭圆曲线 NIST B-163、NIST B-233 和 NIST B-283 上,当预计算点个数分别为 2 和 5 时,新算法比 Purohit 算法效率提高了 36% 和 42%,比赖忠喜等(赖忠喜,张占军,陶东娅. 椭圆曲线中直接计算  $7P$  的方法及其应用[J]. 计算机应用, 2013, 33(7): 1870–1874.) 所提的算法效率提高了 8% 和 11%。该算法可应用到智能卡等存储资源受限的领域中,使其对敏感数据加解密更安全、更高效。

**关键词:**椭圆曲线密码;标量乘法;边信道攻击;多基数系统;半点运算;随机数

**中图分类号:** TP309.2; TP309.7 **文献标志码:** A

## Effective multi-base scalar multiplication algorithm with side-channel attack resistance

YIN Heng<sup>1\*</sup>, JIANG Chaohui<sup>2</sup>, FU Wei<sup>3</sup>

(1. College of Big Data and Information Engineering, Guizhou University, Guiyang Guizhou 550025, China;

2. College of Computer Science and Technology, Guizhou University, Guiyang Guizhou 550025, China;

3. Electric Power Research Institute, State Grid Hubei Electric Power Company, Wuhan Hubei 430077, China)

**Abstract:** To raise the safety and efficiency of algorithm on Elliptic Curve Cryptography (ECC), a new multi-base scalar multiplication algorithm was presented based on original side-channel attack and scalar multiplication algorithm. In order to enhance the algorithm's security, random number and the masking technology of base point were introduced to hide the related side-channel informations of the algorithm. Meanwhile, fast point halving and the multi-base representation of scalar were combined to improve the algorithm's efficiency. According to security analysis, the algorithm can resist various side-channel attacks well. Results of the actual experiments also show that the efficiency of the new method was improved about 36% – 42% over the Purohit's method and about 8% – 11% over the Lai's method (LAI Z, ZHANG Z, TAO D. Algorithm for directly computing  $7P$  elliptic curves and its application[J]. Journal of Computer Applications, 2013, 33(7): 1870 – 1874.) on the elliptic curves recommended by National Institute of Standards and Technology (NIST) including NIST B-163, NIST B-233, NIST B-283, when the number of pre-computation points were 2 and 5 respectively. The new algorithm can be applied to the domains of smart cards and other limited storage resources, making it more secure and efficient to the encryption and decryption of sensitive data.

**Key words:** Elliptic Curve Cryptography (ECC); scalar multiplication; side-channel attack; multi-base number system; point halving; random number

## 0 引言

椭圆曲线密码(Elliptic Curve Cryptography, ECC)较之于 RSA 等其他传统密码,具有安全性高、计算量小、处理速度快、存储空间占用小、带宽要求低等突出优点,尤其适用于智能卡、手机等处理能力、存储空间、带宽和功耗受限的嵌入式移动环境<sup>[1-2]</sup>。然而近年来,边信道攻击(Side-Channel Attack, SCA)却对智能卡中的 ECC 算法带来了巨大的威胁。

标量乘法是 ECC 最关键、最耗时的运算,其安全性和效率直接影响着 ECC 的整体安全性和实现效率。虽然现有的

ECC 标量乘法具有较好的安全性和计算效率,但仍不能满足许多特定应用场合的需要,围绕标量乘法提高其安全性和计算效率成为目前研究的重点。文献[3]的抗功耗攻击标量乘算法利用基点掩码和随机数及循环操作虽具备一定的抗功耗分析攻击能力,但其预计算量过大且采用双基数系统,因而效率较低。文献[4]则用冗余度更高的多基数表示标量,并用查表和随机数的方法保证算法的安全性,但需存储大量预计算点,计算效率也不高。文献[5-6]结合半点运算和多基链的思想,降低了标量乘算法的计算复杂度,但都因其安全性不高,易遭受边信道攻击。文献[7]给出了一种计算  $7P$  的快速

收稿日期: 2014-06-03; 修回日期: 2014-07-25。 基金项目: 贵州省科学技术基金资助项目(黔科合 J 字[2012]2128 号)。

作者简介: 尹恒(1988-),男,湖北孝感人,硕士研究生,CCF 会员,主要研究方向: 椭圆曲线密码学; 蒋朝惠(1965-),男,四川广安人,教授,CCF 会员,主要研究方向: 椭圆曲线密码学; 付威(1989-),男,湖北孝感人,硕士,主要研究方向: 电力系统自动化。

标量乘法,但安全性难以得到保证。赖中喜等<sup>[8]</sup>在文献[7]的基础上构造了一种用除法多项式计算 $7P$ 的高效标量乘法,进一步提高了算法的运算效率,但其基点容易遭受边信道攻击,故其安全性有待加强。因此,本文从抵抗多种边信道攻击和计算性能优化两方面综合考虑,通过恰当地引入随机数和利用基点掩码技术,并结合快速的半点运算和多基表示标量,给出一种具有较强安全性和执行效率高的标量乘法。

## 1 背景知识

定义在二元域 $F_{2^m}$ 上的椭圆曲线 $E^{[9-10]}$ :

$$y^2 + xy = x^3 + ax^2 + b; a, b \in F_{2^m}; b \neq 0$$

在椭圆曲线 $E$ 上一点 $P = (x_1, y_1)$ 满足 $P \neq -P$ ,则仿射坐标系下倍点运算公式 $2P = (u, v)$ 可由式(1)计算:

$$\begin{cases} \lambda = x_1 + y_1/x_1 \\ u = \lambda^2 + \lambda + a \\ v = x_1^2 + u(\lambda + 1) \end{cases} \quad (1)$$

在椭圆曲线 $E$ 上另一点 $Q = (x_2, y_2)$ 满足 $P \neq \pm Q$ ,则点加运算 $P + Q = (u, v)$ 可由式(2)计算:

$$\begin{cases} \lambda = (y_1 + y_2)/(x_1 + x_2) \\ u = \lambda^2 + \lambda + x_1 + x_2 + a \\ v = \lambda(x_1 + u) + u + y_1 \end{cases} \quad (2)$$

设 $I$ 表示 $F_{2^m}$ 上的求逆运算, $M$ 表示 $F_{2^m}$ 上乘法运算, $S$ 表示 $F_{2^m}$ 上平方运算,则由式(1)~(2)可得点加运算( $A$ )的计算量为 $I + 2M + S$ ,倍点运算( $D$ )的计算量为 $I + 2M + 2S$ 。

点加和倍点运算是 ECC 最基本的运算,它们两者构成了标量乘法。标量乘法的计算过程可以用式(3)表示:

$$Q = kP = P + P + \cdots + P (k \text{ 个 } P \text{ 相加}) \quad (3)$$

其中: $k$ 为正整数的私钥, $P$ 是椭圆曲线上的基点, $Q$ 是公钥。式(3)表示有 $k$ 个 $P$ 点作点加运算。由于标量乘法包含密钥 $k$ ,这自然而然地成为了各种攻击的目标。虽然对给定的 $k$ 和 $P$ 计算 $Q$ 比较容易,但由椭圆曲线离散对数问题知,对给定的 $Q$ 和 $P$ 计算 $k$ 却相当困难<sup>[3]2973</sup>。

在计算标量乘中最典型的即是使用二进制标量乘法<sup>[11]</sup>,该算法流程如下:

输入  $P \in E(K), k = (k_{n-1}, k_{n-2}, \dots, k_1, k_0)_2$ 。  
输出  $Q = kP$ 。  
1)  $Q \leftarrow 0$ ;  
2) for  $i$  from  $n-1$  to 0, do:  
     $Q \leftarrow 2Q$ ;  
    if  $k_i = 1, Q \leftarrow Q + P$ ;  
3) return  $Q$

## 2 边信道攻击的类型及手段

边信道攻击,又称信息泄露攻击。它主要利用密码设备运行中无意间泄露的功耗或时间等信息来揭示密钥的值。根据攻击手段不同,可以将其分为简单功耗分析(Simple Power Analysis, SPA)和差分功耗分析(Differential Power Analysis, DPA)。目前还出现了针对椭圆曲线密码系统的零值点功耗分析(Refined Power Analysis, RPA)、零值寄存器功耗分析(Zero-value Power Analysis, ZPA)和倍点攻击(Double Attack, DA)。

SPA 攻击利用标量乘法中,倍点和点加运算功耗的差异性,从功耗波形上直接得到密钥的分布,进而推测出密钥。DPA 攻击通过采集大量明文每次标量乘法运算的功耗曲线,并利用统计分析方法对其分类,再根据功耗曲线上的峰值变化猜测出被攻击的密钥位,依此类推,逐位破解,从而得到密钥<sup>[3]2973</sup>。

RPA 攻击是对 DPA 的一种改进,在基点 $P$ 的坐标已知的条件下,利用 ECC 上某些坐标分量为零的特殊点进行功耗差异攻击。ZPA 是 RPA 的进一步延伸,它对标量乘运算过程中出现的某些零值寄存器进行攻击。即便采用随机化投影坐标或随机化曲线的措施对其也无济于事,因此 ECC 易受 RPA 和 ZPA 攻击<sup>[3]2974</sup>。

DA 攻击主要针对从向左向右的二进制标量乘法。分别用标量算法对 $P$ 和 $nP$ 进行运算,观察得出的两条功耗曲线中完全一样的功耗片段。在计算 $nP_1$ 和 $nP_2$ 过程中,若 $P_1 = P_2$ ,则此处的功耗曲线将完全相同<sup>[4]</sup>。

传统的 ECC 标量乘法极易遭受边信道攻击,如二进制标量乘法中,针对不同的 $k_i$ ,每次循环所需的操作可能也会不同,当 $k_i = 1$ 时会比 $k_i = 0$ 时多一次点加操作,这样通过分析算法的运行时间或功率消耗就能很容易地确定密钥 $k$ 相应的位。为防范此种攻击,算法的执行过程必须独立于密钥 $k$ 。

## 3 安全高效的多基标量乘法

### 3.1 整数的多基表示

设 $B = \{b_i | i = \{1, 2, \dots, l\}, i \in \mathbb{N}_+\}$ 为一小整数集合,则任意整数 $k$ 均可表示成下面的形式:

$$\sum_{i=1}^m s_i b_1^{e_{i1}} b_2^{e_{i2}} \cdots b_l^{e_{il}}; s_i = \pm 1$$

其中: $\{e_{i1}\}, \{e_{i2}\}, \dots, \{e_{il}\}$ 为单调递减序列,且 $s_i = \pm 1$ 。基集在多基表示中为 $\{b_1, b_2, \dots, b_l\}$ , $m$ 则是多基链的链长。当基集取 $\{2, 3\}$ 时,为双基链。双基表示是高冗余的,表示长度非常短;与双基表示相比,多基表示冗余度更高,表示长度更短,因而能明显地提高 ECC 标量乘法运算效率。

### 3.2 半点运算

半点运算是倍点运算的逆运算<sup>[6]163</sup>。

设 $P = (x, y)$ 是二元域椭圆曲线上的一点,且满足 $P \neq -P$ ,则在仿射坐标下,点 $P$ 的倍点运算 $Q = 2P = (u, v)$ 可根据式(4)~(6)求得:

$$\lambda = x + y/x \quad (4)$$

$$u = \lambda^2 + \lambda + a \quad (5)$$

$$v = x^2 + u(\lambda + 1) \quad (6)$$

半点运算与倍点运算刚好相反,即给定 $Q(u, v)$ ,计算 $P(x, y)$ ,使得 $Q = 2P$ 。半点运算公式可由倍点运算公式快速求得,其求解过程如下:

- 1) 通过式(5)求出 $\lambda$ ;
- 2) 将 $\lambda$ 回代到式(6)中,求解出 $x$ ;
- 3) 把所求出的 $x$ 和 $\lambda$ 代入到式(4)中解得 $y$ 。

假如在标量乘运算中全部以半点运算来代替倍点运算,则计算速度能够提高39%<sup>[12]</sup>。在此,用 $I, S, M$ 分别表示求逆,平方及乘法运算。表1给出了在二元域中不同运算的开销情况。

表 1 二元域中不同运算的开销

运算	运算开销	运算	运算开销
$P/2^{[13]}$	$2M$	$3P \pm Q^{[7]}$	$2I + 9M + 3S$
$P/2 \pm Q^{[13]}$	$I + 5M$	$3^k P^{[10]}$	$I + (14k + 12)M$
$P \pm Q^{[7]}$	$I + 2M + S$	$5P^{[14]}$	$I + 13M + 5S$
$2P^{[7]}$	$I + 2M + S$	$5^k P^{[15]}$	$I + (16k + 3)M + (5k + 1)S$
$2P \pm Q^{[7]}$	$I + 9M + 2S$	$7P^{[8]}$	$I + 20M + 6S$
$3P^{[7]}$	$I + 7M + 4S$	$7^k P^{[8]}$	$I + (21k + 3)M + (5k + 1)S$

### 3.3 安全高效的标量乘法

本节将表 1 中的底层域快速算法应用到基于半点运算和底为(2,3,5,7)的多基链中来计算 ECC 标量乘法,并通过恰当的使用随机数来提高算法安全性。

本文中  $k$  表示成:

$$\sum_{i=1}^m s_i (1/2)^{b_i} 3^{t_i} 5^{p_i} 7^{h_i}; |s_i| \in S$$

其中:  $m$  是多基链的长度,  $\{b_i\}$ 、 $\{t_i\}$ 、 $\{p_i\}$ 、 $\{h_i\}$  为单调递减的 4 个序列,  $S$  是由和 3,5,7 互素的奇数所组成的系数集, 记系数集  $S_j$  由前  $j+1$  个元素所组成, 如  $S_1 = \{1, 11\}$ ,  $S_2 = \{1, 11, 13\}$ ,  $S_3 = \{1, 11, 13, 17, 19, 23\}$ 。具体生成该表示形式的算法参见文献[6]<sup>164</sup>, 以下为基于该表示形式的多基标量乘的具体算法。

算法 1 抗边信道攻击的高效多基标量乘法。

输入 整数  $k = \sum_{i=1}^m s_i \left(\frac{1}{2}\right)^{b_i} 3^{t_i} 5^{p_i} 7^{h_i}$ , 其中  $s_i \in \{-1, 1\}$ ,  $b_1 \geq b_2 \geq \dots \geq b_m \geq 0$ ;  $t_1 \geq t_2 \geq \dots \geq t_m \geq 0$ ;  $p_1 \geq p_2 \geq \dots \geq p_m \geq 0$ ;  $h_1 \geq h_2 \geq \dots \geq h_m \geq 0$ ; 点  $P \in E(F_{2^n})$ 。

输出 曲线  $E$  上的一点  $kP \in E(F_{2^n})$ 。

- 1) 生成  $E(F_{2^n})$  上随机点  $R = \text{random}()$ ;
- 2)  $Q \leftarrow s_i P + R$ ;
- 3) for  $i$  from 1 to  $m-1$  do
  - 4)  $u \leftarrow b_i - b_{i+1}$ ;
  - 5)  $v \leftarrow t_i - t_{i+1}$ ;
  - 6)  $w \leftarrow p_i - p_{i+1}$ ;
  - 7)  $z \leftarrow h_i - h_{i+1}$ ;
  - 8) if  $z = 1$ ,  $Q \leftarrow (7^z Q)$ ; //SP 运算
  - 9) else  $Q \leftarrow (7^z Q)$ ; //k-SP 运算
  - 10) if  $w = 1$ ,  $Q \leftarrow (5^w Q)$ ; //FP 运算
  - 11) else  $Q \leftarrow (5^w Q)$ ; //k-FP 运算
  - 12) if  $v = 1$ ,  $Q \leftarrow (3^v Q)$ ; //TP 运算
  - 13) else  $Q \leftarrow (3^v Q)$ ; //k-TP 运算
  - 14)  $Q \leftarrow (1/2)^u Q$ ;
  - 15)  $Q \leftarrow Q + s_{i+1} P$ ;
  - 16)  $i = i + 1$ ;
- 17) End for
- 18)  $Q \leftarrow (1/2)^{b_m} Q$ ;
- 19) if  $t_m = 1$ ,  $Q \leftarrow (3^t Q)$ ; //TP 运算
- 20) else  $Q \leftarrow (3^t Q)$ ; //k-TP 运算
- 21) if  $p_m = 1$ ,  $Q \leftarrow (5^p Q)$ ; //FP 运算
- 22) else  $Q \leftarrow (5^p Q)$ ; //k-FP 运算
- 23) if  $h_m = 1$ ,  $Q \leftarrow (7^h Q)$ ; //SP 运算
- 24) else  $Q \leftarrow (7^h Q)$ ; //k-SP 运算
- 25) return  $Q - R$

在上述算法中, 用 H、HA、A、TP、 $k$ -TP、FP、 $k$ -FP、SP、 $k$ -SP 分别表示  $P/2$ 、 $P/2 \pm Q$ 、 $P \pm Q$ 、 $3P$ 、 $3^k P$ 、 $5P$ 、 $5^k P$ 、 $7P$ 、 $7^k P$  快速运算。这些运算均可由计算公式快速求得, 其中 SP 和  $k$ -SP 运算采用文献[8] 算法计算, 而  $k$ -FP 运算采用文献[15] 算法计算。

本文算法中, 共需要进行  $m-1$  次迭代, 第  $i$  次迭代运算的计算量记为  $Y_i$ , 则:

$$Y_i = (\delta_{z_i,1} \times \text{SP} + (1 - \delta_{z_i,1}) \times (z_i - \text{SP})) + (\delta_{w_i,1} \times \text{FP} + (1 - \delta_{w_i,1}) \times (w_i - \text{FP})) + (\delta_{v_i,1} \times \text{TP} + (1 - \delta_{v_i,1}) \times (v_i - \text{TP})) + (u_i \times \text{H} + \text{A})$$

其中: 当  $i = j$  时,  $\delta_{i,j} = 1$ ; 反之, 当  $i \neq j$  时,  $\delta_{i,j} = 0$ 。

故算法总的计算量记为  $Y$ , 则:

$$Y = \sum_{i=1}^{m-1} Y_i + Y_m = \sum_{i=1}^{m-1} Y_i + b_m \times \text{H} + (\delta_{h_m,1} \times \text{SP} + (1 - \delta_{h_m,1}) \times (h_m - \text{SP})) + (\delta_{w_m,1} \times \text{FP} + (1 - \delta_{w_m,1}) \times (w_m - \text{FP})) + (\delta_{t_m,1} \times \text{TP} + (1 - \delta_{t_m,1}) \times (t_m - \text{TP}))$$

## 4 安全性和效率分析

### 4.1 安全性分析

本文算法采用了基点掩码方法, 即  $kP = (kP + R) - R$ , 随机地生成 ECC 上的点  $R$ , 再将点  $R$  减掉。算法步骤中的第 1) 步生成 ECC 上的随机点  $R$ , 因为每次产生的  $R$  不同, 赋值阶段的每一步都有随机性, 使得标量乘法的输入跟功耗没有相关性, 故无法利用多条功耗曲线进行统计分析来恢复密钥相应信息, 可抵御 DPA 攻击。从第 3) ~ 17) 步的循环过程中, 最后均是“半点-点加”循环操作, 与传统二进制算法中的“点加-倍点……”循环模式不一样, 因此 SPA 攻击者无法利用功耗曲线上出现的功耗差异特征进行攻击, 故可抵御 SPA 功耗攻击。随机数的恰当引入以及多基数系统来表示标量, 使得攻击者在算法运行过程中不能够准确地掌握其“0”值的功耗, 基点的坐标也不能够被预先知道, 所以能抵御 RPA 与 ZPA 攻击。随机数的生成和标量的重编码, 则不能够仅仅通过观察两条功耗曲线中相同的功耗片段来推出密钥的相关信息, 从而使得 DA 攻击无法凑效。因此, 本文算法具备了全面抗边信道攻击的能力。与传统的二进制算法和文献[5-6,8] 中基点未加保护的多基标量乘法相比, 本文算法的安全性得到了增强。

### 4.2 效率分析

目前, 文献[5-6,8] 是利用多基链来计算标量乘法中运算效率较高的算法。本文在 NIST 推荐的椭圆曲线 NIST B-163、NIST B-233 和 NIST B-283 上, 比较了文献[5-6,8] 算法和本文算法的底层运算量。针对每一条曲线, 分别随机地选取 10000 组接近域长的大整数标量  $k$ , 表 2 给出了这 4 种算法所需要的平均底层域的运算量(其中  $N$  为预存储点数)。在二元域  $F_{2^n}$  椭圆曲线上, 一般选取  $I = 8M$ 。

表2 4种多基数算法运算量比较

算法	N	NIST B-163 ( $k=160$ b)			NIST B-233 ( $k=233$ b)			NIST B-283 ( $k=283$ b)		
		I	M	总运算量	I	M	总运算量	I	M	总运算量
文献[5]算法	0	79.04	711.38	1343.70M	113.18	1012.29	1917.73M	138.01	1221.41	2325.49M
文献[6]算法	2	51.53	621.37	1033.61M	74.71	891.63	1489.31M	90.42	1093.48	1816.84M
	5	44.65	580.43	937.63M	64.75	839.28	1357.28M	78.55	1026.13	1654.53M
文献[8]算法	2	39.69	616.37	933.89M	55.73	858.81	1304.65M	68.17	1054.22	1599.58M
	5	34.38	578.36	853.40M	49.49	826.37	1222.29M	60.34	1009.51	1492.23M
本文算法	2	30.92	613.15	855.31M	40.31	833.61	1156.09M	48.90	1026.78	1417.98M
	5	25.99	577.64	785.56M	36.22	816.90	1106.66M	44.27	998.05	1352.21M

由表2可知:在NIST推荐的三个二元域椭圆曲线上,文献[5]算法、文献[6]算法、文献[8]算法、本文算法所需总运算量依次减少。具体的,当 $N=2$ 时,本文算法在曲线NIST B-163上比文献[5]和文献[8]算法的运算量分别减少了36.5%和8.4%;当 $N=5$ 时,运算量分别减少了41.5%和8.0%。当 $N=2$ 时,本文算法在曲线NIST B-233上比文献[5]和文献[8]算法的运算量分别减少了39.7%和11.4%;当 $N=5$ 时,运算量分别减少了42.3%和9.5%。当 $N=2$ 时,本文算法在曲线NIST B-283上比文献[5]和文献[8]算法的运算量分别减少了39.0%和11.4%;当 $N=5$ 时,运算量分别减少了42.0%和9.4%。

## 5 结语

目前,大多数的椭圆曲线多基标量乘法都难以解决好安全性和效率两者之间的矛盾。本文提出一种新的(2,3,5,7)-多基标量乘法,利用随机数和基点掩码技术,全面保证了算法抗边信道攻击的性能,能抵抗SPA、DPA、ZPA及DA攻击;同时通过扩大多基链的系数集和使用半点运算,使得标量表示更短更稀疏,从而降低了算法的计算复杂度。安全性分析及实验结果表明,该算法同时提高了抗边信道攻击的能力和标量乘法的运算效率,较好地兼顾了算法的安全性和实现效率。在智能卡等其他存储资源受限的领域中,使用本文算法能使椭圆曲线密码体制加解密的实现更加安全、高效。

## 参考文献:

- [1] YAO J, ZHANG T. ECC algorithm for preventing side-channel attack[J]. Journal of Computer Applications and Software, 2013, 30(5): 203-205. (姚建波, 张涛. 抗侧信道攻击的椭圆曲线密码算法[J]. 计算机应用与软件, 2013, 30(5): 203-205.)
- [2] YAO J, ZHANG T. Safe and effective elliptic encryption algorithm resistance against side-channel attack[J]. Journal of Application Research of Computers, 2012, 29(12): 4639-4643. (姚建波, 张涛. 抗侧信道攻击的安全有效椭圆加密算法[J]. 计算机应用研究, 2012, 29(12): 4639-4643.)
- [3] WANG Z, ZHAO J. Resisting power analysis attack scheme based on signed double-based number system[J]. Journal of Computer Applications, 2011, 31(11): 2973-2975. (王正义, 赵俊阁. 基于带符号双基数系统的抗功耗攻击方案算法[J]. 计算机应用, 2011, 31(11): 2973-2975.)
- [4] TONG L, LIU N, QIAN J. Improved against power analysis of elliptic curve scalar multiplication algorithm[J]. Computer Engineering and Applications, 2011, 47(33): 68-70. (童莲, 刘宁, 钱江. 改进的抗能量分析的椭圆曲线标量乘法[J]. 计算机工程与应用, 2011, 47(33): 68-70.)
- [5] PUROHIT G N, RAWAT S A, KUMAR M. Elliptic curve point multiplication using MBNR and point halving[J]. International Journal of Advanced Networking and Applications, 2012, 3(5): 1329-1337.
- [6] HONG Y, GUI F, DING Y. Extended algorithm for scalar multiplication based on point halving and MBNS[J]. Computer Engineering, 2011, 37(4): 163-165. (洪银芳, 桂丰, 丁勇. 基于半点和多基表示的标量乘法扩展算法[J]. 计算机工程, 2011, 37(4): 163-165.)
- [7] PUROHIT G N, RAWAT A S. Fast scalar multiplication in ECC using the multi base number system[J]. International Journal of Computer Science Issues, 2011, 8(1): 131-137.
- [8] LAI Z, ZHANG Z, TAO D. Algorithm for directly computing 7P elliptic curves and its application[J]. Journal of Computer Applications, 2013, 33(7): 1870-1874. (赖忠喜, 张占军, 陶东娅. 椭圆曲线中直接计算7P的方法及其应用[J]. 计算机应用, 2013, 33(7): 1870-1874.)
- [9] WANG Y, ZHANG C, ZHANG B. Improved fast algorithm of scalar multiplication for fix base point[J]. Computer Science, 2013, 40(10): 135-138. (王玉玺, 张串绒, 张柄虹. 一种改进的固定基点标量乘快速算法[J]. 计算机科学, 2013, 40(10): 135-138.)
- [10] YIN X, ZHAO R, HOU H, et al. Fast DBNS scalar multiplication algorithm based on halving operation[J]. Journal of Computer Applications, 2009, 29(5): 1285-1288. (殷新春, 赵荣, 侯洪洋, 等. 基于折半运算的快速双基数标量乘法[J]. 计算机应用, 2009, 29(5): 1285-1288.)
- [11] THOMAS C, ARNAUD T. On-the-fly multi-base recoding for ECC scalar multiplication without pre-computations[C]// Proceedings of the 21st IEEE Symposium on Computer Arithmetic. Piscataway: IEEE Press, 2013: 219-228.
- [12] KNUDSEN E W. Elliptic scalar multiplication using point halving[C]// Proceedings of ASIA CRYPT 1999, LNCS 1716. Berlin: Springer-Verlag, 1999: 135-149.
- [13] HANKERSON D, MENEZES A J, VANSTONE S. Guide to elliptic curve cryptography[M]. Berlin: Springer-Verlag, 2004.
- [14] MISHRA P K, DIMITROV V. Efficient quintuple formulas for elliptic curves and efficient scalar multiplication using multibase number representation[C]// ISC 2007: Proceedings of the 10th International Conference on Information Security, LNCS 4779. Berlin: Springer-verlag, 2007: 390-406.
- [15] DENG W. Research on scalar multiplication of elliptic curve cryptography[D]. Kunming: Kunming University of Science and Technology, 2012. (邓维勇. 椭圆曲线密码体制中标量乘法研究[D]. 昆明: 昆明理工大学, 2012.)