第32卷 第23期 计 算 机 工 程 2006年12月
Vol.32 No.23 Computer Engineering December 2006
·安全技术· 文章编号：1000—3428(2006)23—0143—02 文献标识码：A 中图分类号：TP309

两类超奇异椭圆曲线的快速标量乘法

张 宁[1]，陈志雄[1,2]，肖国镇[1]
(1. 西安电子科技大学ISN国家重点实验室信息保密研究所，西安 710071 2；2. 莆田学院数学系，莆田 351100)

摘 要：研究了特征为2和3的域上的超奇异椭圆曲线的快速标量乘法。该两类曲线适合建立可证明安全的密码体制，利用这两类曲线的复乘性质，结合Frobenius自同态和可以简单计算的自同态，给出了一种不用预计算的快速算法，相较IEEE1363标准算法，计算效率分别提高了4倍和3倍。

关键词：密码学；椭圆曲线；标量乘法

Fast Scalar Multiplication on Two Family of Supersingular Elliptic Curve

ZHANG Ning[1], CHEN Zhixiong[1,2], XIAO Guozhen[1]
(1. Information Security & Privacy Institute in ISN, Xidian University, Xi'an 710071; 2. Department of Mathematics, Putian College, Putian 351100)

【Abstract】 Fast scalar multiplication on two family of supersingular elliptic curves in characteristic 2 and 3 is discussed. Provable secure cryptographic scheme can be obtained on these curves. With the complex multiplication property of these curves, a fast algorithm without precomputation is derived from Frobenius endomorphism and another fast endomorphism, which is 4 times and 3 times faster than IEEE1363 standard method.

【Key words】 Cryptography; Elliptic curve; Scalar multiplication

椭圆曲线密码(ECC)是基于椭圆曲线离散对数问题(ECDLP)的一类公钥密码，其中超奇异椭圆曲线由于存在MOV攻击和FR攻击一直被避免使用，但是最近的一些研究中表明，有3类超奇异椭圆曲线可以用来构造可证明安全的密码体制[1～3]。基于椭圆曲线的复乘理论， Koblitz最早提出了利用Frobenius自同态计算点的标量乘的算法[4]，在CRYPTO'01[5]上Gallant、Lamber和Vanstone提出了利用可快速计算的自同态计算标量乘的GLV算法构思，使得复乘在标量乘法中得到了完全的利用。本文采用Frobenius自同态以及两类曲线各自的一种自同态组合给出一种新的算法。

1 背景介绍

设 P 是一素数，n 是一正整数，记 $q=p^n$，记 F_q 是特征为 P 的有限域。定义在有限域 F_q 上的椭圆曲线 $E(F_q)$ 是指下面的方程在 F_q 上的解连同一个特殊元素 O 所组成的集合：

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x^4+a_6 \quad a_i\in F_q \tag{1}$$

$x,y\in F_q$，在 $E(F_q)$ 的元素之间有一个自然的群运算法则能使其构成一个加法群，其中 O 是单位元。可以说椭圆曲线 $E(F_q)$ 是一个有限加法群。关于椭圆曲线及椭圆曲线密码的进一步内容可参阅文献[6～8]，这里不再赘述。

现设 $P=(x,y)$ 是椭圆曲线 $E(F_q)$ 上的一点，k 为一整数。令 $Q=kP$，则椭圆曲线 $E(F_q)$ 上的标量乘法是指已知 k 和 P 计算 Q。在椭圆曲线密码体制的实现中，标量乘法是关键。相对于标量乘法所用时间，其它计算所用时间都可忽略不计。标量乘法的现有标准算法 IEEE1363 中，用完全不连接表示(Non-Adjacent-Form，NAF)法表示 k，即 $k=(e_{m-1}e_{m-2}...e_0)_2$，其中 $e_i=-1,0,1$， $0\le i<m$ 其中 e_i 为0的概率为 $\frac{2}{3}$，算法如下：

算法 1

Input $P=(x,y)$， $k=(e_{m-1}e_{m-2}...e_0)_{NAF}$
$Q\leftarrow P$
for $i=m-2$ down to 0 do
$Q\leftarrow 2Q+e_iP$
Output Q

此算法的计算量为 $\frac{4}{3}m$ 次点运算。本文以这种基本算法为标准讨论新的快速算法。下面首先介绍 Frobenius 自同态的有关概念，再引出超奇异椭圆曲线的一些概念。

用 ϕ 表示方程(1)在 F_q 的代数闭域 $\overline{F_q}$ 上的Frobenius自同态，$\phi:(x,y)\to(x^q,y^q)$；$O\to O$，其中， $x,y\in\overline{F_q}$ 且满足方程(1)。则 ϕ 满足方程 $\phi^2-t\phi+q=0$，其中 $|t|\le 2\sqrt{q}$ 称为Frobenius自同态 ϕ 的迹，根据Weil定理[7]并且有 $\#E(F_q)=q+1-t$，这里 $\#E(F_q)$ 表示曲线 $E(F_q)$ 上点的个数。

设 $P=(x,y)\in F_q$，则有 $\phi(P)=(x^q,y^q)$， $\phi^2(P)=(x^{q^2},y^{q^2})$，…，$\phi^n(P)=(x^{q^n},y^{q^n})$。在 F_q 中，当采用正规基表示域中元素时，上述各式子右边的计算是非常容易的(循环移位即可)。

对于一个椭圆曲线 E，所有的自同态，包括零同态，构成一个自同态环，表示为 $\mathrm{End}(E)$，这个自同态环中的常数同态，即 $\varphi_n:P\to nP$，其中 n 为整数，构成子环，与整数环 Z 同

基金项目：国家“973”计划基金资助项目(G1999035804)；福建省自然科学基金资助项目(A0540011)
作者简介：张 宁(1979－)，女，博士生，主研方向：公钥密码学信息与网络安全；陈志雄，博士生；肖国镇，教授、博导
收稿日期：2005-12-06 **E-mail：**znlady@163.com

构，当 $\mathrm{End}(E)\neq Z$ 时，即自同态中除了常数同态还有其它的同态类型时，称椭圆曲线 E 具有复乘，当椭圆曲线的基域特征不为 0，一般来说有限域椭圆曲线都是具有复乘的。Frobenius 自同态就是一种非常数的同态。

超奇异椭圆曲线有很多种定义方法，这里根据 Frobenius 自同态 ϕ 的迹 t 的值来定义。这也是最直观的一种方法。

定理 若E是定义于特征为P的有限域F_q上的椭圆曲线，则当且仅当以下条件之一成立时E是超奇异椭圆曲线：(1) $p|t$ ；(2) p=2,3 时 $j(E)$=0 ； $p\geq 5$ 时， t=0 。

对于超奇异椭圆曲线，存在MOV[9]演化法。这种方法将基于该椭圆曲线的ECDLP通过weil对使其嵌入到F_q (定义该曲线的有限域)的一个扩域 F_{q^k} 上，然后利用对 F_{q^k} 上的DLP上的求解方法最终对ECDLP求解。这里的这个 k 称为椭圆曲线的安全MOV指数。也就是说对于椭圆曲线， $E(F_q)$ 上的ECDLP的安全性相当于 F_{q^k} 上的DLP。而对于超奇异椭圆曲线，已经证明， $k\leq 6$ 。这一类椭圆曲线中有 3 类[10]是可以构造符合要求的密码机制，本文讨论其中特征为 2 和 3 的 2 类快速标量乘法。

2 快速标量乘法

本节分别对这 2 类超奇异椭圆曲线进行讨论。这 2 类曲线可以用来构造低带宽可证明安全的密码体制，比如短签名，基于身份的密码体制 2。

2.1 特征为 2 的超奇异椭圆曲线

对于 $a\in\{0,1\}$， n 为与 6 互素的整数，椭圆曲线

$$E(F_{2^n}):y^2+y=x^3+x+a \tag{2}$$

这一类超奇异椭圆曲线的 MOV 指数为 4， 并且有 $\phi^2-2(-1)^a\phi+2=0$ 。对于 $E(F_{2^n})$ 上点 $P_1=(x_1,y_1)$ 和 $P_2=(x_2,y_2)$ ，$P_3=P_1+P_2=(x_3,y_3)$ ，根据群法则定义，有 $-O=O$ $-P_1=(x_1,-y_1)$ ，$P+O=O+P=p$ ，以及

$$\begin{cases} P_3=O & & P_1=-P_2 \\ x_3=\lambda^2,\ y_3=\lambda(x_1+x_3)+y_1+1 & \lambda=x_1{}^2+1 & P_1=P_2 \\ x_3=\lambda^2+x_1+x_2,\ y_3=\lambda(x_1+x_3)+y_1+1 & \lambda=\dfrac{y_1+y_2}{x_1+x_2} & P_1\neq -P_2 \end{cases}$$

由上式得到： $2P=(x^4+1,x^4+y^4)$ 。考虑映射： $\mu:(x,y)\to(x+1,x+y)$; $O\to O$ 。

因为 $(x+y)^2+(x+y)=(x+1)^3+(x+1)+a$ 成立，可以证明映射 μ 是 $E(F_{2^n})$ 上的自同态。利用 Frobenius 自同态和 μ 自同态，组合一种可简单计算的自同态 $\lambda:(x,y)\to(x^4+1,\ x^4+y^4)$ ，即 $\lambda(P)=\mu(\phi^2(P))$ 。自同态 λ 相较域中的乘法运算量可以忽略不计，可以把标准算法中求 $2Q$ 的步骤用 λQ 来代替，这种快速算法的运算量为 1/3n 次点运算，运算速度大约是原来的 4 倍，运算效率提高了约 75%。对于不同的 m 值，根据 LiDIA 的标准运算时间，仿真结果如表 1。

表 1 特征为 2 的超奇异椭圆曲线(时间单位：μs)

n 的值	倍点	点加	同态运算	算法 1	新算法	效率节省
163	123	124	2	26 786	7 009	74.1%
191	146	148	2	37 308	9 805	74.4%
239	199	202	2	63 654	16 332	74.8%

注:其中 $j(E)$ 为椭圆曲线 E 的 j 不变量，具体值参见文献[7]。

进一步考虑，计算得出 $4P=(x^{16},1+y^{16})$，可以构造其它的组合同态来简化计算，当然这样需要预计算，但是计算效率提高更大，本文将不再进一步研究，仅提出思路。

2.2 特征为 3 的超奇异椭圆曲线

对于 $a\in\{-1,1\}$， n 为与 6 互素的整数椭圆曲线

$$E(F_{3^n}):y^2=x^3-x+a \tag{3}$$

这类超奇异椭圆曲线的 MOV 阶为 6,其中 $\phi^2+3a\phi+3=0$ 。对于 $E(F_{3^n})$ 上点 $P_1=(x_1,y_1)$ 和 $P_2=(x_2,y_2)$ ， $P_3=P_1+P_2=(x_3,y_3)$ ，根据群法则定义，有 $-O=O$ $-P_1=(x_1,-y_1)$ ， $P+O=O+P=p$ 和

$$\begin{cases} P_3=O & & P_1=-P_2 \\ x_3=\lambda^2+x_1,\ y_3=-\lambda^3-y_1 & \lambda=1/y_1 & P_1=P_2 \\ x_3=\lambda^2-x_1-x_2,\ y_3=y_1+y_2-\lambda^3 & \lambda=\dfrac{y_1-y_2}{x_1-x_2} & P_1\neq -P_2 \end{cases}$$

根据上式可得： $3p=(((x)^3)^3-a,-((y)^3)^3)$ 。首先讨论映射 $\sigma:(x,y)\to(x-a,-y)$ $O\to O$ ，可以证明 σ 是 $E(F_{3^m})$ 上的自同态。因为 $(-y)^2=(x-a)^3-(x-a)+a$ 成立。利用 Frobenius 自同态和 σ 自同态，可以组合一种可以简单计算的自同态， $\lambda:(x,y)\to(x^9-a,-y^9)$ ，这是 ϕ 和 σ 的组合，即 $\lambda(P)=\sigma(\phi^2(P))$ 。显然映射 σ 的计算量相较域乘等运算可以忽略不计，此时对于标量乘法， $Q=kP$ ， $k=(e_{n-1}e_{n-2}...e_1e_0)_2$ 是 k 的带符号的三进制表示，其中 $e_i=-1,0,1$ 。算法如下：

Input $P=(x_1,y_1)$ ， $k=(e_{n-1}e_{n-2}...e_0)_3$
$Q\leftarrow P$
For $i=n-2$ downto 0 do
$Q\leftarrow \sigma Q+e_iP$
Output Q

下面给出 k 的带符号的三进制表示的算法：

算法 STF(Signed-Ternary Form)

Input k	then $n\leftarrow -1$
Set $S\leftarrow<>$	$k=(k-n)/3$
While $k>0$ do	prepend n to S
$n\leftarrow k \bmod 3$	Endwhile
if $n=2$	Output S

在新的标量乘法中，需要计算 $\frac{2}{3}n$ 次点加，而在标准算法中需要计算 $\frac{4}{3}n\log_2 3$ 次点加运算(这里认为点加和倍点运算的运算量相同)，这样，计算效率提高了约 68%。

表 2 特征为 3 的超奇异椭圆曲线(时间单位：μs)

m 的值	倍点	点加	同态运算	算法 1	新算法	效率节省
163	123	124	1	42 590	13 855	67.5%
191	146	148	1	59 320	19 419	67.7%
239	199	202	1	101 210	32 425	67.9%

3 结束语

本文讨论 2 类超奇异椭圆曲线上的标量乘法，利用这 2 种曲线上的复乘，分别使用了这 2 种曲线上的一种可快速计算的自同态与自同态组合构造的一种映射，构造出的映射可在几乎不耗费计算资源的条件下求出 2 倍点(对基域特征为 2 的曲线)和 3 倍点(对基域特征为 3 的曲线),并给出了求标量 k 带符号的三进制表示的算法。所得新的标量乘法均不需要预计算，比标准算法计算效率分别提高了约 75%和 68%。

因为超奇异椭圆曲线的性质，利用它们的复乘，可以构造效率更高的标量乘算法，比如文献[11]和文献[4]中所提到的 Frobenius 展式法，但是这种方法求 Frobenius 展式的方法和运算量都有待研究；本文中提到的λ也可以作为有效的同态，构成同态环，可以讨论λ展式法或一些其它可以简单计算并且展式的长度比较短的同态的展式，这些都是可以提高椭圆曲线标量乘法效率的一些思路。

（下转第 150 页）