Weil配对求解椭圆曲线离散对数的实施分析*

胡 建 军

(兰州文理学院 数字媒体学院，甘肃 兰州 730010)

摘 要： Weil配对广泛应用于加密、解密、签名、密码交换和密码体制安全分析中. 1993年, Menezes等利用Weil配对有效地将超奇异椭圆曲线的离散对数约减到有限域上的离散对数, 基于Weil配对的椭圆曲线密码体制遭受严峻挑战, 然而, 基于Weil配对的椭圆曲线密码体制的应用并未止步. 为此, 分析了适合Weil配对椭圆曲线的特征, 指出适合Weil配对的椭圆曲线是具有二元循环群结构的曲线, 一元群结构的超奇异椭圆曲线通过嵌入度的方式能够构造出二元群结构的超奇异椭圆曲线. 同时, 为了方便理解Weil配对的实施, 列出了适合Weil配对安全的常见椭圆曲线. 最后, 聚焦了MOV攻击嵌入度为偶数的超奇异椭圆的实施过程, 利用PARI软件验证了分析结论, 指出了PARI和SageMath软件在设计上存在的缺陷.

关键词： 有限域; 超奇异椭圆曲线; 扭曲群; 离散对数; Weil配对

DOI： 10.13568/j.cnki.651094.651316. 2024.01.09.0001

中图分类号： TP309.7 **文献标识码：** A **文章编号：** 2096-7675(2024)03-0329-07

引文格式： 胡建军. Weil配对求解椭圆曲线离散对数的实施分析[J]. 新疆大学学报(自然科学版中英文)，2024，41(3)：329-335+343.

英文引文格式： HU Jianjun. Implementation analysis of Weil pairing for solving discrete logarithms of elliptic curves[J]. Journal of Xinjiang University(Natural Science Edition in Chinese and English)，2024，41(3)：329-335+343.

Implementation Analysis of Weil Pairing for Solving Discrete Logarithms of Elliptic Curves

HU Jianjun

(*School of Digital Media, Lanzhou University of Arts and Science, Lanzhou Gansu 730010, China*)

Abstract： Weil pairing is widely used in encryption, decryption, signature, cryptographic exchange and cryptosystem security analysis. In 1993, Menezes et al. used Weil pairing to effectively reduce the discrete logarithm of a supersingular elliptic curve to the discrete logarithm over a finite field, so the elliptic curve cryptosystem based on Weil pairing was seriously challenged. However, the application of elliptic curve cryptosystem based on Weil pairing has not stopped. For this reason, the characteristics of elliptic curves suitable for Weil pairing are analyzed, and it is pointed out that the elliptic curves suitable for Weil pairing are curves with binary cyclic group structure, and the hypersingular elliptic curves with monadic group structure can be constructed by means of embedding degree. At the same time, in order to facilitate the understanding of the implementation of Weil pairing, common elliptic curves suitable for Weil pairing safety are listed. Finally, we focus on the implementation process of MOV attack with even embedding degree of supersingular elliptic curve, verify the analysis results by using PARI software, and point out the design flaws of PARI and SageMath software.

Key words： finite field; hypersingular elliptic curve; torsion group; discrete logarithm; Weil pairing

0 引 言

基于配对的密码学近年来受到广泛关注, 并正在作为下一代密码系统进行标准化[1]. 配对的作用是将椭圆曲线子群中的离散对数约减到有限域中的离散对数. 1993年, Menezes等[2]利用Weil配对有效地将超奇异椭圆曲线的离散对数约减到有限域上的离散对数, 这种攻击被称为MOV攻击. 类似的, 1999年, Frey等[3]利用Tate配对

* **收稿日期：** 2024-01-09

基金项目： 兰州文理学院服务地方经济社会发展计划项目“椭圆曲线密码关键技术研究”（2021FWDF15）.

作者简介： 胡建军（1971—），男，硕士，教授，主要从事信息安全、协议工程的研究，E-mail：Hujj518@126.com.

将迹2椭圆曲线的离散对数约减到有限域中的离散对数, 这种攻击称为FR攻击. 这些攻击方法为人们选择安全的椭圆曲线提供了遵循. 除此之外, 寻找基于配对的能够有效计算的椭圆曲线也是人们研究的热点[1,4−6], 称为配对友好椭圆曲线(Pairing-Friendly Elliptic Curves, PF-EC). 众所周知, 并不是所有的椭圆曲线都适合Weil配对. 为此, 分析了适合Weil配对椭圆曲线的特征, 指出适合Weil配对的椭圆曲线是具有二元循环群结构的曲线, 一元群结构的超奇异椭圆曲线通过嵌入度的方式构造出二元群结构的超奇异椭圆曲线, 即超奇异椭圆曲线的Weil配对的实施需要曲线的转换. 同时, 为了方便理解Weil配对的实施, 列出了适合Weil配对安全的常见椭圆曲线. 最后, 聚焦了MOV攻击嵌入度为偶数的超奇异椭圆的实施过程, 并利用PARI软件验证了分析结论.

1 Weil配对的椭圆曲线

1.1 椭圆曲线的特征

设$p>3$是一个大素数, F_p为素数有限域, 椭圆曲线E是一个形如$E: y^2=x^3+Ax+B$的方程, 其中$A,B\in F_p$, 且$\triangle$=-16$(4A^3+27B^2)\neq 0$, 点$(x,y)\in F_p\times F_p$是方程$E: y^2=x^3+Ax+B$的一个解. $E(F_p)$表示F_p上所有满足方程$E: y^2=x^3+Ax+B$解的点集, 包括无穷远点O. $E(F_p)$上“+”运算定义如下:

$$(x,y)+O=O+(x,y)=(x,y) \tag{1}$$

$$(x,y)+(x,\text{-}y)=O \tag{2}$$

若$y\neq 0$, 令$\lambda=(3x^2+A)/2y$, 则$(x_3,y_3)=2(x,y)$, 其中

$$x_3=\lambda^2-2x,\ y_3=\lambda(x-x_3)-y \tag{3}$$

若$x_1\neq x_2$, 令$\mu=(y_2-y_1)/(x_2-x_1)$, 则$(x_3,y_3)=(x_1,y_1)+(x_2,y_2)$, 其中

$$x_3=\mu^2-x_1-x_2,\ y_3=\mu(x_1-x_3)-y_1 \tag{4}$$

因此, $(E(F_p),+)$是一个以O为单位元的阿贝尔群.

假设$N=\#E(F_p)$是E的阶, 由Hasse定理[7]可知$|p+1-N|\leq 2\sqrt{p}$, $N=p+1-t$, 其中t是椭圆曲线的迹, $|t|\leq 2\sqrt{p}$.

假设$P\in E(F_p)$, $n\geq 2$是一个整数, 则$E[n]=\{P\in E(F_p)|nP=O\}$表示$n$的扭曲子群, P表示$E[n]$上的一个扭曲点, $<P>$表示由P生成的子群. $Q\in <P>\subseteq E[n]$是不同于P的一个点. $E[n]$上的离散对数问题是指: 已知$Q=lP$, 其中$l\in\{0,1,\cdots,n-1\}$, 求l的值.

1.2 Weil配对的性质

设$q=p^m$, $m\geq 1$, $K=F_q$表示一个有限域, 用$Char(K)$表示域K的特征, 当$Char(K)>0$时, 有$Char(K)=p$.

引理 1[8] 假定E是定义在域K上的一条椭圆曲线. $n\geq 2$是一个正整数, 且$p\nmid n$, 或者$Char(K)=0$, 则$E[n]\cong Z/nZ\oplus Z/nZ$. 如果$Char(K)>0$且$p|n$, 令$p\nmid n'$, 则$n=p^r n'$, $E[n]\cong Z/n'Z\oplus Z/n'Z$或者$E[n]\cong Z/nZ\oplus Z/n'Z$.

假定E是定义在域K上的一条椭圆曲线, $n\geq 2$是一个整数, 且$p\nmid n$, 则映射$e_n: E[n]\times E[n]\to\mu_n$称为Weil配对. 若$T,S,T_1,T_2,S_1,S_2\in E[n]$, 则Weil配对具有如下性质[9−10]:

(I) 双线性

$$e_n(T_1+T_2,S)=e_n(T_1,S)e_n(T_2,S) \tag{5}$$

$$e_n(T,S_1+S_2)=e_n(T,S_1)e_n(T,S_2) \tag{6}$$

(II) 交替性

$$e_n(T,T)=e_n(S,S)=1 \tag{7}$$

$$e_n(T,S)=e_n(S,T)^{-1} \tag{8}$$

(III) 非退化

若$e_n(S,T)=1$, 则

$$T=O\text{或}S=O \tag{9}$$

(IV) 相容性

若$P\in E[nh]$, $Q\in E[n]$, 则

$$e_{nh}(P,Q)=e_n(hP,Q) \tag{10}$$

(V) 伽罗瓦恒等

若$\sigma\in Gal(\Omega/K)$, 则

$$e_n(S,T)^\sigma=e_n(S^\sigma,T^\sigma) \tag{11}$$

假设$\{T_1,T_2\}$是扭曲群$E[n]$的一个基, 则由Weil配对的性质可知, $e_n(T_1,T_2)$是第n个本原单位根.

2　Weil配对实施的椭圆曲线

2.1　Weil配对椭圆曲线群的结构

定义 1　如果$p|t$, 即椭圆曲线的特征p整除椭圆曲线的迹t, 则称椭圆曲线为超奇异椭圆曲线.

除超奇异椭圆曲线、迹等于1和2的曲线外[11−13], 其它的椭圆曲线称为普通椭圆曲线.

引理 2[14]　如果$\gcd(n,p)=1$, 则$E[n]\subset E(F_p)$当且仅当如下3个条件成立: (i) $n^2|N$; (ii) $n|p-1$; (iii) 要么$\phi\in Z$, 要么$\theta((t^2-4p)/n^2)\subset End_{F_p}(E)$.

由Weil配对的性质(7)可知, 基于Weil配对的离散对数求解, 其配对的两个点必须是独立的, 也就是两个点分属不同的子群. 由于子群的阶一定整除群的阶, 即$n|N$, 又由于Weil配对的两个点线性无关, 由引理2可知$n^2|N$. 从而判断Weil配对是否能够有效实施, 首先要验证椭圆曲线的群结构是否是二元的, 如果是二元的, 且子阶$n\geq 3$(等于2时不存在离散对数), 则可以求解2倍点以上的离散对数(尽管利用Weil配对求解因数小的倍点的离散对数没有意义, 但是可以求解). 其次, 参与配对的两个点都是n阶的.

定理 1　假设E是一条F_q上阶为$q+1$的超奇异椭圆曲线, 即$t=0$, 如果$nP=O$, 则$E[n]\subseteq E(F_{q^2})$.

证明　根据有限域上Frobenius自同态的性质$\phi_q(P)=P^q=P$, 和Frobenius自同态的特征多项式$\phi_q^2-t\phi_q+q=0$, 以及假设$t=0$, 可得$\phi_q^2=-q$. 将点P代入等式$\phi_q^2=-q$可得$\phi_q^2(P)=-qP$. 从而$\phi_q^2(P)=-qP\equiv P(\bmod N)$, 即$\phi_q^2(P)=P$. 因为$\phi_q^2(P)\in E(F_{q^2})$, $P\in E[n]$, 所以$E[n]\subseteq E(F_{q^2})$.

由定理1可知, 如果椭圆曲线的群是一元的, 需要验证椭圆曲线是否是超奇异的, 如果是超奇异的, 则可以在嵌入度为2的椭圆曲线上求解椭圆曲线的离散对数, 因为嵌入度为2的超奇异椭圆曲线的群结构是二元的, 这是MOV攻击类型的一种.

由以上分析可知, Weil配对椭圆曲线群的特征要么是两个循环子群, 要么是一个循环子群, 但是椭圆曲线必须是超奇异的. 另外, 配对的两个点必须是同阶且来自不同的子群, 阶$n\geq 3$.

2.2　超奇异椭圆曲线

除迹为0的椭圆曲线是超奇异椭圆曲线外, 根据定义1还有其它迹不为0的超奇异椭圆曲线, 下面给出MOV攻击的其它4类曲线, 见引理3.

引理 3[2,7]　假设E是一条F_q上阶为$q+1-t$的超奇异椭圆曲线. 则有6类嵌入度$k\leq 6$的超奇异椭圆曲线.

(i) $k=1$, $t=\pm 2\sqrt{q}$, 且m是偶数;

(ii) $k=2$, $t=0$, 且$E(F_q)\cong Z_{q+1}$;

(iii) $k=2$, $t=0$, 且$E(F_q)\cong Z_{(q+1)/2}\oplus Z_2$, $q\equiv 3(\bmod\ 4)$;

(iv) $k=3$, $t=\pm\sqrt{q}$, 且m是偶数;

(v) $k=4$, $t=\pm\sqrt{2q}$, 且$p=2$, m是奇数;

(vi) $k=6$, $t=\pm\sqrt{3q}$, 且$p=3$, m是奇数.

由引理3(i)可知, $N=(\sqrt{q}\pm 1)^2$, 因此椭圆曲线由两个循环子群构成, 子群的大小为$\sqrt{q}+1$或$\sqrt{q}-1$, 即$E(F_q)\cong Z_{\sqrt{q}+1}\oplus Z_{\sqrt{q}+1}$或$E(F_q)\cong Z_{\sqrt{q}-1}\oplus Z_{\sqrt{q}-1}$.

引理3(ii)和(iii)的群结构在条件中已经给出, 这里不再赘述. 引理3(iv), (v)和(vi)的群结构与m的值有关, 在有限域F_q上椭圆曲线总是可以进行复数乘, 这一特征能够构造出椭圆曲线群的二元结构.

引理 4[8]　令$\#E(F_p)=N=p+1-t$, 记$X^2-tX+p=(X-\alpha)(X-\beta)$, 则$\#E(p^m)=p^m+1-(\alpha^m+\beta^m)$.

定理 2　假设素数$p\geq 5$, 则定义在F_p上的超奇异椭圆曲线, 在偶嵌入度m上仍为超奇异椭圆曲线.

证明 令$q=p^m$, 由于定义在F_p上椭圆曲线是超奇异的, 因此$p|t$. 由引理4可知, $\alpha^2+t\alpha+p=0$, $\beta^2+t\beta+p=0$, 又m为偶数, 从而$\alpha^{m-2}\geq 0$, $\beta^{m-2}\geq 0$, 有$\alpha^m=t\alpha^{m-1}-p\alpha^{m-2}$, $\beta^m=t\beta^{m-1}-p\beta^{m-2}$, 将两式相加可得$\alpha^m+\beta^m=t(\alpha^{m-1}+\beta^{m-1})-p(\alpha^{m-2}+\beta^{m-2})$. 因为$p|t$, $p|p$, 因此$p|\alpha^m+\beta^m$, 满足定义1, 从而定义在F_p上的超奇异椭圆曲线, 在偶嵌入度m上仍为超奇异椭圆曲线.

依据引理3和定义1, 可以寻找到如下条件和形状的超奇异椭圆曲线[5,8].

特征为2形如$y^2+ay=x^3+bx+c$的椭圆曲线为超奇异椭圆曲线.

假设奇素数$p\equiv 2(\mathrm{mod}\ 3)$, 则定义在$F_p$上(包含嵌入度$k=2$)形如$y^2=x^3+a(a\neq 0)$的椭圆曲线为超奇异椭圆曲线. 假设素数$p\equiv 3(\mathrm{mod}\ 4)$, 则定义在$F_p$上(包含嵌入度$k=2$)形如$y^2=x^3+ax(a\neq 0)$的椭圆曲线为超奇异椭圆曲线. 假设$d$是奇数, 则定义在$F_{2^d}$上且嵌入度$k=4$形如$y^2+y=x^3+x+a(a=0$或$a=1)$的椭圆曲线为超奇异椭圆曲线. 假设$2,3\nmid d$, 则定义在$F_{3^d}$上且嵌入度$k=6$形如$y^2=x^3-x\pm 1$的椭圆曲线为超奇异椭圆曲线. 假设素数$p\geq 5$, 则定义在$F_p$上嵌入度等于1或2形如$y^2=x^3+ax+b(a\neq 0,b\neq 0)$的椭圆曲线为超奇异椭圆曲线.

2.3 配对友好椭圆曲线

定义 2 假设E是一条F_q上阶为$N=q+1-t$的椭圆曲线, 且有一个素数$r|N$, 其中$q=p^m$, 则E有安全的参数k, k是满足$r|q^k-1$的最小的正整数.

为了便于识别配对友好椭圆曲线, 引入文献[4]嵌入度为10的一个例子.

$p=61\ 099\ 963\ 271\ 083\ 128\ 746\ 073\ 769\ 567\ 944\ 870\ 354\ 270\ 161\ 646\ 150\ 914\ 794\ 603$

$n=61\ 099\ 963\ 271\ 083\ 128\ 746\ 073\ 769\ 567\ 450\ 502\ 219\ 087\ 145\ 916\ 434\ 839\ 626\ 301$

$A=$-3, $B=1\ 112\ 775\ 869\ 471\ 458\ 154\ 129\ 950\ 648\ 198\ 203\ 893\ 613\ 615\ 552\ 476\ 491\ 488\ 167$

椭圆曲线$E:y^2=x^3+Ax+B$定义在F_p上, p和n都是196位的素数. 由于$n|p^{10}-1$且$n\nmid p^k-1$(对于$k<10$), 因此这条曲线的嵌入度为10.

配对友好椭圆曲线(PF-EC)是有安全参数k的椭圆曲线. 下面给出一个构造配对友好安全椭圆曲线的引理.

表 1 配对友好椭圆曲线的类型

族类	k	D	$r(x)$	$p(x)$	$t(x)$
BN	12	-3	$36x^4+36x^3+18x^2+6x+1$	$36x^4+36x^3+24x^2+6x+1$	$6x^2+1$
$BLS12$	12	-3	x^4-x^2+1	$(x^6-2x^5+2x^3+x+1)/3$	$x+1$
$BLS24$	24	-3	x^8-x^4+1	$(x^{10}-2x^9+x^8-x^6+2x^5-x^4+x^2+x+1)/3$	$x+1$
$MNT3$	3	D	$12x^2\mp 6x+1$	$12x^2-1$	$-1\pm 6x$
$MNT4$	4	D	x^2+1或x^2+2x+2	x^2+x+1	$-x$或$x+1$
$MNT6$	6	D	$4x^2\mp 2x+1$	$4x^2+1$	$1\pm 2x$
$GMV6$ ($h=4$)	6	D	$4x^2+2x+1=\Phi_6(t-1)$	$16x^2+10x+5$	$2x+2$
			$28x^2+10x+1=\Phi_6(t-1)/7$	$112x^2+54x+7$	$14x+4$
			$28x^2+18x+3=\Phi_6(t-1)/7$	$112x^2+86x+17$	$14x+6$
			$52x^2+14x+1=\Phi_6(t-1)/13$	$208x^2+30x+1$	$-26x-2$
			$52x^2+38x+7=\Phi_6(t-1)/13$	$208x^2+126x+19$	$-26x-8$
$KSS16$	16	-4	$(x^9+48x^4+625)/61\ 550$	$(x^{10}+2x^9+5x^8+48x^6+152x^5+240x^4+625x^2+2\ 398x+3\ 125)/980$	$(2x^5+41x+35)/35$
$KSS18$	18	-3	$(x^6+37x^3+343)/343$	$(x^8+5x^7+7x^6+37x^5+188x^4+259x^3+343x^2+1\ 763x+2\ 401)/21$	$(x^4+16x+7)/7$

引理 5[1,4] 对于$k>0$的整数, 假定$\Phi_k(x)$是第k个分圆多项式, $t(x)$是一个有整系数的多项式的迹, $r(x)$是一个$\Phi_k(t(x)-1)$的不可约因子, 并且$f(x)=4p(x)-t(x)^2$. 对于一个无平方的正整数D, 点(x_0,y_0)是方程$Dy^2=f(x)$的一个解, 其中$p(x_0)$和$r(x_0)$都是素数. 对于较小的D, 有一个有效的复数乘算法, 该算法构造一条定义在$F_p(x_0)$上

的椭圆曲线E, 其中$E(F_p(x_0))$有素数阶, 且椭圆曲线E的嵌入度至多是k.

由引理5可知, $r(x)=p(x)+1-t(x)$, $r(x)$和$p(x)$是不可约多项式, $r(x)|\Phi_k(t(x)-1)$, $Dy^2=4p(x)-t(x)^2$有无穷多个整数解(x,y). 因此, 配对友好椭圆曲线是有限定条件的椭圆曲线.

常见的配对友好椭圆曲线有8种, 这些椭圆曲线是根据科学家名字的首字母和嵌入度的大小命名的, 即嵌入度为12, 24和48的BLS(Barreto-Lynn-Scott)曲线, 类型有BLS12-381, BLS12-446, BLS12-445, BLS12-638, BLS24-477, BLS48-575; BN(Barreto-Naehrig)曲线, 类型有BN-158, BN-254R, BN-256R, BN-256I, BN-382, BN-446, BN-638; 嵌入度为3, 4和6的MNT(Miyaji-Nakabayashi-Takano)曲线, 嵌入度为6和协因子4的GMV(Galbraith-McKee-Valenca)曲线及嵌入度为16和18的KSS(Kachisa-Schaefer-Scott)曲线. 这些曲线的参数选择见表1[1,15−16]. Cocks-Pinch等提出的构造配对友好椭圆曲线的方法是最为有效的方法之一, BLS和BW(Brezing-Weng)方法是CP方法的推广.

不同类型的曲线, 对安全位的要求各异, 如平坦曲线BN-382和Pluto-Eris的安全位为128位, Tweedle曲线的安全位为126位, Pasta曲线的安全位为100位[15]. 对于配对友好椭圆曲线的实施, 文献[1]列出了许多支持椭圆曲线的加密库和配对操作.

3　PARI软件的实施分析

从以下3种类型的实例分析Weil配对的实施, 包括普通椭圆曲线, 很小有限域上的椭圆曲线和较大有限域上的椭圆曲线. 配对友好椭圆曲线实施较为复杂, 不是本研究的重点, 不再验证.

3.1　普通椭圆曲线的实例

已知$p=1\ 009$, $E(F_p):y^2=x^3+37x$. 下面利用PARI软件验证在各子阶上求解离散对数的情况, 过程如下:

$p=1\ 009$

$E=ellinit([0,0,0,37,0],p)$

$ellgroup(E)//[70,14]$

$[P,Q]=ellgenerators(E)//[[\mathrm{Mod}(493,1\ 009),\mathrm{Mod}(478,1\ 009)],[\mathrm{Mod}(856,1\ 009),\mathrm{Mod}(687,1\ 009)]]$

$W=[49,20]$

$U=ellmul(E,W,5)//[\mathrm{Mod}(375,1\ 009),\mathrm{Mod}(504,1\ 009)]$

$V=ellmul(E,P,10)//[\mathrm{Mod}(634,1\ 009),\mathrm{Mod}(270,1\ 009)]$

由测试可知, 群的结构为[70,14], 所以是二元结构. 阶为$\#E(F_p)=980\neq 1\ 009+1$, $1\ 009(\mathrm{mod}\ 4)=1\neq 3$, 且$14^2|980$, $14|1\ 008$, 所以该曲线为普通椭圆曲线, 可以实施Weil配对. 验证发现$70P=70[493,478]=O$, $7W=7[49,20]=O$, $14V=14[634,270]=O$. 从曲线E的群结构可知, 其有3个扭曲群, 分别是$E[14]\times E[14]$, $E[7]\times E[7]$和$E[2]\times E[2]$.

首先, 验证在阶为14的扭曲群上求解椭圆曲线离散对数的情况, 过程如下:

$ellweilpairing(E,W,V,14)//302$

$ellweilpairing(E,U,V,14)//105$

验证$302^5\equiv 105(\mathrm{mod}\ 1\ 009)$, 这表明在阶为14的扭曲群上正确求解了椭圆曲线的离散对数.

其次, 验证在阶为7的扭曲群上求解椭圆曲线离散对数的情况, 过程如下:

$ellweilpairing(E,W,V,7)//859$

$ellweilpairing(E,U,V,7)//431$

验证$859^5\equiv 431(\mathrm{mod}\ 1\ 009)$, 这表明在阶为7的扭曲群上正确求解了椭圆曲线的离散对数.

3.2　较小域上的超奇异椭圆曲线

已知$p=43$, $E(F_p):y^2=x^3+3x$.下面利用PARI软件测试曲线的特征, 过程如下:

$p=43$

$E=ellinit([0,0,0,3,0],p)$

$ellgroup(E)//[22,2]$

$[P,Q]=ellgenerators(E)//[[\mathrm{Mod}(12,43),\mathrm{Mod}(1,43)],[\mathrm{Mod}(16,43),\mathrm{Mod}(4,43)]]$

因为曲线的阶$\#E(F_p)=44=p+1$, 迹为0, 所以曲线E是超奇异的. 从群的结构来看, 曲线E仅有1个阶为2的扭曲群$E[2]\times E[2]$. 阶为2的扭曲群上不存在离散对数. 现在, 在嵌入度为2的域上来看椭圆曲线离散对数的求解情况.

$i=ffgen(p^2,'i)$

$E2=ellinit([0,0,0,3,0],i)$

$ellgroup(E2)//[44,44]$

$[P,Q]=ellgenerators(E2)//[[10\times i+37,20\times i+36],[38\times i+38,29\times i+4]]$

在嵌入度为2的域上, 曲线E有4个扭曲群, 分别是$E[44]\times E[44]$, $E[11]\times E[11]$, $E[4]\times E[4]$和$E[2]\times E[2]$.

首先, 验证在阶为44的扭曲群上求解椭圆曲线离散对数的情况, 过程如下:

$V=ellmul(E2,P,25)//[10\times i+39,5\times i+8]$

$wV=ellweilpairing(E2,V,Q,44)//35\times i+30$

$wP=ellweilpairing(E2,P,Q,44)//i+2$

$ffdlog(wV,wP,44)//25$

这表明在阶为44的扭曲群上正确求解了椭圆曲线的离散对数.

其次, 验证在阶为11的扭曲群上求解椭圆曲线离散对数的情况, 过程如下:

$S=ellmul(E2,P,4)//[19\times i+24,11\times i+20]$

$T=ellmul(E2,Q,4)//[23,14]$

$V=ellmul(E2,S,6)//[19\times i+16,25\times i+20]$

$wV=ellweilpairing(E2,V,T,11)//40\times i+38$

$wS=ellweilpairing(E2,S,T,11)//21\times i+34$

$ffdlog(wV,wS,11)//6$

这表明在阶为11的扭曲群上正确求解了椭圆曲线的离散对数.

接着, 验证在阶为4的扭曲群上求解椭圆曲线离散对数的情况, 过程如下:

$S=ellmul(E2,P,11)//[35\times i+9,12\times i+10]$

$T=ellmul(E2,Q,11)//[8\times i+34,23\times i+1]$

$V=ellmul(E2,S,3)//[35\times i+9,31\times i+33]$

$wV=ellweilpairing(E2,V,T,4)//5\times i+24$

$wS=ellweilpairing(E2,S,T,4)//38\times i+19$

$ffdlog(wV,wS,4)//3$

这表明在阶为4的扭曲群上正确求解了椭圆曲线的离散对数.

为了验证定理2的正确性,下面观察嵌入度为4的离散对数求解情况.

$i=ffgen(p^4,'i)$

$E2=ellinit([0,0,0,3,0],i)$

$ellgroup(E2)//[1\ 848,1\ 848]$

$[P,Q]=ellgenerators(E2)//[[22\times i^3+20\times i^2+35\times i+37,13\times i^3+23\times i^2+19\times i+3],[5\times i^3+36\times i^2+19\times i+4,37\times i^3+11\times i^2+30\times i+33]]$

$U=ellmul(E2,P,44)//[21\times i^3+21\times i^2+12,2\times i^3+40\times i^2+42\times i+21]$

$wU=ellweilpairing(E2,U,Q,1\ 848)//19$

$wP=ellweilpairing(E2,P,Q,1\ 848)//37\times i^3+37\times i^2+32$

$ffdlog(wU,wP,1\ 848)//44$

从上面的测试可以看出, 嵌入度4曲线仍为超奇异椭圆曲线.

3.3 较大域上的超奇异椭圆曲线

应用文献[8]的$E1$曲线. 已知$p=2^{48}+180\ 307$, $E(F_p):y^2=x^3-44x+9$, $P=[0,3]$, $Q=[8,13]$, 求$Q=xP$的x. 下面利用PARI软件测试曲线的特征, 过程如下:

$p=2^{48}+180\ 307//281\ 474\ 976\ 890\ 963$

$E=ellinit([0,0,0,-44,9],p)$

$ellgroup(E)//[281\ 474\ 976\ 890\ 964]$

因为曲线的阶$\#E(F_p)=281\ 474\ 976\ 890\ 964=p+1$, 迹为0, 所以曲线$E$是超奇异的. 从群的结构来看, 曲线$E$仅有1个阶为281 474 976 890 964的群, 即为一元群结构, 不适合Weil配对. 下面观察在嵌入度为2的域上求解椭圆曲线离散对数的情况.

$i=ffgen(p^2,'i)$

$E2=ellinit([0,0,0,-44,9],i)$

$ellgroup(E2)//[281\ 474\ 976\ 890\ 964,281\ 474\ 976\ 890\ 964]$

此时, 曲线的群结构为二元结构, 可以实施Weil配对.

$P=[0,3]$

$Q=[8,13]$

$[S,T]=ellgenerators(E2)//[[158\ 501\ 156\ 329\ 781\times i+175\ 970\ 746\ 882\ 325,134\ 607\ 571\ 385\ 497\times i+158\ 408\ 230\ 203\ 504],[98\ 137\ 829\ 604\ 480\times i+132\ 283\ 139\ 307\ 198,87\ 541\ 178\ 687\ 425\times i+128\ 722\ 298\ 571\ 253]]$

$wQ=ellweilpairing(E2,Q,T,281\ 474\ 976\ 890\ 964)//98\ 845\ 775\ 270\ 225\times i+251\ 588\ 554\ 012\ 177$

$wP=ellweilpairing(E2,P,T,281\ 474\ 976\ 890\ 964)//73\ 673\ 700\ 922\ 132\times i+2\ 252\ 264\ 390\ 002$

$fflog(wQ,wP,281\ 474\ 976\ 890\ 964)//214\ 161\ 860\ 163\ 611$

$elllog(E,Q,P)//214\ 161\ 860\ 163\ 611$

由上述验证可知, $Q=214\ 161\ 860\ 163\ 611P$. 这说明在嵌入度为2的域上成功求解椭圆曲线点的离散对数, MOV攻击有效. 此软件的测试与文献[8]的结果不一致, 文献[8]的结果为$Q=2\ 141\ 618\ 601\ 636P$, 这说明PARI软件和SageMath软件的设计存在漏洞, 但无论如何, 超奇异椭圆曲线上的离散对数可以在多项式时间求解. 另外, 文献[8]的$E3$曲线不是超奇异椭圆曲线, 因为$p=2^{48}+228\ 055$不是素数.

上述所有实验表明, 只要椭圆曲线群的结构是二元的, 且阶大于等于3, 都可以在相应阶上求解与该阶相匹配的点的离散对数.

4　结 论

1) 证明了$p\geq 5$素数有限域上超奇异椭圆曲线在偶嵌入度上仍为超奇异椭圆曲线.

2) 分析了适合Weil配对椭圆曲线的特征, 指出适合Weil配对的椭圆曲线是具有二元循环群结构的曲线, 一元群结构的超奇异椭圆曲线通过嵌入度的方式能够构造出二元群结构的超奇异椭圆曲线, 即一元超奇异椭圆曲线的Weil配对的离散对数需要在构造出的二元群结构进行. 实验表明, 只要椭圆曲线群的结构是二元的, 且阶大于等于3, 都可以在相应阶上求解与该阶相匹配的点的离散对数.

3) 指出了PARI和SageMath软件设计上存在的漏洞. 同时, 指出了文献[8]的$E3$曲线不是超奇异椭圆曲线.

软件是验证理论的重要工具, 相同的参数, PARI和SageMath软件却得出不同的结果, 这对理论研究的可靠性产生挑战. 未来的工作中, 将进一步探究PARI和SageMath软件究竟谁对理论的支持更加准确, 进而确保理论研究的准确性和可靠性. 另外, 超奇异椭圆曲线在实践中能否安全使用, 需要进一步研究.

参考文献：

[1] KUMAR M. Design and analysis of pairing-friendly elliptic curves for cryptographic primitives[D]. New Delhi：Jawaharlal Nehru University，2023.

[2] MENEZES A J，OKAMOTO T，VANSTONE S A. Reducing elliptic curve logarithms to logarithms in a finite field[J]. IEEE Transactions on Information Theory，1993，39(5)：1639-1646.

[3] FREY G，MULLER M，RUCK H G. The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems[J]. IEEE Transactions on Information Theory，1999，45(5)：1717-1719.

[4] FREEMAN D. Constructing pairing-friendly elliptic curves with embedding degree 10[M]//Lecture Notes in Computer Science. Berlin，Heidelberg：Springer Berlin Heidelberg，2006：452-465.

(下转第343页)