学　　号：2020212175　　密　级：公开

合肥工业大学

Hefei University of Technology

本科毕业设计（论文）

UNDERGRADUATE THESIS

类　　型：	论文
题　　目：	椭圆曲线的同源与密码学应用的研究
专业名称：	数学与应用数学
入学年份：	2020 级
学生姓名：	邱修煜
指导教师：	张神星 副研究员
学院名称：	数学学院
完成时间：	2024 年 6 月

合　肥　工　业　大　学

本科毕业设计（论文）

椭圆曲线的同源与密码学应用的研究

学生姓名：邱修煜

学生学号：2020212175

指导教师：张神星 副研究员

专业名称：数学与应用数学

学院名称：数学学院

2024 年 6 月

A Dissertation Submitted for the Degree of Bachelor

Research on the Isogenies of Elliptic Curves and Its Applications on Cryptography

By

Qiu Xiuyu

Hefei University of Technology

Hefei, Anhui, P.R.China

June, 2024

毕业设计（论文）独创性声明

本人郑重声明：所呈交的毕业设计（论文）是本人在指导教师指导下进行独立研究工作所取得的成果。据我所知，除了文中特别加以标注和致谢的内容外，设计（论文）中不包含其他人已经发表或撰写过的研究成果，也不包含为获得合肥工业大学　或其他教育机构的学位或证书而使用过的材料。对本文成果做出贡献的个人和集体，本人已在设计（论文）中作了明确的说明，并表示谢意。

毕业设计（论文）中表达的观点纯属作者本人观点，与合肥工业大学无关。

毕业设计（论文）作者签名：邱修煜 签名日期：2024 年 5 月 23 日

毕业设计（论文）版权使用授权书

本学位论文作者完全了解　合肥工业大学　有关保留、使用毕业设计（论文）的规定，即：除保密期内的涉密设计（论文）外，学校有权保存并向国家有关部门或机构送交设计（论文）的复印件和电子光盘，允许设计（论文）被查阅或借阅。本人授权　合肥工业大学　可以将本毕业设计（论文）的全部或部分内容编入有关数据库，允许采用影印、缩印或扫描等复制手段保存、汇编毕业设计（论文）。

（保密的毕业设计（论文）在解密后适用本授权书）

学位论文作者签名：邱修煜　　指导教师签名：张神星

签名日期：　2024 年 5 月 23 日　　签名日期：2024 年 5 月 24 日

摘　要

基于椭圆曲线的密码学是现代密码学中的一个重要研究课题。Luca De Feo 等人提出的新方案 SQISign 是后量子密码学中目前最紧凑的签名方案, 但由于 SQISign 的设计较为复杂, 故而对 SQISign 的运算速度进行优化是一个有价值的问题。通过 Deuring 的结论, SQISign 的实现可分为两个部分: 在椭圆曲线上的运算, 以及在四元数代数上的相关运算。对于在椭圆曲线上的运算, SQISign 原论文是在 Weierstrass 曲线上计算的。

本文对于 SQISign 的原理进行研究, 通过利用 Weil 配对来实现对二维椭圆曲线离散对数问题的一维化, 使得 Pohlig-Hellman 算法求解该问题成为可能, 并引入了 Montgomery 梯子方法来加速椭圆曲线有理点的计算。同时对原论文中在某指定序模内生成指定范数之元素的算法进行探究, 通过研究方程形式确定该方程存在解不存在的情况, 并且得到了部分情况下方程是否存在根的判定方法。通过提前判定根的存在性, 使得 FullRepresentInteger 算法速度进一步得到优化。

关键词：椭圆曲线；同源；离散对数

ABSTRACT

Cryptographic protocols based on elliptic curves have gained more and more attention in modern cryptography. The new scheme SQISign proposed by Luca De Feo et al. is currently the most compact signature scheme in post-quantum cryptography. However, due to the complexity of SQISign's design, optimizing its computational speed is a valuable problem. According to Deuring Correspondence theorem, the implementation of SQISign can be divided into two parts: operations on elliptic curves and operations in quaternion algebra. For operations on elliptic curves, the original paper of SQISign computes on Weierstrass curves.

This article studies the principles of SQISign, utilizing the Weil pairing to reduce the two-dimensional elliptic curve discrete logarithm problem to one dimension, making it possible to solve this problem using the Pohlig-Hellman algorithm. It also introduces the Montgomery Ladder method to accelerate the computation of rational points on elliptic curves. Additionally, it explores the algorithm from the original paper for generating elements with specified norms within a certain modulus, investigating the conditions under which the equation has or does not have solutions. A method for determining whether the equation has roots in certain cases is derived. By determining the existence of roots in advance, the speed of the FullRepresentInteger algorithm is further optimized.

KEYWORDS: Elliptic Curve; Isogeny; Discrete Logarithms

目 录

符号说明

$x(P), X(P), Z(P)$　点 P 的 x-坐标, 以及点 P 的射影坐标

$k, \bar{k}$　数域 k 以及其代数闭包 $\bar{k}$

$\#A$　集合 A 的势

$\deg \phi$　同源 ϕ 的度

$k[x_i]_{i=1}^m$　域 k 上的多项式环

1 绪论

1.1 背景介绍

基于椭圆曲线的密码学是现代密码学中的一个重要研究课题。在公钥密码学体系中, 通常情况下基于椭圆曲线的方法能以较低的存储占用以达到与其他方案相当的安全性, 这也正是基于椭圆曲线的密码学之优势所在。随着计算机架构的发展与量子计算机概念的落地, 人们逐渐意识到传统的椭圆曲线密码学已经不能满足后量子时代对安全的需求了: 运行在量子计算机上的算法将能够以较低的代价攻破传统的椭圆曲线签名与密钥交换方案。准确来说, 由于运行在量子计算机上的 Shor 算法能更快破解 ECDSA, ECDH 等传统方案。在这个背景下, 基于椭圆曲线同源问题的方案在 1997 年 Couveignes[1] 的工作中首次提出。Couveignes 发现 $\mathbb{F}_q$ 上通常椭圆曲线的自同态环是一个虚二次域中的序模, 而该序模 O 的理想类群 cl(O) 的群作用能够天然地实现 Diffie 与 Hellman 的密钥交换算法, 故得到了首个同源的密码学应用。在过去的数十年中, 随着人们对后量子密码的日益重视, 基于同源的密码学也得到了显著的发展。然而 Childs, Jao 与 Soukharev 发现对 Couveignes 等[2] 提出的方案的破解可等价于阿贝尔隐藏子群问题的破解, 这正是 Shor 算法能解决的。况且该方案的实现也过于慢了。考虑到 Childs-Jao-Soukharev 攻击依赖于 cl(O) 的交换性, 这能导出 O 的交换性。而若 O 不交换则该攻击自然不能奏效。这也是为何超奇异椭圆曲线从此被引入同源加密, 因为超奇异椭圆曲线的自同态环是一个四元数代数中的极大序模, 他并不交换[3]。而 GCL 哈希函数与 SIDH 密钥交换协议的提出则使得超奇异椭圆曲线之间的同源成为研究的重点。与此同时, 基于同源的签名方案也成为了研究的热门方向。Galbraith, Petit 和 Silva 的签名方案是首个应用 KLPT 算法的构造性密码学应用[4], 但他们的工作几乎停留在理论的层面上。而 De Feo[5] 等人提出的新方案 SQISign 则将 KLPT 算法进行推广, 使其适用范围提高到了任意极大序模上, 并提供了完整的签名方案的 C 语言与 Magma 语言实现。

尽管基于同源的密码学保持了与传统的椭圆曲线密码学的密钥短和签名长度短的优势, 其也继承了传统椭圆曲线密码学实现的运算时间长等缺点。故针对相关方案的实现优化是十分现实的问题, 在该层面上看对算法的优化是当前同源密码学的一个十分有意义的方向。同时, 考虑到密码学算法的优化不仅仅与速度有关, 如算法实现的时长不是常量, 则可能存在的侧信道攻击将会降低算法的安全性。如上限制使得对于相关算法的优化变得相对受限。

1.2 本文的主要工作

通过 Deuring 的结论, SQISign 的实现可分为两个部分: 在椭圆曲线上的运算, 以及在四元数代数上的相关运算。对于在椭圆曲线上的运算, SQISign 原论文是在 Weierstrass 曲线上计算的。若能将 Weierstrass 曲线换成 Edwards 曲线或是 Montgomery 曲线, 则存在 Montgomery 梯子方法以加速相关运算, 本文将 Montgomery 梯子方法引入了 SQISign, 对离散对数计算进行了加速。另外, SQISign 提出了新的理想转换算法, 其中存在的求离散对数问题是一个二维离散对数问题, 本文通过 Weil 配对方法将其转换成了普通的一维离散对数问题, 并通过 Pohlig-Hellman 算法加速求解。同时本文对平方和方程解的存在性做了讨论, 进而加速了 FullRepresentInteger 算法的运算。

2 基础知识

2.1 椭圆曲线

如无标注, 本节定义与定理等均来自 Silverman[6]。令 k 为某域, 令 $\bar{k}$ 为其代数闭包。

定义 2.1 (椭圆曲线) 椭圆曲线是亏格 $g = 1$ 的光滑射影代数曲线。

定义 2.2 (射影空间) 维数 n 的射影空间, 记做 $\mathbb{P}^n$ 或者 $\mathbb{P}^n(\bar{k})$, 是所有 $(n+1)$-有序对

$$(x_0, \cdots, x_n) \in \bar{k}^{n+1},$$

以使得 $(x_0, \cdots, x_n) \neq (0, \cdots, 0)$ 在等价关系

$$(x_0, \cdots, x_n) \sim (y_0, \cdots, y_n),$$

当且仅当存在 $\lambda \in \bar{k}$ 使得对任意 i, $x_i = \lambda y_i$ 下的商集。

对于 $(x_0, \cdots, x_n)$ 的等价类, 习惯性记为 $(x_0 : \cdots : x_n)$, 称其为射影点. 对于k-有理点的集合, 记为 $\mathbb{P}^n(k)$, 定义为

$$\mathbb{P}^n(k) = \left\{(x_0 : \cdots : x_n) \in \mathbb{P}^n \middle| x_i \in k\text{对任意 } i\right\}.$$

通过固定任意坐标 $x_n = 0$, 可定义一个维数为 $n-1$ 的射影空间, 称之为在无穷远点的超平面; 该超平面上的点则称为在无穷远的点。

从现在开始假定域 k 的特征不为 2 或 3, 这样则能极大简化椭圆曲线的表示。对于通常的定义, 参见 Silverman[6]Chap. III。

定义 2.3 (Weierstrass 方程) 在 k 上定义的椭圆曲线是 $\mathbb{P}^2(\bar{k})$ 中方程

$$Y^2Z = X^3 + aXZ^2 + bZ^3,$$

的轨迹, 其中 $a, b \in k$ 且 $4a^3 + 27b^2 \neq 0$。

通常把方程 (2.3)写成如下的仿射形式。通过定义坐标方程 $x = X/Z$ 及 $y = Y/Z$, 等价地定义椭圆曲线为方程

$$y^2 = x^3 + ax + b$$

的轨迹, 并令无穷元的点为 $\infty_E = (0 : 1 : 0)$。

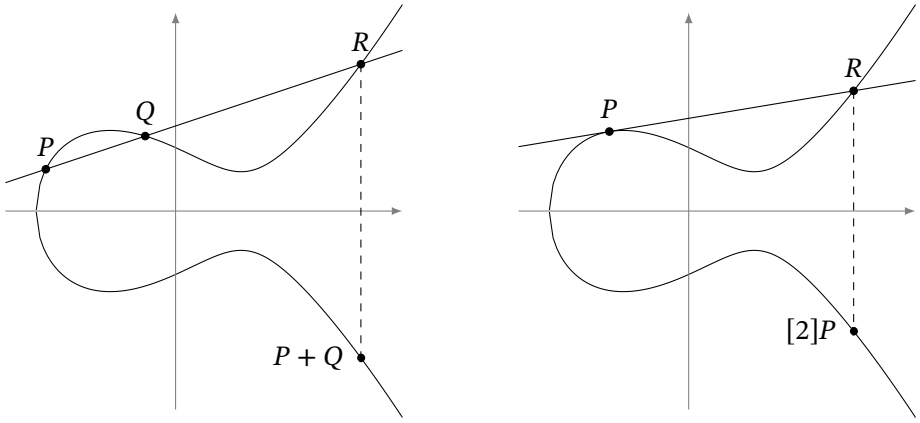

图 2.1　定义于 $\mathbb{R}$ 上的椭圆曲线, 以及群运算律的几何表示

当域特征不为 2 或 3 时, 可证明任意亏格为 1 的光滑射影曲线带特定点 ∞_E 同构于 Weierstrass 方程, 方法是将 ∞_E 映射到无穷远点 $(0:1:0)$。由于任意椭圆曲线都由三次方程定义, 由 Bézout 定理知 $\mathbb{P}^2$ 上任意直线交曲线于 3 点, 在考虑重数的情况下。

定义 2.4　令 $E: y^2 = x^3+ax+b$ 为一椭圆曲线。令 $P_1 = (x_1, y_1)$ 及 $P_2 = (x_2, y_2)$ 为 E 上不同于无穷远点的两点, 则可定义 E 上二元运算 $\oplus$ 为

- $P \oplus \infty_E = \infty_E \oplus P = P$ 对于任意 $P \in E$ 成立;
- 若 $x_1 = x_2$ 且 $y_1 = -y_2$, 则 $P_1 \oplus P_2 = \infty_E$;
- 否则令

$$\lambda = \begin{cases} \frac{y_2-y_1}{x_2-x_1} & \text{若 } P \neq Q, \\ \frac{3x_1^2+a}{2y_1} & \text{若 } P = Q, \end{cases}$$

则点 $(P_1 \oplus P_2) = (x_3, y_3)$ 定义为

$$x_3 = \lambda^2 - x_1 - x_2,$$
$$y_3 = -\lambda x_3 - y_1 + \lambda x_1.$$

可知上述运算率定义的二元运算定义一交换群, 故可将 $\oplus$ 直接写做 $+$。P 的 n 次标量乘记为 $[n]P$。当 E 定义于 k 上时, 其上的k-有理点写做 $E(k)$。图 2.1展示了定义于 $\mathbb{R}$ 上椭圆曲线群律的图像展示。

现在考虑椭圆曲线的群结构。对于挠的部分可以由以下命题简单刻画, 该命题出自 Silverman[6]Coro. 6.4。

命题 2.1　令 E 为定义于代数闭域 k 上的椭圆曲线, 令 $m \neq 0$ 为整数。则 E 的 m-挠群记做 $E[m]$ 有如下结构

- $E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$ 若 k 的特征不整除 m;

- 若 $p>0$ 为 k 的特征, 则

$$E[p^i] \simeq \begin{cases} \mathbb{Z}/p^i\mathbb{Z} & \text{对任意 } i \geqslant 0, \text{或} \\ \{\infty_E\} & \text{对任意 } i \geqslant 0。 \end{cases}$$

当 k 不是代数闭的, 记 $E[m]$ 为 $E(\bar{k})$ 的 $m-$ 挠子群, 也即代数闭域上的挠点。容易知道, $E[m]$ 可能也可能不完全在 $E[k]$ 内, 但其总能包含于 k 的阶不超过 m^2 的有限扩张中。

对于定义在正特征 p 的域上的曲线, $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$ 的情况称之为通常的, 而 $E[p] \simeq \{\infty_E\}$ 的情况称之为超奇异的。

命题 2.2 (j-不变量)　令 $E: y^2 = x^3 + ax + b$ 为一椭圆曲线, 定义 E 的j-不变量为

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

两个曲线在代数闭域 $\bar{k}$ 上同构, 当且仅当二者有相同的 j-不变量。

定义 2.5 (同源)　椭圆曲线间的非常量的态射称为同源。

以下定理见 Silverman[6]III, Th. 4.8。

定理 2.3　令 E, E' 为定义在域 k 上的椭圆曲线, 并令 $\phi: E \to E'$ 为二者间的同源。则有

- ϕ 为一群态射;
- ϕ 的核有限;
- 若 k 是代数闭的, 则 ϕ 是满的。

由对偶同源定理知同源是等价关系。

定义 2.6 (度, 可分性)　令 $\phi: E \to E'$ 为一定义于 k 上同源, 并且令 $k(E), k(E')$ 为 E, E' 的函数域。通过将 ϕ 与 $k(E')$ 中元素复合, 即得 $k(E)$ 的子域, 记做 $\phi^*(k(E'))$。

1. ϕ 的度定义为 $\deg\phi = [k(E): \phi^*(k(E'))]$。
2. ϕ 是可分的, 不可分的, 或 纯不可分的若其函数域扩张如此。

以下定理来自 Silverman[6]II, Th. 2.4。

定理 2.4　关于度与可分性有以下性质成立:

1. ϕ 的度总是有限的。
2. 若 ϕ 可分, 则 $\deg\phi = \#\ker\phi$。
3. 若 ϕ 纯不可分, 则 $\deg\phi$ 是 k 的特征的幂。
4. 一同源可被分解为可分同源和纯不可分同源之积。

若同源的核的大小等于其的度, 则称该同源是可分的。考虑到本文中考虑同源均为可分同源, 故可将 $\deg\phi := \#\ker\phi$ 作为度的定义。

定义 2.7 (自同态环)　考虑椭圆曲线 E, E', 对于两个 $E \to E'$ 的映射 ϕ, ψ 可按函数加法的方法定义 $(\phi+\psi)(P) = \phi(P) + \psi(P)$ 的 $\phi+\psi$ 也为同源, 故得到阿贝尔群 $\mathrm{Hom}(E, E')$。而对于自同态 $E \to E$, 映射之间可以复合。故自同态组成的集合构成一个环 $\mathrm{End}(E)$。

最典型的自同态即乘以 m 自同态, 定义为

$$[m] : P \mapsto [m]P.$$

该同态的核即为 m 阶挠群 $E[m]$。

对于椭圆曲线 E 以及其上任意有限子群 G, 存在一可分同源 $\phi : E \to E/G$, 使得该同源的核 $\ker\phi = G$, 该同源在同构意义下唯一。通过 Vélu 公式可从同源的核来求得同源本身。

Deuring 对椭圆曲线的自同态环作出了分类, 这需要一些四元数代数的知识。

定理 2.5 (Deuring)　令 E 为一定义在特征为 p 的域上的椭圆曲线。环 $\mathrm{End}(E)$ 同态于以下情况:

- $\mathbb{Z}$;
- 一个二次虚域内的序模 O; 此时称 E 有 O 下的复乘;
- 仅当 $p > 0$, 一 $B_{p,\infty}$ 中极大序模 O; 此时称 E 有 O 下的四元数乘。称这种情况下的 E 为超奇异的。

2.2 四元数代数与序模

如无标注, 本节定义与定理等均来自 Voight[7]。

定义 2.8 (四元数代数)　一个$\mathbb{Q}$ 上的四元数代数是一个形式为

$$K = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q},$$

的代数, 其中生成元满足关系

$$0 \neq i^2 \in \mathbb{Q}, \quad 0 \neq j^2 \in \mathbb{Q}, \quad k = ij = -ji.$$

若 $i^2 = a$ 且 $j^2 = b$, 则记该代数为 $\left(\frac{a,b}{\mathbb{Q}}\right)$。

四元数代数的任意元素可写作 $\alpha = t + xi + yj + zk$, 其中 $t, x, y, z \in \mathbb{Q}$。其中元素的实部为 $\mathrm{Re}(\alpha) = t$, 虚部为 $\mathrm{Im}(\alpha) = xi + yj + zk$。共轭 $\overline{\alpha}$ 由反转虚部符号实现;

$\overline{\alpha} = t - xi - yj - zk$。约化范数和约化迹对应定义为

$$\mathrm{Nrd}(\alpha) := \alpha\overline{\alpha} = t^2 - ax^2 - by^2 + abz^2, \quad \mathrm{Tr}(\alpha) := \alpha + \overline{\alpha} = 2t. \tag{2.1}$$

这启发了如下定义。

定义 2.9 四元数代数 $\left(\frac{a,b}{\mathbb{Q}}\right)$ 的范数型为多项式 $t^2 - ax^2 - by^2 + abz^2 \in \mathbb{Q}[t,x,y,z]$。

令 p 为一素数, 令 K 为 $\mathbb{Q}$ 上的四元数代数。称 K 在 p 处分裂, 若 $K \otimes \mathbb{Q}_p \cong M_2(\mathbb{Q}_p)$。这等价于范数型在 $\mathbb{Q}_p$ 上有非平凡零点。否则, 称四元数代数在 p 点分歧。

称 K 于 ∞ 分歧, 若范数型在 $\mathbb{R}$ 上无零点。这等价于 a, b 同时为负数。

四元数代数的约化判别式是分歧点的素数之积。对任意素数 p, 存在同态意义下唯一的四元数代数使得有判别式 p, 记做 $B_{p,\infty}$。其准确在 p 和 ∞ 处分歧。主要关注的四元数代数为 $B_{p,\infty}$; 事实证明其是椭圆曲线语境中最有研究价值的一个, 因为其含有所有特征为 p 的域上超奇异椭圆曲线的自同态环。

定义 2.10 ($B_{p,\infty}$ 中的分式理想) $B_{p,\infty}$ 中的分式理想是一个秩为 4 的 $\mathbb{Z}$-格 $I \subset B_{p,\infty}$。理想的约化范数定义为理想的元素的约化范数的最大公因数 gcd, 即 $N(I) = \mathrm{Nrd}(I) := \gcd\{N(\alpha) \mid \alpha \in I\}$。

若 $I \subset J$ 为两个分式理想, 则其作为阿贝尔群的指数 $[J : I]$ 等于 $(N(I)/N(J))^2$。若 $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ 为 I 的 $\mathbb{Z}$-基, 则定义 I 的约化判别式为 $\mathrm{discrd}(I) := |\det(\mathrm{Tr}(\alpha_i\overline{\alpha_j}))_{1\leqslant i,j\leqslant 4}|^{1/2}$; 其与基的选择无关。

定义 2.11 ($B_{p,\infty}$ 中的序模) $O \subset B_{p,\infty}$ 是一个 $B_{p,\infty}$ 中的格, 若其同时为含幺子环, 则称其为序模。称 O 是极大的, 若其不严格包含于其他序模。一个序模是极大的, 当且仅当其约化判别式为 p。

给定分式理想 $I \subset B_{p,\infty}$, 称 $O_L(I) := \{\alpha \in B_{p,\infty} \mid \alpha I \subset I\}$ 为其*左序模*, $O_R(I) := \{\alpha \in B_{p,\infty} \mid I\alpha \subset I\}$ 为其*右序模*。称 I 为分式左 (对应的, 右) O-理想若 $O \subset O_L(I)$ (对应的, $O \subset O_R(I)$)。

一个 (左或右) O-理想 I 称为整的, 若 $I \subset O$ (这也是通常对理想的定义)。

例 2.1 对于 $p \equiv 3 \pmod 4$, $B_{p,\infty} \cong \left(\frac{-1,-p}{\mathbb{Q}}\right)$。则 $O_0 = \left\langle 1, i, \frac{1+j}{2}, \frac{i+ij}{2} \right\rangle$ 为 $B_{p,\infty}$ 的极大理想。考虑 O_0 的范数型, 有

$$\begin{aligned} f(x,y,z,t) &= \left(x + yi + \frac{z(1+j)}{2} + \frac{t(i+ij)}{2}\right)\left(x - yi - \frac{z(1+j)}{2} - \frac{t(i+ij)}{2}\right) \\ &= (x + t/2)^2 + (y + z/2)^2 + p((z/2)^2 + (t/2)^2). \end{aligned}$$

2.3 同源的交换图

为描述 SQISign 的算法, 需要部分对同源的交换图的术语。该部分参考 De Feo 等[5]。

考虑椭圆曲线 E_0, E_1 与 E_2 以及可分同源 $\phi_1 : E_0 \to E_1, \phi_2 : E_0 \to E_2$, 其中 ϕ_1 与 ϕ_2 的度互素, 分别为 N_1, N_2。则存在第四条曲线 E_3 以及两个前推同源 $[\phi_1]_*\phi_2$ 与 $[\phi_2]_*\phi_1$ 分别从 E_1 和 E_2 映射到 E_3, 满足 $\deg([\phi_1]_*\phi_2) = N_2$ 且 $\deg([\phi_2]_*\phi_1) = N_1$。其中 $[\phi_1]_*\phi_2$ 与 $[\phi_2]_*\phi_1$ 分别定义为以 $\phi_1(\ker(\phi_2))$ 和 $\phi_2(\ker(\phi_1))$ 为核的可分同源。

与前推同源对偶的记号为 拉回同源: 给定 $\phi_1 : E_0 \to E_1$ 以及 $\rho_2 : E_1 \to E_3$, 其度互素, 则可定义 ρ_2 通过 ϕ_1 的拉回为 $[\phi_1]^*\rho_2 = [\hat{\phi}_1]_*\rho_2$。由定义可得 $\phi_2 = [\phi_1]^*[\phi_1]_*\phi_2$。

为将前推和拉回应用到理想上, 定义 $[I]_*J$ 为理想 $I_{[\phi_J]_*\phi_I}$, 对应 ϕ_J 通过 ϕ_I 的前推。同样地定义 $[I]^*J$。

令 $I_1 = I_{\phi_1}, I_2 = I_{\phi_2}, J_1 = [I_2]_*I_1, J_2 = [I_1]_*I_2$, 以及 $K = I_{[\phi_2]_*\phi_1 \circ \phi_2}$, 则有以下引理。该引理来自 De Feo 等[5]。

引理 2.6 若 N_1 与 N_2 互素, 则理想 J_1, J_2 与 K 是良定义的, 且有如下公式成立:

1. $K = I_1 \cap I_2$.
2. $J_2 = I_1^{-1}(I_1 \cap I_2), J_1 = I_2^{-1}(I_1 \cap I_2)$.
3. $I_2 = [I_1]^*J_2 = I_1J_2 + N_2\mathcal{O}_0, I_1 = I_2J_1 + N_1\mathcal{O}_0$.

2.4 SQISign

SQISign 是一个以 Deuring 对应的运算为基础的签名方案, 而该方案的性能瓶颈在于极大序模的理想到椭圆曲线同源的对应的计算。原始方案系采用有理挠点的方案, 故运算速度较慢, 若有更快的 KLPT 算法改进, 则能对 SQISign 起到加速的作用。该部分参考 De Feo 等人的工作[5,8-9]。

首先引入光滑数, 该类数字在离散对数的求解中有重要作用。

定义 2.12 (光滑数) 设 $k \in \mathbb{Z}$, 若有 $k = \prod_i p_i^{k_i}$, 则 k 为 $(\max p_i)$-光滑数。当 $\max p_i$ 足够小时, 称 k 为光滑数。

SQISign 提出了如下的身份验证协议, 并使用 Fiat-Shamir 变换来将其转化为签名方案。

初始化 生成长为 2λ 比特的素数 $p \equiv 3 \pmod 4$, 其中 λ 为安全参数。定义 $\mathbb{F}_p$ 上超奇异椭圆曲线 $E_0 : y^2 = x^3 + x$, 其中 $j(E_0) = 1728, \mathrm{End}(E_0) = O_0$。选取一长

表 2.1　Deuring 对应与 SQISign 论文的工作

$\mathbb{F}_{p^2}$ 上的超奇异 j-不变量 $j(E)$(在 Galois 共轭意义下唯一)	$\mathcal{B}_{p,\infty}$ 中的极大序模 $\mathcal{O} \cong \mathrm{End}(E)$(在同构意义下唯一)
(E_1, φ) , 其中 $\varphi : E \to E_1$	I_φ 整的左 $\mathcal{O}$-理想以及右 $\mathcal{O}_1$-理想
$\theta \in \mathrm{End}(E_0)$	主理想 $\mathcal{O}\theta$
$\overline{\deg(\varphi)}$	$n(I_\varphi)$
$\hat{\varphi}$	$\overline{I_\varphi}$
$\varphi : E \to E_1, \psi : E \to E_1$	等价理想 $I_\varphi \sim I_\psi$
$\mathbb{F}_{p^2}$ 上的超奇异 j-不变量	$\mathrm{Cl}(\mathcal{O})$
$\tau \circ \rho : E \to E_1 \to E_2$	$I_{\tau\circ\rho} = I_\rho \cdot I_\tau$
SQISign 的工作	级 (Level) 为 N 的 Eichler 序模 $\mathfrak{O} = \mathcal{O} \cap \mathcal{O}_1$
N-同源 (同构意义下唯一)	$\mathrm{Cl}(\mathfrak{O})$

为 λ 比特的奇光滑数 D_c, 取 $D = 2^e$, 其中 e 大于 $2-$ 同源图 $\mathcal{G}_2(\mathbb{F}_p)$ 的直径。

密钥生成 选择一素数 $N_\tau \sim p^{1/4}$, 任取一 $N_\tau-$ 同源 $\tau : E_0 \to E_A$。密钥即为同源 τ (注意 τ 的度也是秘密的), 而公钥则为像曲线 E_A。

承诺 证明者生成随机同源 $\psi_1 : E_0 \to E_1$, 将 E_1 发给验证者。

挑战 验证者将一度为 D_c 的循环同源 $\psi_2 : E_1 \to E_2$ 发送给证明者。

回复 通过同源 $\psi_2 \circ \psi_1 \circ \hat{\tau} : E_A \to E_2$, 证明者构造一度为 D 的同源 $\omega : E_A \to E_2$, 使得 $\hat{\psi_2} \circ \omega$ 为循环同源, 并将 ω 发给验证者。

验证 若同源 $\omega : E_A \to E_2$ 的度为 D 且 $\hat{\psi_2} \circ \omega$ 为循环同源, 则验证通过。否则验证不通过。

由于 I_τ 的约化范数为一大素数, 故直接使用 Vélu 公式计算对应的 τ 较复杂。为更便利计算出 E_A 的系数, 可利用 KLPT 算法将 I_τ 转换成约化范数为 2^{e_τ} 的等价理想 I_2, 其对应的同源为一个 $E_0 \to E_2$ 的度为 2^{e_τ} 的同源。或者也可采用以下方法同时生成 I_τ 和 I_2: 首先找到约化范数为 $N_\tau 2^{e_\tau}$ 的 $\gamma' \in \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$, 然后令 $I_\tau = \langle \gamma', N_\tau \rangle, I_2 = \langle \bar{\gamma'}, 2^{e_\tau} \rangle$。后一种方法更为高效, 故已应用于当前实现中。

2.5 SigningKLPT 算法

KLPT 算法首次由 Kohel 等[10] 提出, 为得到 $\mathrm{End}(E_A) \cong \mathcal{O}_A$ 中 I_A 的等价同源, SQISign 的作者对 KLPT 算法进行推广, 提出了 SigningKLPT 算法, 需要的算法如下:

- **EquivalentRandomEichlerIdeal**(I, N_τ): 给定左 $\mathcal{O}_A-$ 理想 I, 输出一约化范数与 N_τ 互素且同构于 I 的理想 K
- **EquivalentPrimeIdeal**(I): 给定左 $\mathcal{O}_0-$ 理想 I, 输出一素约化范数的最小等价左 $\mathcal{O}_0-$ 理想
- **RepresentInteger**$_{\mathcal{O}_0}(M)$: 给定整数 $M > p$, 输出约化范数为 M 的 $\gamma \in \mathbb{Z} + \mathbb{Z}i +$

$\mathbb{Z}j + \mathbb{Z}k \subseteq \mathcal{O}_0$

- **IdealModConstraint**(I, γ): 给定约化范数为 N 的左 $\mathcal{O}_0-$ 理想 I, 输出 $(C_0 : D_0) \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ 使得 $\gamma\mu_0 \in I$, 其中 $\mu_0 = j(C_0 + iD_0)$
- **EichlerModConstraint**(I, γ, δ): 给定约化范数为 N 的左 $\mathcal{O}_0-$ 理想 I, 约化范数与 N 互素的 $\gamma, \delta \in \mathcal{O}_0$, 输出 $(C_1 : D_1) \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ 使得 $\gamma\mu_1\delta \in \mathbb{Z} + I$, 其中 $\mu_1 = j(C_1 + iD_1)$
- **StrongApproximation**$_{l^e}(N, C, D)$: 给定 $N, C, D \in \mathbb{Z}$, 输出约化范数为 l^e 的 $\mu = \lambda\mu_0 + N\mu_1$, 其中 $\mu_0 = j(C + iD)$, $\mu_1 \in \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$

算法 2.1 SigningKLPT(I_τ, I)

Data: 约化范数为 N_τ 的 $(\mathcal{O}_0, \mathcal{O}_A)-$ 理想 I_τ, 左 $\mathcal{O}_A-$ 理想 I
Result: 约化范数为 l^e 的左 $\mathcal{O}-$ 理想 J 满足 $I \sim J$

1 $K \leftarrow$ **EquivalentRandomEichlerIdeal**(I, N_τ);
2 $K' \leftarrow [I_\tau]^*(K)$;
3 $L \leftarrow$ **EquivalentPrimeIdeal**(K'), $N \leftarrow \mathrm{Nrd}(L)$;
4 取 $\delta \in K'$ 使得 $L = K'\frac{\bar{\delta}}{\mathrm{Nrd}(K')}$;
5 $e_0 \leftarrow e_0(N)$, $e_1 \leftarrow e - e_0$;
6 $\gamma \leftarrow$ **RepresentInteger**$_{\mathcal{O}_0}(Nl^{e_0})$;
7 $(C_0 : D_0) \leftarrow$ **IdealModConstraint**(I_τ, γ, δ);
8 $(C_1, D_1) \leftarrow$ **EichlerModConstraint**(I_τ, γ, δ);
9 $C \leftarrow$ **CRT**$_{N,N_\tau}(C_0, C_1)$, $D \leftarrow$ **CRT**$_{N,N_\tau}(D_0, D_1)$。若 $l^e p(C^2 + D^2)$ 非二次剩余, 则返回步骤 6;
10 $\mu \leftarrow$ **StrongApproximation**$_{l^{e_1}}(NN_\tau, C, D)$;
11 $\beta \leftarrow \gamma\mu$;
12 $J \leftarrow [I_\tau]^*(L\frac{\beta}{\mathrm{Nrd}(L)})$;
13 返回 J.

然而 De Feo 等发现算法 2.1 存在安全隐患, 故其将 **RepresentInteger** 替换成如下 **FullRepresentInteger** 来计算 γ.

- **FullRepresentInteger**$_{\mathcal{O}_0}(M)$: 给定整数 $M > p$, 输出约化范数整除 M 的 $\gamma \in \mathcal{O}_0 \backslash 2\mathcal{O}$

2.6 理想到同源的转换

需要注意到的是 SQISign 的性能瓶颈在于对于理想 I_σ 到同源 σ 之间的转换。在 SQISign 的实现中, 该转换需要将度为 2^e 的同源 σ 分解成一系列度为 2^a 的同源 $\phi_i, i = 1, 2, \cdots, n$ 使得

$$\sigma = \phi_n \circ \cdots \circ \phi_2 \circ \phi_1, \tag{2.2}$$

其中 $2^a || p + 1$ (也即 $a = \mathrm{ord}_2(p + 1)$)。理想到同源转换的核心在于给定度为 2^a 的核为 $\langle P \rangle$ 同源 ϕ_K, 对应的同源 $I = \langle \alpha, 2^a \rangle$ 可通过计算 $\langle [C]P + [D]\theta(P) \rangle$ 的核来得到,

其中 $\theta \in \mathcal{O}_A \backslash (\mathbb{Z} + K + 2\mathcal{O}_A)$ 有光滑约化范数, 且满足 $\alpha(C + D\theta) \in K$。在这个过程中需要以下两个算法:

- **SpecialEichlerNorm**$_T(\mathcal{O}, K)$: 给定极大序模 $\mathcal{O}$ 以及约化范数为 l 的左 $\mathcal{O}-$ 理想 K, 输出约化范数整除 T^2 的 $\beta \in \mathcal{O} \backslash (\mathbb{Z} + K)$, 其中 T 为使得 $\gcd(T, l) = 1$ 且 $T | p^2 - 1$ 成立的参数
- **IdealToIsogeny**(I): 给定约化范数整除 T 的理想 $I \subseteq \mathcal{O}_0$, 输出对应的同源 ϕ_I

算法 2.2描述了如何计算 ϕ_I, 该算法中最为耗时的步骤是对 $Q = \theta(P) = \hat{\phi}_2 \circ \phi_1(P)$ 的计算。为改善效率, 通过算法 2.3通过利用 $\mathrm{Trd}\,\theta$ 得到 $[C]P + [D]Q$ 的 x-坐标相较 $Q = \theta(P)$ 更快。

算法 2.2 **IdealToIsogenyEichler**$_{2^a}(\mathcal{O}, I, J, \phi_J, P)$

Data: 约化范数为 2^a 的左 $\mathcal{O}-$ 理想 I, 约化范数为 $2^{\cdot}$ 的 $(\mathcal{O}_0, \mathcal{O})-$ 理想 J, 以及对应的同源 ϕ_J, $E[2^a] \cap \ker(\hat{\phi}_J)$ 的一个生成元 P
Result: 度为 2^a 的同源 ϕ_I

$K \leftarrow \bar{J} + 2^a\mathcal{O}$;
$\theta \leftarrow$ **SpecialEichlerNorm**$_T(\mathcal{O}, K + 2\mathcal{O})$;
选择 $\alpha \in I$, 使得 $I = \mathcal{O}\langle \alpha, 2^a \rangle$;
计算 C, D 使得 $\alpha(C + D\theta) \in K$ 且 $\gcd(C, D, 2) = 1$;
取 $n_1 | T, n_2 | T$, 使得 $n_1 n_2 = \mathrm{Nrd}\,\theta$, 计算 $H_1 = \mathcal{O}\langle \theta, n_1 \rangle$, $H_2 = \mathcal{O}\langle \bar{\theta}, n_2 \rangle$;
$L_i \leftarrow [J]^* H_i$, $\phi_i \leftarrow [\phi_j]_*$**IdealToIsogeny**$(L_i)$, 对 $i = 1, 2$;
计算 $Q \leftarrow \hat{\phi}_2 \circ \phi_1(P)$;
计算核为 $\langle [C]P + [D]Q \rangle$ 的同源 ϕ_I;
返回 ϕ_I.

算法 2.3 **EndomorphismEvaluation**$(\phi_1, \phi_2, C, D, t, P)$

Data: $E \to E'$ 的同源 ϕ_1, ϕ_2, 标量 C, D, 约化范数 $\mathrm{Trd}(\theta) = \mathrm{Trd}(\hat{\phi}_2 \circ \phi_1)$, 一点 $P \in E[2^a]$
Result: $[C]P + [D]Q$ 的 $x-$ 坐标

计算 Q 使得 $\langle P, Q \rangle = E[2^a]$, 计算 $P + Q$;
计算 $x_{\phi_1(P)}$,$x_{\phi_1(Q)}$,$x_{\phi_2(P)}$,$x_{\phi_2(P)}$,$x_{\phi_2(P+Q)}$;
计算 s_1, s_2 使得 $x_{\phi_1(P)} = x([s_1]\phi_2(P) + [s_2]\phi_2(Q))$;
计算 s_3, s_4 使得 $x_{\phi_1(Q)} = x([s_3]\phi_2(P) + [s_4]\phi_2(Q))$;
改变 (s_1, s_2), (s_3, s_4) 的符号, 直到 $(s_1 + s_4)\deg(\phi_2) \equiv \mathrm{Trd}(\theta) \pmod{2^a}$;
计算 $x_R = x([C + s_1 D \deg(\phi_2)]P + [s_2 D \deg(\phi_2)]Q)$;
返回 x_R.

3 Montgomery 梯子方法

3.1 递推关系

考虑到 SQISign 是基于 Deuring 对应具体运算的签名方案, 其包含椭圆曲线上的运算与在四元数代数上的相关运算。

对于椭圆曲线上点的数乘运算, 存在较朴素方法更优且较简单的实现方案, 如对于 Edwards 曲线和 Montgomery 曲线, Montgomery[11] 提出了 Montgomery 梯子方法, 可以更高效地计算。Bernstein 和 Lange[12] 给出了关于 Montgomery 梯子方法的相关细节。

定义 3.1 (Montgomery 曲线)　定义于域 K 上的 Montgomery 曲线是由方程

$$M_{A,B} : By^2 = x^3 + Ax^2 + x$$

确定的椭圆曲线, 其中 $A, B \in K$, 且 $B(A^2 - 4) \neq 0$。

实际上, Montgomery 曲线是某种 Weierstrass 曲线。SQISign 的实现中所使用的 $y^2 = x^3 + x$ 正属于 Montgomery 曲线, 故通过 Montgomery 梯子方法, 可对其进行改进。考虑 $x = X/Z$, $y = Y/Z$, 则有 Montgomery 曲线的射影形式, 方程如下

$$BY^2Z = X^3 + AX^2Z + XZ^2.$$

考虑 Montgomery 曲线上的点列 $P_1, P_2, \cdots, P_n, \cdots$, 不妨设 $P_i = (X_i : Y_i : Z_i)$, 通过计算可得到以下关系

$$\begin{aligned} X_{2n} &= (X_n^2 - Z_n^2)^2, & X_{2n+1} &= 4(X_nX_{n+1} - Z_nZ_{n+1})^2Z_1, \\ Z_{2n} &= 4X_nZ_n(X_n^2 + AX_nZ_n + Z_n^2), & Z_{2n+1} &= 4(X_nZ_{n+1} - Z_nX_{n+1})^2X_1 \end{aligned}$$

当 $n \geqslant 1$ 时成立。通过一定变形可进一步降低运算的次数:

$$\begin{aligned} X_{2n} &= (X_n - Z_n)^2(X_n + Z_n)^2, \\ Z_{2n} &= ((X_n + Z_n)^2 - (X_n - Z_n)^2) \\ &\quad \left((X_n + Z_n)^2 + \frac{A-2}{4}((X_n + Z_n)^2 - (X_n - Z_n)^2)\right), \\ X_{2n+1} &= ((X_n - Z_n)(X_{n+1} + Z_{n+1}) + (X_n + Z_n)(X_{n+1} - Z_{n+1}))^2Z_1, \\ Z_{2n+1} &= ((X_n - Z_n)(X_{n+1} + Z_{n+1}) - (X_n + Z_n)(X_{n+1} - Z_{n+1}))^2X_1 \end{aligned} \tag{3.1}$$

对于该递归关系的成立, 考虑定理 3.1,

定理 3.1 [6] 考虑椭圆曲线 $E: y^2 = x^3 + x$, 可定义除多项式 $\psi_m \in \mathbb{Z}[x, y]$,

$$\psi_1 = 1, \qquad \psi_2 = 2y,$$
$$\psi_3 = 3x^4 + 6x^2 - 1, \qquad \psi_4 = 4y(x^6 + 5x^4 - 5x^2 - 1),$$
$$\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}, \qquad 4y\omega_n = \psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2.$$
$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3, \text{当 } n \geqslant 2,$$
$$2y\psi_{2n} = \psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2), \text{ 当 } n \geqslant 3,$$

令 $P = (x, y) \in E$, 则有

$$[n]P = \left(\frac{\phi_n(P)}{\psi_n(P)^2}, \frac{\omega_n(P)}{\psi_n(P)^3}\right).$$

通过计算可得以下递归式

$$\psi_{n+m}\psi_{n-m}\psi_r^2 = \psi_{n+r}\psi_{n-r}\psi_m^2 - \psi_{m+r}\psi_{m-r}\psi_n^2, \text{ 对任意 } n > m > r.$$

令 $n = 2$ 时, 有

$$\begin{aligned}\frac{\phi_2(P)}{\psi_2(P)^2} &= \frac{x\psi_2^2 - \psi_3\psi_1}{\psi_2^2} = x - \frac{3x^4 + 6x^2 - 1}{4y^2} \\ &= x - \frac{3x^4 + 6x^2 - 1}{4(x^3 + x)} \\ &= \frac{(x^2 - 1)^2}{4(x^3 + x)}.\end{aligned}$$

不妨设 $x = X/Z$, 则有

$$\begin{aligned}\frac{X(2P)}{Z(2P)} &= \frac{(X(P)^2 - Z(P)^2)^2}{4Z(P)(X(P)^3Z(P) - X(p)Z(P)^3)} \\ &= \frac{(X(P)^2 - Z(P)^2)^2}{4(X(P)Z(P)(X(P)^2 + Z(P)^2))}.\end{aligned}$$

当 $n = 3$ 时, 考虑 $3P = 2P + P$ 即可。

例 3.1 考虑 $y^2 = x^3 + x$ 在 $\mathbb{F}_{13}$ 中, 点 $P = (2 : 6 : 1)$ 的标量乘。

首先将 $x(5P)$ 的运算转换成 X_5 和 Z_5 的运算, 有

$$x(5P) = X_5/Z_5.$$

由(3.1)可知

$$X_5 = ((X_2 - Z_2)(X_3 + Z_3) + (X_2 + Z_2)(X_3 - Z_3))^2 Z_1,$$
$$Z_5 = ((X_2 - Z_2)(X_3 + Z_3) - (X_2 + Z_2)(X_3 - Z_3))^2 X_1,$$

故可通过(3.1)计算 X_3, Z_3 与 X_2, Z_2 来得到 X_5, Z_5:

$$X_3 = ((X_1 - Z_1)(X_2 + Z_2) + (X_1 + Z_1)(X_2 - Z_2))^2 Z_1,$$
$$Z_3 = ((X_1 - Z_1)(X_2 + Z_2) - (X_1 + Z_1)(X_2 - Z_2))^2 X_1,$$
$$X_2 = (X_1 - Z_1)^2 (X_1 + Z_1)^2,$$
$$Z_2 = ((X_1 + Z_1)^2 - (X_1 - Z_1)^2)\left((X_1 + Z_1)^2 - 10((X_1 + Z_1)^2 - (X_1 - Z_1)^2)\right).$$

通过计算得到

$$x(5P) = 8.$$

3.2 椭圆曲线的坐标与运算效率

上节对椭圆曲线的坐标使用了 (X, Z) 的表示方法。实际上在椭圆曲线的不同坐标下的加法与数乘在效率上存在区别。特别是对于计算机的实现, 有限域的除法相较加法与乘法更为缓慢。故在实现中往往不使用仿射坐标, 而是使用射影坐标以尽量减少除法的使用。

与此同时, 考虑到对于 P_i 每个 x_i, 当 y_1 确定时 y_i 总是确定的。但上节中只使用了 (X, Z) (考虑 $x = X/Z$), 那么 y 总是有 3 种可能性: 两个解, 一个解, 以及没有解。

例 3.2 举例: $y^2 + 1 = 0$ 在 $\mathbb{F}_5$ 中有两个解, 在 $\mathbb{F}_7$ 中没有解, $y^2 = 0$ 在 $\mathbb{F}_p$ 中有一个解。

但只要确定 y_1, 则 y_i 都能被确定; 而从反方向来看, 对于省略掉 y 的坐标系统, 仅凭 x_{k-1} 和 x_1 是无法得到 x_k 的: 考虑 y_{k-1} 和 y_1 的符号不同, x_k 存在两种可能, 而对应的 y_k 亦存在两种可能: 这样得到的 P_k 有四种可能性! 而上节中提出的递归定义 (X_i, Z_i) 正好给出了 y_i 的一种。

过去曾出现过一种使用 Jacobi 坐标的方式[13], 具体地, 其令 $x = X/Z^3, y = Y/Z^2$。Hamburg 总结了椭圆曲线加速运算的方法[14], 说明了 Jacobi 坐标在当前已经过时, Montgomery 梯子方法较 Jacobi 坐标方法有更优秀的效果。但使用射影坐标的方法依然是有效的。

3.3 差分加链方法

Bernstein 提出了差分加链方法。差分加链是一种加链, 其中每加入一个新元素 $m + n$, 需保证 $m, n, m - n$ 均在链中之前出现过。

上一节所述 X_{2n}, X_{2n+1} 与 Z_{2n}, Z_{2n+1} 的式子可以进一步总结为 $a_{m+n} =$

$f(a_m, a_n, a_{n-m})$ 的形式: 可令 $a_{2n} = f(a_n, a_n, a_0)$, $a_{2n+1} = f(a_n, a_{n+1}, a_1)$。这就是说 $(X_n, Z_n, X_{n+1}, Z_{n+1})$ 也具有差分加链的性质。这样的性质在椭圆曲线上出现并不令人惊讶, 毕竟已经知道椭圆曲线的数乘可以由除多项式来表示。也即定理 3.1。考虑 P_{2n} 由 P_n 得到, P_{2n+1} 由 P_{2n} 和 P 得到, 不难总结得出算法 3.1.

算法 3.1　DoubleAndAdd(n, P)

Data: 点 P, 正整数 n.
Result: nP.
将 n 用二进制表示 $n = n_0 + 2n_1 + 2^2 n_2 + \cdots + 2^k n_k$;
for $i \leftarrow 0$ **to** k **do**
　　if $n_i = 0$ **then**
　　　　$P_i \leftarrow 2P_{i/2}$
　　end
　　else
　　　　$P_i \leftarrow P_{i-1} + P$
　　end
end
return P_n.

但该方案存在一定缺陷, 具体体现为攻击者能够通过某种侧信道攻击, 通过计算算法使用的时间来获取输入的信息等。实际上由于椭圆曲线上点的加法与数乘存在时间差异, 通过计时来得到 n 是有可能的。

3.4 Montgomery 梯子

可定义一递归公式。固定 (X_1, Z_1), 由公式可得 (X_2, Z_2, X_3, Z_3)。令

$$\begin{aligned} L_n &= (X_n, Z_n, X_{n+1}, Z_{n+1}), \\ f_0(X_n, Z_n, X_{n+1}, Z_{n+1}) &= (X_{2n}, Z_{2n}, X_{2n+1}, Z_{2n+1}), \\ f_1(X_{n+1}, Z_{n+1}, X_n, Z_n) &= (X_{2n+1}, Z_{2n+1}, X_{2n}, Z_{2n}). \end{aligned} \tag{3.2}$$

如此即可将 (3.1)转化为递归形式:

$$\begin{aligned} L_{2n} &= f_0(L_n), \\ L_{2n+1} &= f_1(L_n). \end{aligned}$$

该方案较算法 3.1有何好处? 至少到目前为止二者同样容易遭受计时攻击的威胁。但通过修改递归公式的形式, 可得到一种常量时间的 Montgomery 梯子算法。

通过引入

$$\begin{aligned} S_0(L_n) &= L_n, \\ S_1(L_n) &= (X_{n+1}, Z_{n+1}, X_n, Z_n), \end{aligned}$$

可等价地将 (3.2)表示为 $f_i = S_i \circ f_0 \circ S_i$。通过这种方式即可确保运算时间为常量。另外, 为了保证不同的 n 循环次数相同, 当用二进制表示 n 时应当在首位填充 0, 使得 k 长度为定值。整理即得算法 3.2。

算法 3.2 **MontgomeryLadder**(n, P, k_0)

Data: 点 P, 正整数 n.
Result: nP.
将 n 用二进制表示 $n = n_0 + 2n_1 + 2^2 n_2 + \cdots + 2^k n_k$;
若 $k < k_0$, 则令 $n_i = 0, \forall k < i \leqslant k_0$;
for $i \leftarrow k_0 - 1$ **to** 0 **do**
    $L \leftarrow S_{n_i \bmod 2}(L)$;
    $L \leftarrow f_0(L)$;
    $L \leftarrow S_{n_i \bmod 2}(L)$;
end
return P_n.

4 应用研究

4.1 离散对数的运算

考虑算法 2.3, 其中对于 s_1, s_2 和 s_3, s_4 的求解实际上属于离散对数问题的求解。例如考虑如下方程

$$\phi_1(P) = [s_1]\phi_2(P) + [s_2]\phi_2(Q),$$

其中 $\phi_1(P), \phi_2(P), \phi_2(Q)$ 的阶为 2^a。这是一个经典的二维离散对数问题。对于通常的多维离散对数问题, Gaudry-Schost 算法能够用来得到对应的解。

定义 4.1 [15] 假定 $\phi_1(P) = [s_1]\phi_2(P) + [s_2]\phi_2(Q)$ 对某些整数 $0 \leqslant s_i < 2^a$ 成立, $i = 1, 2$. 定义集合 $T, W \subseteq \mathbb{Z}^2$:

$$T = \{(a_1, a_2) \in \mathbb{Z}^2 : 0 \leqslant a_i < 2^a, i = 1, 2\},$$
$$W = (n_1, n_2) + T.$$

类似于 Pollard 袋鼠算法, 该算法运行时进行大量随机游走, 其中一半的游走为温驯游走, 也即形式为 $[a_1]\phi_2(P) + [a_2]\phi_2(Q)$ 的游走, 其中 $(a_1, a_2) \in T$。另一半游走为野蛮游走, 其中任意游走呈现为 $\phi_1(P) + [b_1]\phi_2(P) + [b_2]\phi_2(Q)$ 的游走, 其中 $(b_1, b_2) \in W$。两类游走同时进行, 直到一方撞到特殊点。当撞到特殊点后, 将特殊点与该方的参数 (也即 W 或 T 中的元素) 储存起来。之后该方在任一随机点重新游走。

当两者均撞到过某特殊点时, 该二维离散对数问题即得到解

$$[a_1]\phi_2(P) + [a_2]\phi_2(Q) = \phi_1(P) + [b_1]\phi_2(P) + [b_2]\phi_2(Q).$$

M. V. Nikolaev[15] 提出了一种改进上述方法的途径, 通过利用集合上的自同构关系, 可降低 Gaudry-Schost 算法的算法复杂度。考虑到曲线 $y^2 = x^3 + x$ 上存在自同构 $\tau : (x, y) \mapsto (x, -y)$, 通过该方法可将复杂度降低至 $(1+\epsilon)2.5066 \times 2^{a/2} + O_\epsilon(2^{a/4})$。然而二维离散对数问题依然比较复杂。实际上, 由于椭圆曲线上的挠群的特殊性质, 存在更为便捷的方法。

4.2 转换到单变量离散对数问题

Weil 对是处理椭圆曲线挠群的有力工具。

定义 4.2 (Weil 对[6]) 对于 $m \in \mathbb{N}$, $E[m] = \{P \in E(\mathbb{F}_{p^n}) : mP = \infty_E\}$, 定义 Weil e_m-对为映射 $e_m : E[m] \times E[m] \to \mathbb{F}_{p^n}$, 使得满足如下条件

$$
\begin{aligned}
e_m(P_1 + P_2, Q) &= e_m(P_1, Q)e_m(P_2, Q), \\
e_m(P, Q_1 + Q_2) &= e_m(P, Q_1)e_m(P, Q_2), \\
e_m(P, P) &= 1, \\
\forall P \in E[m]\backslash\{\infty_E\}, \exists Q \in E[m], &\text{s.t. } e_m(P, Q) \neq 1.
\end{aligned}
$$

由 $e_m(P, P) = 1$ 知,

$$
\begin{aligned}
1 &= e_m(P + Q, P + Q) \\
&= e_m(P + Q, P)e_m(P + Q, Q) \\
&= e_m(P, P)e_m(Q, P)e_m(P, Q)e_m(Q, Q) \\
&= e_m(P, Q)e_m(Q, P),
\end{aligned}
$$

故 $e_m(P, Q) = \frac{1}{e_m(Q,P)}$, 也即 e_m 是反对称的。Silverman[6] 书中证明了 Weil 配对的存在性。

考虑到方程中的元素 $\phi_1(P), \phi_2(P), \phi_2(Q)$ 均为挠群 $E[2^a]$ 中元素, 故通过 Weil 配对, 存在相较朴素的对二维离散对数问题的求解方案更为快速的方法。如 Reza Azarderakhsh 等[16] 提出一种将椭圆曲线上的二维离散对数问题转换成有限域上的离散对数问题的方法。不妨令 e 为 $E[2^a]$ 上的 Weil 对映射, 发现

$$
\begin{aligned}
e(\phi_2(P), \phi_1(P)) &= e(\phi_2(P), [s_1]\phi_2(P) + [s_2]\phi_2(Q)) \\
&= e(\phi_2(P), [s_1]\phi_2(P))e(\phi_2(P), [s_2]\phi_2(Q)) \\
&= e(\phi_2(P), \phi_2(Q))^{s_2}, \\
e(\phi_2(Q), \phi_1(P)) &= e(\phi_2(Q), [s_1]\phi_2(P) + [s_2]\phi_2(Q)) \\
&= e(\phi_2(Q), [s_1]\phi_2(P))e(\phi_2(Q), [s_2]\phi_2(Q)) \\
&= e(\phi_2(Q), \phi_2(P))^{s_1} \\
&= e(\phi_2(P), \phi_2(Q))^{-s_1}.
\end{aligned}
$$

通过上面的转换, 即将二维离散对数问题转换为两个一维离散对数问题, 剩下的问题即是如何求出 $e(\phi_2(P), \phi_1(P))$, $e(\phi_2(Q), \phi_1(P))$ 以及 $e(\phi_2(P), \phi_2(Q))$ 了。

实际上对于一般的多维离散对数问题, 如

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= y_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= y_2, \\ \cdots &= \cdots, \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n &= y_n, \end{aligned}$$

其中 $x_i, y_i \in R_1, a_{ij} \in \mathbb{Z}$, 若存在这样的双线性函数 $f(x,y) : R_1 \times R_1 \to R_2$, 使得

$$\begin{aligned} f(x_1 + x_2, y) &= f(x_1, y) + f(x_2, y), \\ f(x, y_1 + y_2) &= f(x, y_1) + f(x, y_2), \\ f(x, x) &= 0, \\ \forall x \in R_1 \backslash \{0\}, f(x, y) &\neq 0, \end{aligned}$$

成立, 则可进行以下操作,

$$\begin{aligned} a_{12}f(x_1, x_2) + \cdots + a_{1n}f(x_1, x_n) &= f(x_1, y_1), \\ a_{22}f(x_1, x_2) + \cdots + a_{2n}f(x_1, x_n) &= f(x_1, y_2), \\ \cdots &= \cdots, \\ a_{n2}f(x_1, x_2) + \cdots + a_{nn}f(x_1, x_n) &= f(x_1, y_n), \end{aligned}$$

也即对方程应用双线性对可减少一个方程未知元, 而对于二维离散对数问题, 自然能将其转换为一维离散对数问题。

而对于 Weil 对的求法, 目前有至少两种行之有效的方法, 其一是 Miller 算法[6]pp. 394, 其二为椭圆网络方法[17]。

注意到原论文[8] 中要求 $p^2 - 1$ 是光滑数, 故对于 $\mathbb{F}_{p^2}$ 上的离散对数问题可使用 Pohlig-Hellman 算法。

Pohlig-Hellman 算法能够利用求离散对数的群的阶的因子分解来加速运算, 考虑到群 $\mathbb{F}_{p^2}^*$ 的阶为 $p^2 - 1$, $\langle e(\phi_2(P), \phi_2(Q)) \rangle$ 的阶必定整除 $p^2 - 1$, 故也为光滑数, 假设有 $|\langle e(\phi_2(P), \phi_2(Q)) \rangle| = \prod_{i=1}^{n} p_i^{k_i}$, 则由该方法计算离散对数的复杂度可降到 $\mathcal{O}\left(\sum_{i=1}^{n} k_i(\log|\langle e(\phi_2(P), \phi_2(Q)) \rangle| + \sqrt{p_i})\right)$。

注 由于 SQISign 协议的可靠性是基于超奇异光滑自同态问题的困难性, 故与传统的基于椭圆曲线离散对数问题的协议相比, 此处 $p^2 - 1$ 的光滑性并不会影响 SQISign 协议的可靠性。

4.3 对计算二平方和的优化

原论文[5,8] 中的 **RepresentInteger** 与 **FullRepresentInteger** 使用了一定随机手段以找到某个四元数以使得其范数为给定整数。下面以 **FullRepresentInteger** 为例讨论优化。其中 **Cornacchia** 的定义参考 Basilla[18]。

该算法的大致思路为首先随机选取两个整数 z,t 使得 $M' := 4M - p(z^2+t^2) > 0$, 然后利用 **Cornacchia** 算法来求得 x,y 使得 $x^2+y^2=M'$。算法的描述如4.1所示。

算法 4.1 **FullRepresentInteger**$_{\mathcal{O}_0}(M)$

Data: $M \in \mathbb{Z}$ 使得 $M > p$。
Result: $\gamma = x + yi + z\frac{i+j}{2} + t\frac{1+k}{2}$, 其中 $\mathrm{Nrd}(\gamma) = M$。
1 令 $m' = \lfloor\sqrt{\frac{4M}{p}}\rfloor$, 取随机整数 $z' \in [-m', m']$;
2 令 $m'' = \lfloor\sqrt{\frac{4M}{p} - (z')^2}\rfloor$, 取随机整数 $t' \in [-m'', m'']$。令 $M' = 4M - p((z')^2 + (t')^2)$;
3 若 **Cornacchia**$(M') = \perp$, 返回步骤 1。否则令 $x', y' =$ **Cornacchia**(M');
4 若 $x' \neq t' \mod 2$ 或 $z' \neq y' \mod 2$, 返回步骤 1;
5 令 $\gamma = (x' + iy' + jz' + kt')/2$;
6 **return** γ。

对于某数 M 是否为二平方和的问题在初等数论中得到过广泛研究, 如 Fermat 平方和定理。

定理 4.1 (Fermat 平方和定理[19]) 奇素数 p 能唯一表示成 $p = m^2 + n^2$, 其中 $m, n \in \mathbb{Z}$, 当且仅当 $p \equiv 1 \pmod 4$。

而对于某些数 m(无论是否是素数) 不存在两平方和的表示这种判定则更为简单。考虑到两奇数平方和, 一奇数一偶数平方和, 两偶数平方和的情况, 无外乎这几种情况:

$$(2k+1)^2 + (2k+1)^2 \equiv 2 \pmod 4,$$
$$(2k+1)^2 + (2k)^2 \equiv 1 \pmod 4,$$
$$(2k)^2 + (2k)^2 \equiv 0 \pmod 4.$$

故 $m \equiv 3 \pmod 4$ 时, 不存在 $a, b \in \mathbb{Z}$ 使得 $m = a^2 + b^2$。故在计算 **Cornacchia** 之前可先判断一次 $m \mod 4$。

一个有趣的问题是, 对于任意 $M > p$, 方程 $4M = x^2 + y^2 + p(z^2 + t^2)$ 是否有解。其中 $p \equiv 3 \pmod 4$。考虑到 Fermat 的二平方和定理, 先考虑如下问题。

问题 是否存在 $M > p$, 使得任何满足 $p(z^2 + t^2) < 4M$ 的 $z, t \in \mathbb{Z}$, 有 $4M -$

$p(z^2+t^2) \equiv 3 \pmod 4$ 恒成立。

只需考虑 $\left(4M - p(z^2+t^2)\right) \mod 4$ 的取值即可。

$$\begin{aligned} 4M - p(z^2+t^2) &\equiv -p(z^2+t^2) \\ &\equiv 3p(z^2+t^2) \\ &\equiv (z^2+t^2) \pmod 4. \end{aligned}$$

但 z^2+t^2 不可能为 $3 \mod 4$, 故无论 M 的取值如何, $4M - p(z^2+t^2)$ 在模 4 意义下总等于某个平方和。这表明需要更强的必要条件来约束 $4M - p(z^2+t^2)$。实际上存在数可表示为二平方和的充要条件。

由于恒等式 (4.1)成立, 故 $p_i \equiv 1 \pmod 4$ 的素数 p_i 之间的乘积始终可表示为二平方和。

$$(a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2. \tag{4.1}$$

而对于 $p'_j \equiv 3 \pmod 4$ 的素数 p'_j, 当其为偶数幂时有 $p_j'^{2k} p_i = (p_j'^{k} a)^2 + (p_j'^{k} b)^2$, $\exists a, b \in \mathbb{Z}$.

定理 4.2 [20] 环 $\mathbb{Z}[i]$ 是主理想整环。考虑 $\mathbb{Z}$ 中的素理想 (p) 经嵌入映射 $\mathbb{Z} \to \mathbb{Z}[i]$ 得到的扩理想可以是如下几种情况:

1. $(2)^e = ((1+i)^2)$, 是 $\mathbb{Z}[i]$ 中一个素理想的平方;
2. 若 $p \equiv 1 \pmod 4$, 则 $(p)^e$ 是两个不同的素理想的乘积;
3. 若 $p \equiv 3 \pmod 4$, 则 $(p)^e$ 是 $\mathbb{Z}[i]$ 中素理想。

而这几种情况为 $\mathbb{Z}[i]$ 中不可约元的所有可能。

由于 $\mathbb{Z}[i]$ 是主理想整环, 则 $\mathbb{Z}[i]$ 是唯一因子分解整环。故 $\mathbb{Z}[i]$ 中元素在允许重排和相伴意义下唯一。

故对于任意的 $a+bi$ 均可在 $\mathbb{Z}[i]$ 中分解为以上几类不可约元。故有

$$a^2+b^2 = N(a+bi) = 2^k \prod_i p_i^{l_i} \prod_j p_j'^{2l'_j},$$

其中 $N(a) = a\bar{a}$, $p_i \equiv 1 \pmod 4$, $p'_j \equiv 3 \pmod 4$。

故对于某数 M 可表示为二平方和 (包含平凡情况 $x = y^2 + 0^2$), 当且仅当 $2 | \operatorname{ord}_{p'_j}(M)$ 对所有 $p'_j | M$ 成立。

注 注意到该条件在模 4 剩余类上并不等价于 $p \equiv 1 \pmod 4$ 和 $p \equiv 3 \pmod 4$, 而是更强的条件。考虑 $6 \equiv 3 \times 2 \equiv 2 \equiv 1 \times 2 \pmod 4$, 而 6 不能表示为平方和, 2 却可以表示为 $2 = 1^2 + 1^2$.

算法 4.2 **FullRepresentInteger**$'_{\mathcal{O}_0}(M)$

Data: $M \in \mathbb{Z}$ 使得 $M > p$。
Result: $\gamma = x + yi + z\frac{i+j}{2} + t\frac{1+k}{2}$, 其中 $\mathrm{Nrd}(\gamma) = M$。

令 $m' = \lfloor\sqrt{\frac{4M}{p}}\rfloor$, 取随机整数 $z' \in [-m', m']$;
令 $m'' = \lfloor\sqrt{\frac{4M}{p} - (z')^2}\rfloor$, 取随机整数 $t' \in [-m'', m'']$。令 $M' = 4M - p((z')^2 + (t')^2)$;
对所有 $p'_j | M'$ 且 $p'_j \equiv 3 \pmod 4$, 若存在 j s.t. $2 \nmid \mathrm{ord}_{p'_j}(M')$, 返回步骤 1;
若 **Cornacchia**$(M') = \perp$, 返回步骤 1。否则令 $x', y' =$ **Cornacchia**(M');
若 $x' \neq t' \mod 2$ 或 $z' \neq y' \mod 2$, 返回步骤 1;
令 $\gamma = (x' + iy' + jz' + kt')/2$;
return γ.

通过以上判定方法, 可将原 **FullRepresentInteger** 改写成算法 4.2的形式。需要注意的是, 存在部分数字, 其不为极大序模中的任何元素的范数。

例 4.1 对于 $p = 19$, 显然有 $p \equiv 3 \pmod 4$。然而不存在元素 $\gamma \in \mathcal{O}_0$ 使得 $\mathrm{Nrd}\,\gamma = 57$。考虑方程

$$228 = 4 \times 57 = x^2 + y^2 + 19(z^2 + t^2),$$

实际上发现 $19 \times (12 - z^2 - t^2) = x^2 + y^2$, 而 $z^2 + t^2 = 12$ 总不成立, 故有 $19 | x^2 + y^2$, 而要使得 $x^2 + y^2$ 存在, 则由 Fermat 平方和定理得 $p^2 | x^2 + y^2$, 故 $p | 12 - z^2 - t^2$。而 $12 = z^2 + t^2$ 无解, $12 - z^2 - t^2 < 19$ 显然成立。故方程无解。

实际上这种情况不算罕见, 表 4.1中是部分使得算法无解的方程参数。故原算法 **FullRepresentInteger** 存在一定可能性是无解的, 因此需要更多假设以确保该算法有解。无解方程中至少有部分方程中的 M 存在显式表示成 p 的函数的方式, 如

表 4.1 使得方程 $4M = x^2 + y^2 + p(z^2 + t^2)$ 无解的部分参数

p	19	23	31	43	47	59	67	67	71	71	79	79	83	83	83
M	57	69	93	129	141	177	79	201	77	213	91	237	95	139	249

以下定理所示, 对于 $M = 3p$ 的情况下, 方程无解。

定理 4.3 对于 $p \geqslant 19$ 且 $p \equiv 3 \pmod 4$, 令 $M = 3p$ 时, 方程

$$4M = x^2 + y^2 + p(z^2 + t^2) \tag{4.2}$$

无解。

证明 当 $M = 3p$ 时, (4.2) 化为 $12p = x^2 + y^2 + p(z^2 + t^2)$, 通过简单化简得 $(12 - z^2 - t^2)p = x^2 + y^2$。

此时有 $p|x^2+y^2$, 若要使得 x^2+y^2 存在, 则由 Fermat 平方和定理得至少要有 $p^2|x^2+y^2$, 故 $p|12-z^2-t^2$。而 $12=z^2+t^2$ 无解, 且 $12-z^2-t^2<19<p$ 显然成立。故方程无解。 ∎

推论 4.4 对于 $p\equiv 3 \pmod 4$, 令 $M=kp$, 当 $0<4k-z^2-t^2<p$ 对于任意 $z,t\in\mathbb{Z}$ 恒成立时, 方程

$$4M=x^2+y^2+p(z^2+t^2) \tag{4.3}$$

无解。

证明 当 $M=kp$ 时, (4.3) 化为 $p(4k-z^2-t^2)=x^2+y^2$, 此时有 $p|x^2+y^2$, 若要使得 x^2+y^2 存在, 则至少有 $p^2|x^2+y^2$ 或 $4k-z^2-t^2=0$, 后者由条件知不存在, 故 $p|4k-z^2-t^2$。且 $12-z^2-t^2<p$ 由题意成立。故方程无解。 ∎

对于部分较小的 M, 可假定其略大于 p, 故可设 $M=p+k$, 其中 $0<k<p$。对于这种情况, 可采用类似方法考虑解的存在性。由于此时 p 的系数较小, 情况较简单。

推论 4.5 对于 $M=p+k$, 其中 $0<k<p$, 当存在奇素数 $p'<p$ 对 $2\nmid \mathrm{ord}_{p'}(p+k)$, $2\nmid \mathrm{ord}_{p'}(p+2k)$, $2\nmid \mathrm{ord}_{p'}(k)$ 均成立, 则方程

$$4M=x^2+y^2+p(z^2+t^2)$$

无解。

证明 考虑方程 $p(4-z^2-t^2)+4k=x^2+y^2$, 考虑 z,t 的取值, 左侧有 3 种可能性, 分别是 $4(p+k)=x^2+y^2$, $2(p+2k)=x^2+y^2$, 以及 $4k=x^2+y^2$。对以上三种情况分别应用解的存在条件即可。 ∎

注 De Feo 等[8]3.1 称 $M-p(z^2+t^2)$ 为由 x^2+y^2 表示的素数, 但原文同样称 M' 可能为近似素数 (素数乘以一平滑数) 或非近似素数。故此处 M' 应当可为任意正整数。

5 总结

SQISign 作为目前基于同源的密码学系统中的一个十分优秀的签名系统, 具有密钥尺寸小且验证过程简单快速等优点。但其签名流程复杂等问题也极大程度制约了 SQISign 的应用。对于这一问题, 学界提出了多种方案对 SQISign 进行改进。例如通过改进其理想同源转换算法等来加速 SQISign 的签名流程, 改进 SQISign 的素数搜索算法来加速 SQISign 的初始化流程等。

本文对于 SQISign 的原理进行研究, 通过利用 Weil 配对来实现对二维椭圆曲线离散对数问题的一维化, 使得 Pohlig-Hellman 算法求解该问题成为可能, 并引入了 Montgomery 梯子方法来加速椭圆曲线有理点的计算。同时对原论文中在某指定序模内生成指定范数之元素的算法进行探究, 通过研究方程形式确定该方程存在解不存在的情况, 并且得到了部分情况下方程是否存在根的判定方法。通过提前判定根的存在性, **FullRepresentInteger** 的速度可进一步得到优化。

参考文献

[1] Couveignes J.M. Hard Homogeneous Spaces[EB/OL]. https://eprint.iacr.org/2006/291, 2006.

[2] Jao D., Soukharev V. A subexponential algorithm for evaluating large degree isogenies[A]. Hanrot G., Morain F., Thomé E. Algorithmic Number Theory[C]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010: 219-233.

[3] Jao D., De Feo L. Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies[A]. Yang B.Y. Post-Quantum Cryptography[C]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011: 19-34.

[4] Galbraith S.D., Petit C., Silva J. Identification protocols and signature schemes based on supersingular isogeny problems[J]. Journal of Cryptology, 2020, 33(1): 130-175.

[5] De Feo L., Kohel D., Leroux A., Petit C., Wesolowski B. Sqisign: Compact post-quantum signatures from quaternions and isogenies[A]. Moriai S., Wang H. Advances in Cryptology – ASIACRYPT 2020[C]. Cham: Springer International Publishing, 2020: 64-93.

[6] Silverman J.H. The arithmetic of elliptic curves[M]. New York: Springer-Verlag, 1992.

[7] Voight J. Quaternion Algebras[M]. Cham: Springer, 2021.

[8] De Feo L., Leroux A., Longa P., Wesolowski B. New Algorithms for the Deuring Correspondence - Towards Practical and Secure SQISign Signatures[A]. Hazay C., Stam M. Advances in Cryptology – EUROCRYPT 2023[C]. Cham: Springer Nature Switzerland, 2023: 659-690.

[9] Lin K., Wang W., Xu Z., Zhao C.A. A Faster Software Implementation of SQISign[EB/OL]. https://eprint.iacr.org/2023/753, 2023.

[10] Kohel D., Lauter K., Petit C., Tignol J.P. On the quaternion ℓ-isogeny path problem[J]. LMS Journal of Computation and Mathematics, 2014, 17(A): 418–432.

[11] Montgomery P.L. Speeding the Pollard and elliptic curve methods of factorization[J]. Mathematics of Computation, 1987, 48: 243-264.

[12] Bernstein D., Lange T. Montgomery curves and the montgomery ladder[M]. Bos J., Lenstra A. Topics in Computational Number Theory Inspired by Peter L. Montgomery. United Kingdom: Cambridge University Press, 2017: 82-115.

[13] 王学理, 裴定一. 现代数学基础丛书: 椭圆与超椭圆曲线公钥密码的理论与实现[M]. 科学出版社, 2006.

[14] Hamburg M. Fast and compact elliptic-curve cryptography[EB/OL]. https://eprint.iacr.org/2012/309, 2012.

[15] Nikolaev M.V. On the complexity of two-dimensional discrete logarithm problem in a finite cyclic group with efficient automorphism[J]. Discrete Mathematics and Applications, 2015, 6 (2): 45-57.

[16] Azarderakhsh R., Jao D., Kalach K., Koziel B., Leonardi C. Key Compression for Isogeny-Based Cryptosystems[A]. Keita E., Goichiro H., Zhang R. Proceedings of the 3rd ACM International Workshop on ASIA Public-Key Cryptography[C]. New York, NY, USA: Association for Computing Machinery, 2016: 1–10.

[17] Stange K.E. The tate pairing via elliptic nets[A]. Takagi T., Okamoto T., Okamoto E., Okamoto T. Pairing-Based Cryptography – Pairing 2007[C]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007: 329-348.

[18] Basilla J.M. On the solution of $x^2 + dy^2 = m$[J]. Proceedings of the Japan Academy, Series A, Mathematical Sciences, 2004, 80(5): 40-41.

[19] McLeman C., McNicholas E., Starr C. Gaussian Number Theory: $\mathbb{Z}[i]$ of the Storm[M]. Cham: Springer International Publishing, 2022: 137-169.

[20] Atiyah M.F., MacDonald I.G. Rings and ideals[M]. London: Addison-Wesley-Longman, 1969: 9-10.

攻读学士学位期间的学术活动及成果情况

1）参加的学术交流与科研项目

（1） 国家级全国大学生创新创业计划《基于半张量积方法的学习行为下的Bayesian Games 研究》成员

2）发表的学术论文（含专利和软件著作权）

[1] **X. Qiu**, Y. Chen, K. Liu, H. Chen, Y. Wu, L. Li, X.Zhao, *Decomposed Subspaces of Ex-Ante Agent Games*, 2023 42nd Chinese Control Conference (CCC), Tianjin, China, 2023, pp. 8121-8125, doi: 10.23919/CCC58697.2023.10240354.

致谢

在我即将完成本科生的学业, 踏上新的人生征程之际, 我要向那些在我本科四年中给予支持和帮助的人们表达最诚挚的感谢。

感谢合肥工业大学的张神星老师, 在他的指导下我完成了毕业论文。感谢常山老师以及他们的讨论班上的同学们, 如果没有他们我可能不会学习椭圆曲线的相关知识。感谢李露露老师, 在他的指导下我在大学阶段受到了一定的科研训练, 参与了大学生的创新创业项目。感谢吴小胜老师, 如果不是参加了他的讨论班我也不会了解素数定理的误差界和黎曼猜想的关系。感谢中科院信工所的于伟老师, 他收留我继续研究, 帮我规划方向。

在我学习期间, 他们不仅传授了我专业知识, 更是耐心指导、悉心关怀。他们的言传身教让我受益匪浅, 使我不断进步。

与此同时, 我要感谢我的同学们, 比如说吴越和陈左扬同学。你们给了我信心, 我们相互鼓励、共同进步。我们一同度过了难忘的大学时光，留下了深刻的友谊和美好的回忆。

此外, 我还要感谢我的父母。哀哀父母, 生我劬劳。如果没有你们的支持, 我如何能进一步发展? 殚竭心力终为子, 可怜天下父母心!

感谢大家!

邱修煜

2024 年 5 月 14 日