

SI-CP-ABE：一类基于同源的密文策略属性基加密方案

陈浙文¹, 陈锦榕², 徐铮³, 周子健¹

(1. 中国人民解放军国防科技大学理学院, 湖南 长沙 410073;

2. 中国人民解放军国防科技大学计算机学院, 湖南 长沙 410073;

3. 合肥国家实验室, 安徽 合肥 230088)

摘要：密文策略属性基加密 (CP-ABE) 是实现细粒度数据访问控制的关键密码学原语。然而, 现有基于双线性映射或格困难问题的方案, 普遍面临系统参数、密钥及密文尺寸较大的问题, 严重制约了其在资源受限场景中的实际部署。针对上述挑战, 提出了一种基于超奇异椭圆曲线同源的密文策略属性基加密 (SI-CP-ABE) 方案。该方案将同源理想类群作用与线性秘密共享方案结合, 在后量子安全环境下实现了高效的细粒度访问控制。在安全性方面, 提出了增强点交换超奇异同源计算型 Diffie-Hellman 假设 (P^+ -CSSCDH) 与增强点交换超奇异同源决策型 Diffie-Hellman 假设 (P^+ -CSSDDH) 两个新的困难假设, 并基于此在选择性安全模型下严格证明了该方案满足选择明文攻击不可区分性。为进一步提升性能, 在该方案的基础上设计了优化方案。此外, 基于 SI-CP-ABE 核心代数结构, 构造了一类具有认证功能的后量子 Naor-Reingold 型伪随机函数, 丰富了后量子密码协议的构建原语。

关键词：同源密码; 密文策略属性基加密; SiGamal; 线性秘密共享方案

中图分类号：TN918.1

文献标志码：A

DOI:10.11959/j.issn.2096-109x.AQ25251

SI-CP-ABE: an isogeny-based ciphertext-policy attribute-based encryption scheme

Chen Xiwen¹, Chen Jinrong², Xu Zheng³, Zhou Zijian¹

1. College of Science, National University of Defense Technology, Changsha 410073, China

2. College of Computer Science and Technology, National University of Defense Technology, Changsha 410073, China

3. Hefei National Laboratory, Hefei 230088, China

Abstract: Ciphertext-policy attribute-based encryption (CP-ABE) serves as a fundamental cryptographic primitive for fine-grained data access control. However, existing schemes, primarily based on bilinear maps or lattice hardness assumptions, generally suffer from large system parameters, key sizes, and ciphertext sizes, which severely restrict their deployment in resource-constrained scenarios. To address this challenge, a novel CP-ABE scheme based on supersingular elliptic curve isogeny (SI-CP-ABE) is proposed. This scheme integrates the action of isogeny ideal class group with linear secret sharing schemes, achieving efficient fine-grained access control in a post-quantum security setting. Regarding security, two new hardness assumptions— P^+ -CSSCDH and P^+ -CSSDDH—are

收稿日期: 2025-10-13; 修回日期: 2026-02-10

通信作者: 周子健, zhouzijian122006@163.com

基金项目: 国家自然科学基金资助项目 (No.62202475, No.12501731, No.12371013); “量子通信与量子计算机” 国家科技重大专项资助项目 (No.2021ZD0302902)

Foundation Items: The National Natural Science Foundation of China (No.62202475, No.12501731, No.12371013), Quantum Science and Technology-National Science and Technology Major Project (No.2021ZD0302902)

proposed, based on which the scheme is rigorously proven to satisfy indistinguishability under chosen plaintext attack in the selective security model. To further enhance performance, an optimized scheme is designed based on SI-CP-ABE. Furthermore, based on the core algebraic structure of SI-CP-ABE, a post-quantum Naor-Reingold-type pseudo-random function with authentication capability is constructed, thereby enriching the building blocks for post-quantum cryptographic protocols.

Key words: isogeny-based cryptography, ciphertext-policy attribute-based encryption, SiGamal, linear secret sharing scheme

0 引言

加密方案是守护互联网数据安全的基石,其有效性的根本前提在于建立公钥与真实身份之间的可靠关联。面对日益复杂的网络应用与数据共享需求,传统“一对一的公钥绑定”模式在灵活性与效率上显露出不足,能够实现一对多、细粒度访问控制的属性基加密^[1](attribute-based encryption, ABE)成为更具适应性的关键技术。

ABE加密框架利用属性集合定义用户的身份和权限,并将灵活可控的访问结构嵌入加密机制中,只有当属性集合满足访问结构时,方案才能解密成功,从而实现对数据资源的细粒度访问。根据属性集合与访问结构的对应关系,可以将ABE方案分为两类,即密钥策略属性基加密^[2](key-policy attribute-based encryption, KP-ABE)方案和密文策略属性基加密^[3](ciphertext-policy attribute-based encryption, CP-ABE)方案。KP-ABE方案将访问结构(访问策略)嵌入用户密钥,适用于对静态资源的共享和访问;CP-ABE方案则将策略嵌入密文,适用于对数据的动态上传和共享,加密者能够随时调整密文消息的权限设置,在去中心化的数据共享环境中展现出显著优势。从密码学框架角度看,ABE也可以被看作利用访问控制策略加密数据应用^[4]中的构造部件,是一种特殊的功能性加密方案,在云存储、物联网接入控制等场景中具有广阔的应用前景。

随着量子计算技术的飞速发展,满足后量子安全要求的加密算法成为研究热点。然而,现有ABE方案多基于双线性配对^[5]或格密码^[6]构造,在参数效率或技术多样性上存在局限。同源密码^[7]因其参数紧凑和安全假设独立于主流格困难问题的独特优势,为构建新一代后量子安全、高效实用的ABE方案提供了富有潜力的新途径。

同源密码虽然在带宽效率上具有显著优势,

但相关研究多局限于密钥交换或基础公钥加密。自Koshiha等^[8]于2016年提出首个基于同源的同源KP-ABE方案以来,基于同源的同源CP-ABE方案鲜有突破,这一研究空白不仅限制了同源密码在动态访问控制中的应用,也制约了后量子ABE技术路线的多样性。

针对上述挑战,本文旨在探索一种基于同源群作用的后量子属性基加密新路径。本文的主要贡献包括:构建了支持线性秘密共享方案(linear secret sharing schemes, LSSS)的同源密文策略属性基加密(supersingular elliptic curve isogeny CP-ABE, SI-CP-ABE)方案,并给出了基于坐标压缩的优化版本;在提出的增强点交换超奇异同源计算型Diffie-Hellman假设(P^+ -CSSDDH)和增强点交换超奇异同源决策型Diffie-Hellman假设(P^+ -CSSCDH)下证明了该方案的安全性;此外,扩展构造了一种抗部分密钥泄露的新型Naor-Reingold型伪随机函数。

本文所构造的方案基于紧凑的密文尺寸,在参数效率上显著优于经典及现有后量子方案,SI-CP-ABE及其衍生的抗泄露的伪随机函数,为物联网等资源受限场景下的细粒度数据共享提供了具备可证明安全性的轻量化解决方案。

全文结构安排如下:第1节概述属性基加密与同源密码学的研究现状,重点分析现有技术路线在后量子环境下面临的挑战与局限性;第2节系统回顾超奇异椭圆曲线同源、理想类群作用及线性秘密共享方案等数学预备知识,明确符号定义;第3节详细阐述本文提出的SI-CP-ABE方案的形式化定义与具体构造流程;第4节对方案进行全面的理论剖析,包括正确性证明、基于新假设的安全性归约,以及与现有主流方案的参数对比和性能评估;第5节扩展核心加密结构,提出一种支持认证并抗部分密钥泄露的Naor-Reingold

型伪随机函数,并论证其安全性;第6节总结全文工作,并对未来研究方向进行展望。

1 相关工作

1.1 属性基加密方案

自 Sahai 等^[1]引入属性基加密概念以来,相关领域迅速发展。在经典计算环境下,基于离散对数问题的 CP-ABE 方案已形成较为完善的理论体系: Bethencourt 等^[3]首次以访问树实现细粒度访问控制; Waters^[9]引入线性私密共享方案 (LSSS) 以支持任意单调访问结构,显著提升了表达能力和安全性。

随着量子计算威胁的迫近,后量子属性基加密的研究重心逐渐向格密码迁移。早期工作如 Zhang 等^[10]于 2011 年基于带错学习 (learning with errors, LWE) 假设构造了首个格上 CP-ABE; Fun 等^[11]于 2015 年基于环 LWE (ring LWE, RLWE) 实现了抗共谋的单调访问结构。近年来,格基 ABE 在功能扩展与效率优化方面取得了一系列重要突破: 2021 年, Varri 等^[12]实现了支持密文关键字搜索的 CP-ABE,在决策 LWE 假设下满足选择明文攻击 (indistinguishability under chosen plaintext attack, IND-CPA) 安全; Qian 等^[13]通过访问树结构与压缩技术优化了密钥复用与密文尺寸。2022 年, Li 等^[14]提出了恒定尺寸密钥的 KP-ABE 方案。2023 年, Huang 等^[15]提出基于 RLWE 的可撤销多权限 CP-ABE 方案,适用于量子安全的云文件共享系统; 同年, Wee 等^[16]从功能承诺中隐式导出高效 CP-ABE,而 Wee^[17]于 2024 年提出的格基压缩技术使参数进一步逼近理论下界。2025 年, Zhang 等^[18]基于标准 LWE 假设构造了支持穿刺、前向安全及用户撤销的 CP-ABE 方案,其安全性建立在标准 LWE 之上,代表了格基 CP-ABE 在功能丰富性和理论严谨性方面的最新突破。在更复杂计算模型方面, Agrawal 等^[19]于 2024 年首次基于格假设构造支持图灵机的 ABE, Dong 等^[20]进一步实现支持随机访问机的 ABE,其密文尺寸与电路规模无关; 2025 年, Cini 等^[21]提出的 KP-ABE 实现了与图灵机运行时间 T 呈线性关系的加密效率与恒定尺寸密钥,同时保持了恒定大小的密钥,并消除了对循环张量 LWE 的依赖。这些方案的安全性

常归约于规避 LWE 假设^[22],该假设也是构建密文大小与电路无关的 CP-ABE^[23]、多输入属性基加密 (multi-input ABE, miABE)^[24]以及无界 ABE^[25]的理论基础。

针对系统架构的优化也是当前属性加密研究的重要方向之一。去中心化属性加密通过多权威或注册机制消除单点依赖: Datta 等^[26]于 2021 年基于 LWE 构造了首个后量子安全的多权威 ABE 方案; Hohenberger 等^[27]于 2023 年首次形式化定义了注册式 ABE, Wee 等^[28]于 2025 年进一步实现了用户数无界的简洁构造。与此同时, ABE 与其他密码原语的融合拓展了其应用边界: Agrawal 等^[29]于 2023 年构建了支持属性加权和多输入 ABE 方案,实现了细粒度数据聚合控制。上述工作从系统架构和功能扩展角度为 ABE 的实用化提供了新思路。

在国内研究中, ABE 方案的实用化与功能拓展同样是研究热点。针对云存储环境下的实际需求,周艺华等^[30]于 2022 年提出了基于属性策略隐藏的可搜索加密方案,将访问控制与关键字搜索、文件存储加密相结合,并通过聚合密钥技术减轻了密钥管理的负担。在访问策略隐私保护方面,张兴兰等^[31]于 2019 年引入群签名技术,实现了 CP-ABE 中访问策略的属性隐藏,在保护策略隐私的同时满足选择明文攻击下的不可区分性。为解决分布式微服务架构中的细粒度访问控制和数据安全通信问题,张智烁等^[32]于 2024 年设计了支持属性立即撤销的可复用属性基签名及其密钥协商方案,实现了签名与访问策略的解耦,显著提升了认证效率。针对工业物联网场景中属性撤销效率低的问题,李晓伟等^[33]于 2025 年提出了一种基于双联盟链的数据共享架构,通过属性单向哈希链实现了属性的高效批量撤销,进一步拓展了 ABE 在分布式系统中的应用。这些工作从不同角度丰富了 ABE 的功能集,为构建更高效、更实用的后量子访问控制方案提供了有益参考。

传统属性基加密体系中的方案多基于双线性配对构建,其安全性依赖经典数论难题,无法抵御量子计算攻击。随着美国国家标准与技术研究院 (national institute of standards and technology, NIST) 后量子密码标准化进程的推进,具备抗

量子能力的新型密码体制成为研究重点。当前,后量子安全的属性基加密方案主要基于格困难问题构造,技术路径相对单一,且普遍存在计算开销大、密钥与密文尺寸较大的问题,制约了其在资源受限场景中的部署。

1.2 同源密码

同源密码因具备抗量子特性及在密钥与带宽方面的优势而受到关注。2011年, Jao等^[7]提出超奇异同源密钥交换 (supersingular isogeny Diffie-Hellman, SIDH) 协议, 其衍生的超奇异同源密钥封装 (supersingular isogeny key encapsulation, SIKE) 方案在 2022 年成为 NIST 后量子密码标准化第 3 轮备选方案中唯一同源候选方案。然而 2023 年, Castryck 等^[34]、Maino 等^[35]和 Robert^[36]提出的攻击方法严重挑战了其安全性。研究者为此提出了 MSIDH^[37]、binSIDH、terSIDH^[38]、FESTA^[39]、QFESTA^[40]、POKÉ^[41]等多种优化变体, 但其稳健性仍需进一步验证。

在另一技术路线上, 2018 年 Castryck 等^[42]提出了交换超奇异同源密钥交换 (commutative supersingular isogeny Diffie-Hellman, CSIDH) 协议。随后, Moriya 等^[43]于 2020 年提出基于 CSIDH 的公钥加密方案: SiGamal 和其压缩版本 C-SiGamal。2021 年, Fouosta 等^[44]提出简化方案 SimS。同年, Bahramian 等^[45]提出首个基于同源的身份基加密 (identity-based encryption, IBE) 方案。2022 年, Fan 等^[46]提出第一个基于同源的抗量子关键词搜索公钥加密方案, 该方案在量子随机预言模型下具有可搜索的密文安全性和陷门信息的不可区分性, 同时保持了较低的计算和通信复杂度。2023 年, Huang 等^[47]提出高效公钥加密方案, 进一步缩减密钥尺寸, 并达到选择密文攻击 (indistinguishability under chosen ciphertext attack, IND-CCA) 安全。2025 年, Dartois 等^[48]提出了名为 PEGASIS 的实用算法, 首次在 CSIDH-4096 等高安全级别下实现了高效的类群作用。这些工作显著拓展了同源密码的应用范围, 为构建同源基 CP-ABE 方案奠定了重要理论基础。

在同源公钥加密方案的实用化方面, Moriya 等^[49]于 2025 年基于带挠点的长同源 (LIT) 图对

SiGamal 进行了优化, 提出了 LIT-SiGamal 方案, 该方案在保持安全性的同时显著提升了加解密效率。实验结果表明, 在 128 位安全级别下密钥生成仅需 1.33 s, 加解密分别在 0.03 s 和 0.09 s 内完成, 是目前 FESTA 系列同源加密方案中首个完整底层语言实现。LIT-SiGamal 与 PEGASIS 等工作的出现, 标志着同源密码正从理论构造迈向实用部署阶段, 为构建高效、可证明安全的同源基 CP-ABE 方案提供了重要的技术储备。

当前, 同源密码的研究多集中于基础协议构造, 在功能性加密等复杂场景中的应用仍较为有限, 特别是 ABE 这类高级原语尚未得到充分探索。为此, 本文将同源密码拓展至 CP-ABE 领域, 提出基于同源理想类群作用的 SI-CP-ABE 方案, 旨在发展基于同源的高级加密功能, 对进一步完善其后量子密码理论框架具有关键意义。

1.3 本文主要工作

针对现有工作中 ABE 方案大都基于传统双线性映射和格困难问题, 且同源密码在 CP-ABE 构造领域尚属空白的现状, 本文提出了基于同源类群作用的 CP-ABE 方案, 旨在为后量子 ABE 提供一条基于不同数学困难问题的新技术路径, 在保持策略表达能力和参数紧凑性的同时, 增强密码学基础的多样性。本文的主要贡献如下。

(1) 设计了基于同源理想类群作用的 CP-ABE (SI-CP-ABE) 方案, 该方案在标准模型下实现了细粒度访问控制, 无须依赖随机预言机。SI-CP-ABE 的密文尺寸为 $2(\ell + 1)\log_2 p$, 其中 p 是方案所需素数, ℓ 是 LSSS 矩阵的行数。通过引入坐标压缩技术, 进一步提出优化方案 CSI-CP-ABE, 其密文尺寸可降至经典双线性对方案 (如 Waters11) 的约 50%。在私钥尺寸方面, CSI-CP-ABE 方案完全摆脱了格基方案中对环维度或格维数的依赖, 私钥尺寸仅与用户属性集大小呈线性关系。理论分析表明, 该方案在公钥、私钥及密文尺寸上相较于现有后量子方案 (如基于 RLWE 的 Tan15 方案^[11]和最近基于 LWE 的 Zhang25 方案^[18]) 具有明显优势。

(2) 给出了该方案在选择安全模型下的严格安全性证明。针对同源类群作用的特性, 本文提出了两个新的困难假设: 计算性假设 P^+ -CSSCDH

和判定性假设 $P^+-CSSDDH$ 。在此基础上,将该方案的安全性归约至这两个假设,严格证明了 SI-CP-ABE 在选择性安全模型下满足 IND-CPA 安全。

(3) 构造了抗泄露且带认证的后量子伪随机函数。基于 SI-CP-ABE 的代数结构,本文进一步设计了一类 Naor-Reingold 型伪随机函数。与传统构造不同,该函数利用共享秘密引入了盲化机制,形式化证明表明,该构造不仅具备伪随机性,还能有效抵御部分密钥泄露攻击,并提供原生的数据认证功能。

2 预备知识

本节阐述了构建基于同源的密文策略属性基加密方案所必需的数学基础与相关模型。首先,明确定义全文使用的符号体系,为后续表述提供一致性基础。其次,形式化描述 CP-ABE 的算法框架及其在选择性安全模型下的安全性定义,并介绍 LSSS 作为表达访问结构的核心工具。最后,介绍超奇异椭圆曲线同源理论的关键概念以及核心命题与定理。

2.1 符号说明

本文使用的符号及其定义见表1。

表1 本文使用的符号及其定义

符号	定义
p	大素数
$\mathbb{F}_p$	特征为 p 的有限域
E	超奇异椭圆曲线
$\mathfrak{a}, [a], \text{cl}(\mathcal{O})$	整理想,理想类,理想类群
PK, MSK, SK, CT	公钥,主私钥,私钥,密文
(M, ρ)	LSSS 访问结构
$\text{Setup}()$	预备算法
$\text{KeyGen}()$	密钥生成算法
$\text{Encryption}()$	加密算法
$\text{Decryption}()$	解密算法

2.2 CP-ABE 加密框架

在数据外包场景下,CP-ABE 方案的架构主要包含4个实体:可信中心(trusted authority, TA)、数据所有者、数据使用者和数据服务方。可信中心指一个被信任的实体,其主要工作是产生系统公开参数和主密钥,而后根据主密钥和用户属性

集合产生用户私钥,它在确保数据安全和访问控制方面起着核心作用;数据所有者制定数据的访问控制策略,并将策略嵌入加密数据中,发送给服务方进行数据共享,相当于对这份数据做了一个粒度可以细化到属性级别的加密访问控制;数据使用者利用从可信中心得到的相应私钥,解密从数据服务方获得的密文,当且仅当用户的属性集合满足密文中内嵌的访问结构时,用户才能够成功解密数据,否则只能得到乱码;数据服务方是指数据的实际存储方,数据所有者在此存储加密后的数据,数据使用者在此下载加密后的数据。CP-ABE 方案架构如图1所示。

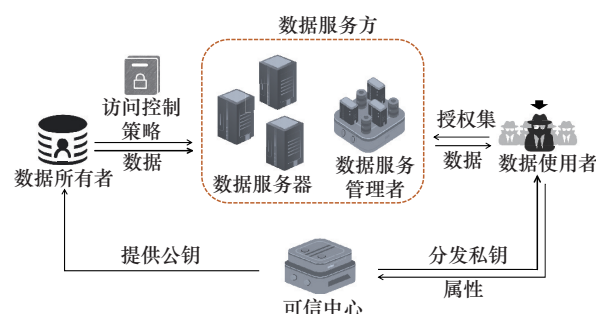


图1 CP-ABE 方案架构

CP-ABE 方案由4个概率多项式时间(PPT)算法构成,具体定义如下。

$\text{Setup}(\lambda, U)$: 初始化算法,输入安全参数 λ 和全体属性集合 U ,输出公共参数 PK ,主密钥 MSK 。

$\text{KeyGen}(MSK, S)$: 密钥生成算法输入主密钥 MSK 和用户属性集合 S ,输出用户私钥 SK 。

$\text{Encryption}(PK, m, \Delta)$: 加密算法输入公共参数 PK ,明文 m 和特定访问结构 Δ ,输出密文 CT ,该密文暗含访问结构 Δ 相关信息。

$\text{Decryption}(PK, CT, SK')$: 解密算法输入公共参数 PK ,内嵌 Δ 的密文 CT 和解密者私钥 SK' ,输出消息 m' 或终止符号“ $\perp$ ”。

正确性 给定安全参数 λ ,若 CP-ABE 方案 $\mathcal{P}(\lambda)$ 对任意明文 m 和 $SK \leftarrow \text{KeyGen}(MSK, S)$, $\Pr[\text{Dec}(SK', PK, \text{Enc}(m, PK, \Delta)) = m] = 1 - \text{negl}(\lambda)$ 成立,其中 $\text{negl}(\lambda)$ 是关于安全参数 λ 的可忽略函数,则 $\mathcal{P}(\lambda)$ 具有解密正确性。 $\text{Enc}()$ 表示加密算法,输入为明文 m 、公钥 PK 和访问结构 Δ ,输出密文; $\text{Dec}()$ 表示解密算法,输入为私钥

SK、公钥PK和密文，输出解密结果。

在CP-ABE方案的安全模型^[9]中，敌手选择对某特定访问结构 Δ^* 进行加密挑战，并且可以要求获取任何不满足 Δ^* 的私钥SK。下面对安全模型进行详细描述。

Setup 挑战者运行Setup算法，并将公共参数PK提供给敌手 $\mathcal{A}$ 。

Phase 1 敌手 $\mathcal{A}$ 可自适应查询任意属性集合 S_q 的私钥 SK_q ，注意这些集合的并集不得满足挑战访问结构 Δ^* 。

Challenge 敌手 $\mathcal{A}$ 提供两个等长消息 m_0 和 m_1 ，挑战者随机选择 $b \in \{0, 1\}$ ，然后对 m_b 和 Δ^* 进行加密操作，生成挑战密文 CT_b ，并交给敌手。

Phase 2 重复Phase 1的过程。需要注意的是，敌手 $\mathcal{A}$ 询问过的所有属性集合并集亦需无法满足挑战所对应的访问结构。

Guess 敌手 $\mathcal{A}$ 输出对 b 的猜测 b' 。若 $b = b'$ ，则敌手 $\mathcal{A}$ 在此攻击游戏中胜利，否则失败。

敌手 $\mathcal{A}$ 赢得此游戏的优势为：

$$\text{Adv}_{\mathcal{A}} = \left| \Pr [b = b'] - \frac{1}{2} \right|。$$

系统在Setup前增设初始化阶段算法，攻击者需在此阶段提供挑战访问结构 Δ^* ，若所有多项式时间敌手在上述游戏中的优势上界为可忽略函数，则称该系统具有选择安全性。本文提出的所有构造均在选择性安全模型下证明其安全性。

注意到CP-ABE方案中常利用线性秘密共享方案高效表达访问结构。这是一种秘密共享机制，允许秘密持有者将秘密分割成多个部分，分配给不同的参与者。只有符合特定授权条件的参与者才能通过线性组合重建原始秘密，非授权组合无法获取任何有用信息^[50]。

定义1 线性秘密共享方案

令 p 为素数， $\mathcal{P} = \{P_1, \dots, P_n\}$ 为参与方集合。定义在 $\mathcal{P}$ 上的秘密共享方案 Π 若满足以下条件，则称其为 $\mathbb{Z}_p$ 上的线性秘密共享方案。

(1) 每个参与者份额构成 $\mathbb{Z}_p$ 上的一个向量。

(2) 存在一个共享生成矩阵 $M_{\ell \times k}$ 和满射函数 $\rho: \{1, \dots, \ell\} \rightarrow \mathcal{P}$ ，将矩阵每一行 i 映射到参

与方 $\rho(i)$ 。对于待共享秘密 $s \in \mathbb{Z}_p$ ，随机选择 $y_2, \dots, y_k \in \mathbb{Z}_p$ ，构成列向量 $\mathbf{v} = (s, y_2, \dots, y_k)^T$ ，则共享向量 $\lambda = M\mathbf{v} = (\lambda_1, \dots, \lambda_\ell)$ ，其中 λ_i 表示共享向量的分量。

2.3 同源密码的数学基础理论

设 K 为有限域，特征为素数 p ， $\bar{K}$ 为其代数闭包。本文固定 K 的特征不为2或3以简化讨论，相关结论可通过适当推广适用于一般特征。

定义2 蒙哥马利(Montgomery)曲线

当 $\text{char}(K) \neq 2$ 时，形如

$$by^2 = x^3 + ax^2 + x \quad (a, b \in K, b(a^2 - 4) \neq 0)$$

的椭圆曲线称为Montgomery曲线，其中非退化条件 $b(a^2 - 4) \neq 0$ 保证了曲线的光滑性。

定义3 同源

设 E_1, E_2 为定义在 K 上的椭圆曲线，同源 $\varphi: E_1 \rightarrow E_2$ 是椭圆曲线间的满射群同态，满足 $\varphi(O_{E_1}) = O_{E_2}$ 。

任意给定有限子群 $G \subset E(\bar{K})$ ，以其为核，可得到典范同源 $\varphi: E \rightarrow E/G$ ，此构造在 K -同构意义下唯一^[51]。

定义4 超奇异椭圆曲线

设 K 为特征 $p > 0$ 的有限域，如果椭圆曲线 E/K 的 p -挠子群 $E[p]$ 在几何上平凡，即：

$$E[p](\bar{K}) = \{O_E\}，$$

则称椭圆曲线 E/K 为超奇异的。

例1 若素数 $p \equiv 3 \pmod{4}$ ，则曲线 $E/\mathbb{F}_p: y^2 = x^3 + x$ 是超奇异的，因其 p -挠群平凡。

$\mathcal{O}$ 是虚二次域的序，全体可逆分式理想在乘法下构成阿贝尔群 $I(\mathcal{O})$ ，其子群 $P(\mathcal{O})$ 由主分式理想生成，即 $P(\mathcal{O}) = \{a \mid a = a\mathcal{O}, a \in K^\times\}$ ， $K^\times$ 表示域 K 中所有非零元素在乘法运算下构成的T恤法群（后文对任意域 F ，记号 $K^\times$ 均表示其乘法群）。由此定义理想类群为商群 $\text{cl}(\mathcal{O}) := I(\mathcal{O})/P(\mathcal{O})$ ，由定义知每个理想类 $[a] \in \text{cl}(\mathcal{O})$ 都有一个整理想的代表元。椭圆曲线 E 到自身的同源称为自同态，其关于加法和复合构成一个环结构，记为自同态环 $\text{End}(E)$ ，记 $\text{End}_p(E)$ 为 $\text{End}(E)$ 中定义在 $\mathbb{F}_p$ 上所有自同态构成的子环。

命题1^[42] 设 $p > 5$ 是一个满足 $p \equiv 3 \pmod{8}$ 的素数，令 E 是定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线。那

么 $\text{End}_p(E) \cong \mathbb{Z}[\pi_p]$ 当且仅当存在 $A \in \mathbb{F}_p$, 使得曲线 E 是 $\mathbb{F}_p$ -同构于曲线 $E_A: Y^2 = X^3 + AX^2 + X$ 的, 其系数定义在有限域 $\mathbb{F}_p$ 上, 其中 π_p 表示椭圆曲线上的 p -Frobenius 映射。此外, 若 A 存在, 则唯一。

对于理想 $\mathfrak{a}$, 我们将 $\mathbb{F}_p$ -同构类 $E/E[\mathfrak{a}]$ 对应的 Montgomery 曲线记为 $[a]E$ 。

定理 1^[43] 设 E 为定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线, 同源 $\Phi_{[a,(E)]}: E \rightarrow [a]E$, 且 $\ker \Phi_{[a,(E)]} = E[\mathfrak{a}] = \bigcap_{\alpha \in \mathfrak{a}_s} \ker \alpha$, 其中 $\mathfrak{a}_s$ 是 $\mathfrak{a}$ 的可分部分, $\ker \alpha$ 表示 $\mathfrak{a}_s$ 中元素的核。那么定义在 $\mathbb{F}_p$ 上的同源满足等式:

$$\Phi_{[b],([a]E)} \circ \Phi_{[a],(E)} = [\pm 1] \circ \Phi_{[a],([b]E)} \circ \Phi_{[b],(E)} \quad (2)$$

将由与点 P 在模 $\{\pm 1\}$ 意义下相同的点构成的等价类记作 αP 。此外, 记 $J(\mathbb{Z}[\pi_p])$ 为所有形如 $(\alpha)l_1^{e_1} \cdots l_n^{e_n}$ 元素的集合, 其中 α 为整数。等价类 $(\alpha)l_1^{e_1} \cdots l_n^{e_n} P$ 对应于 αP 在由理想 $l_1^{e_1} \cdots l_n^{e_n}$ 定义的同源映射下的像类。

3 基于同源的 CP-ABE 方案设计

本节旨在构造基于超奇异同源理想类群作用的 SI-CP-ABE 方案, 其核心设计思想是利用群作用的自由传递性与交换性来模拟经典方案中的双线性配对结构, 并通过线性秘密共享方案矩阵将复杂的访问策略嵌入同源路径的演化过程中。

在选择性安全模型下, 本方案满足选择明文攻击不可区分性。将证明, 若底层 P^+ -CSSDDH 假设成立, 则任何多项式时间内的攻击者都无法以不可忽略的优势攻破该方案。需要说明的是, 该方案的设计与安全性论证均基于诚实参与方假设, 暂不考虑拜占庭参与方情形。

为了平衡计算效率与通信开销, 本节首先阐述基础方案 SI-CP-ABE 的具体构造, 随后进一步提出基于坐标压缩技术的优化方案 CSI-CP-ABE。

3.1 方案描述

SI-CP-ABE 方案遵循标准的 CP-ABE 框架, 涉及 4 个多项式时间算法: Setup、KeyGen、Encryption 和 Decryption。该方案由可信中心、数据所有者和数据使用者三方分别运行完成, 方案逻辑架构如图 2 所示。

可信中心: 执行 Setup 算法生成系统公钥 PK 与主私钥 MSK, 并执行 KeyGen 算法为合法用户

根据其属性集合 S 生成对应的用户私钥 SK。

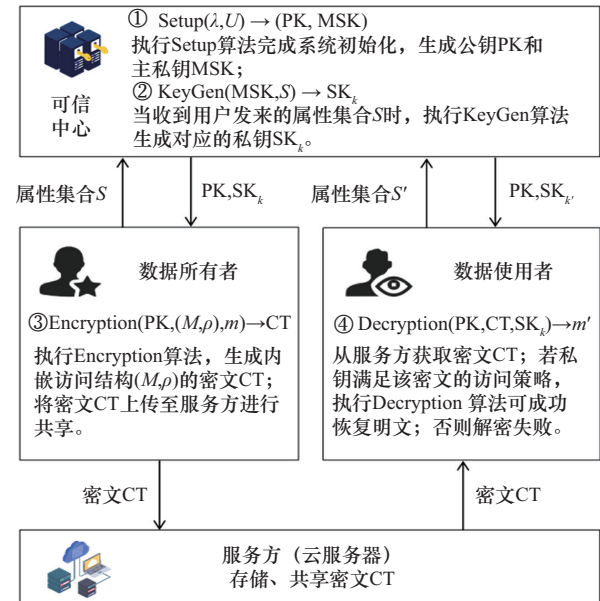


图2 SI-CP-ABE 方案逻辑架构

数据所有者: 拥有明文数据 m , 并制定访问策略 $(M_{\ell \times k}, \rho)$ 。其执行 Encryption 算法, 利用系统公钥 PK 将 m 加密为密文 CT, 该密文内嵌了策略 $(M_{\ell \times k}, \rho)$ 。随后, CT 被上传至服务方 (如云服务器) 进行共享。

数据使用者: 从服务方获取密文 CT, 并从可信中心处获得与其属性匹配的私钥 SK。若其属性集合 S 满足密文中的访问策略 $(M_{\ell \times k}, \rho)$, 则执行 Decryption 算法可成功恢复明文 m ; 否则解密失败。

具体而言, 算法 Setup、KeyGen、Encryption 和 Decryption 分别定义如下。

算法 1 系统初始化算法 Setup

输入 安全参数 λ , 系统属性全集大小 U

输出 系统公钥 PK, 主私钥 MSK

- 1) 选取素数 $p = 2^r \cdot \ell_1 \cdots \ell_n - 1$, 其中 r 为正整数, $\ell_i (i = 1, \dots, n)$ 为互异的小奇素数
- 2) 定义超奇异椭圆曲线 $E_i: Y^2 Z = X^3 + XZ^2$
- 3) 选取点 $P_i \in {}_R E_i(\mathbb{F}_p)$, 满足 $\text{ord}(P_i) = 2^r$
- 4) 随机均匀选取理想 $\mathfrak{r} \in J(\mathbb{Z}[\pi_p])$
- 5) $E_0 \leftarrow [\mathfrak{r}] E_i$
- 6) $P_0 \leftarrow \mathfrak{r} P_i$
- 7) **for** $i = 1$ **to** U **do**
- 8) 随机选取 $a_i \in J(\mathbb{Z}[\pi_p])$

9) $E_i \leftarrow [a_i] E_t$
 10) $P_i \leftarrow a_i P_t$
 11) **end**
 12) 随机选取 $t_j \in \mathbb{Z}_p^U$
 13) $T \leftarrow \{t_1, \dots, t_U\}$
 14) 构造双射 $f: \{\text{全体属性}\} \rightarrow \{t_j | t_j \in T\}$
 15) $\text{PK} \leftarrow (E_0, P_0, E_i, P_i), i \in [1, U]$
 16) $\text{MSK} \leftarrow (t, a_1, a_2, \dots, a_U, f)$
 17) **return** (PK, MSK)

算法2 生成用户私钥 KeyGen

输入 主私钥 MSK, 用户属性集合 S

输出 用户私钥 SK_k

1) 随机选取理想 $u_k \in J(\mathbb{Z}[\pi_p])$, 满足其范数为奇数 // k 用来标记不同用户
 2) **for** each $i \forall f^{-1}(t_i) \in S$ **do**
 3) $a'_i \leftarrow u_k r a_i^{-1}$
 4) 计算 $\deg(a_i u_k)$ // $\deg(a_i u_k)$ 表示 $a_i u_k$ 的度数 degree
 5) **end**
 6) $\text{SK}_k \leftarrow (\{u_k, (a'_i, t_i, \deg(a_i u_k)) | \forall f^{-1}(t_i) \in S\})$
 7) **return** SK_k

算法3 根据访问策略加密明文 Encryption

输入 系统公钥 PK, 访问结构 $(M_{\ell \times k}, \rho)$, 明文 $m \in \mathbb{Z}_{2^{(r-2)}}$

输出 密文 CT

1) $m \leftarrow 2m + 1 \in (\mathbb{Z}/2^r\mathbb{Z})^\times$
 2) 随机均匀选取整数 $\beta \in (\mathbb{Z}/2^r\mathbb{Z})^\times, b_1, \dots, b_n \in \mathbb{Z}_p$
 3) $b \leftarrow (\beta) I_1^{b_1} \dots I_n^{b_n} \in J(\mathbb{Z}[\pi_p])$
 4) 随机选取奇数 $s \in (\mathbb{Z}/2^r\mathbb{Z})^\times$, 整数 $y_2, \dots, y_k \in \mathbb{Z}_p$
 5) $\mathbf{v} \leftarrow (s, y_2, \dots, y_k)^T$
 6) **for** $i = 1$ **to** ℓ **do**
 7) $\lambda_i \leftarrow M_i \mathbf{v}$
 8) **end**
 9) $E'_0 \leftarrow [b] E_0$
 10) $P'_0 \leftarrow b(s(2m + 1)P_0)$
 11) **for** $i = 1$ **to** ℓ **do**

12) $j \leftarrow \rho(i)$ // 获取第 i 行属性索引
 13) $E'_i \leftarrow [b] E_j$
 14) $P'_i \leftarrow b(\lambda_i P_j)$
 15) **end**
 16) $\text{CT} \leftarrow (E'_0, P'_0, E'_i, P'_i), i \in [1, \ell]$
 17) **return** CT

算法4 当属性满足策略时解密密文 Decryption

输入 系统公钥 PK, 密文 CT, 用户私钥 SK_k

输出 解密消息 m' 或错误标识 $\perp$

1) Parse CT as $((E'_0, P'_0), \{(E'_i, P'_i)\}_{i \in [1, \ell]})$ // 将密文 CT 解析为曲线 E'_0 、点 P'_0 以及 ℓ 个曲线-点对 (E'_i, P'_i)

2) Parse SK_k as

$(\{u_k, (a'_i, t_i, \deg(a_i u_k)) | \forall f^{-1}(t_i) \in S\})$ // 将用户私钥 SK_k 解析为盲因子 u_k 及属性相关的三元组列表

3) **for** each $i \forall f^{-1}(t_i) \in S$ **do**

4) **if** $E_0 \neq [u_k]^{-1} [a'_i] E_i$ **then**

5) **return** $\perp$

6) **end**

7) **end**

8) $I \leftarrow \{i | \rho(i) \in S\} \subset \{1, 2, \dots, \ell\}$

9) **if** S 不满足 $(M_{\ell \times k}, \rho)$ **then**

10) **return** $\perp$

11) **end**

12) 计算常数 $\{\omega_i \in \mathbb{Z}_p\}_{i \in I}$, 使得 $\sum_{i \in I} \omega_i \lambda_i = s$

13) 计算 $\sum_{i \in I} \frac{1}{\deg(a_i u_k)} u_k^{-1} a'_i (\omega_i P'_i)$

14) $M \leftarrow \text{PH}\left(P'_0, \sum_{i \in I} \frac{1}{\deg(a_i u_k)} u_k^{-1} a'_i (\omega_i P'_i)\right)$

// PH($\cdot$) 表示调用 Pohlig-Hellman 算法

15) **if** M 的最高有效位为 1 **then**

16) $M \leftarrow 2^r - M$

17) **end**

18) $m' \leftarrow (M - 1)/2$

19) **return** m'

注1 如果 $\{\lambda_i\}_{i \in I}$ 是矩阵 M 对秘密 s 的有效份额, 那么存在一组常数 $\{\omega_i \in \mathbb{Z}_p\}_{i \in I}$, 使得 $\sum_{i \in I} \omega_i \lambda_i = s$, 且重构系数 $\{\omega_i\}$ 可在多项式时间

内确定, 其计算复杂度仅取决于矩阵 $\mathbf{M}$ 的规模。

注2 在密钥生成算法中, $u_k \tau a_i^{-1}$ 的运算为理想类的乘法。

注3 在解密过程中计算线性组合 $\sum_{i \in I} \frac{1}{\deg(a_i u_k)} u_k^{-1} a_i'(\omega_i P_i')$ 涉及多个理想类对点的独立作用。由于各项计算相互间无数据依赖关系, 在实际部署中, 可采用多线程或分布式计算架构并行执行各 $\frac{1}{\deg(a_i u_k)} u_k^{-1} a_i'(\omega_i P_i')$ 的计算, 从而将本步骤的时间复杂度从 $O(|I|)$ 降低至近 $O(1)$, 有效提升解密效率, 增强方案在资源受限环境下的实用性。

注4 解密算法第1步为验证曲线 E_0 与 E_i 是否满足 $E_0 = [u_k]^{-1} [a_i'] E_i$, 其建立在系统参数真实可信的基础上。为防止主动攻击者恶意伪造或篡改公开参数, 本文推荐在实际系统中, 可信中心对所有公开参数 $(E_0, P_0, \{E_i, P_i\}_{i=1}^U)$ 生成数字签名。用户在执行属性验证前, 需首先验证这些参数的签名有效性。

3.2 核心点的选取与证明

为确保 SI-CP-ABE 方案中参数生成的正确性与效率, 需明确阶为 2^r 的点的选取方法。为此, 本节介绍文献[43]中的重要命题, 为该点的选取提供关键理论依据。注意到, 该命题结论(1)的证明已在原文中给出, 而结论(2)的证明尚属空白。本文将系统完成结论(2)的证明, 从而为该选取方法建立完备的理论基础。

定义5 横坐标函数

设 E 是定义在域 K 上的 Montgomery 曲线, 取 $E(\bar{K}) \setminus \{(0:1:0)\}$ 中点 $P = (X:Y:Z)$ 。定义函数:

$$x: E \rightarrow \bar{K}, x(P) := X/Z;$$

$$y: E \rightarrow \bar{K}, y(P) := Y/Z。$$

命题2^[43] 设素数 p 满足 $p \equiv 3 \pmod{4}$, E 是定义在 $\mathbb{F}_p$ 上的超奇异 Montgomery 型椭圆曲线, 满足 $\text{End}_p(E) \cong \mathbb{Z}[\pi_p]$ 。取椭圆曲线 E 上点 P ,

若 $P \in E[\pi_p - 1] \setminus E[2]$, 则

$$x(P) \in (\mathbb{F}_p^\times)^2 \Leftrightarrow P \in 2E[\pi_p - 1]。$$

若 $P \in E[\pi_p + 1] \setminus E[2]$, 则

$$x(P) \notin (\mathbb{F}_p^\times)^2 \Leftrightarrow P \in 2E[\pi_p + 1]。$$

其中, 符号 “ $\setminus$ ” 表示集合差, $P \in E[\pi_p - 1] \setminus E[2]$ 表示点 P 属于子群 $E[\pi_p - 1]$, 但不属于 $E[2]$, 即 P 不是2阶点, 也不是无穷远点。

下面对结论(2)进行证明。

(充分性) 若 $P \in 2E[\pi_p + 1]$, 欲证 $x(P) \notin (\mathbb{F}_p^\times)^2$ 。

取 $Q \in E[\pi_p + 1]$, 满足 $P = 2Q$, 那么

$$\pi_p(P) = \pi_p(2Q) = 2\pi_p(Q) = -2Q = -P,$$

即 $P \in E[\pi_p + 1]$ 。根据 Montgomery 曲线的倍点公式, 得

$$x(P) = \frac{(x(Q)^2 - 1)^2}{4y(Q)^2}。$$

由于 $Q \in E[\pi_p + 1]$, 那么有 $\pi_p(Q) = -Q$, 即 $(x(Q)^p, y(Q)^p) = (x(Q), -y(Q))$ 。进一步地, 对等式 $y(Q)^p = -y(Q)$ 两边同时取 p 次幂, 可得 $(y(Q)^p)^p = (-y(Q))^p$ 。因此有

$$y(Q)^{p^2} = (-1)^p y(Q)^p = (-1)(-y(Q)) = y(Q)。$$

故当 $p \geq 3$ 时, $y(Q) \in \mathbb{F}_{p^2}/\mathbb{F}_p$, 那么有

$$y(Q)^2 \in (\mathbb{F}_{p^2}/\mathbb{F}_p)^2 \quad (1)$$

注意到 $x(Q) \in \mathbb{F}_p$, 所以 $(x(Q)^2 - 1)^2 \in (\mathbb{F}_p)^2$, 而 $y(Q)^2 \notin (\mathbb{F}_p)^2$, 故根据点 P 横坐标和点 Q 坐标的数量关系可知, $x(P) \notin (\mathbb{F}_p^\times)^2$ 。

(必要性) 若 $x(P) \notin (\mathbb{F}_p^\times)^2$, 欲证 $P \in 2E[\pi_p + 1]$ 。

情况1 令椭圆曲线 $E = E_0$,

$$E_0: Y^2 Z = X^3 + XZ^2。$$

假设 $P \notin 2E[\pi_p + 1]$ 。取点

$$Q = (x_1, y_1) \in E[\pi_p + 1] \setminus E[2],$$

满足 $x_1 \in \mathbb{F}_p^\times$ 且 $x_1^2 + 1 \notin (\mathbb{F}_p^\times)^2$ 。根据式(1)可得

$$y_1^2 = x_1(x_1^2 + 1) \notin (\mathbb{F}_p^\times)^2,$$

可推得 $x_1 \in (\mathbb{F}_p^\times)^2$, 那么由命题充分性证明可知 $Q \notin 2E[\pi_p + 1]$ 。

取 $R = P - Q$, 下证 $R \in 2E[\pi_p + 1]$ 。设 $P = 2P'$, $Q = 2Q'$, 其中 P', Q' 是代数闭包域上的点。鉴于 $P, Q \in E[\pi_p + 1] \setminus E[2]$ 且 $P, Q \notin 2E[\pi_p + 1]$, 则 $(\pi_p + 1)P = \mathcal{O}$, 从而可推导出 $2(\pi_p + 1)P' = \mathcal{O}$, 即表明 $(\pi_p + 1)P'$ 是一个2阶点。同理, $(\pi_p + 1)Q'$ 也是一个2阶点。注意到椭圆曲线 E 在 $\bar{\mathbb{F}_p}$ 上最多有3个非零2阶点, 分别记 S_1, S_2, S , 其中 $\pi_p(S_1) = S_2$, $\pi_p(S_2) = S_1$, S 是 Frobenius 映射下的不动点, 即 $\pi_p(S) = S$ 。下面证明 $R \in 2E[\pi_p + 1]$ 。

(1) 假设 $(\pi_p + 1)P' = S_1$, $(\pi_p + 1)Q' = S_2$ 。

(a) $S_1 = S_2$

有 $(\pi_p + 1)P' - (\pi_p + 1)Q' = \mathcal{O}$, 这表明 $\pi_p(P' - Q') = -(P' - Q')$, 进而得出 $P' - Q' \in E[\pi_p + 1]$ 。因此,

$$R = P - Q = 2(P' - Q') \in 2E[\pi_p + 1].$$

(b) $S_1 \neq S_2$

考虑

$$(\pi_p + 1)(P' - S_1) = S_1 + S_2 - S_1 = S_2,$$

故 $(\pi_p + 1)(P' - S_1 - Q') = \mathcal{O}$, 即

$$P' - S_1 - Q' \in E[\pi_p + 1],$$

所以 $R = P - Q = 2(P' - S_1 - Q') \in 2E[\pi_p + 1]$ 。

(2) 假设 $(\pi_p + 1)P' = S$, $(\pi_p + 1)Q' = S_1$,

那么有

$$(\pi_p + 1)(P' + Q' - S_1) =$$

$$S + S_1 - (S_1 + S_2) = S_1 =$$

$$(\pi_p + 1)Q',$$

故 $(\pi_p + 1)(P' + Q' - S_1 - Q') = \mathcal{O}$, 即

$$P' - S_1 \in E[\pi_p + 1],$$

所以有 $2P' = P \in 2E[\pi_p + 1]$ 。

这与假设 $P \notin 2E[\pi_p + 1]$ 矛盾, 故舍弃。

(3) 其他情况可通过调整 P 的选取, 找到满足条件的点或推导出矛盾。

令 $R = (x_2, y_2)$, 因 $R \in 2E[\pi_p + 1]$, 故 $x_2 \notin (\mathbb{F}_p^\times)^2$ 。由式(1)知

$$y_2^2 = x_2(x_2^2 + 1) \notin (\mathbb{F}_p^\times)^2,$$

从而可推断出 $(x_2^2 + 1) \in (\mathbb{F}_p^\times)^2$ 。注意到 $R = P - Q$, 由 Montgomery 曲线加法公式得:

$$x(P) = \left(\frac{y(R) - y(Q)}{x(R) - x(Q)} \right)^2 - x(R) - x(Q) = \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2 = \frac{\left(\sqrt{x_1(x_2^2 + 1)} - \sqrt{x_2(x_1^2 + 1)} \right)^2}{(x_2 - x_1)^2}.$$

由 $x_1, (x_2^2 + 1) \in (\mathbb{F}_p^\times)^2$ 且 $x_2, (x_1^2 + 1) \notin (\mathbb{F}_p^\times)^2$ 可知

$$\left(\sqrt{x_1(x_2^2 + 1)} - \sqrt{x_2(x_1^2 + 1)} \right)^2 \in (\mathbb{F}_p^\times)^2,$$

$$(x_2 - x_1)^2 \in (\mathbb{F}_p^\times)^2.$$

因此, $x(P) \in (\mathbb{F}_p^\times)^2$ 。

情况 2 下面讨论一般 Montgomery 曲线情况。根据文献[52], 存在一个理想类 $[a] \in \text{cl}(\mathbb{Z}[\pi_p])$, 使得 $E = E_0/E_0[a]$ 。选择代表元 a 作为与 $\pi_p + 1$ 互素的整理想, 此时存在一个定义在 $\mathbb{F}_p$ 上的同源 $\varphi: E_0 \rightarrow E$, 其次数与 $p + 1$ 互素。该同源映射 φ 从 $E_0[\pi_p + 1]$ 到 $E[\pi_p + 1]$ 诱导一个

双射, 并将 $2E_0[\pi_p + 1]$ 映射到 $2E[\pi_p + 1]$ 。依据文献[53]中关于 Montgomery 曲线间奇数次同源的计算公式, 对于 $P \in E_0[\pi_p + 1]$, 当且仅当 $x(\varphi(P)) \in (\mathbb{F}_p^\times)^2$ 时, $x(P) \in (\mathbb{F}_p^\times)^2$ 。因此, 一般情况可由 $E = E_0$ 的情况推出。

综上所述, 若点 $P \in 2E[\pi_p + 1]$, 则

$$x(P) \notin (\mathbb{F}_p^\times)^2 \Leftrightarrow P \in 2E[\pi_p + 1].$$

若定义素数 $p = 2^r \ell_1 \cdots \ell_n - 1$, 其中 $\ell_1, \dots, \ell_n$ 是互异的小奇素数, 且 $r \geq 3$, 则利用二次互反律验证可知 $2, \ell_1, \dots, \ell_n$ 在 $\mathbb{F}_p$ 中均为平方剩余。设 E 为超奇异椭圆曲线, 其方程为 $Y^2Z = X^3 + aX^2Z + XZ^2$ 。由命题 2 可知, $E(\mathbb{F}_p)$ 上横坐标为这些小奇素数乘积的点属于 $2E[\pi_p - 1]$, 该点的阶可能被 2 整除。因此, 在生成 $E(\mathbb{F}_p)$ 中阶为 2^r 的点时, 需排除这些点。而 $E(\mathbb{F}_p)$ 上横坐标为 $\{2, \ell_1, \dots, \ell_n\}$ 中某些项乘积取反的点, 不属于 $2E[\pi_p - 1]$, 故在生成阶为 2^r 的点时, 可优先从 $\{-2, -3, \dots, -p + 1\}$ 中选取点的横坐标。

4 方案安全性及效率分析

本节旨在对 SI-CP-ABE 方案进行全面的理论评估。首先, 通过理论推导验证方案的正确性; 其次, 在选择性安全模型下, 通过将方案安全性严格规约至底层同源困难假设, 证明其抗攻击能力; 最后, 通过系统性的参数对比与效率分析, 论证本方案在资源受限场景下的实用价值。

4.1 正确性分析

在第 3 节形式化描述的 SI-CP-ABE 方案算法基础之上, 本节先直观地阐述 SI-CP-ABE 方案的代数结构与正确性逻辑, 该方案核心构造如图 3 所示, 其刻画了系统参数、密钥与密文组件在群作用下的演化路径。基于同源类群作用的交换性与自由传递性, 可以清晰地看到解密过程中各分量如何通过不同的运算路径汇聚至同一点, 从而实现明文的正确恢复。

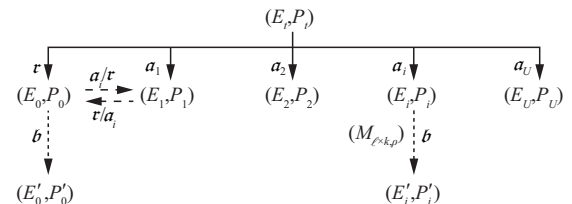


图 3 SI-CP-ABE 方案核心构造示意

由图3可知, $E'_i = [b][a_i]E_i$, $P'_i = ba_i\lambda_i P_i$, 注意到对于任意的理想类 I_i 及其共轭 $\bar{I}_i$, 有

$$I_i \bar{I}_i = [\ell_i],$$

其中 $\ell_i = \deg[I_i]$ 。此外, 由定理1可知:

$$\begin{aligned} & \sum_{i \in I} \frac{1}{\deg(a_i u_k)} u_k^{-1} a'_i (\omega_i P'_i) \\ &= \sum_{i \in I} \frac{1}{\deg(a_i u_k)} u_k^{-1} u_k \tau a_i^{-1} (\omega_i b \lambda_i a_i P_i) \\ &= \pm b \tau (s \cdot P_i) \\ &= \pm b (s \cdot P_0). \end{aligned}$$

注意到 $P'_0 = b(s(2m+1)P_0)$, 因此解密者可以利用 Pohlig-Hellman 算法得到 $M = 2m+1$ 或 $2^r - (2m+1)$ 。由于明文 m 的比特长度小于 $r-2$, 所以 $2m+1$ 的最高有效位始终为0。因此, 若 M 的最高有效位为1, 则取 $M = 2^r - (2m+1)$ 。调整后, 加密者最终得到 $M = 2m+1$ 作为 Pohlig-Hellman 算法的解, 那么 $m' = (M-1)/2 = m$, 即方案满足解密正确性。

4.2 安全性分析

P-CSSCDH 假设和 P-CSSDDH 假设为 SiGamal 方案提供了基础的安全性保证^[43], 即在隐藏同源映射下计算固定点像点是困难的。而 P^+ -CSSDDH 假设是在 SiGamal 环境中的自然延伸, 故可认为该同源困难假设是合理且有效的。

假设1 增强点交换超奇异同源计算型 Diffie-Hellman 假设 (P^+ -CSSCDH 假设)

设 p 是一个素数, 满足 $p = 2^r \cdot \ell_1 \cdots \ell_n - 1$, 其中 $\ell_i (i = 1, \dots, n)$ 是互异小奇素数。设椭圆曲线 $E_i: Y^2Z = X^3 + XZ^2$, 均匀选取 $E_i(\mathbb{F}_p)$ 上阶为 2^r 的随机点 P_i , 取 $J(\mathbb{Z}[\pi_p])$ 中随机元素 $a_1, \dots, a_U, b, \tau$ 。设 λ 为 p 的位长。 P^+ -CSSCDH 假设成立, 则对于任意高效算法 $\mathcal{A}$, 有:

$$\Pr \left[s \tau b P_i = P^* \mid \begin{array}{l} s \xleftarrow{\$} \{2k+1\} \in (\mathbb{Z}/2^r\mathbb{Z}), \\ P_i \xleftarrow{\$} E_i(\mathbb{F}_p)_{\text{order } 2^r}, \\ a_1, \dots, a_U \leftarrow J(\mathbb{Z}[\pi_p]), \\ b, \tau \leftarrow J(\mathbb{Z}[\pi_p]) \\ P^* \leftarrow \mathcal{A}([\tau] E_i, r P_i, [a_i] E_i, \\ a_i P_i, [b][a_i] E_i, \\ b a_i P_i, [b][\tau] E_i) \end{array} \right] < \text{negl}(\lambda), \text{ 其中 } s \xleftarrow{\$} \{2k+1\} \in (\mathbb{Z}/2^r\mathbb{Z}), \text{ 表}$$

示从 $\mathbb{Z}/2^r\mathbb{Z}$ 随机选取奇数 s 。

假设2 增强点交换超奇异同源决策型 Diffie-Hellman 假设 (P^+ -CSSDDH 假设)

设 p 为素数, 且满足 $p = 2^r \cdot \ell_1 \cdots \ell_n - 1$, 其中 $\ell_i (i = 1, \dots, n)$ 为互异小奇素数。令 E_i 为定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线, 取 $E_i(\mathbb{F}_p)$ 上阶为 2^r 的随机点 P_i 。在 $J(\mathbb{Z}[\pi_p])$ 中随机选取范数为奇数的理想 $a_1, \dots, a_U, b, \tau$, 设 Q 为 $([b][\tau]E_i)(\mathbb{F}_p)$ 上阶为 2^r 的随机点, λ 为 p 的位长。若 P^+ -CSSDDH 假设成立, 则对于任意高效算法 $\mathcal{A}$, 有:

$$\Pr \left[b = b^* \mid \begin{array}{l} s \xleftarrow{\$} \{2k+1\} \in (\mathbb{Z}/2^r\mathbb{Z}) \\ P_i \xleftarrow{\$} E_i(\mathbb{F}_p)_{\text{order } 2^r}, \\ a_1, \dots, a_U \leftarrow J(\mathbb{Z}[\pi_p]), \\ b, \tau \leftarrow J(\mathbb{Z}[\pi_p]) \\ Q \xleftarrow{\$} ([b][\tau]E_i)(\mathbb{F}_p)_{\text{order } 2^r}, \\ b \xleftarrow{\$} \{0,1\}, \\ R_0 = s b \tau P, R_1 = Q, \\ b^* \leftarrow \mathcal{A}([\tau] E_i, \tau P_i, [a_i] E_i, \\ a_i P_i, [b][a_i] E_i, \\ b a_i P_i, [b][\tau] E_i, \\ R_b) \end{array} \right] - \frac{1}{2} < \text{negl}(\lambda).$$

接下来, 在上述假设条件下证明 SI-CP-ABE 方案的安全性。

定理2 设 λ 是安全参数, 若 P^+ -CSSCDH 假设成立, 且敌手 $\mathcal{A}$ 选取的挑战矩阵 M^* 的行列维度均不超过 p , 则在选择性安全模型下, SI-CP-ABE 方案是在选择性安全模型下抗选择性明文攻击的单向性 (OW-sCPA) 安全的。

证明 选定挑战访问结构 (M^*, ρ^*) , 若该方案不是 OW-sCPA 安全的, 则存在高效算法 $\mathcal{A}$, 可以从公钥 $PK = (E_0, P_0, E_i, P_i)$ 与密文 $CT = ([b]E_i, b\lambda_i P_i, [\tau][b]E_i, b(s(2m+1))P_0)$ 中以高概率 $\omega\left(\frac{1}{\text{poly}(\lambda)}\right)$ 恢复出隐藏明文 m ,

$\omega\left(\frac{1}{\text{poly}(\lambda)}\right)$ 用于描述敌手成功的优势, 如果敌手的优势是 $\omega\left(\frac{1}{\text{poly}(\lambda)}\right)$, 那么该优势不可忽略, 意味着

方案不安全；反之，若优势是可忽略的，则方案安全。

其中 $\frac{1}{\text{poly}(\lambda)}$ 表示某个多项式倒数， $\omega()$ 是 little-

omega 渐近符号，表示一个函数增长得比括号内的函数更快。基于此，构建新敌手 $\mathcal{A}'$ ，使其能够从

$(E_0, P_0, E_i, P_i, [b]E_i, bP_i, [\tau][b]E_i)$ 中以高概率输出 $srbP_i$ 。具体过程如下。

从 $[\tau][b]E_i$ 中随机选取阶为 $2'$ 的点 Q ，调用算法 $\mathcal{A}$ 计算

$$m = \mathcal{A}(E_0, P_0, E_i, P_i, [b]E_i, b\lambda_i P_i, [b]E_0, Q)。$$

此时， $Q = s(2m+1)b\tau P_i$ 以高概率成立。注意到 $(2m+1) \in (\mathbb{Z}/2'\mathbb{Z})^*$ ，即 $(2m+1)$ 在模 $2'$ 的整数环中存在乘法逆元。计算 $\frac{1}{(2m+1)}Q$ ，并将其设定为敌手 $\mathcal{A}'$ 的输出，那么该输出将以高概率等于 $sbrP_i$ ，因此 $\mathcal{A}'$ 是一个高效算法。这与 P^+ -CSSCDH 假设矛盾。

综上所述，该方案是 OW-sCPA 安全的。

定理 3 设 λ 是安全参数，若 P^+ -CSSDDH 假设成立，且敌手 $\mathcal{A}$ 选取的挑战矩阵 M^* 的行列维度均不超过 p ，则在选择性安全模型下，SI-CP-ABE 方案是 IND-sCPA 安全的。

证明 选定挑战访问结构 (M^*, ρ^*) ，假设针对该方案存在敌手 $\mathcal{A}$ 以优势 $\text{Adv}_{\mathcal{A}}^{\text{SI-CP-ABE}}(\lambda)$ 区分明文 m_0 与 m_1 的加密结果。

接下来构造新敌手 $\mathcal{A}'$ ，使其从

$$(E_0, P_0, E_i, P_i, [b]E_i, bP_i, [\tau][b]E_i, R_b)$$

中以概率 $\text{Adv}_{\mathcal{A}}^{\text{SI-CP-ABE}}(\lambda) + \frac{1}{2}$ 输出 b ，其中 $R_0 = srbP_i$ ， $R_1 = Q$ 。具体过程如下。

在 $\{0,1\}$ 中随机均匀选取 b' ，并计算 $(2m_{b'}+1)R_b$ ，调用 $\mathcal{A}$ 得

$$\bar{b} = \mathcal{A}(E_0, P_0, E_i, P_i, [b]E_i, b\lambda_i P_i, [\tau][b]E_i, (2m_{b'}+1)R_b)。$$

若 $b' = \bar{b}$ ， $\mathcal{A}'$ 输出 0；否则输出 1。

下面分析 $\mathcal{A}'$ 输出正确 b 的概率。

(1) 当 $b = 0$ 时， $\bar{b} = b'$ 的概率为

$$\text{Adv}_{\mathcal{A}}^{\text{SI-CP-ABE}}(\lambda) + \frac{1}{2} \text{ 或 } -\text{Adv}_{\mathcal{A}}^{\text{SI-CP-ABE}}(\lambda) + \frac{1}{2}。$$

(2) 当 $b = 1$ 时，由于 $R_1 = Q$ 是一个随机点，敌手 $\mathcal{A}$ 无法从 $(2m_{b'}+1)R_1$ 中获取任何关于 $m_{b'}$ 的信息，故 $\bar{b} = b'$ 的概率为 $\frac{1}{2}$ 。由此可得

$$\begin{aligned} \text{Adv}_{\mathcal{A}'}^{P^+, \text{CSSDDH}}(\lambda) &\geq \left| \Pr[\bar{b} = b | b = 1] \cdot \Pr[b = 1] + \right. \\ &\quad \left. \Pr[\bar{b} = b | b = 0] \cdot \Pr[b = 0] - \frac{1}{2} \right| = \\ &\quad \left| \frac{1}{2} \pm \text{Adv}_{\mathcal{A}}^{\text{SI-CP-ABE}}(\lambda) + \frac{1}{2} + \frac{1}{2} - 1 \right| = \\ &\quad \frac{1}{2} \text{Adv}_{\mathcal{A}}^{\text{SI-CP-ABE}}(\lambda)。 \end{aligned}$$

综上所述，若 P^+ -CSSDDH 假设成立，则在选择性安全模型下，有

$$\text{Adv}_{\mathcal{A}}^{\text{SI-CP-ABE}}(\lambda) \leq 2 \text{Adv}_{\mathcal{A}'}^{P^+, \text{CSSDDH}}(\lambda) < \text{negl}(\lambda)，$$

因此，敌手 $\mathcal{A}$ 的优势上界为可忽略函数，可说明该方案具有 IND-sCPA 安全性。

注 5 敌手通过计算从 E_i 到 E_0 的群元素 $[u_k^{-1}][a_i']$ 对方案进行攻击，这种攻击方法与攻击 SiGamal 相同。因此，在相同的安全参数下，该方案的安全级别与 SiGamal 相同。

注 6 上述方案不是 IND-sCCA 安全的。在选定挑战访问结构后，明文 m 对应的输出密文为 $\text{CT}^* = (E'_i, P'_i, E'_0, P'_0 = b(s(2m+1)P_0))$ ， $i \in [1, \ell]$ 。

若取 $3P'_0$ ，则可得到 $3b(s(2m+1)P_1)$ 。由于 $3(2m+1) = 2(3m+1) + 1$ ，敌手能够利用明文 m 对应的输出密文计算出 $(3m+1)$ 对应的输出密文。因此，该方案不满足 IND-sCCA 安全性。

注 7 在上述方案中，所有计算涉及的点均通过其横坐标来描述，即加密方发送给解密方的密文形式为 $(E'_i, x(P'_i), E'_0, x(P'_0))$ 。在某些情况下，可以通过隐藏 E'_i 和 E'_0 曲线方程来减小密文尺寸，即密文为 $\text{CT} = (x(P'_i), x(P'_0))$ ，称为 CSI-CP-ABE。然而，如文献[44]所示，这种方法仍不足以保证方案实现 IND-CCA 安全性。攻击者能够从给定密文有效推导出 $3m+1$ 的密文，违反 IND-CCA 安全要求。

4.3 参数比较与性能验证

为评估 CSI-CP-ABE 方案的参数性能，本节选取以下 3 个代表性方案进行对比：Waters11 方案^[9]基于双线性对，是标准模型下 LSSS 访问结构的经典构造；Tan15 方案^[11]基于 RLWE，是格基 ABE 的早期方案，为后续众多基于 RLWE 的 ABE 方案提供经典架构；Zhang25 方案^[18]基于 LWE，实现了穿刺、前向安全等扩展功能，反映

了格基ABE的最新进展。上述3个方案覆盖了从经典密码到后量子密码、从基础构造到功能扩展的主要技术路径,其与CSI-CP-ABE的参数对比见表2,其中 p 表示满足不同安全级别的大素数, U 表示系统属性全集大小, ℓ 表示LSSS矩阵的行数; $d = 2^r > 2$ 表示环-LWE问题中多项式 $f(x) = x^d + 1$ 的次数; n 表示LWE问题中格的维数, m 表示LWE矩阵列数,其大小约为 $n \log p$, $|W|$ 表示AND-gates访问结构中所涉及的属性总数。

由表2可知,CSI-CP-ABE方案在参数尺寸上具有一定优势,其公钥尺寸略大于Waters11方案,但显著小于Tan15和Zhang25方案;私钥尺寸不仅远小于Zhang25方案,相较于Tan15还摆脱了对环维度 d 的依赖。需要说明的是,Zhang25方案采用AND-gates访问结构,其策略规模由属性总数 $|W|$ 刻画;而Waters11、Tan15及本文方案均采用表达能力更强的LSSS访问结构,以秘密共享矩阵的行数 ℓ 作为开销指标。当访问策略退化为单纯的与门时,属性总数与LSSS的行数在数值上近似相等。在密文尺寸方面,CSI-CP-ABE与访问结构规模呈低阶线性关系,优于Tan15和Zhang25方案,且仅为Waters11方案密文尺寸的一半。此外,相较于Zhang25方案中格维数 n 和矩阵列数 m 平方级放大的参数规模,本文方案完全摆脱了对格维数的依赖,在存储和传输效率上展现出更优的实用价值。

下面通过仿真实验检验CSI-CP-ABE方案各算法的性能。实验基于CSIDH-512参数集^[42],在3.80 GHz CPU、16 GB内存平台上使用Magma实现。对CSI-CP-ABE各算法进行性能验证($U = 100$, $\ell = 50$, $|I| = 5$),各算法性能验证结果见表3。

在方案实际部署中,Setup与Encryption操作主要由服务器或上级机构执行,而终端用户仅需

执行Decryption计算。实验表明,在该参数下用户解密时间约为7.554 s,具有较好的实用性。

表3 CSI-CP-ABE方案各算法性能验证结果

算法	类群作用次数	时长
Setup(λ, U)	101次	127.159 s
Encryption(PK, ($M_{\ell \times k}, \rho$), m)	51次	64.209 s
Decryption(CT, SK)	6次	7.554 s
总计	158次	198.922 s

需要说明的是,当前测试结果是对串行执行环境下的最坏情况进行评估得到的。通过采用并行计算架构对关键计算模块进行优化,特别是对类群作用等核心运算进行并行化处理,预计可实现显著性能提升。本方案基于CSIDH-512参数集实现,可达到NIST后量子安全级别1,是基于同源理想类群作用的CP-ABE方案。

CSI-CP-ABE方案在保证加密功能完整的基础上,通过优化密钥与密文的参数设计,实现了公钥、私钥及密文尺寸的显著缩减。这不仅降低了密钥管理与数据传输的存储开销,还提升了方案在多属性复杂访问结构场景中的适用性。对于资源受限的环境而言,这些改进具有重要实用价值,能够有效提高系统的运行效率并增强其扩展能力。

5 新型Naor-Reingold型伪随机函数

伪随机函数的安全性易受部分密钥泄露影响。本文基于SI-CP-ABE方案,提出一种改进的Naor-Reingold型伪随机函数,通过引入共享秘密 s 以实现输出盲化,有效抵御由部分密钥泄露导致的安全威胁。此外,该函数具备认证功能,可检测并防止数据篡改,显著增强了实际应用中的安全性和数据完整性,满足了现代密码学对密钥管理与数据完整性验证的双重需求。

表2 Waters11、Tan15、Zhang25和CSI-CP-ABE的参数对比

方案	安全假设	公钥尺寸	私钥尺寸	密文尺寸
Waters11 ^[9]	双线性对	$(U + 3) \log_2 p$	$(S + 2) \log_2 p$	$2(\ell + 1) \log_2 p$
Tan15 ^[11]	RLWE	$d(U + 2) \log_2 p$	$d(S + 1) \log_2 p$	$d(\ell + 1) \log_2 p$
Zhang25 ^[18]	LWE	$> 2mn(U + 1) \log_2 p$	$m^2(U + 1)^2 \log_2 p$	$> m^2(2U - W) \log_2 p$
CSI-CP-ABE	同源	$2(U + 1) \log_2 p$	$< (2 S + 1) \log_2 p$	$(\ell + 1) \log_2 p$

5.1 伪随机函数构造

令素数 p 满足 $p = 2^r \ell_1 \cdots \ell_n - 1$, 其中 $\ell_i (i = 1, \dots, n)$ 是互异的小奇素数。定义超奇异椭圆曲线 $E_0: Y^2 Z = X^3 + XZ^2$, 取 $E_0(\mathbb{F}_p)$ 上阶为 2^r 的随机点 P_0 。定义集合 $\mathcal{A} = (a_1, \dots, a_t)$, 其中 $a_i (i = 1, \dots, t)$ 为用户从 $\mathbb{Z}[\pi_p]$ 中随机选取的范数为奇数的整理想。从 $(\mathbb{Z}/2^r\mathbb{Z})^\times$ 中随机选取奇数 s , 从 $\mathbb{Z}_p^n$ 中随机选取元素 $y_2, \dots, y_k$, 构成向量 $\mathbf{v} = (s, y_2, \dots, y_k)^T$, 其中 s 表示待共享秘密。设 (M, ρ) 为 LSSS 访问结构, 计算 $\lambda_i = M_i \mathbf{v}$, M_i 是矩阵 M 的第 i 行对应的向量, $i = 1, \dots, \ell$ 。

定义函数 $f_{p, E_0, P_0, \mathcal{A}, S}(x) = (v_x \parallel \lambda_1 \parallel \dots \parallel \lambda_\ell)$, 其中输入 $x = (x_1, \dots, x_t)$, v_x 满足

$$a_0 \prod_{i=1}^t a_i^{x_i} P_0 = s(2v_x + 1) P_{[a_0] \prod_{i=1}^t [a_i]^{x_i} E_0}.$$

接下来将证明, 在 P^+ -CSSDDH 假设和 CSSDDH* 假设下, $f_{p, E_0, P_0, \mathcal{A}, S}$ 是伪随机函数, 其中 CSSDDH* 假设是对 CSSDDH 假设的推广^[43]。在给出具体证明前, 先介绍 CSSDDH* 假设的定义。

假设 3 交换超奇异同源决策型 Diffie-Hellman* 假设 (CSSDDH* 假设)

令素数 p 满足 $p = 2^r \cdot \ell_1 \cdots \ell_n - 1$, 其中 $\ell_i (i = 1, \dots, n)$ 是互异的小奇素数。设 $E_0: Y^2 Z = X^3 + XZ^2$ 是定义在 $\mathbb{F}_p$ 上的椭圆曲线。取 $\text{cl}(\mathbb{Z}[\pi_p])$ 中随机元素 $[a]$, $[b]$ 和 $[c]$ 。设 p 比特长度为 λ 。若对于任意高效算法 $\mathcal{A}$, 有

$$\Pr \left[b = b^* \mid \begin{array}{l} [a], [b], [c] \leftarrow \text{cl}(\mathbb{Z}[\pi_p]), \\ b \xleftarrow{\$} \{0, 1\}, \\ F_0 := [a][b]E_0, \\ F_1 := [c]E_0, \\ b^* \leftarrow \mathcal{A}(E_0, [a]E_0, [b]E_0, F_b) \end{array} \right] - \frac{1}{2} < \text{negl}(\lambda),$$

则 CSSDDH* 假设成立。

5.2 伪随机函数证明

下面给出 $f_{p, E_0, P_0, \mathcal{A}, S}$ 是伪随机函数的证明。

定理 4 令素数 p 满足 $p = 2^r \cdot \ell_1 \cdots \ell_n - 1$, 其中 $\ell_1, \dots, \ell_n$ 是互异的小奇素数。定义 $E_0: Y^2 Z = X^3 + XZ^2$ 是一个超奇异椭圆曲线。设 $\mathcal{A}$ 是一个概率多项式时间敌手, 若 P^+ -CSSDDH 假设和

CSSDDH* 假设成立, 则 $f_{p, E_0, P_0, \mathcal{A}, S}$ 是伪随机函数, 满足

$$\Pr \left[b = b^* \mid \begin{array}{l} P_0 \xleftarrow{\$} E_0(\mathbb{F}_p)[2^r], \\ b \xleftarrow{\$} \{0, 1\}, \\ \mathcal{A} \leftarrow J(\mathbb{Z}[\pi_p])^{t+1}, \\ f_0 := f_{p, E_0, P_0, \mathcal{A}}, \\ f_1 \xleftarrow{\$} \mathcal{R}, \\ b^* \leftarrow \mathcal{A}^{f_b(\cdot)}(p, E_0, P_0) \end{array} \right] - \frac{1}{2} < \text{negl}(\lambda),$$

其中, $\mathcal{R}$ 表示从 $\{0, 1\}^t$ 到 $\{0, 1\}^{r-2}$ 的一族函数, λ 为 p 的比特长度, $\mathcal{A}$ 表示理想的集合 $\{a_1, \dots, a_t\}$, $a_i (i = 1, \dots, t)$ 为用户从 $\mathbb{Z}[\pi_p]$ 中随机选取的范数为奇数的整理想。

为证明定理 4, 需引入引理 1, 该引理的证明与文献[43]中引理 2 的证明类似, 故此处省略具体推导过程。

引理 1 令比特长度为 λ 的素数 p 满足 $p = 2^r \cdot \ell_1 \cdots \ell_n - 1$, 其中 $\ell_1, \dots, \ell_n$ 是互异的小奇素数, 记 $v = \text{Poly}(\lambda)$ 是一个小整数。如果 P^+ -CSSDDH 假设和 CSSDDH* 假设成立, 那么任何概率多项式时间敌手的优势 $\text{Adv}_{\mathcal{A}}$ 上界为可忽略函数 $\text{negl}(\lambda)$, 其中

$$\text{Adv}_{\mathcal{A}} = \Pr \left[b = b^* \mid \begin{array}{l} P_0 \xleftarrow{\$} E_0(\mathbb{F}_p)[2^r], \\ a \leftarrow J(\mathbb{Z}[\pi_p]), \\ b_1, \dots, b_v \leftarrow J(\mathbb{Z}[\pi_p]), \\ c_1, \dots, c_v \leftarrow J(\mathbb{Z}[\pi_p]), \\ F_0^{(i)} := [a][b_i]E_0, \\ R_0^{(i)} := sab_i P_0, \\ F_1^{(i)} := [c_i]E_0, \\ R_1^{(i)} := c_i P_0, \\ b^* \leftarrow \mathcal{A}(E_0, P_0, [a]E_0, \\ \quad aP_0, \{[b_i]E_0, \\ \quad b_i P_0, F_b^{(i)}, \\ \quad R_b^{(i)}\}_{i=1, \dots, v}) \end{array} \right] - \frac{1}{2}.$$

下面基于引理 1, 给出定理 4 的证明。

定理 4 的证明沿用文献[43]中定理 3 的证明思路。令 $a, b_1, \dots, b_v, c_1, \dots, c_v$ 为 $J(\mathbb{Z}[\pi_p])$ 中范数为奇数的随机元素, 定义 $F_0^{(j)} := [a][b_j]E_0$, $R_0^{(j)} := sab_j P_0$, $F_1^{(j)} := [c_j]E_0$ 以及 $R_1^{(j)} := c_j P_0$,

$f_0 := f_{p, E_0, P_0, \mathcal{A}}$, $f_1 \xleftarrow{s} \mathcal{R}$, 其中 s 表示共享秘密, $\mathcal{R}$ 表示从 $\{0, 1\}^t$ 到 $\{0, 1\}^{r-2}$ 的一族函数。设敌手 $\mathcal{A}$ 的查询为 $x^{(1)}, \dots, x^{(v)}$, 现构造

$$S_{p,b} := (p, E_0, P_0, [a]E_0, aP_0, \{[b_j]E_0, b_jP_0, F_b^{(j)}, R_b^{(j)}\}_{j=1, \dots, v}),$$

其中 $b \in \{0, 1\}$ 。

接下来构建概率多项式时间敌手 $\mathcal{A}'$ 。首先 $\mathcal{A}'$ 接收 $S_{p,b}$, 并从 $\{1, \dots, t\}$ 中随机选取元素 q , 随机选取范数为奇数的 $a_{q+1}, \dots, a_t \in J(\mathbb{Z}[\pi_p])$; 而后 $\mathcal{A}'$ 将 (p, E_0, P_0) 传给敌手 $\mathcal{A}$, 并对敌手 $\mathcal{A}$ 的询问进行响应; 最后 $\mathcal{A}'$ 输出 $\mathcal{A}$ 的结果。若敌手 $\mathcal{A}$ 能以不可忽略的优势正确区分 f_0 的输出和真正随机函数 f_1 的输出, 则敌手 $\mathcal{A}'$ 能以不可忽略的优势解决 P^+ -CSSDDH 或 CSSDDH* 问题, 这与假设矛盾。下面介绍敌手 $\mathcal{A}'$ 对 $\mathcal{A}$ 的响应方式。

对于敌手 $\mathcal{A}$ 的查询 $x^{(v')}$, 若 $x_q^{(v')} = 1$, 则 $\mathcal{A}'$ 响应

$$\left(\prod_{i=q+1, \dots, t} [a_i]^{x_i^{(v')}} F_b^{(j)}, \prod_{i=q+1, \dots, t} a_i^{x_i^{(v')}} R_b^{(j)} \right);$$

若 $x_q^{(v')} = 0$, 则 $\mathcal{A}'$ 响应

$$\left(\prod_{i=q+1, \dots, t} [a_i]^{x_i^{(v')}} [b_j]E_0, \prod_{i=q+1, \dots, t} s a_i^{x_i^{(v')}} b_j P_0 \right),$$

其中 $v' = 1, \dots, v$,

$j = j(v') =$

$$\min \left\{ v'' \mid (x_1^{(v'')}, \dots, x_{q-1}^{(v'')}) = (x_1^{(v')}, \dots, x_{q-1}^{(v')}) \right\}.$$

注意到 j 保证了相同前缀的查询将获得相同的响应。

由引理 1 可知, 对于 $i = 1, \dots, t$,

$$\left| \Pr [\mathcal{A}'(S_{p,0}) = 1 \mid q = i] - \Pr [\mathcal{A}'(S_{p,1}) = 1 \mid q = i] \right| < \text{negl}(\lambda) \text{ 成立}.$$

由敌手 $\mathcal{A}'$ 构造可知,

$$\begin{aligned} & \Pr [\mathcal{A}'(S_{p,1}) = 1 \mid q = i] \\ &= \Pr [\mathcal{A}'(S_{p,0}) = 1 \mid q = i + 1], \\ \Pr [\mathcal{A}'(S_{p,0}) = 1 \mid q = 1] &= \Pr [\mathcal{A}^{f_0}(p, E_0, P_0) = 1], \\ \Pr [\mathcal{A}'(S_{p,1}) = 1 \mid q = v] \\ &= \Pr [\mathcal{A}^{f_1}(p, E_0, P_0) = 1] \text{ 成立}. \end{aligned}$$

那么有

$$\left| \Pr [\mathcal{A}^{f_0}(p, E_0, P_0) = 1] - \Pr [\mathcal{A}^{f_1}(p, E_0, P_0) = 1] \right| =$$

$$\begin{aligned} & \left| \Pr [\mathcal{A}'(S_{p,0}) = 1 \mid q = 1] - \Pr [\mathcal{A}'(S_{p,1}) = 1 \mid q = t] \right| \leq \\ & \sum_{q=1}^t \left| \Pr [\mathcal{A}'(S_{p,0}) = 1 \mid q = i] - \Pr [\mathcal{A}'(S_{p,1}) = 1 \mid q = i] \right| < t \cdot \text{negl}(\lambda), \end{aligned}$$

即

$$\Pr \left[b = b^* \mid \begin{array}{l} P_0 \xleftarrow{s} E_0(\mathbb{F}_p)[2^r], \\ b \xleftarrow{s} \{0, 1\}, \\ \mathcal{A} \leftarrow J(\mathbb{Z}[\pi_p])^{t+1} \\ f_0 := f_{p, E_0, P_0, \mathcal{A}}, \\ f_1 \xleftarrow{s} \mathcal{R}, \\ b^* \leftarrow \mathcal{A}^{f_b}(p, E_0, P_0) \end{array} \right] - \frac{1}{2} < \text{negl}(\lambda)$$

成立。

结论得证。

通过引入共享秘密 s 作为盲化因子, 有效提升了 Naor-Reingold 型伪随机函数的安全性, 抵御部分密钥泄露带来的威胁。具体而言, 共享秘密 s 在函数输出中起到混淆作用, 即使攻击者获取了部分密钥信息, 也难以还原完整的函数输出, 从而降低了密钥泄露的风险。同时, 该函数具备认证功能, 通过在函数输出中嵌入与秘密 s 有关的认证信息, 使得只有满足特定访问结构的用户才能验证数据的合法性, 同时任何对数据的篡改都将导致认证失败, 从而使得数据的完整性受到破坏时能被及时发现。

6 结束语

本文系统研究了基于同源理想类群作用的属性基加密方案, 提出了 SI-CP-ABE 方案及其压缩变体 CSI-CP-ABE 方案, 在 CSIDH 同源密码体系中实现了细粒度访问控制, 为后量子环境下的数据安全共享提供了新思路。

当前基于单权威和用户盲化的同源基 CP-ABE 方案是实现同源密码有效实用化的第一步, 未来工作将围绕两个方向展开: 一是研究基于同源理想类群作用的外包 CP-ABE 方案, 进一步丰富同源加密技术的应用场景并提升其实用性, 同时加强方案的抗共谋性和效率; 二是设计基于同源理想类群作用的 KP-ABE 方案, 探索同源密码在更多访问控制场景中的应用。

参考文献:

- [1] Sahai A, Waters B. Fuzzy identity-based encryption[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer, 2005: 457-473.
- [2] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//Proceedings of the 13th ACM conference on Computer and communications security. New York: ACM, 2006: 89-98.
- [3] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]//2007 IEEE symposium on security and privacy (SP'07). Oakland, California: IEEE, 2007: 321-334.
- [4] Boneh D, Sahai A, Waters B. Functional encryption: definitions and challenges[C]//Theory of Cryptography Conference. Berlin, Heidelberg: Springer, 2011: 253-273.
- [5] Joux A. A one round protocol for tripartite Diffie - Hellman[C]//International Algorithmic Number Theory Symposium. Berlin, Heidelberg: Springer, 2000: 385-393.
- [6] Peikert C. A decade of lattice cryptography[J]. Foundations and Trends^W in Theoretical Computer Science. 2016, 10(4): 283-424.
- [7] Jao D, De Feo L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies[C]//International Workshop on Post-Quantum Cryptography. Berlin, Heidelberg: Springer, 2011: 19-34.
- [8] Koshiba T, Takashima K. Pairing cryptography meets isogeny: a new framework of isogenous pairing groups[J]. Cryptology and Information Security Series, 2016: 1138.
- [9] Waters B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[C]//International Workshop on Public Key Cryptography. Berlin, Heidelberg: Springer, 2011: 53-70.
- [10] Zhang J, Zhang Z. A ciphertext policy attribute-based encryption scheme without pairings[C]//International Conference on Information Security and Cryptology. Berlin, Heidelberg: Springer, 2011: 324-340.
- [11] Fun T S, Samsudin A. Lattice ciphertext-policy attribute-based encryption from ring-LWE[C]//2015 International Symposium on Technology Management and Emerging Technologies (ISTMET). Piscataway: IEEE Press, 2015: 258-262.
- [12] Varri U S, Pasupuleti S K, Kadambari K V. CP-ABSEL: Ciphertext-policy attribute-based searchable encryption from lattice in cloud storage[J]. Peer-to-Peer Networking and Applications. 2021, 14(3): 1290-1302.
- [13] Qian X, Wu W. An efficient ciphertext policy attribute-based encryption scheme from lattices and its implementation[C]//2021 IEEE 6th International Conference on Computer and Communication Systems (ICCCS). 2021: 732-742.
- [14] Li H, Lin H, Luo J. ABE for circuits with constant-size secret keys and adaptive security[C]//Theory of Cryptography Conference. Cham: Springer Nature Switzerland, 2022: 680-710.
- [15] Huang B, Gao J, Li X. Efficient lattice-based revocable attribute-based encryption against decryption key exposure for cloud file sharing[J]. Journal of Cloud Computing. 2023, 12(1): 37.
- [16] Wee H, Wu D J. Lattice-based functional commitments: Fast verification and cryptanalysis[C]//International Conference on the Theory and Application of Cryptology and Information Security. Singapore: Springer Nature Singapore, 2023: 201-235.
- [17] Wee H. Circuit ABE with poly (depth, λ)-sized ciphertexts and keys from lattices[C]//Annual International Cryptology Conference. Cham: Springer Nature Switzerland, 2024: 178-209.
- [18] Zhang T, Jiang M, Luo F, et al. A Lattice-based puncturable CP-ABE scheme with forward security for cloud-assisted IoT[J]. IEEE Internet of Things Journal. 2025, 12(14): 26538-26554.
- [19] Agrawal S, Kumari S, Yamada S. Attribute based encryption for Turing machines from lattices[C]//Annual International Cryptology Conference. Cham: Springer Nature Switzerland, 2024: 352-386.
- [20] Dong F, Hao Z, Mook E, et al. Laconic function evaluation and ABE for RAMs from (ring-) LWE[C]//Annual International Cryptology Conference. Cham: Springer Nature Switzerland, 2024: 107-142.
- [21] Cini V, Wee H. Faster ABE for Turing Machines from Circular Evasive LWE[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer Nature Switzerland, 2025: 94-125.
- [22] Brzuska C, Ünal A, Woo I K Y. Evasive LWE assumptions: definitions, classes, and counterexamples[C]//International Conference on the Theory and Application of Cryptology and Information Security. Singapore: Springer Nature Singapore, 2024: 418-449.
- [23] Wee H. Optimal broadcast encryption and CP-ABE from evasive lattice assumptions[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer Nature Switzerland, 2022: 217-241.
- [24] Agrawal S, Rossi M, Yadav A, et al. Constant input attribute based (and predicate) encryption from evasive and tensor LWE[C]//Annual International Cryptology Conference. Cham: Springer Nature Switzerland, 2023: 532-564.
- [25] Cini V, Wee H. Unbounded ABE for circuits from LWE, revisited[C]//International Conference on the Theory and Application of Cryptology and Information Security. Singapore: Springer Nature Singapore, 2024: 238-267.
- [26] Datta P, Komargodski I, Waters B. Decentralized multi-authority ABE for DNF s from LWE[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer International Publishing, 2021: 177-209.
- [27] Hohenberger S, Lu G, Waters B, et al. Registered attribute-based encryption[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer Nature Switzerland, 2023: 511-542.

- [28] Wee H, Wu D J. Unbounded distributed broadcast encryption and registered ABE from succinct LWE[C]//Annual International Cryptology Conference. Cham: Springer Nature Switzerland, 2025: 204-235.
- [29] Agrawal S, Tomida J, Yadav A. Attribute-based multi-input FE (and more) for attribute-weighted sums[C]//Annual International Cryptology Conference. Cham: Springer Nature Switzerland, 2023: 464-497.
- [30] 周艺华, 扈新宇, 李美奇, 等. 云环境下基于属性策略隐藏的可搜索加密方案[J]. 网络与信息安全学报, 2022, 8(2): 112-121.
- Zhou Y H, Hu X Y, Li M Q, et al. Searchable encryption scheme based on attribute policy hiding in a cloud environment[J]. Chinese Journal of Network and Information Security. 2022, 8(2): 112-121.
- [31] 张兴兰, 崔遥. 基于群签名的属性加密方案[J]. 网络与信息安全学报, 2019, 5(1): 15-21.
- Zhang X L, Cui Y. Attribute-based encryption scheme with group signatures[J]. Chinese Journal of Network and Information Security. 2019, 5(1): 15-21.
- [32] 张智烁, 杨会喜, 黄文, 等. 支持属性立即撤销的可复用属性基签名及其密钥协商方案[J]. 网络与信息安全学报, 2024, 10(2): 81-94.
- Zhang Z S, Yang H X, Huang W, et al. Reusable attribute-based signature with attribute revocation and authenticated key agreement[J]. Chinese Journal of Network and Information Security. 2024, 10(2): 81-94.
- [33] 李晓伟, 张维江, 段文钰, 等. 基于双联盟链的工业物联网安全数据共享架构[J]. 网络与信息安全学报, 2025, 11(4): 73-85.
- Li X W, Zhang W J, Duan W Y, et al. Secure data sharing architecture for industrial Internet of Things based on dual consortium chains[J]. Chinese Journal of Network and Information Security. 2025, 11(4): 73-85.
- [34] Castryck W, Decru T. An efficient key recovery attack on SIDH (preliminary version)[PP]. Cryptology ePrint Archive[2015-10-13]. Cryptology ePrint Archive: 2022/975.
- [35] Maino L, Martindale C, Panny L, et al. A direct key recovery attack on SIDH[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer Nature Switzerland, 2023: 448-471.
- [36] Robert D. Breaking SIDH in polynomial time[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer Nature Switzerland, 2023: 472-503.
- [37] Fouotsa T B, Moriya T, Petit C. M-SIDH and MD-SIDH: countering SIDH attacks by masking information[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer Nature Switzerland, 2023: 282-309.
- [38] Basso A, Fouotsa T B. New SIDH countermeasures for a more efficient key exchange[C]//International Conference on the Theory and Application of Cryptology and Information Security. Singapore: Springer Nature Singapore, 2023: 208-233.
- [39] Basso A, Maino L, Pope G. FESTA: fast encryption from supersingular torsion attacks[C]//International Conference on the Theory and Application of Cryptology and Information Security. Singapore: Springer Nature Singapore, 2023: 98-126.
- [40] Nakagawa K, Onuki H. QFESTA: efficient algorithms and parameters for FESTA using quaternion algebras[C]//Annual International Cryptology Conference. Cham: Springer Nature Switzerland, 2024: 75-106.
- [41] Basso A, Maino L. POKÉ: A compact and efficient PKE from higher-dimensional isogenies[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer Nature Switzerland, 2025: 94-123.
- [42] Castryck W, Lange T, Martindale C, et al. CSIDH: an efficient post-quantum commutative group action[C]//International Conference on the Theory and Application of Cryptology and Information Security. Cham: Springer International Publishing, 2018: 395-427.
- [43] Moriya T, Onuki H, Takagi T. SiGamal: a supersingular isogeny-based PKE and its application to a PRF[C]//International Conference on the Theory and Application of Cryptology and Information Security. Cham: Springer International Publishing, 2020: 551-580.
- [44] Fouotsa T B, Petit C. SimS: a simplification of SiGamal[C]//International Conference on Post-Quantum Cryptography. Cham: Springer International Publishing, 2021: 277-295.
- [45] Bahramian M, Hajirezaei E. An identity-based encryption scheme using isogeny of elliptic curves[J]. Facta Universitatis, Series: Mathematics and Informatics. 2021: 1451-1460.
- [46] Fan Q, He D, Chen J, et al. Isoga: an isogeny-based quantum-resist searchable encryption scheme against keyword guessing attacks[J]. IEEE Systems Journal. 2022, 17(2): 2101-2112.
- [47] Huang W, Luo M, Peng C, et al. FleS: A compact and parameter-flexible supersingular isogeny based public key encryption scheme[C]//International Conference on Provable Security. Cham: Springer Nature Switzerland, 2023: 290-308.
- [48] Dartois P, Eriksen J K, Fouotsa T B, et al. PEGASIS: practical effective class group action using 4-dimensional isogenies[C]//Annual International Cryptology Conference. Cham: Springer Nature Switzerland, 2025: 67-99.
- [49] Moriya T, Stopar M. LIT-SiGamal: an efficient isogeny-based PKE based on a LIT diagram[C]//International Conference on the Theory and Application of Cryptology and Information Security. Singapore: Springer Nature Singapore, 2025: 275-306.
- [50] Beimel A. Secure schemes for secret sharing and key distribution [D]. Haifa: Israel Institute of Technology, 1996.
- [51] Silverman J H. The arithmetic of elliptic curves[M]. New York: Springer, 2009.
- [52] Waterhouse W C. Abelian varieties over finite fields[J]. Annales scientifiques de l'École normale supérieure. 1969, 2(4): 521-560.
- [53] Costello C, Hisil H. A simple and compact algorithm for SIDH with arbitrary degree isogenies[C]//International Conference on the Theory and Application of Cryptology and Information Security. Cham: Springer International Publishing, 2017: 303-329.

[作者简介]



陈浙文 (2001-), 女, 国防科技大学硕士生, 主要研究方向为同源基后量子密码。



徐铮 (1994-), 男, 合肥国家实验室副研究员, 主要研究方向为基于同源的后量子密码。



陈锦榕 (1996-), 男, 国防科技大学博士生, 主要研究方向为后量子公钥密码算法。



周子健 (1990-), 男, 中国人民解放军国防科技大学副教授, 主要研究方向为代数曲线和后量子密码。