



基于SM9的标识条件广播代理重加密

Identity-Based Conditional Broadcast Proxy Re-encryption Based on SM9

|         |                                                                                                                |
|---------|----------------------------------------------------------------------------------------------------------------|
| 期刊：     | 中国科学: 信息科学                                                                                                     |
| 稿件ID：   | SSI-2025-0426.R3                                                                                               |
| 稿件栏目：   | 论文                                                                                                             |
| 作者提交日期： | 2026-02-24                                                                                                     |
| 参与作者列表： | 刘行, 明洋, 王晨豪, 赵一                                                                                                |
| 关键词：    | SM9, 条件广播代理重加密, 细粒度授权, 策略控制, 隐私保护                                                                              |
| 英文关键词：  | SM9, conditional broadcast proxy re-encryption, fine-grained authorization, policy control, privacy-preserving |
| 学科领域：   | 信息安全                                                                                                           |
| 专题：     |                                                                                                                |

# 基于 SM9 的标识条件广播代理重加密

刘行, 明洋\*, 王晨豪, 赵一

长安大学信息工程学院, 西安 710018

\* 通信作者. E-mail: yangming@chd.edu.cn

国家自然科学基金 (批准号: 62472049, 62072054)、陕西省重点研发计划 (批准号: 2024GX-YBXM-078)、陕西省自然科学基金基础研究计划 (批准号: 2025JC-YBMS-741) 资助项目

**摘要** 标识条件广播代理重加密允许数据所有者根据预设条件向一组数据请求者细粒度地分享外包密文的解密权限, 广泛应用于数据交易、分级数据开放和服务订阅等方面. 然而, 已有方案在系统建立时限制了数据请求者数量且面临数据请求者标识隐私泄露问题. SM9 标识加密作为我国自主研发的标识密码算法, 已在金融、医疗和政务等关键领域深度应用, 但其仅支持一对一数据共享无法满足灵活的多样化需求. 针对上述问题, 本文基于 SM9 标识加密算法提出一种标识条件广播代理重加密方案 SM9-IB-CBPRES. 该方案借鉴集合承诺思想嵌入条件集合到密文和重加密密钥, 实现多条件控制下的细粒度授权, 利用拉格朗日插值多项式隐藏数据请求者信息, 满足任意数量数据请求者的同时消除隐私泄露风险. 针对授权灵活性受限问题, 本文基于密钥策略属性基加密思想设计扩展方案 SM9-IB-CBPRES+, 该方案利用单调张成方案分割用户私钥, 将条件集合一致性匹配优化为策略满足性判定, 实现策略控制下的细粒度授权. 安全性分析表明所提方案在随机谕言机模型下能够抵抗静态选择明文攻击和合谋攻击. 性能分析表明, 所提方案在效率上与已有方案相当, 同时在功能与实用性上显著增强.

**关键词** SM9, 条件广播代理重加密, 细粒度授权, 策略控制, 隐私保护

## 1 引言

近年来, 随着数字经济的高质量发展, 数据作为数字时代的新型生产要素, 有效改善和提升了各传统生产要素的生产力, 促进了社会生产关系的升级和优化. 随着云计算迅速发展, 越来越多用户将数据外包到云存储服务器中以释放本地资源, 实现便捷的按需访问. 同时, 为保障数据隐私性以及数据本身价值, 通常采用加密后外包范式处理数据, 即用户在上传数据之前对其进行加密操作<sup>[1~3]</sup>. 然而, 如何将加密后的数据安全有效地授权给他人成为一项重要挑战.

代理重加密 (proxy re-encryption, PRE)<sup>[4]</sup> 作为极具应用前景的密码学原语, 在保护数据机密性的同时实现密文转换功能, 进而支持高效的授权. 具体来说, 数据所有者能够生成重加密密钥, 使得代理者将数据拥有者的密文转换为数据请求者可解的密文. 标识代理重加密 (identity-based PRE, IB-PRE)<sup>[5]</sup> 结合 PRE 与标识密码<sup>[6]</sup>, 解决传统公钥基础设施下 PRE 中固有的证书管理问题.

引用格式: 刘行, 明洋, 王晨豪, 等. 基于 SM9 的标识条件广播代理重加密. 中国科学: 信息科学, 在审文章

Liu H, Ming Y, Wang C H, et al. Identity-based conditional broadcast proxy re-encryption based on SM9. Sci Sin Inform, for review

<https://www.sciengine.com/doi/10.1360/SSI-2025-0426>

<http://infocn.scichina.com>

然而, 在 PRE/IB-PRE 中, 一旦数据拥有者为数据请求者生成重加密密钥, 代理者将拥有转换其所有密文的能力. 现实场景中数据拥有者可能只希望与数据请求者共享某一类密文, 而非所有密文, 即细粒度授权. 此外, PRE/IB-PRE 仅支持一对一授权. 当数据拥有者想要为多个数据请求者授权解密权限时, 需要分别为每一个请求者生成重加密密钥. 同时, 代理者需使用不同重加密密钥执行多次重加密操作, 导致计算和通信资源浪费. 为实现一对多和细粒度授权, 标识条件广播代理重加密 (identity-based conditional broadcast PRE, IB-CBPRE)<sup>[7]</sup> 概念被提出, 其利用广播加密思想 (允许数据拥有者为多个数据请求者生成重加密密钥), 同时在密文和重加密密钥中嵌入指定条件 (当密文中条件和重加密密钥中条件一致时, 代理者才能进行重加密操作). 然而, 文献 [7] 仅支持在密文和重加密密钥中嵌入单个条件, 表达能力较弱, 限制授权灵活性. 为此, 文献 [8~12] 利用访问结构优化条件控制表达能力, 允许数据拥有者在密文或重加密密钥中嵌入授权策略, 实现了表达能力更强的细粒度授权.

不幸的是, 上述方案的设计均由国外标识加密算法衍生而来, 缺乏适用于国产密码算法的相关研究. 面向国家核心技术自主可控战略需求, 我国自主研发了包含数字签名算法、密钥交换协议、密钥封装机制和公钥加密算法的国密 SM9 标识密码算法<sup>[13]</sup>. 2021 年 10 月, SM9 全系列算法被纳入国际 ISO/IEC 标准并广泛应用于多个重要领域, 有效解决现实场景中安全问题. 针对 SM9 仅适用于一对一应用场景问题, 学者们构造基于 SM9 的标识广播加密<sup>[14~16]</sup>、容错标识加密<sup>[17]</sup>、属性基加密<sup>[18,19]</sup> 等方案. 然而, 上述方案不支持密文转换功能, 灵活性较差, 无法满足复杂的多元化数据共享需求. 为此, 文献 [20,21] 研究基于 SM9 的标识 (广播) 代理重加密方案, 为 SM9 体系提供一对多授权和密文转换支持.

**现有研究局限性及技术挑战.** 本文总结现有研究局限性如下: 1) 现有多条件细粒度授权机制面临效率与表达能力的权衡. 尽管策略控制下的细粒度授权方法支持复杂条件组合控制, 但其普遍受制于较大的计算和通信开销. 如文献 [22] 所述, 对于大多数实际场景, 多条件值“与”门逻辑已足够适用. 因此, 有必要为 IB-CBPRE 设计高效的多条件控制下细粒度授权方法, 以满足不同场景中多样化条件授权需求. 实现该目标的一种直观思路是在文献 [7] 中生成多个密文并分割数据为多份确保条件满足时可恢复数据, 但是密文与重加密密钥的匹配以及消除潜在的通信开销增长成为亟待解决的难题. 因此, 核心挑战在于如何设计一种机制, 既能紧凑表达和嵌入多个条件, 又能实现高效的条件匹配验证, 从而在满足细粒度授权需求同时避免系统效率下降. 2) 现有隐私保护机制在实用性与可证安全性之间存在鸿沟. 一方面, 已有方案<sup>[7~12]</sup> 在系统建立阶段限定了一次可授权的数据请求者数量, 导致系统无法支持大规模数据请求者同时授权, 实用性有待优化. 另一方面, 重加密密文的解密需要所有数据请求者的标识信息, 导致数据请求者敏感的标识信息随重加密密钥/密文显式传输, 引发隐私泄露风险. 尽管已有学者<sup>[23~25]</sup> 尝试在标识广播代理重加密体系下解决上述问题, 但其在安全性和实用性上仍存在缺陷. 具体来说, 基于隐藏标识向量的方案<sup>[25]</sup> 难以在暴力攻击下保障标识隐私且系统参数与最大标识长度线性相关. 相比之下, 基于拉格朗日插值的方法<sup>[23,24]</sup> 无需在系统建立阶段指定标识相关信息 (如可授权数量和标识长度), 增强了系统实用性. 然而, 文献 [23,24] 中重加密密文安全性缺乏形式化证明且文献 [24] 无法抵抗合法用户的内部攻击, 数据机密性存在隐患. 因此, 关键挑战在于如何建立既支持任意规模数据请求者集又提供严格形式化安全证明的隐私保护框架. 3) 现有方案与 SM9 密码体系深度兼容性不足. 如前所述, 已有 IB-CBPRE 方案<sup>[7~12]</sup> 均基于国外算法构造, 难以适配国产密码算法. 尽管已有研究<sup>[20,21]</sup> 尝试将代理重加密机制与 SM9 结合, 但其为实现密文转换功能而修改 SM9 核心参数结构 (如将原公开参数中生成元设为主私钥), 致使其兼容性较差 (即无法直接集成至现行 SM9 系统) 且破坏标准统一性. 此外, 文献 [21] 同样面临已有 IB-CBPRE 方案中存在的实用性差和未考虑数据请求者标识信息保护问题. 因此, 根本性挑战为如何在严格遵守 SM9 算法参数体系与代数结构前提下, 无损嵌入细粒度授权机制, 增强数据共享灵活性.

综上, 本文研究在国密 SM9 体系下构建支持多条件/策略控制下细粒度授权的、实用且隐私保护的标识条件广播代理重加密方案. 本文主要贡献如下.

- 基于 SM9 标识加密算法, 提出一种标识条件广播代理重加密方案 SM9-IB-CBPRE. 该方案 (主) 私钥格式与 SM9 算法一致, 因此能够与现行 SM9 系统高度兼容. 借助集合承诺思想, 该方案将条件集合压缩为一个简洁的承诺并嵌入至密文和重加密密钥结构中, 将条件集合一致性匹配问题转化为承诺等性校验问题 (其正确性由集合承诺的绑定性保证), 实现多条件控制下的细粒度授权. 同时, 集合承诺简洁性隐式地避免了通信开销线性增长问题. 通过在重加密密钥中采用随机数重用技术生成广播封装密文并基于拉格朗日插值技术建立多项式以隐藏数据请求者相关信息, 该方案无需传输敏感标识信息, 保障数据请求者隐私同时实现恒定解密开销. 此外, 由于无需限定数据请求者数量, 所提方案实现了对大规模数据请求者的无缝支持, 显著提高系统实用性.
- 在 SM9-IB-CBPRE 的基础上, 融合密钥策略属性基加密思想, 设计扩展方案 SM9-IB-CBPRE<sup>+</sup>, 优化条件集合一致性匹配问题为策略满足性判定问题, 有效增强授权灵活性. 该方案利用单调张成方案表达授权策略, 分割用户私钥并嵌入重加密密钥以应对多条件值“与”门逻辑难以支持的复杂授权需求, 将代理者重加密能力严格限制于条件集合满足该策略的密文, 实现策略控制下细粒度授权.
- 基于  $q$ -DBDHI 假设和  $q$ -SDH 假设, 在随机谕言机模型下, 证明所提方案能够实现静态选择明文攻击下不可区分性和合谋攻击下抗泄露性. 同时, 通过与已有方案进行的理论和实验分析, 验证所提方案在实现更丰富功能的同时取得更优的计算效率, 更适用于多用户场景.

## 2 相关工作

2007 年, Green 等<sup>[5]</sup>将代理重加密<sup>[4]</sup>引入到标识密码体系<sup>[6]</sup>中, 提出标识代理重加密 (IB-PRE) 概念, 避免传统公钥基础设施下代理重加密方案中的证书管理问题. 为支持细粒度授权, Shao 等<sup>[26]</sup>结合条件代理重加密<sup>[27]</sup>的思想, 构建标识条件代理重加密 (identity-based conditional PRE, IB-CPRE) 方案. 该方案中, 数据拥有者在重加密密钥和密文中分别指定一个条件值, 使得只有两者条件一致时, 重加密操作才能成功. Zhou 等<sup>[28]</sup>基于全安全标识加密方案<sup>[29]</sup>设计全安全的 IB-CPRE 方案. Liang 等<sup>[30,31]</sup>在标准模型中研究选择密文安全的单跳和多跳 IB-CPRE 方案. Yao 等<sup>[32]</sup>基于文献<sup>[30,31]</sup>, 提出支持单跳条件委派和多跳密文进化的 IB-PRE 方案. 通过引入代理辅助的 IB-CPRE 机制, Li 等<sup>[33]</sup>构建高效的可撤销端到端加密消息传输系统. 考虑到上述方案仅支持单条件的“与”门匹配, Ge 等<sup>[34]</sup>基于访问树结构设计支持策略控制的 IB-CPRE 方案, 实现多条件的“或”门匹配. 此外, 文献<sup>[35]</sup>提出灵活的隐私保护数据共享方案. 该方案在生成委派密钥时, 采用线性秘密共享技术分割用户私钥, 实现细粒度授权.

然而, 上述方案仅实现一对一授权, 难以应用于多用户场景. Xu 等<sup>[7]</sup>结合广播加密和标识条件代理重加密思想, 提出标识条件广播代理重加密 (IB-CBPRE) 方案, 实现恒定长度密文. 进一步, Huang 等<sup>[8,9]</sup>分别基于密文和密钥策略属性基加密嵌入访问树和属性集合到初始密文和重加密密钥中, 提出条件控制授权的 IB-CBPRE 方案. 然而, 在文献<sup>[8,9]</sup>中, 用户生成有效重加密密钥的前提在于其拥有密钥生成中心分发的条件私钥, 灵活性依旧受限. Ge 等<sup>[10]</sup>基于文献<sup>[29]</sup>方法, 构建策略控制授权的微视频订阅系统, 支持一对多和细粒度授权且无需条件私钥分发. Deng 等<sup>[11]</sup>结合广播授权<sup>[7]</sup>和策略控制<sup>[35]</sup>方法, 提出基于策略的广播访问授权体制. 考虑到恶意数据拥有者信息泄露造成的未授权访问及未定义的读写控制, 基于文献<sup>[11]</sup>和访问控制加密, Sun 等<sup>[12]</sup>设计具有策略驱动动态授权的可净化跨域访问控制协议. 然而, 上述机制均面临着实用性差及隐私泄露等问题.

SM9 算法作为我国自主研发的密码算法自提出后得到广泛研究. Cheng 等<sup>[36]</sup>对密钥封装和公钥加密算法进行严格安全证明. 文献<sup>[37]</sup>给出数字签名算法的形式化证明并基于更弱假设提出新的密钥封装机制. Liu 等<sup>[20]</sup>提出基于 SM9 的 IB-PRE 方案. Zhang 等<sup>[38]</sup>基于 0/1 编码技术设计前向安全的密文等值测试方案. 针对多用户场景, 文献<sup>[14~16]</sup>分别研究选择明文安全、选择密文安全和隐私保护的标识广播加密方案. Li 等<sup>[39]</sup>针对 SM9 标识加密不支持内积函数功能, 提出基于 SM9 的分层标识广播内积函数加密方案. Liu 等<sup>[17]</sup>设

表 1 主要符号  
Table 1 Main Symbols

| Symbol                      | Description                                   | Symbol                    | Description                       |
|-----------------------------|-----------------------------------------------|---------------------------|-----------------------------------|
| $\lambda$                   | Security parameter                            | $pp$                      | Public parameter                  |
| $id_o$                      | Identity of data owner                        | $sk_{id_o}$               | Identity secret key of data owner |
| $R = \{id_0, \dots, id_l\}$ | Identity set of data requester                | $W = \{w_1, \dots, w_n\}$ | Condition set                     |
| $sk_{id_j}$                 | Identity secret key of $j$ -th data requester | $(A, \rho)$               | Authorization policy              |
| $C_{id_o}$                  | Original ciphertext                           | $K$                       | Encapsulated key                  |
| $RK_{id_o \rightarrow R}$   | Re-encryption key                             | $C'_R$                    | Re-encrypted ciphertext           |

计支持大属性域的容错标识加密方案. 文献 [18, 19] 构造密文策略和密钥策略属性基加密方案, 实现细粒度访问控制. 针对代理重加密系统中不可信代理者返回错误转换结果问题, Liu 等<sup>[21]</sup> 提出可验证公平标识广播代理重加密机制, 使得数据请求者能够验证重加密密文正确性同时确保诚实代理者免受问责.

综上所述, 目前针对标识条件代理重加密的授权机制和广播通信等方面研究成果较为丰富, 然而对于隐私保护、实用性以及与国密算法的结合方面的研究却未引起广泛关注. 此外, 未见有关基于 SM9 的支持细粒度授权的标识条件广播加密相关研究. 因此, 本文在以上工作的基础上, 结合 SM9 算法, 研究支持多条件/策略控制下细粒度授权的、实用的、隐私保护的标识条件广播代理重加密.

### 3 预备知识

#### 3.1 符号定义

本文使用的符号及其说明如表1所示.

#### 3.2 双线性配对

令  $\mathbb{F}_p$  为定义椭圆曲线的素数域, 其中  $p$  为基域特征. 设  $\mathbb{G}_1$  和  $\mathbb{G}_2$  为素数  $N$  阶加法循环群,  $\mathbb{G}_T$  为素数  $N$  阶乘法循环群, 双线性映射  $e: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$  满足下列性质: (1) 双线性: 对于任意  $P_1 \in \mathbb{G}_1, P_2 \in \mathbb{G}_2, a, b \in \mathbb{Z}_N^*$ , 有  $e(aP_1, bP_2) = e(P_1, P_2)^{ab}$ ; (2) 非退化性: 至少存在元素  $P_1 \in \mathbb{G}_1, P_2 \in \mathbb{G}_2$ , 使得  $e(P_1, P_2) \neq 1_{\mathbb{G}_T}$ ; (3) 可计算性: 对于任意  $P_1 \in \mathbb{G}_1, P_2 \in \mathbb{G}_2$ , 存在多项式时间算法计算  $e(P_1, P_2)$ .

令  $\mathcal{BP} = (e, p, N, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$  为双线性群, 若  $\mathbb{G}_1 = \mathbb{G}_2$ , 则称为对称双线性群; 否则为非对称双线性群. 在非对称双线性群中, 存在从  $\mathbb{G}_2$  到  $\mathbb{G}_1$  的公开可计算同态映射  $\varphi$ . SM9 算法基于非对称双线性群构造. 本文采用仿射坐标系下的坐标表示方法对群  $\mathbb{G}_1$  中元素进行表示, 即  $P_1 = (x_{P_1}, y_{P_1})$ , 其中  $x_{P_1}, y_{P_1} \in \mathbb{F}_p$ .

**假设 1** ( $q$ -DBDHI 假设) 给定  $(P, Q, aQ, \dots, a^q Q, Z) \in \mathbb{G}_1 \times \mathbb{G}_2^{q+1} \times \mathbb{G}_T$ ,  $q$ -DBDHI 问题为判断  $Z = e(P, Q)^{\frac{1}{a}}$  是否成立, 其中  $a \in \mathbb{Z}_N^*$  未知. 若任意多项式时间敌手  $\mathcal{A}$  解决  $q$ -DBDHI 问题优势  $\text{Adv}_{\mathcal{A}}^{q\text{-DBDHI}} = |\Pr[\mathcal{A}(P, Q, aQ, \dots, a^q Q, Z) = e(P, Q)^{\frac{1}{a}}] - \Pr[\mathcal{A}(P, Q, aQ, \dots, a^q Q, Z) \neq e(P, Q)^{\frac{1}{a}}]|$  可忽略, 则  $q$ -DBDHI 假设成立.

**假设 2** ( $q$ -SDH 假设) 给定  $(P, Q, aQ, \dots, a^q Q) \in \mathbb{G}_1 \times \mathbb{G}_2^{q+1}$ ,  $q$ -SDH 问题为输出  $(\omega, \frac{1}{a+\omega} \cdot P) \in \mathbb{Z}_N^* \times \mathbb{G}_1$ , 其中  $a \in \mathbb{Z}_N^*$  未知. 若任意多项式时间敌手  $\mathcal{A}$  解决  $q$ -SDH 问题优势  $\text{Adv}_{\mathcal{A}}^{q\text{-SDH}} = |\Pr[\mathcal{A}(P, Q, aQ, \dots, a^q Q) = (\omega, \frac{1}{a+\omega} \cdot P)]|$  可忽略, 则  $q$ -SDH 假设成立.

### 3.3 集合承诺

集合承诺允许承诺者对一个有界集合  $W$  进行承诺, 并支持对完整集合和其任意子集  $T \subseteq W$  进行打开, 其由初始化 (根据安全参数  $\lambda$  和集合尺寸上界  $t$  生成公开参数  $pp$ )、承诺 (输出集合  $W$  的承诺  $\Lambda_W$  和打开信息  $op$ )、打开承诺 (验证  $\Lambda_W$  是否为  $op$  下对  $W$  的有效承诺)、打开子集 (生成子集关系  $T \subseteq W$  的证据  $\pi$ ) 和验证子集 (利用  $\pi$  验证  $T$  是否为  $\Lambda_W$  中集合的子集) 算法组成, 具体定义可见文献 [40]. 集合承诺须满足简洁性、绑定性、隐藏性和子集可靠性. 简洁性要求承诺和证据的尺寸为  $O(\lambda + \log t)$ . 绑定性确保攻击者不能将一个承诺打开为两个不同集合  $(W, W')$ . 隐藏性要求承诺  $\Lambda_W$  不会泄漏集合  $W$  相关的任何信息. 子集可靠性确保攻击者无法为一个非子集  $T' \not\subseteq W$  生成有效子集证据  $\pi'$ .

文献 [40] 在非对称双线性群中给出一个具体的集合承诺方案. 该方案在公开参数  $pp = (\mathcal{BP}, P_1, P_2, \{\alpha^i \cdot P_1, \alpha^i \cdot P_2\}_{i \in [1, t]})$  下通过首一多项式形式对集合  $W = \{w_1, \dots, w_n\}$  生成承诺  $\Lambda_W = r \cdot f_W(\alpha) \cdot P_1$ , 利用多项式除法生成证据  $\pi = r \cdot f_{W \setminus T}(\alpha) \cdot P_1$  并通过  $e(\Lambda_W, P_2) = e(\pi, f_T(\alpha) \cdot P_2)$  验证子集关系, 其中  $f_W(x) = \prod_{i=1}^n (w_i + x)$  且  $r \in \mathbb{Z}_N^*$  为打开信息. 本文借鉴上述集合承诺思想对条件集合进行压缩, 以解决通信开销增长问题并确保条件集合一致性匹配正确性. 为此, 承诺仅需满足简洁性和绑定性核心性质. 故本文生成承诺为  $\Lambda_W = r \cdot H_4(f_W(\alpha))$ , 其中  $H_4$  为密码学哈希函数且  $\alpha$  为用户标识相关的可公开计算信息.

### 3.4 拉格朗日插值

给定非重复的  $l+1$  个点  $(x_0, y_0), (x_1, y_1), \dots, (x_l, y_l) \in \mathbb{F}_p \times \mathbb{F}_p$ , 存在唯一  $l$  阶多项式  $F(x) \in \mathbb{F}_p[x]$  使得  $F(x_i) = y_i$ , 其中  $i \in [0, l]$ . 该多项式可通过有限域  $\mathbb{F}_p$  上拉格朗日插值技术进行重构, 即

$$F(x) = \sum_{i=0}^l y_i \cdot \prod_{0 \leq k \neq i \leq l} \frac{x - x_k}{x_i - x_k} = \sum_{i=0}^l v_i \cdot x^i.$$

### 3.5 访问结构

令  $\mathcal{W}$  为条件域, 集合  $\mathbb{W} \subseteq 2^{\mathcal{W}}$  称为单调的, 如果对于任意的  $B, C \subseteq \mathcal{W}$ , 由  $B \in \mathbb{W}$  且  $B \subseteq C$  可得  $C \in \mathbb{W}$ . 访问结构是  $\mathcal{W}$  上所有非空子集构成的单调集合  $\mathbb{W}$ , 即  $\mathbb{W} \subseteq 2^{\mathcal{W}} \setminus \{\emptyset\}$ .

单调访问结构可由单调布尔公式表示. 布尔公式属于一类称为单调张成方案的更通用的函数, 其由一个  $n_1 \times n_2$  的矩阵  $A$  和映射  $\rho: \{1, \dots, n_1\} \rightarrow \mathcal{W}$  组成. 文献 [41] 给出从任意布尔公式到单调张成方案的通用转换, 其中  $A$  中每一个元素属于  $\{-1, 0, 1\}$ . 令  $W$  为一个条件集合, 定义集合  $I = \{i | \rho(i) \in W\} \subseteq \{1, \dots, n_1\}$ , 若存在一组常量  $\{m_i\}_{i \in I}$  使得  $\sum_{i \in I} m_i A_i = (1, 0, \dots, 0)$ , 则称  $W$  满足  $(A, \rho)$ , 其中  $A_i$  为  $A$  的第  $i$  行. 若采用文献 [41] 方法生成单调张成方案, 则  $m_i$  为 0 或 1.

### 3.6 SM9 密钥封装机制

SM9 标识密码算法<sup>[13]</sup> 由数字签名算法、密钥交换协议、密钥封装机制和公钥加密算法组成. 为便于理解, 本节给出 SM9 密钥封装机制的描述, 其由如下算法组成.

• **Setup**( $\lambda$ )  $\rightarrow (pp, msk)$ . 给定安全参数  $\lambda$ , 输出公共参数  $pp = (\mathcal{BP}, P_1, P_2, P_{pub} = sP_1, hid, H, KDF)$  和主私钥  $msk = s \in \mathbb{Z}_N^*$ , 其中  $P_1$  和  $P_2$  分别为群  $\mathbb{G}_1$  和  $\mathbb{G}_2$  的生成元,  $hid$  为密钥生成函数标识,  $H: \{0, 1\}^* \rightarrow \mathbb{Z}_N^*$  为密码学哈希函数,  $KDF: \{0, 1\}^* \rightarrow \{0, 1\}^{klen}$  为密钥派生函数,  $klen$  为封装密钥长度.

• **Extract**( $msk, id$ )  $\rightarrow sk_{id}$ . 给定主私钥  $msk$  和用户标识  $id$ , 输出私钥  $sk_{id} = \frac{s}{(s + H(id || hid))} \cdot P_2$ .

• **Encrypt**( $id$ )  $\rightarrow (C, K)$ . 给定用户标识  $id$ , 输出封装密文  $C = r \cdot (P_{pub} + H(id || hid) \cdot P_1)$  和封装密钥  $K = KDF(C || \gamma || id)$ , 其中  $r \in \mathbb{Z}_N^*$ ,  $\gamma = e(P_{pub}, P_2)^r$ .

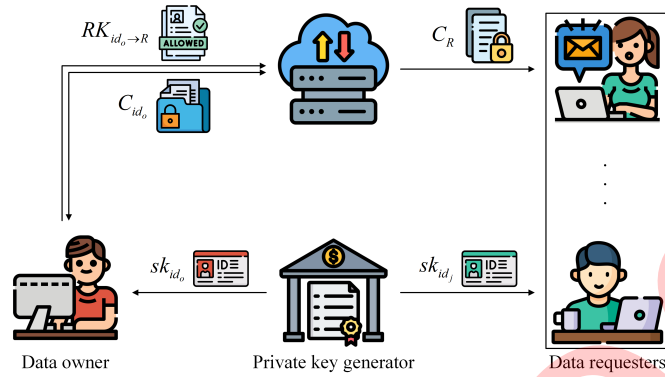


图 1 系统模型

Figure 1 System Model

- $\text{Decrypt}(C, id, sk_{id}) \rightarrow K'$ . 给定封装密文  $C$ , 用户标识和私钥  $(id, sk_{id})$ , 输出封装密钥  $K' = \text{KDF}(C || \gamma' || id)$ , 其中  $\gamma' = e(C, sk_{id})$ .

### 3.7 标识条件广播代理重加密系统模型

标识条件广播代理重加密 (IB-CBPRE)<sup>[7,10]</sup> 系统模型如图1所示, 包含四类实体: 密钥生成中心 (private key generator, PKG)、云服务器 (cloud server, CS)、数据拥有者 (data owner, DO) 和多个数据请求者 (data requesters, DRs).

- PKG: 负责生成并公布公共参数, 并在收到 DO 和 DR 的注册请求时为其颁发私钥.
- CS: 提供存储服务, 即存储数据拥有者上传的数据密文. 同时充当代理者提供密文转换服务, 即根据细粒度的授权需求, 使用重加密密钥将 DO 可解的密文转换为一组 DR 可解的密文.
- DO: 对数据进行加密生成数据密文并将其外包至 CS, 以减少本地存储资源. 此外, 为支持细粒度授权, 其嵌入数据对应的条件值 (如文件类型、日期、安全级别等) 至数据密文中. 通过生成重加密密钥, DO 能够与一组 DR 共享外包数据.
- DRs: 获得 DO 的细粒度授权后, 在 CS 处下载密文, 使用私钥解密得到数据.

在 IB-CBPRE 中, PKG 和 DO 是完全可信的实体. 具体来说, PKG 建立整个系统并诚实地为所有用户颁发私钥, DO 外包自己的数据至云服务器并可控地向 DRs 细粒度分享外包密文解密权限. CS 和 DRs 是诚实但好奇的半可信实体. 一方面, CS 诚实地提供密文存储和重加密服务, 但试图从密文中获取底层数据. 另一方面, DRs 可能会尝试访问超出 DO 授权范围的数据. 同时, 掌握重加密密钥的 CS 可能会与 DRs 进行合谋, 共同推断 DO 的私钥. 此外, 位于公共信道上的窃听者也会试图获取 DO 的外包数据.

### 3.8 标识条件广播代理重加密形式化定义及安全模型

IB-CBPRE 方案由如下 7 个多项式时间算法组成. 为有效集成 SM9 算法, 本文只给出 IB-CBPRE 的密钥封装, 即加密算法和解密算法输出封装密钥.

- $\text{Setup}(\lambda)$ . 该算法由 PKG 执行, 输入安全参数  $\lambda$ , 输出公共参数  $pp$  和主私钥  $msk$ .
- $\text{Extract}(msk, id)$ . 该算法由 PKG 执行, 输入主私钥  $msk$  和用户标识  $id$ , 输出私钥  $sk_{id}$ .
- $\text{Encrypt}(id_o, W)$ . 该算法由 DO 执行, 输入数据拥有者标识  $id_o$  和条件集合  $W$ , 输出初始密文  $C_{id_o}$  和封装密钥  $K$ .

- $\text{Re-KeyGen}(id_o, sk_{id_o}, R, W')$ . 该算法由 DO 执行, 输入数据所有者标识和私钥  $(id_o, sk_{id_o})$ , 数据请求者标识集合  $R$  和条件集合  $W'$ , 输出重加密密钥  $RK_{id_o \rightarrow R}$ .
- $\text{Re-Encrypt}(C_{id_o}, W, RK_{id_o \rightarrow R}, W')$ . 该算法由 CS 执行, 输入初始密文  $C_{id_o}$  和对应的条件集合  $W$  以及重加密密钥  $RK_{id_o \rightarrow R}$  和对应的条件集合  $W'$ , 若  $W$  与  $W'$  匹配, 输出重加密密文  $C'_R$ ; 否则, 输出  $\perp$ .
- $\text{Decrypt}(C_{id_o}, id_o, sk_{id_o})$ . 该算法由 DO 执行, 输入初始密文  $C_{id_o}$ , 数据所有者标识和私钥  $(id_o, sk_{id_o})$ , 输出封装密钥  $K'$ .
- $\text{Re-Decrypt}(C'_R, id_o, id_j, sk_{id_j})$ . 该算法由  $\text{DR}_j$  执行, 输入重加密密文  $C'_R$ , 数据所有者标识  $id_o$ , 数据请求者标识和私钥  $(id_j, sk_{id_j})$ , 输出封装密钥  $K'$ .

**正确性.** 对于任意的安全参数  $\lambda$ , 用户标识  $id_o$  和  $id_j$ , 标识集合  $R$ , 条件集合  $W$  和  $W'$ , 若  $id_j \in R$  且  $W$  与  $W'$  匹配, 有

$$\Pr \left[ \begin{array}{l} (pp, msk) \leftarrow \text{Setup}(\lambda) \\ sk_{id_o} \leftarrow \text{Extract}(msk, id_o) \\ sk_{id_j} \leftarrow \text{Extract}(msk, id_j) \\ (C_{id_o}, K) \leftarrow \text{Encrypt}(id_o, W) \\ RK_{id_o \rightarrow R} \leftarrow \text{Re-KeyGen}(id_o, sk_{id_o}, R, W') \\ C'_R \leftarrow \text{Re-Encrypt}(C_{id_o}, W, RK_{id_o \rightarrow R}, W') \\ K' \leftarrow \text{Decrypt}(C_{id_o}, id_o, sk_{id_o}) \\ K' \leftarrow \text{Re-Decrypt}(C'_R, id_o, id_j, sk_{id_j}) \end{array} \right] = 1.$$

IB-CBPRe 方案应满足静态选择明文攻击下不可区分性 (indistinguishability against selective identity and chosen plaintext attack, IND-sID-CPA) 与合谋攻击下抗泄露性 (leakage resistance against collusion attack, LR-CA). 本文通过敌手  $\mathcal{A}$  和挑战者  $\mathcal{C}$  之间的游戏刻画 IND-sID-CPA 和 LR-CA 的定义.

**定义 1** (IND-sID-CPA) 若任意多项式时间敌手  $\mathcal{A}$  在游戏 IND-sID-CPA-Or 和 IND-sID-CPA-Re 中优势可忽略, 则 IB-CBPRe 方案是 IND-sID-CPA 安全的.

游戏 IND-sID-CPA-Or:

- **初始化.**  $\mathcal{A}$  声明要攻击的挑战标识  $id^*$  和条件集合  $W^*$ .  $\mathcal{C}$  运行  $\text{Setup}(\lambda) \rightarrow (pp, msk)$  并发送公共参数  $pp$  给  $\mathcal{A}$ .
- **询问阶段 1.**  $\mathcal{A}$  适应性地进行以下询问:
  - (1) 私钥询问. 给定  $id_i$ ,  $\mathcal{C}$  运行  $\text{Extract}(msk, id_i) \rightarrow sk_{id_i}$  并返回  $sk_{id_i}$  给  $\mathcal{A}$ . 限制条件为  $id_i \neq id^*$ .
  - (2) 重加密密钥询问. 给定  $(id_i, R_i, W_i)$ ,  $\mathcal{C}$  运行  $\text{Re-KeyGen}(id_i, sk_{id_i}, R_i, W_i) \rightarrow RK_{id_i \rightarrow R_i}$  并返回  $RK_{id_i \rightarrow R_i}$  给  $\mathcal{A}$ . 限制条件为当  $id_i = id^*$  时,  $W_i$  与  $W^*$  不匹配.
- **挑战.**  $\mathcal{C}$  运行  $\text{Encrypt}(id^*, W^*) \rightarrow (C_{id^*}, K^*)$ , 随机选择  $b \in \{0, 1\}$ , 设定  $K_b^* = K^*$ , 并返回  $(C_{id^*}, K_0^*, K_1^*)$  给  $\mathcal{A}$ , 其中  $K_{1-b}^*$  为  $\mathcal{C}$  选取的随机封装密钥.
- **询问阶段 2.**  $\mathcal{A}$  继续进行询问阶段 1 中的询问.
- **猜测.**  $\mathcal{A}$  输出猜测  $b'$ . 若  $b' = b$ , 则  $\mathcal{A}$  赢得游戏. 定义  $\mathcal{A}$  的优势为

$$\text{Adv}_{\mathcal{A}, \text{IB-CBPRe}}^{\text{IND-sID-CPA-Or}} = \left| \Pr[b' = b] - \frac{1}{2} \right|.$$

游戏 IND-sID-CPA-Re:

- **初始化.**  $\mathcal{A}$  声明要攻击的挑战标识集合  $R^*$ .  $\mathcal{C}$  运行  $\text{Setup}(\lambda) \rightarrow (pp, msk)$  并发送公共参数  $pp$  给  $\mathcal{A}$ .
- **询问阶段 1.**  $\mathcal{A}$  适应性地进行以下询问:

- (1) 私钥询问. 给定  $id_i$ ,  $\mathcal{C}$  运行  $\text{Extract}(msk, id_i) \rightarrow sk_{id_i}$  并返回  $sk_{id_i}$  给  $\mathcal{A}$ . 限制条件为  $id_i \notin R^*$ .
- (2) 重加密密钥询问. 给定  $(id_i, R_i, W_i)$ ,  $\mathcal{C}$  运行  $\text{Re-KeyGen}(id_i, sk_{id_i}, R_i, W_i) \rightarrow RK_{id_i \rightarrow R_i}$  并返回  $RK_{id_i \rightarrow R_i}$  给  $\mathcal{A}$ .
- 挑战.  $\mathcal{C}$  随机选择标识  $id$  以及匹配的条件集合  $W$  和  $W'$ , 运行  $\text{Encrypt}(id, W) \rightarrow (C_{id}, K^*)$ ,  $\text{Re-KeyGen}(id, sk_{id}, R^*, W)$ ,  $RK_{id \rightarrow R^*}$ ,  $\text{Re-Encrypt}(C_{id}, W, RK_{id \rightarrow R^*}, W') \rightarrow C'_{R^*}$ , 随机选择  $b \in \{0, 1\}$ , 设定  $K_b^* = K^*$ , 并返回  $(C'_{R^*}, K_0^*, K_1^*)$  给  $\mathcal{A}$ , 其中  $K_{1-b}^*$  为  $\mathcal{C}$  选取的随机封装密钥.
- 询问阶段 2.  $\mathcal{A}$  继续进行询问阶段 1 中的询问.
- 猜测.  $\mathcal{A}$  输出猜测  $b'$ . 若  $b' = b$ , 则  $\mathcal{A}$  赢得游戏. 定义  $\mathcal{A}$  的优势为

$$\text{Adv}_{\mathcal{A}, \text{IB-CBPRe}}^{\text{IND-sID-CPA-Re}} = \left| \Pr[b' = b] - \frac{1}{2} \right|.$$

**定义 2** 若任意多项式时间敌手  $\mathcal{A}$  在游戏 LR-CA 中优势可忽略, 则 IB-CBPRe 方案是 LR-CA 安全的. 游戏 LR-CA:

- 初始化.  $\mathcal{A}$  声明要攻击的挑战标识  $id^*$ .  $\mathcal{C}$  运行  $\text{Setup}(\lambda) \rightarrow (pp, msk)$  并发送公共参数  $pp$  给  $\mathcal{A}$ .
- 询问阶段.  $\mathcal{A}$  适应性地进行以下询问:
- (1) 私钥询问. 与游戏 IND-sID-CPA-Or 相同.
- (2) 重加密密钥询问. 给定  $(id_i, R_i, W_i)$ ,  $\mathcal{C}$  运行  $\text{Re-KeyGen}(id_i, sk_{id_i}, R_i, W_i) \rightarrow RK_{id_i \rightarrow R_i}$  并返回  $RK_{id_i \rightarrow R_i}$  给  $\mathcal{A}$ .
- 输出.  $\mathcal{A}$  输出私钥  $sk'_{id^*}$ . 若  $sk'_{id^*} = sk_{id^*}$ , 则  $\mathcal{A}$  赢得游戏. 定义  $\mathcal{A}$  的优势为

$$\text{Adv}_{\mathcal{A}, \text{IB-CBPRe}}^{\text{LR-CA}} = |\Pr[sk'_{id^*} = sk_{id^*}]|.$$

## 4 基于 SM9 的标识条件广播代理重加密方案

本节在 SM9 密钥封装机制基础上融合代理重加密和隐私保护广播加密思想, 提出标识条件广播代理重加密方案 SM9-IB-CBPRe 和扩展方案 SM9-IB-CBPRe<sup>+</sup>.

### 4.1 SM9-IB-CBPRe 具体构造

为支持多条件控制下的细粒度授权, SM9-IB-CBPRe 借鉴集合承诺思想<sup>[40]</sup> 将条件集合  $W = \{w_1, \dots, w_n\}$  压缩为  $\Lambda_W$  并生成一个简洁承诺与传统标识代理重加密中的重加密控制密文融合, 产生条件控制密文  $c_1$ . 相应地, 在重加密密钥中, 使用  $\alpha \cdot H_3(\theta) \cdot H_4(\Lambda_{W'})$  盲化用户私钥  $sk_{id}$ . 得到  $rk_2$ , 其中  $\theta$  可视为广播封装密文  $rk_0$  对应的广播封装密钥,  $\Lambda_{W'}$  对应条件集合  $W' = \{w'_1, \dots, w'_n\}$  的聚合结果,  $\alpha$  用于防止合谋攻击. 故仅当  $\Lambda_W = \Lambda_{W'}$  时 (即  $W = W'$ ), 云服务器可利用初始密文和重加密密钥正确生成重加密密文, 其包含广播封装密文和由  $H_3(\theta)$  盲化的  $\gamma$ . 解密重加密密文时, 数据请求者通过广播封装密文恢复  $\theta$  后进行去盲, 即可得到正确的封装密钥. 此外, SM9-IB-CBPRe 采用拉格朗日插值多项式构造重加密密钥中的广播封装密文, 确保重加密密文的解密无需数据请求者标识集合, 保证数据请求者标识隐私不被泄露同时支持任意数量数据请求者. SM9-IB-CBPRe 具体构造如下.

- $\text{Setup}(\lambda) \rightarrow (pp, msk)$ . 给定安全参数  $\lambda$ , PKG 执行:
- (1) 生成双线性群  $\mathcal{BP} = (e, p, N, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$ , 其中  $p$  为基域特征,  $N$  为大素数且  $N > 2^\lambda$ . 随机选择生成元  $P_1 \in \mathbb{G}_1$  和  $P_2 \in \mathbb{G}_2$ ;

- (2) 随机选择  $s \in \mathbb{Z}_N^*$ , 计算  $P_{pub} = sP_1$ ,  $u = e(P_{pub}, P_2)$ , 选择密钥生成函数标识  $hid$ ;
- (3) 随机选择四个密码学哈希函数  $H_1, H_2, H_3 : \{0, 1\}^* \rightarrow \mathbb{Z}_N^*$ ,  $H_4 : \{0, 1\}^* \rightarrow \mathbb{G}_2$ , 及一个密钥派生函数  $KDF : \{0, 1\}^* \rightarrow \{0, 1\}^{klen}$ , 其中  $klen$  为封装密钥长度;
- (4) 输出公共参数  $pp = (\mathcal{BP}, P_1, P_2, P_{pub}, u, hid, H_1, H_2, H_3, H_4, KDF)$  和主私钥  $msk = s$ .
- $\text{Extract}(msk, id) \rightarrow sk_{id}$ . 给定主私钥  $msk$  和用户标识  $id$ , PKG 计算  $sk_{id} = \frac{s}{(s + H_1(id||hid))} \cdot P_2$  并输出私钥  $sk_{id}$ .
  - $\text{Encrypt}(id_o, W) \rightarrow (C_{id_o}, K)$ . 给定数据所有者标识  $id_o$  和条件集合  $W = \{w_1, \dots, w_n\}$ , DO 执行:
    - (1) 随机选择  $r \in \mathbb{Z}_N^*$ , 计算  $\gamma = u^r$ ;
    - (2) 计算  $c_0 = r \cdot (P_{pub} + H_1(id_o||hid) \cdot P_1)$ ,  $\Lambda_W = \prod_{i=1}^n (H_1(id_o||hid) + H_2(w_i))$ ,  $c_1 = r \cdot H_4(\Lambda_W)$ ;
    - (3) 输出初始密文  $C_{id_o} = (c_0, c_1)$  和封装密钥  $K = KDF(\gamma||id_o)$ .
  - $\text{Re-KeyGen}(id_o, sk_{id_o}, R, W') \rightarrow RK_{id_o \rightarrow R}$ . 给定数据所有者标识和私钥  $(id_o, sk_{id_o})$ , 数据请求者标识集合  $R = \{id_0, \dots, id_l\}$  和条件集合  $W' = \{w'_1, \dots, w'_n\}$ , DO 执行:
    - (1) 随机选择  $\alpha, \beta \in \mathbb{Z}_N^*$ , 计算  $\theta = u^\beta$ ;
    - (2) 对于  $i \in [0, l]$ , 计算  $h_i = H_1(id_i||hid)$ ,  $C_i = \beta \cdot (P_{pub} + h_i \cdot P_1) = (x_i, y_i)$ ;
    - (3) 通过拉格朗日插值生成多项式  $F_1(x) = \sum_{i=0}^l x_i \cdot \prod_{0 \leq k \neq i \leq l} \frac{x - h_k}{h_i - h_k} = \sum_{i=0}^l v_{1,i} \cdot x^i \in \mathbb{F}_p[x]$  和  $F_2(x) = \sum_{i=0}^l y_i \cdot \prod_{0 \leq k \neq i \leq l} \frac{x - h_k}{h_i - h_k} = \sum_{i=0}^l v_{2,i} \cdot x^i \in \mathbb{F}_p[x]$ , 设定  $rk_0 = (v_{1,0}, \dots, v_{1,l}, v_{2,0}, \dots, v_{2,l})$ ;
    - (4) 计算  $rk_1 = \alpha \cdot (P_{pub} + H_1(id_o||hid) \cdot P_1)$ ,  $\Lambda_{W'} = \prod_{i=1}^n (H_1(id_o||hid) + H_2(w'_i))$ ,  $rk_2 = sk_{id_o} + \alpha \cdot H_3(\theta) \cdot H_4(\Lambda_{W'})$ ;
    - (5) 输出重加密密钥  $RK_{id_o \rightarrow R} = (rk_0, rk_1, rk_2)$ .
  - $\text{Re-Encrypt}(C_{id_o}, W, RK_{id_o \rightarrow R}, W') \rightarrow RK_{id_o \rightarrow R}$ . 给定初始密文  $C_{id_o}$  和对应的条件集合  $W$  以及重加密密钥  $RK_{id_o \rightarrow R}$  和对应的条件集合  $W'$ , 若  $W \neq W'$ , CS 输出  $\perp$ . 否则, CS 计算  $c'_0 = e(c_0, rk_2)$ ,  $c'_1 = rk_0$ ,  $c'_2 = e(rk_1, c_1)$  并输出重加密密文  $C'_R = (c'_0, c'_1, c'_2)$ .
  - $\text{Decrypt}(C_{id_o}, id_o, sk_{id_o}) \rightarrow K'$ . 给定初始密文  $C_{id_o}$ , 数据所有者标识和私钥  $(id_o, sk_{id_o})$ , DO 计算  $\gamma' = e(c_0, sk_{id_o})$  并输出封装密钥  $K' = KDF(\gamma'||id_o)$ .
  - $\text{Re-Decrypt}(C'_R, id_j, sk_{id_j}) \rightarrow K'$ . 给定重加密密文  $C'_R$ , 数据请求者标识和私钥  $(id_j, sk_{id_j})$ , DR<sub>j</sub> 执行:
    - (1) 计算  $h_j = H_1(id_j||hid)$ ,  $x'_j = F_1(h_j) = \sum_{i=0}^l v_{1,i} \cdot h_j^i$ ,  $y'_j = F_2(h_j) = \sum_{i=0}^l v_{2,i} \cdot h_j^i$  并恢复  $C'_j = (x'_j, y'_j)$ , 其中  $(v_{1,0}, \dots, v_{1,l}, v_{2,0}, \dots, v_{2,l}) = c'_1$ ;
    - (2) 计算  $\theta' = e(C'_j, sk_{id_j})$ ,  $\gamma' = \frac{c'_0}{c'_2 H_3(\theta')}$ ;
    - (3) 输出封装密钥  $K' = KDF(\gamma'||id_o)$ .

#### 4.2 SM9-IB-CBPRE 正确性分析

**算法 Decrypt 正确性分析.** 假设  $C_{id_o} = (c_0, c_1)$  为正确的初始密文, 对应数据所有者标识为  $id_o$ , 则有

$$\gamma' = e(c_0, sk_{id_o}) = e(r \cdot (P_{pub} + H_1(id_o||hid) \cdot P_1), \frac{s}{(s + H_1(id_o||hid))} \cdot P_2) = e(rP_1, sP_2) = u^r = \gamma.$$

由  $\gamma' = \gamma$  可得  $K' = KDF(\gamma'||id_o) = K' = KDF(\gamma||id_o) = K$ .

**算法 Re-Decrypt 正确性分析.** 假设  $C_{id_o} = (c_0, c_1)$  为正确的初始密文, 对应数据拥有者标识和条件集合分别为  $id_o$  和  $W = \{w_1, \dots, w_n\}$ ;  $RK_{id_o \rightarrow R} = (rk_0, rk_1, rk_2)$  为正确的重加密密钥, 对应数据拥有者标识、条件集合和数据请求者标识集合分别为  $id_o$ 、 $W' = \{w'_1, \dots, w'_n\}$  和  $R = \{id_0, \dots, id_l\}$ , 则重加密密文  $C'_R$  为

$$\begin{aligned} c'_0 &= e(c_0, rk_2) = e(r \cdot (P_{pub} + H_1(id_o || hid) \cdot P_1), sk_{id_o} + \alpha \cdot H_3(\theta) \cdot H_4(\Lambda_{W'})) \\ &= \gamma \cdot e(r \cdot (P_{pub} + H_1(id_o || hid) \cdot P_1), \alpha \cdot H_3(\theta) \cdot H_4(\prod_{i=1}^n (H_1(id_o || hid) + H_2(w'_i))))), \\ c'_1 &= (v_{1,0}, \dots, v_{1,l}, v_{2,0}, \dots, v_{2,l}), \\ c'_2 &= e(rk_1, c_1) = e(\alpha \cdot (P_{pub} + H_1(id_o || hid) \cdot P_1), r \cdot H_4(\Lambda_W)) \\ &= e(\alpha \cdot (P_{pub} + H_1(id_o || hid) \cdot P_1), r \cdot H_4(\prod_{i=1}^n (H_1(id_o || hid) + H_2(w_i)))). \end{aligned}$$

若  $W = W'$  且第  $j$  个数据请求者标识  $id_j \in R$ , 则有

$$\begin{aligned} x'_j &= F_1(h_j) = \sum_{i=0}^l v_{1,i} \cdot h_j^i = x_j, \quad y'_j = F_2(h_j) = \sum_{i=0}^l v_{2,i} \cdot h_j^i = y_j, \\ C'_j &= (x'_j, y'_j) = (x_j, y_j) = C_j = \beta \cdot (P_{pub} + h_j \cdot P_1), \\ \theta' &= e(C'_j, sk_{id_j}) = e(\beta \cdot (P_{pub} + h_j \cdot P_1), \frac{s}{(s + H_1(id_j || hid))} \cdot P_2) = e(\beta P_1, s P_2) = u^\beta = \theta, \\ \gamma' &= \frac{c'_0}{c'_2 H_3(\theta')} = \frac{\gamma \cdot e(r \cdot (P_{pub} + H_1(id_o || hid) \cdot P_1), \alpha \cdot H_3(\theta) \cdot H_4(\prod_{i=1}^n (H_1(id_o || hid) + H_2(w'_i))))}{e(\alpha \cdot (P_{pub} + H_1(id_o || hid) \cdot P_1), r \cdot H_4(\prod_{i=1}^n (H_1(id_o || hid) + H_2(w_i))))^{H_3(\theta')}} = \gamma. \end{aligned}$$

故可得  $K' = KDF(\gamma' || id_o) = K' = KDF(\gamma || id_o) = K$ .

### 4.3 SM9-IB-CBPRES<sup>+</sup> 具体构造

在 SM9-IB-CBPRES 中, 云服务器成功执行重加密操作的前提在于  $W = W'$ , 即初始密文与重加密密钥中条件集合须完全一致. 尽管集合承诺思想的采用使得 SM9-IB-CBPRES 压缩多个条件至单一群元素的同时无需条件值按序相等, 但其本质仍旧为通过“与”门结构实现授权控制, 致使灵活性受限. 本小节结合密钥策略属性基加密思想对 SM9-IB-CBPRES 进行扩展, 给出 SM9-IB-CBPRES<sup>+</sup> 方案, 以实现策略控制下的细粒度授权. 具体来说, 重加密密钥中的条件集合被实例化为一个由单调张成方案表达的单调访问结构  $\mathbb{W} = (A, \rho)$  (称为授权策略), 数据拥有者根据该策略对私钥及用于盲化的  $\alpha \cdot H_3(\theta) \cdot P'_2$  进行分割. 同时, 初始密文被附加一组对应于条件集合  $W = \{w_1, \dots, w_n\}$  的条件控制密文  $\{c_{2,i}, c_{3,i}\}_{i \in [1,n]}$ . 这样, 将 SM9-IB-CBPRES 中的条件集合一致性匹配优化为策略满足机制, 即只有当初始密文中  $W$  满足重加密密钥中  $(A, \rho)$  时, 云服务器才能够生成正确的重加密密文. SM9-IB-CBPRES<sup>+</sup> 具体构造如下所示.

• **Setup**( $\lambda$ )  $\rightarrow (pp, msk)$ . 该算法与 SM9-IB-CBPRES 中算法 **Setup** 相同, 除了  $pp$  中额外包含生成元  $P'_2, P''_2 \in \mathbb{G}_2$  且不包含  $H_4$ .

• **Extract**( $msk, id$ )  $\rightarrow sk_{id}$ . 该算法与 SM9-IB-CBPRES 中算法 **Extract** 相同.

• **Encrypt**( $id_o, W$ )  $\rightarrow (C_{id_o}, K)$ . 给定数据拥有者标识  $id_o$  和条件集合  $W = \{w_1, \dots, w_n\}$ , DO 执行:

- (1) 随机选择  $r, k_{w_1}, \dots, k_{w_n} \in \mathbb{Z}_N^*$ , 计算  $\gamma = u^r$ ,  $c_0 = r \cdot (P_{pub} + H_1(id_o || hid) \cdot P_1)$ ,  $c_1 = r P'_2$ ;
- (2) 对于  $i \in [1, n]$ , 计算  $c_{2,w_i} = r P''_2 + k_{w_i} \cdot (P'_2 + H_2(w_i) \cdot P_2)$ ,  $c_{3,w_i} = k_{w_i} \cdot (P_{pub} + H_1(id_o || hid) \cdot P_1)$ ;
- (3) 输出初始密文  $C_{id_o} = (c_0, c_1, \{c_{2,w_i}, c_{3,w_i}\}_{i \in [1,n]})$  和封装密钥  $K = KDF(\gamma || id_o)$ .

•  $\text{Re-KeyGen}(id_o, sk_{id_o}, R, W') \rightarrow RK_{id_o \rightarrow R}$ . 给定数据拥有者标识和私钥  $(id_o, sk_{id_o})$ , 数据请求者标识集合  $R = \{id_0, \dots, id_l\}$  和条件集合  $W' = (A, \rho)$ , 其中  $A$  是一个  $n_1 \times n_2$  的矩阵,  $\rho$  映射  $A$  的第  $i$  行  $A_i = (A_{i,1}, \dots, A_{i,n_2})$  为一个条件值, DO 执行:

- (1) 随机选择  $\alpha, \beta, r_2, \dots, r_{n_2}, t_2, \dots, t_{n_2}, z_1, \dots, z_{n_1} \in \mathbb{Z}_N^*$ , 计算  $\theta = u^\beta$ ;
- (2) 对于  $i \in [0, l]$ , 计算  $h_i = H_1(id_i || hid)$ ,  $C_i = \beta \cdot (P_{pub} + h_i \cdot P_1) = (x_i, y_i)$ ;
- (3) 通过拉格朗日插值生成多项式  $F_1(x) = \sum_{i=0}^l x_i \cdot \prod_{0 \leq k \neq i \leq l} \frac{x-h_k}{h_i-h_k} = \sum_{i=0}^l v_{1,i} \cdot x^i \in \mathbb{F}_p[x]$  和  $F_2(x) = \sum_{i=0}^l y_i \cdot \prod_{0 \leq k \neq i \leq l} \frac{x-h_k}{h_i-h_k} = \sum_{i=0}^l v_{2,i} \cdot x^i \in \mathbb{F}_p[x]$ , 设定  $rk_0 = (v_{1,0}, \dots, v_{1,l}, v_{2,0}, \dots, v_{2,l})$ ;
- (4) 计算  $rk_1 = \alpha \cdot (P_{pub} + H_1(id_o || hid) \cdot P_1)$ ;
- (5) 对于  $i \in [1, n_1]$ , 计算  $rk_{2,i} = A_{i,1} \cdot sk_{id_o} + \sum_{j=2}^{n_2} A_{i,j} \cdot t_j \cdot P_2 + A_{i,1} \cdot \alpha \cdot H_3(\theta) \cdot P'_2 + \sum_{j=2}^{n_2} A_{i,j} \cdot r_j \cdot P'_2 + z_i P''_2$ ,  $rk_{3,i} = z_i \cdot (P'_2 + H_2(\rho(i)) \cdot P_2)$ ,  $rk_{4,i} = z_i \cdot (P_{pub} + H_1(id_o || hid) \cdot P_1)$ ;
- (6) 输出重加密密钥  $RK_{id_o \rightarrow R} = (rk_0, rk_1, \{rk_{2,i}, rk_{3,i}, rk_{4,i}\}_{i \in [1, n_1]})$ .

•  $\text{Re-Encrypt}(C_{id_o}, W, RK_{id_o \rightarrow R}, W') \rightarrow RK_{id_o \rightarrow R}$ . 给定初始密文  $C_{id_o}$  和对应的条件集合  $W$  以及重加密密钥  $RK_{id_o \rightarrow R}$  和对应的条件集合  $W' = (A, \rho)$ , 若  $W$  与  $W'$  不匹配, 即  $W$  不满足  $(A, \rho)$ , CS 输出  $\perp$ . 否则, CS 执行:

- (1) 定义集合  $I = \{i | \rho(i) \in W\} \subseteq \{1, \dots, n_1\}$ , 则存在一组常量  $\{m_i\}_{i \in I}$  使得  $\sum_{i \in I} m_i A_i = (1, 0, \dots, 0)$ ;
- (2) 计算  $c'_0 = e(c_0, \prod_{i \in I} m_i \cdot rk_{2,i}) \cdot \prod_{i \in I} \frac{e(m_i \cdot c_{3, \rho(i)}, rk_{3,i})}{e(m_i \cdot rk_{4,i}, c_{2, \rho(i)})}$ ,  $c'_1 = rk_0$ ,  $c'_2 = e(rk_1, c_1)$ ;
- (3) 输出重加密密文  $C'_R = (c'_0, c'_1, c'_2)$ .

- $\text{Decrypt}(C_{id_o}, id_o, sk_{id_o}) \rightarrow K'$ . 该算法与 SM9-IB-CBPRES 中算法 Decrypt 相同.
- $\text{Re-Decrypt}(C'_R, id_j, sk_{id_j}) \rightarrow K'$ . 该算法与 SM9-IB-CBPRES 中算法 Re-Decrypt 相同.

#### 4.4 SM9-IB-CBPRES<sup>+</sup> 正确性分析

算法 Decrypt 正确性分析与 SM9-IB-CBPRES 相同.

**算法 Re-Decrypt 正确性分析.** 假设  $C_{id_o} = (c_0, c_1, \{c_{2,w_i}, c_{3,w_i}\}_{i \in [1, n]})$  为正确的初始密文, 对应数据拥有者标识和条件集合分别为  $id_o$  和  $W = \{w_1, \dots, w_n\}$ ;  $RK_{id_o \rightarrow R} = (rk_0, rk_1, rk_2)$  为正确的重加密密钥, 对应数据拥有者标识、条件集合和数据请求者标识集合分别为  $id_o$ 、 $W' = (A, \rho)$  和  $R = \{id_0, \dots, id_l\}$ . 若  $W$  满足  $(A, \rho)$ , 则对于集合  $I = \{i | \rho(i) \in W\} \subseteq \{1, \dots, n_1\}$ , 存在一组常量  $\{m_i\}_{i \in I}$  使得  $\sum_{i \in I} m_i A_i = (1, 0, \dots, 0)$ . 那么  $c'_0$  中含用户私钥的部分可基于单调张成方案恢复为

$$\begin{aligned} \prod_{i \in I} m_i \cdot rk_{2,i} &= \prod_{i \in I} m_i \cdot (A_{i,1} \cdot sk_{id_o} + \sum_{j=2}^{n_2} A_{i,j} \cdot t_j \cdot P_2 + A_{i,1} \cdot \alpha \cdot H_3(\theta) \cdot P'_2 + \sum_{j=2}^{n_2} A_{i,j} \cdot r_j \cdot P'_2 + z_i P''_2) \\ &= sk_{id_o} + \alpha \cdot H_3(\theta) \cdot P'_2 + \prod_{i \in I} m_i \cdot z_i P''_2, \end{aligned}$$

故, 可得

$$\begin{aligned} e(c_0, \prod_{i \in I} m_i \cdot rk_{2,i}) &= e(r \cdot (P_{pub} + H_1(id_o || hid) \cdot P_1), sk_{id_o} + \alpha \cdot H_3(\theta) \cdot P'_2 + \prod_{i \in I} m_i \cdot z_i P''_2) \\ &= \gamma \cdot e(P_{pub} + H_1(id_o || hid) \cdot P_1, r \cdot \alpha \cdot H_3(\theta) \cdot P'_2 + r \cdot \prod_{i \in I} m_i \cdot z_i P''_2), \end{aligned}$$

同时,  $e(P_{pub} + H_1(id_o||hid) \cdot P_1, r \cdot \prod_{i \in I} m_i \cdot z_i P_2'')$  可通过  $\prod_{i \in I} \frac{e(m_i \cdot c_{3,\rho(i)}, rk_{3,i})}{e(m_i \cdot rk_{4,i}, c_{2,\rho(i)})}$  消除, 即

$$\begin{aligned} \prod_{i \in I} \frac{e(m_i \cdot c_{3,\rho(i)}, rk_{3,i})}{e(m_i \cdot rk_{4,i}, c_{2,\rho(i)})} &= \prod_{i \in I} \frac{e(m_i \cdot k_{\rho(i)} \cdot (P_{pub} + H_1(id_o||hid) \cdot P_1), z_i \cdot (P_2' + H_2(\rho(i)) \cdot P_2))}{e(m_i \cdot z_i \cdot (P_{pub} + H_1(id_o||hid) \cdot P_1), rP_2'' + k_{\rho(i)} \cdot (P_2' + H_2(\rho(i)) \cdot P_2))} \\ &= \frac{1}{e(\prod_{i \in I} m_i \cdot z_i \cdot (P_{pub} + H_1(id_o||hid) \cdot P_1), rP_2'')}, \end{aligned}$$

因此, 重加密密文  $C'_R$  为

$$\begin{aligned} c'_0 &= e(c_0, \prod_{i \in I} m_i \cdot rk_{2,i}) \cdot \prod_{i \in I} \frac{e(m_i \cdot c_{3,\rho(i)}, rk_{3,i})}{e(m_i \cdot rk_{4,i}, c_{2,\rho(i)})} \\ &= \frac{\gamma \cdot e(P_{pub} + H_1(id_o||hid) \cdot P_1, r \cdot \alpha \cdot H_3(\theta) \cdot P_2' + r \cdot \prod_{i \in I} m_i \cdot z_i P_2'')}{e(\prod_{i \in I} m_i \cdot z_i \cdot (P_{pub} + H_1(id_o||hid) \cdot P_1), rP_2'')} \\ &= \gamma \cdot e(r \cdot (P_{pub} + H_1(id_o||hid) \cdot P_1), \alpha \cdot H_3(\theta) \cdot P_2'), \\ c'_1 &= (v_{1,0}, \dots, v_{1,l}, v_{2,0}, \dots, v_{2,l}), \\ c'_2 &= e(rk_1, c_1) = e(\alpha \cdot (P_{pub} + H_1(id_o||hid) \cdot P_1), rP_2'). \end{aligned}$$

若第  $j$  个数据请求者标识  $id_j \in R$ , 则有

$$\begin{aligned} x'_j &= F_1(h_j) = \sum_{i=0}^l v_{1,i} \cdot h_j^i = x_j, \quad y'_j = F_2(h_j) = \sum_{i=0}^l v_{2,i} \cdot h_j^i = y_j, \\ C'_j &= (x'_j, y'_j) = (x_j, y_j) = C_j = \beta \cdot (P_{pub} + h_j \cdot P_1), \\ \theta' &= e(C'_j, sk_{id_j}) = e(\beta \cdot (P_{pub} + h_j \cdot P_1), \frac{s}{(s + H_1(id_j||hid))} \cdot P_2) = e(\beta P_1, sP_2) = u^\beta = \theta, \\ \gamma' &= \frac{c'_0}{c_2^{H_3(\theta')}} = \frac{\gamma \cdot e(r \cdot (P_{pub} + H_1(id_o||hid) \cdot P_1), \alpha \cdot H_3(\theta) \cdot P_2')}{e(\alpha \cdot (P_{pub} + H_1(id_o||hid) \cdot P_1), rP_2')^{H_3(\theta')}} = \gamma. \end{aligned}$$

故可得  $K' = KDF(\gamma' || id_o) = K' = KDF(\gamma || id_o) = K$ .

## 5 安全性分析

SM9-IB-CBPRES 和 SM9-IB-CBPRES<sup>+</sup> 方案应满足密文不可区分性和私钥抗泄露性. 前者旨在保障静态选择明文攻击下数据机密性, 后者旨在防止由数据请求者与云服务器合谋引发的用户私钥泄露.

### 5.1 SM9-IB-CBPRES 安全性分析

SM9-IB-CBPRES 方案密文不可区分性通过定理 1 证明. 该方案在 SM9 封装密文  $c_0$  基础上增加条件控制密文  $c_1$  构成初始密文. 基于  $q$ -DBDHI 假设, 引理 1 证明了敌手无法区分真实封装密钥与随机封装密钥, 实现初始密文不可区分性. 该方案中重加密密文由 SM9 广播封装密文  $c'_1$  和由广播封装密钥  $\theta$  盲化后的封装密钥  $\gamma$  组成. 引理 2 证明了在  $q$ -DBDHI 假设下敌手无法区分真实广播封装密钥与随机广播封装密钥, 实现重加密密文不可区分性. 同时, 通过在重加密密钥中引入随机因子  $\alpha$ , 即  $rk_2 = sk_{id_o} + \alpha \cdot H_3(\theta) \cdot H_4(\Lambda_{W'})$ , 方案确保即使  $\theta$  泄漏也无法提取  $sk_{id_o}$ . 基于  $q$ -SDH 假设, 定理 2 证明了敌手无法输出挑战标识下有效私钥, 满足私钥抗泄露性.

**定理 1** 令方案中的哈希函数  $H_1$  和  $H_4$  为随机谕言机, 若  $q$ -DBDHI 假设成立, 则 SM9-IB-CBPRES 方案满足 IND-sID-CPA 安全性.

**证明** 该定理由引理 1 和引理 2 证明.

**引理 1** 假定存在敌手  $\mathcal{A}$  能够以不可忽略的优势  $\epsilon$  赢得 IND-sID-CPA-Or 游戏, 则存在算法  $\mathcal{B}$  能够以不可忽略的优势解  $q$ -DBDHI 问题.

**证明** 给定  $q$ -DBDHI 实例  $(P, Q, aQ, \dots, a^q Q, Z)$ ,  $\mathcal{B}$  的目标是判断  $Z = e(P, Q)^{\frac{1}{a}}$  是否成立.

• **初始化.**  $\mathcal{A}$  输出挑战标识  $id^*$  和条件集合  $W^* = \{w_1^*, \dots, w_n^*\}$ .  $\mathcal{B}$  随机选择  $\kappa_1, \dots, \kappa_{q-1}, \kappa^* \in \mathbb{Z}_N^*$ , 计算  $\xi_i = \kappa^* - \kappa_i$ , 其中  $i \in [1, q-1]$ .  $\mathcal{B}$  生成多项式  $f(x) = \prod_{i=1}^{q-1} (x - \xi_i) = \sum_{i=0}^{q-1} \vartheta_i \cdot x^i$ , 隐式设定  $s = (a - \kappa^*)$ , 计算  $P_2 = f(a) \cdot Q = \sum_{i=0}^{q-1} \vartheta_i \cdot a^i Q$ ,  $P_1 = \varphi(P_2)$ ,  $I = a \cdot P_2 = \sum_{i=0}^{q-1} \vartheta_i \cdot a^{i+1} Q$ ,  $P_{pub} = \varphi(I - \kappa^* \cdot P_2) = \varphi((a - \kappa^*) \cdot P_2) = (a - \kappa^*) \cdot P_1 = s \cdot P_1$ ,  $u = e(P_{pub}, P_2)$ ,  $\Lambda_{W^*} = \prod_{i=1}^n (\kappa^* + H_2(w_i^*))$ .  $\mathcal{B}$  返回公共参数  $pp$  给  $\mathcal{A}$ .

• **询问阶段 1.**  $\mathcal{A}$  能够适应性地进行随机谕言机  $H_1$  和  $H_4$  询问, 私钥询问和重加密密钥询问.

- (1)  $H_1$  询问.  $\mathcal{B}$  维护由元组  $(id_i, \kappa_i)$  构成的初始为空的列表  $\mathcal{L}_{H_1}$ . 当  $\mathcal{A}$  对  $id_i$  进行  $H_1$  询问时, 若  $(id_i, \kappa_i) \in \mathcal{L}_{H_1}$ ,  $\mathcal{B}$  返回  $\kappa_i$  给  $\mathcal{A}$ . 否则, 当  $id_i = id^*$  时,  $\mathcal{B}$  添加  $(id_i, \kappa^*)$  至  $\mathcal{L}_{H_1}$  中并返回  $\kappa^*$  给  $\mathcal{A}$ ; 当  $id_i \neq id^*$ ,  $\mathcal{B}$  添加  $(id_i, \kappa_i)$  至  $\mathcal{L}_{H_1}$  中并返回  $\kappa_i$  给  $\mathcal{A}$ .
- (2)  $H_4$  询问.  $\mathcal{B}$  维护由元组  $(\Lambda_{W_i}, \mu_i, \Gamma_i)$  构成的初始为空的列表  $\mathcal{L}_{H_4}$ . 当  $\mathcal{A}$  对  $\Lambda_{W_i}$  进行  $H_4$  询问时, 若  $(\Lambda_{W_i}, \mu_i, \Gamma_i) \in \mathcal{L}_{H_4}$ ,  $\mathcal{B}$  返回  $\Gamma_i$  给  $\mathcal{A}$ . 否则, 当  $\Lambda_{W_i} = \Lambda_{W^*}$  时,  $\mathcal{B}$  随机选择  $\mu^* \in \mathbb{Z}_N^*$ , 计算  $\Gamma^* = \mu^* \cdot I$ , 添加  $(\Lambda_{W^*}, \mu^*, \Gamma^*)$  至  $\mathcal{L}_{H_4}$  中并返回  $\Gamma^*$  给  $\mathcal{A}$ . 当  $\Lambda_{W_i} \neq \Lambda_{W^*}$  时,  $\mathcal{B}$  随机选择  $\mu_i \in \mathbb{Z}_N^*$ , 计算  $\Gamma_i = (\mu_i + 1) \cdot I - \kappa^* \cdot P_2$ , 添加  $(\Lambda_{W_i}, \mu_i, \Gamma_i)$  至  $\mathcal{L}_{H_4}$  中并返回  $\Gamma_i$  给  $\mathcal{A}$ .
- (3) 私钥询问.  $\mathcal{B}$  维护由元组  $(id_i, sk_{id_i})$  构成的初始为空的列表  $\mathcal{L}_{sk}$ . 当  $\mathcal{A}$  对  $id_i$  进行私钥询问时, 其中  $id_i \neq id^*$ , 若  $(id_i, sk_{id_i}) \in \mathcal{L}_{sk}$ ,  $\mathcal{B}$  返回  $sk_{id_i}$  给  $\mathcal{A}$ . 否则,  $\mathcal{B}$  生成多项式  $f_i(x) = \prod_{j=1, j \neq i}^{q-1} (x - \xi_j) = \sum_{j=0}^{q-2} \vartheta_{i,j} \cdot x^j$ , 计算  $sk_{id_i} = f_i(a) \cdot Q = \sum_{j=0}^{q-2} \vartheta_{i,j} \cdot a^j Q$ , 添加  $(id_i, sk_{id_i})$  至  $\mathcal{L}_{sk}$  中并返回给  $\mathcal{A}$ .
- (4) 重加密密钥询问. 当  $\mathcal{A}$  对  $(id_i, R_i = \{id_{i_0}, \dots, id_{i_l}\}, W_i = \{w_{i_1}, \dots, w_{i_n}\})$  进行重加密密钥询问时, 若  $(id_i, sk_{id_i}) \notin \mathcal{L}_{sk}$ ,  $\mathcal{B}$  对  $id_i$  进行私钥询问. 若  $id_i = id^*$ , 则  $\Lambda_{W_i} = \prod_{j=i_1}^{i_n} (\kappa^* + H_2(w_j)) \neq \Lambda_{W^*}$ ,  $\mathcal{B}$  随机选择  $\beta \in \mathbb{Z}_N^*$ , 计算  $\theta = u^\beta$ , 提取  $(\Lambda_{W_i}, \mu_i, \Gamma_i) \in \mathcal{L}_{H_4}$ , 隐式设定  $\alpha = -\frac{1}{H_3(\theta) \cdot a}$ ; 对于  $j \in [i_0, i_l]$ , 提取  $(id_j, \kappa_j) \in \mathcal{L}_{H_1}$ , 计算  $C_j = \beta \cdot (P_{pub} + \kappa_j \cdot P_1) = (x_j, y_j)$ ; 通过拉格朗日插值生成多项式  $F_1(x) = \sum_{j=i_0}^{i_l} x_j \cdot \prod_{0 \leq k \neq j \leq l} \frac{x - \kappa_k}{\kappa_j - \kappa_k} = \sum_{j=0}^{i_l} v_{i,1,j} \cdot x^j \in \mathbb{F}_p[x]$  和  $F_2(x) = \sum_{j=i_0}^{i_l} y_j \cdot \prod_{0 \leq k \neq j \leq l} \frac{x - \kappa_k}{\kappa_j - \kappa_k} = \sum_{j=0}^{i_l} v_{i,2,j} \cdot x^j \in \mathbb{F}_p[x]$ , 设定  $rk_0 = (v_{i,1,0}, \dots, v_{i,1,i_l}, v_{i,2,0}, \dots, v_{i,2,i_l})$ ; 计算  $rk_1 = -\frac{1}{H_3(\theta)} \cdot P_1$ ,  $rk_2 = -\mu_i \cdot P_2$ ; 返回  $RK_{id^* \rightarrow R_i} = (rk_0, rk_1, rk_2)$  给  $\mathcal{A}$ . 若  $id_i \neq id^*$ , 当  $(id_i, sk_{id_i}) \notin \mathcal{L}_{sk}$ ,  $\mathcal{B}$  对  $id_i$  进行私钥询问. 随后,  $\mathcal{B}$  运行  $\text{Re-KeyGen}(id_i, sk_{id_i}, R_i, W_i) \rightarrow RK_{id_i \rightarrow R_i}$  并返回  $RK_{id_i \rightarrow R_i}$  给  $\mathcal{A}$ .

• **挑战.**  $\mathcal{B}$  随机选择  $r \in \mathbb{Z}_N^*$ , 定义多项式  $\Phi(x) = x \cdot g(x) = r \cdot \kappa^* \cdot (f(x))^2 + \eta = \sum_{i=0}^{2q-2} \phi_i \cdot x^i$ , 则有  $r \cdot \kappa^* \cdot (f(x))^2 \cdot x^{-1} = g(x) - \eta \cdot x^{-1}$ , 其中  $\eta \in \mathbb{Z}_N^*$ ,  $g(x)$  为  $2q-3$  阶多项式且  $e(P, Q)^{g(a)}$  可计算. 随后,  $\mathcal{B}$  提取  $(\Lambda_{W^*}, \mu^*, \Gamma^*) \in \mathcal{L}_{H_4}$ ; 计算  $\gamma^* = \frac{Z^\eta \cdot e(P_1, P_2)^r}{e(P, Q)^{g(a)}}$ ,  $c_0^* = r \cdot P_1$ ,  $c_1^* = r \cdot \mu^* \cdot P_2$ ,  $C_{id^*} = (c_0^*, c_1^*)$ ,  $K^* = \text{KDF}(\gamma^* || id^*)$ ; 随机选择  $b \in \{0, 1\}$ , 设定  $K_b^* = K^*$ ; 从封装密钥空间中随机选取  $K_{1-b}^*$ ; 返回  $(C_{id^*}, K_0^*, K_1^*)$  给  $\mathcal{A}$ .

• **询问阶段 2.**  $\mathcal{A}$  继续进行询问阶段 1 中的询问.

• **猜测.**  $\mathcal{A}$  输出猜测  $b'$ . 若  $b' = b$ , 则  $\mathcal{A}$  赢得游戏.

如果  $Z = e(P, Q)^{\frac{1}{a}}$ , 设  $r^* = \frac{r}{a}$ , 则

$$c_0^* = r \cdot P_1 = \frac{r}{a} \cdot (a - \kappa^* + \kappa^*) \cdot P_1 = r^* \cdot (s + \kappa^*) \cdot P_1 = r^* \cdot (P_{pub} + \kappa^* \cdot P_1),$$

$$c_1^* = r \cdot \mu^* \cdot P_2 = \frac{r}{a} \cdot \mu^* \cdot a P_2 = r^* \cdot \mu^* \cdot I = r^* \cdot H_4\left(\prod_{i=1}^n (H_1(id^* || hid) + H_2(w_i^*))\right),$$

$$\gamma^* = \frac{Z^\eta \cdot e(P_1, P_2)^r}{e(P, Q)^{g(a)}} = \frac{e(P_1, P_2)^r}{e(P, Q)^{g(a) - \frac{\eta}{a}}} = \frac{e(P_1, P_2)^r}{e(P, Q)^{\frac{r \cdot \kappa^* \cdot (f(a))^2}{a}}} = e(P_1, P_2)^{r - \frac{r \cdot \kappa^*}{a}} = e(P_1, P_2)^{(a - \kappa^*) \cdot \frac{r}{a}} = u^{r^*}.$$

因此,  $C_{id^*}$  是  $K_b^*$  的有效封装密文, 则  $\Pr[b' = b] = \frac{1}{2} + \epsilon$ .

如果  $Z \neq e(P, Q)^{\frac{1}{a}}$ , 由于  $Z$  是群  $\mathbb{G}_T$  中的随机元素, 那么  $\gamma^*$  为均匀随机的, 则  $K_b^*$  与  $C_{id^*}$  独立且无关, 即  $\Pr[b' = b] = \frac{1}{2}$ .

综上, 若  $\mathcal{A}$  以优势  $\epsilon$  赢得 IND-sID-CPA-Or 游戏, 则  $\mathcal{B}$  解  $q$ -DBDHI 问题优势为

$$\text{Adv}_{\mathcal{B}}^{q\text{-DBDHI}} = \left| \Pr[b' = b | Z = e(P, Q)^{\frac{1}{a}}] - \Pr[b' = b | Z \neq e(P, Q)^{\frac{1}{a}}] \right| = \left| \frac{1}{2} + \epsilon - \frac{1}{2} \right| = \epsilon.$$

**引理 2** 假定存在敌手  $\mathcal{A}$  能够以不可忽略的优势  $\epsilon$  赢得 IND-sID-CPA-Re 游戏, 则存在算法  $\mathcal{B}$  能够以不可忽略的优势解  $q$ -DBDHI 问题.

**证明** 给定  $q$ -DBDHI 实例  $(P, Q, aQ, \dots, a^q Q, Z)$ ,  $\mathcal{B}$  的目标是判断  $Z = e(P, Q)^{\frac{1}{a}}$  是否成立. 首先证明当  $l = 1$  时, 即挑战标识集合  $R^* = \{id^*\}$ , 若  $\mathcal{A}$  能够以不可忽略的优势  $\epsilon_1$  赢得 IND-sID-CPA-Re 游戏, 则  $\mathcal{B}$  能够通过调用  $\mathcal{A}$  来解  $q$ -DBDHI 问题.

- **初始化.**  $\mathcal{A}$  输出挑战标识集合  $R^* = \{id^*\}$ . 其它设置与引理 1 相同.
- **询问阶段 1.**  $\mathcal{A}$  能够适应性地进行随机谕言机  $H_1$  和  $H_4$  询问, 私钥询问和重加密密钥询问, 其中  $H_1$  询问和私钥询问的响应与引理 1 相同.
  - (1)  $H_4$  询问.  $\mathcal{B}$  维护由元组  $(\Lambda_{W_i}, \mu_i, \Gamma_i)$  构成的初始为空的列表  $\mathcal{L}_{H_4}$ . 当  $\mathcal{A}$  对  $\Lambda_{W_i}$  进行  $H_4$  询问时, 若  $(\Lambda_{W_i}, \mu_i, \Gamma_i) \in \mathcal{L}_{H_4}$ ,  $\mathcal{B}$  返回  $\Gamma_i$  给  $\mathcal{A}$ . 否则,  $\mathcal{B}$  随机选择  $\mu_i \in \mathbb{Z}_N^*$ , 计算  $\Gamma_i = (\mu_i + 1) \cdot I - \kappa^* \cdot P_2$ , 添加  $(\Lambda_{W_i}, \mu_i, \Gamma_i)$  至  $\mathcal{L}_{H_4}$  中并返回  $\Gamma_i$  给  $\mathcal{A}$ .
  - (2) 重加密密钥询问. 当  $\mathcal{A}$  对  $(id_i, R_i = \{id_{i_0}, \dots, id_{i_l}\}, W_i = \{w_{i_1}, \dots, w_{i_n}\})$  进行重加密密钥询问时, 若  $(id_i, sk_{id_i}) \notin \mathcal{L}_{sk}$ ,  $\mathcal{B}$  对  $id_i$  进行私钥询问. 若  $id_i = id^*$ ,  $\mathcal{B}$  随机选择  $\beta \in \mathbb{Z}_N^*$ , 计算  $\theta = u^\beta$ ,  $\Lambda_{W_i} = \prod_{j=i_1}^{i_n} (\kappa^* + H_2(w_j))$ , 提取  $(\Lambda_{W_i}, \mu_i, \Gamma_i) \in \mathcal{L}_{H_4}$ , 隐式设定  $\alpha = \frac{1}{H_3(\theta) \cdot a}$ ; 对于  $j \in [i_0, i_l]$ , 提取  $(id_j, \kappa_j) \in \mathcal{L}_{H_1}$ , 计算  $C_j = \beta \cdot (P_{pub} + \kappa_j \cdot P_1) = (x_j, y_j)$ ; 通过拉格朗日插值生成多项式  $F_1(x) = \sum_{j=i_0}^{i_l} x_j \cdot \prod_{0 \leq k \neq j \leq l} \frac{x - \kappa_k}{\kappa_j - \kappa_k} = \sum_{j=0}^{i_l} v_{i,1,j} \cdot x^j \in \mathbb{F}_p[x]$  和  $F_2(x) = \sum_{j=i_0}^{i_l} y_j \cdot \prod_{0 \leq k \neq j \leq l} \frac{x - \kappa_k}{\kappa_j - \kappa_k} = \sum_{j=0}^{i_l} v_{i,2,j} \cdot x^j \in \mathbb{F}_p[x]$ , 设定  $rk_0 = (v_{i,1,0}, \dots, v_{i,1,i_l}, v_{i,2,0}, \dots, v_{i,2,i_l})$ ; 计算  $rk_1 = -\frac{1}{H_3(\theta)} \cdot P_1$ ,  $rk_2 = -\mu_i \cdot P_2$ ; 返回  $RK_{id^* \rightarrow R_i} = (rk_0, rk_1, rk_2)$  给  $\mathcal{A}$ . 若  $id_i \neq id^*$ , 当  $(id_i, sk_{id_i}) \notin \mathcal{L}_{sk}$ ,  $\mathcal{B}$  对  $id_i$  进行私钥询问. 随后,  $\mathcal{B}$  运行  $\text{Re-KeyGen}(id_i, sk_{id_i}, R_i, W_i) \rightarrow RK_{id_i \rightarrow R_i}$  并返回  $RK_{id_i \rightarrow R_i}$  给  $\mathcal{A}$ .
- **挑战.**  $\mathcal{B}$  随机选择标识  $id$  和条件集合  $W_i = W'_i = \{w_{i_1}, \dots, w_{i_n}\}$ ,  $\gamma^* \in \mathbb{G}_T$ ,  $r^*, \alpha^*, \beta \in \mathbb{Z}_N^*$ , 定义多项式  $\Phi(x) = x \cdot g(x) = \beta \cdot \kappa^* \cdot (f(x))^2 + \eta = \sum_{i=0}^{2q-2} \phi_i \cdot x^i$ , 则有  $\beta \cdot \kappa^* \cdot (f(x))^2 \cdot x^{-1} = g(x) - \eta \cdot x^{-1}$ , 其中  $\eta \in \mathbb{Z}_N^*$ ,  $g(x)$  为  $2q-3$  阶多项式且  $e(P, Q)^{g(a)}$  可计算. 随后,  $\mathcal{B}$  计算  $\Lambda_W = \prod_{i=1}^{i_n} (H_1(id || hid) + H_2(w_i))$ , 提取  $(\Lambda_{W_i}, \mu_i, \Gamma_i) \in \mathcal{L}_{H_4}$ ; 计算  $\theta^* = \frac{Z^{\eta \cdot e(P_1, P_2)^\beta}}{e(P, Q)^{g(a)}}$ ,  $C_1^* = \beta \cdot P_1 = (x_1^*, y_1^*)$ ,  $c_0^* = \gamma^* \cdot e(r^* \cdot (P_{pub} + H_1(id || hid) \cdot P_1), \alpha^* \cdot H_3(\theta^*) \cdot \Gamma_i)$ ,  $c_2^* = e(\alpha^* \cdot (P_{pub} + H_1(id || hid) \cdot P_1), r^* \cdot \Gamma_i)$ ,  $K^* = \text{KDF}(\gamma^* || id)$ ; 设定  $c_1^* = (v_{1,0}^* = x_1^*, v_{2,0}^* = y_1^*)$ ,  $C_{R^*}' = (c_0^*, c_1^*, c_2^*)$ ; 随机选择  $b \in \{0, 1\}$ , 设定  $K_b^* = K^*$ ; 从封装密钥空间中随机选取  $K_{1-b}^*$ ; 返回  $(C_{R^*}', K_0^*, K_1^*)$  给  $\mathcal{A}$ .

- **询问阶段 2.**  $\mathcal{A}$  继续进行询问阶段 1 中的询问.
- **猜测.**  $\mathcal{A}$  输出猜测  $b'$ . 若  $b' = b$ , 则  $\mathcal{A}$  赢得游戏.

类似于引理 1 分析, 当  $l = 1$  时,  $\mathcal{B}$  解  $q$ -DBDHI 问题优势为

$$\text{Adv}_{\mathcal{B}}^{q\text{-DBDHI}} = \left| \Pr[b' = b | Z = e(P, Q)^{\frac{1}{a}}] - \Pr[b' = b | Z \neq e(P, Q)^{\frac{1}{a}}] \right| = \left| \frac{1}{2} + \epsilon_1 - \frac{1}{2} \right| = \epsilon_1.$$

结合文献 [42](定理 4.1) 可得  $\text{Adv}_{\mathcal{A}, \text{SM9-IB-CBPRE}}^{\text{IND-sID-CPA-Re}} \leq l \cdot \epsilon_1 = l \cdot \text{Adv}_{\mathcal{B}}^{q\text{-DBDHI}}$ .

综上, 若  $\mathcal{A}$  以优势  $\epsilon$  赢得 IND-sID-CPA-Re 游戏, 则  $\mathcal{B}$  解  $q$ -DBDHI 问题优势  $\text{Adv}_{\mathcal{B}}^{q\text{-DBDHI}} \geq \frac{\epsilon}{l}$ .

**定理 2** 令方案中的哈希函数  $H_1$  和  $H_4$  为随机谕言机, 若  $q$ -SDH 假设成立, 则 SM9-IB-CBPRES 方案满足 LR-CA 安全性.

**证明** 假定存在敌手  $\mathcal{A}$  能够以不可忽略的优势  $\epsilon$  赢得 LR-CA 游戏, 则存在算法  $\mathcal{B}$  能够以不可忽略的优势解  $q$ -SDH 问题. 给定  $q$ -SDH 实例  $(P, Q, aQ, \dots, a^q Q)$ ,  $\mathcal{B}$  的目标是输出  $(\omega, \frac{1}{a+\omega} \cdot P) \in \mathbb{Z}_N^* \times \mathbb{G}_1$ .

• **初始化.**  $\mathcal{A}$  输出挑战标识  $id^*$ .  $\mathcal{B}$  随机选择  $\kappa_1, \dots, \kappa_{q-1}, \kappa^*, \mu \in \mathbb{Z}_N^*$ , 计算  $\xi_i = \kappa^* - \kappa_i$ , 其中  $i \in [1, q-1]$ .  $\mathcal{B}$  生成多项式  $f(x) = \prod_{i=1}^{q-1} (x + \kappa_i) = \sum_{i=0}^{q-1} \vartheta_i \cdot x^i$ , 隐式设定  $s = a$ ; 计算  $P_2 = f(a) \cdot Q = \sum_{i=0}^{q-1} \vartheta_i \cdot a^i Q$ ,  $P_1 = \varphi(P_2)$ ,  $P'_2 = \mu P_2$ ,  $P_{pub} = \varphi(\sum_{i=0}^{q-1} \vartheta_i \cdot a^{i+1} Q) = \varphi(a \cdot P_2) = s \cdot P_1$ ,  $u = e(P_{pub}, P_2)$ ; 返回公共参数  $pp$  给  $\mathcal{A}$ .

• **询问阶段 1.**  $\mathcal{A}$  能够适应性地进行随机谕言机  $H_1$  和  $H_4$  询问, 私钥询问和重加密密钥询问, 其中  $H_1$  询问的响应与引理 1 相同.

(1)  $H_4$  询问.  $\mathcal{B}$  维护由元组  $(\Lambda_{W_i}, \mu_i, \Gamma_i)$  构成的初始为空的列表  $\mathcal{L}_{H_4}$ . 当  $\mathcal{A}$  对  $\Lambda_{W_i}$  进行  $H_4$  询问时, 若  $(\Lambda_{W_i}, \mu_i, \Gamma_i) \in \mathcal{L}_{H_4}$ ,  $\mathcal{B}$  返回  $\mu_i \cdot P_2$  给  $\mathcal{A}$ . 否则,  $\mathcal{B}$  随机选择  $\mu_i \in \mathbb{Z}_N^*$ , 添加  $(\Lambda_{W_i}, \mu_i, \Gamma_i)$  至  $\mathcal{L}_{H_4}$  中并返回  $\mu_i \cdot P_2$  给  $\mathcal{A}$ .

(2) 私钥询问.  $\mathcal{B}$  维护由元组  $(id_i, sk_{id_i})$  构成的初始为空的列表  $\mathcal{L}_{sk}$ . 当  $\mathcal{A}$  对满足  $id_i \neq id^*$  的  $id_i$  进行私钥询问时, 若  $(id_i, sk_{id_i}) \in \mathcal{L}_{sk}$ ,  $\mathcal{B}$  返回  $sk_{id_i}$  给  $\mathcal{A}$ ; 否则, 生成多项式  $f_i(x) = \prod_{j=1, j \neq i}^{q-1} (x + \kappa_j) = \sum_{j=0}^{q-2} \vartheta_{i,j} \cdot x^j$ , 计算  $sk_{id_i} = a \cdot f_i(a) \cdot Q = \sum_{j=0}^{q-2} \vartheta_{i,j} \cdot a^{j+1} Q$ , 添加  $(id_i, sk_{id_i})$  至  $\mathcal{L}_{sk}$  中并返回给  $\mathcal{A}$ .

(3) 重加密密钥询问. 当  $\mathcal{A}$  对  $(id_i, R_i = \{id_{i_0}, \dots, id_{i_l}\}, W_i = \{w_{i_1}, \dots, w_{i_n}\})$  进行重加密密钥询问时, 若  $id_i = id^*$ ,  $\mathcal{B}$  随机选择  $\alpha', \beta \in \mathbb{Z}_N^*$ , 计算  $\theta = u^\beta$ ,  $\Lambda_{W_i} = \prod_{j=1}^{i_n} (\kappa^* + H_2(w_j))$ , 提取  $(\Lambda_{W_i}, \mu_i, \Gamma_i) \in \mathcal{L}_{H_4}$ , 隐式设定  $\alpha = \frac{1}{H_3(\theta) \cdot \mu_i} \cdot (\alpha' - \frac{s}{s + \kappa^*})$ ; 对于  $j \in [i_0, i_l]$ , 提取  $(id_j, \kappa_j) \in \mathcal{L}_{H_1}$ , 计算  $C_j = \beta \cdot (P_{pub} + \kappa_j \cdot P_1) = (x_j, y_j)$ ; 通过拉格朗日插值生成多项式  $F_1(x) = \sum_{j=i_0}^{i_l} x_j \cdot \prod_{0 \leq k \neq i \leq l} \frac{x - \kappa_k}{\kappa_j - \kappa_k} = \sum_{j=0}^{i_l} v_{i,1,j} \cdot x^j \in \mathbb{F}_p[x]$  和  $F_2(x) = \sum_{j=i_0}^{i_l} y_j \cdot \prod_{0 \leq k \neq i \leq l} \frac{x - \kappa_k}{\kappa_j - \kappa_k} = \sum_{j=0}^{i_l} v_{i,2,j} \cdot x^j \in \mathbb{F}_p[x]$ , 设定  $rk_0 = (v_{i,1,0}, \dots, v_{i,1,i_l}, v_{i,2,0}, \dots, v_{i,2,i_l})$ ; 计算  $rk_1 = \frac{1}{H_3(\theta) \cdot \mu_i} \cdot (\alpha' \cdot P_{pub} + \alpha' \cdot \kappa^* \cdot P_1 - P_{pub})$ ,  $rk_2 = \alpha' \cdot P_2$ ; 返回  $RK_{id^* \rightarrow R_i} = (rk_0, rk_1, rk_2)$  给  $\mathcal{A}$ . 若  $id_i \neq id^*$ , 当  $(id_i, sk_{id_i}) \notin \mathcal{L}_{sk}$ ,  $\mathcal{B}$  对  $id_i$  进行私钥询问. 随后,  $\mathcal{B}$  运行  $\text{Re-KeyGen}(id_i, sk_{id_i}, R_i, W_i) \rightarrow RK_{id_i \rightarrow R_i}$  并返回  $RK_{id_i \rightarrow R_i}$  给  $\mathcal{A}$ .

• **输出.**  $\mathcal{A}$  输出私钥  $sk'_{id^*}$ . 若  $e(P_{pub} + \kappa^* P_1, sk'_{id^*}) = u$ , 则  $\mathcal{A}$  赢得游戏.  $\mathcal{B}$  定义多项式  $\Phi(x) = x \cdot f(x) = \sum_{i=0}^q \phi_i \cdot x^i$ , 利用长整除法表示  $\Phi(x) = (x + \kappa^*) \cdot g(x) + \eta$ , 其中  $\eta \in \mathbb{Z}_N^*$ ,  $g(x)$  为  $q-1$  阶多项式且  $g(a) \cdot Q$  可计算. 最终,  $\mathcal{B}$  输出  $(\kappa^*, \varphi(\frac{1}{\eta} \cdot (sk'_{id^*} - g(a) \cdot Q)))$  为  $q$ -SDH 实例的解.

由于  $sk'_{id^*} = \frac{s}{s + \kappa^*} \cdot P_2 = \frac{1}{a + \kappa^*} \cdot a \cdot f(a) \cdot Q = \frac{1}{a + \kappa^*} \cdot \Phi(a) \cdot Q$ , 则

$$\varphi(\frac{1}{\eta} \cdot (sk'_{id^*} - g(a) \cdot Q)) = \varphi(\frac{1}{\eta} \cdot (\frac{1}{a + \kappa^*} \cdot \Phi(a) \cdot Q - g(a) \cdot Q)) = \frac{1}{\eta} \cdot \frac{\eta}{a + \kappa^*} \cdot P = \frac{1}{a + \kappa^*} \cdot P.$$

综上, 若  $\mathcal{A}$  以优势  $\epsilon$  赢得 LR-CA 游戏, 则  $\mathcal{B}$  解  $q$ -SDH 问题优势  $\text{Adv}_{\mathcal{B}}^{q\text{-SDH}} = \epsilon$ .

## 5.2 SM9-IB-CBPRES<sup>+</sup> 安全性分析

与 SM9-IB-CBPRES 方案思想相同, 定理 3 在  $q$ -DBDHI 假设下证明 SM9-IB-CBPRES<sup>+</sup> 方案满足密文不可区分性, 即敌手既无法区分真实封装密钥与随机封装密钥又无法区分真实广播封装密钥与随机广播封装密钥. 同时, 基于  $q$ -SDH 假设, 定理 4 证明敌手无法输出挑战标识下有效私钥, 实现私钥抗泄露性.

**定理 3** 令方案中的哈希函数  $H_1$  为随机谕言机, 若  $q$ -DBDHI 假设成立, 则 SM9-IB-CBPRES<sup>+</sup> 方案满足 IND-sID-CPA 安全性.

**证明** 该定理由引理 3 和引理 4 证明.

**引理 3** 假定存在敌手  $\mathcal{A}$  能够以不可忽略的优势  $\epsilon$  赢得 IND-sID-CPA-Or 游戏, 则存在算法  $\mathcal{B}$  能够以不可忽略的优势解  $q$ -DBDHI 问题.

**证明** 给定  $q$ -DBDHI 实例  $(P, Q, aQ, \dots, a^q Q, Z)$ ,  $\mathcal{B}$  的目标是判断  $Z = e(P, Q)^{\frac{1}{a}}$  是否成立.

- **初始化.**  $\mathcal{A}$  输出挑战标识  $id^*$  和条件集合  $W^* = \{w_1^*, \dots, w_n^*\}$ .  $\mathcal{B}$  随机选择  $\kappa_1, \dots, \kappa_{q-1}, \kappa^*, \mu, \nu \in \mathbb{Z}_N^*$ , 计算  $\xi_i = \kappa^* - \kappa_i$ , 其中  $i \in [1, q-1]$ .  $\mathcal{B}$  生成多项式  $f(x) = \prod_{i=1}^{q-1} (x - \xi_i) = \sum_{i=0}^{q-1} \vartheta_i \cdot x^i$ , 隐式设定  $s = (a - \kappa^*)$ , 计算  $P_2 = f(a) \cdot Q = \sum_{i=0}^{q-1} \vartheta_i \cdot a^i Q$ ,  $P_1 = \varphi(P_2)$ ,  $I = a \cdot P_2 = \sum_{i=0}^{q-1} \vartheta_i \cdot a^{i+1} Q$ ,  $P'_2 = \mu \cdot I$ ,  $P''_2 = \nu \cdot I$ ,  $P_{pub} = \varphi(I - \kappa^* \cdot P_2) = \varphi((a - \kappa^*) \cdot P_2) = (a - \kappa^*) \cdot P_1 = s \cdot P_1$ ,  $u = e(P_{pub}, P_2)$ .  $\mathcal{B}$  返回公共参数  $pp$  给  $\mathcal{A}$ .

- **询问阶段 1.**  $\mathcal{A}$  能够适应性地进行随机谰言机  $H_1$  询问, 私钥询问和重加密密钥询问, 其中  $H_1$  询问和私钥询问的响应与引理 1 相同. 当  $\mathcal{A}$  对  $(id_i, R_i = \{id_{i_0}, \dots, id_{i_l}\}, W_i = (A_i, \rho_i))$  进行重加密密钥询问时,  $A_i$  是一个  $n_{i,1} \times n_{i,2}$  的矩阵,  $\rho_i$  映射  $A$  的第  $k$  行  $A_{i,k} = (A_{i,k,1}, \dots, A_{i,k,n_{i,2}})$  为一个条件值. 若  $id_i = id^*$ ,  $\mathcal{B}$  随机选择  $\alpha, \beta \in \mathbb{Z}_N^*$ ,  $R \in \mathbb{G}_2$ , 计算  $\theta = u^\beta$ ,  $\Lambda_{W_i} = \prod_{j=i_1}^{i_n} (\kappa^* + H_2(w_j))$ , 提取  $(\Lambda_{W_i}, \mu_i, \Gamma_i) \in \mathcal{L}_{H_4}$ ; 对于  $j \in [i_0, i_l]$ , 提取  $(id_j, \kappa_j) \in \mathcal{L}_{H_1}$ , 计算  $C_j = \beta \cdot (P_{pub} + \kappa_j \cdot P_1) = (x_j, y_j)$ ; 通过拉格朗日插值生成多项式  $F_1(x) = \sum_{j=i_0}^{i_l} x_j \cdot \prod_{0 \leq k \neq j \leq l} \frac{x - \kappa_k}{\kappa_j - \kappa_k} = \sum_{j=0}^{i_l} v_{i,1,j} \cdot x^j \in \mathbb{F}_p[x]$  和  $F_2(x) = \sum_{j=i_0}^{i_l} y_j \cdot \prod_{0 \leq k \neq j \leq l} \frac{x - \kappa_k}{\kappa_j - \kappa_k} = \sum_{j=0}^{i_l} v_{i,2,j} \cdot x^j \in \mathbb{F}_p[x]$ , 设定  $rk_0 = (v_{i,1,0}, \dots, v_{i,1,i_l}, v_{i,2,0}, \dots, v_{i,2,i_l})$ ; 计算  $rk_1 = \alpha \cdot (P_{pub} + H_1(id_o || hid) \cdot P_1)$ ; 对于  $i \in [1, n_1]$ , 计算  $rk_{2,i} = A_{i,1} \cdot R + \sum_{j=2}^{n_2} A_{i,j} \cdot t_j \cdot P_2 + A_{i,1} \cdot \alpha \cdot H_3(\theta) \cdot P'_2 + \sum_{j=2}^{n_2} A_{i,j} \cdot r_j \cdot P'_2 + z_i P''_2$ ,  $rk_{3,i} = z_i \cdot (P'_2 + H_2(\rho(i)) \cdot P_2)$ ,  $rk_{4,i} = z_i \cdot (P_{pub} + H_1(id_o || hid) \cdot P_1)$ ; 返回  $RK_{id^* \rightarrow R_i} = (rk_0, rk_1, \{rk_{2,k}, rk_{3,k}, rk_{4,k}\}_{k \in [1, n_{i,1}]})$  给  $\mathcal{A}$ . 结合文献 [7](定理 3) 和文献 [11](定理 2) 可知, 若 DBDH 假设成立, 则  $\mathcal{A}$  无法区分随机的重加密密钥和格式良好的重加密密钥. 若  $id_i \neq id^*$ , 当  $(id_i, sk_{id_i}) \notin \mathcal{L}_{sk}$ ,  $\mathcal{B}$  对  $id_i$  进行私钥询问. 随后,  $\mathcal{B}$  运行  $\text{Re-KeyGen}(id_i, sk_{id_i}, R_i, W_i) \rightarrow RK_{id_i \rightarrow R_i}$  并返回  $RK_{id_i \rightarrow R_i}$  给  $\mathcal{A}$ .

- **挑战.**  $\mathcal{B}$  随机选择  $r, k_{w_1^*}, \dots, k_{w_n^*} \in \mathbb{Z}_N^*$ , 定义多项式  $\Phi(x) = x \cdot g(x) = r \cdot \kappa^* \cdot (f(x))^2 + \eta = \sum_{i=0}^{2q-2} \phi_i \cdot x^i$ , 则有  $r \cdot \kappa^* \cdot (f(x))^2 \cdot x^{-1} = g(x) - \eta \cdot x^{-1}$ , 其中  $\eta \in \mathbb{Z}_N^*$ ,  $g(x)$  为  $2q-3$  阶多项式且  $e(P, Q)^{g(a)}$  可计算. 随后,  $\mathcal{B}$  计算  $\gamma^* = \frac{Z^{\eta \cdot e(P_1, P_2)^r}}{e(P, Q)^{g(a)}}$ ,  $c_0^* = r \cdot P_1$ ,  $c_1^* = r \cdot \mu \cdot P_2$ ; 对于  $i \in [1, n]$ , 计算  $c_{2,w_i^*}^* = r \cdot \nu \cdot P_2 + k_{w_i^*} \cdot (P'_2 + H_2(w_i^*) \cdot P_2)$ ,  $c_{3,w_i^*}^* = k_{w_i^*} \cdot (P_{pub} + \kappa^* \cdot P_1)$ ,  $C_{id^*}^* = (c_0^*, c_1^*, \{c_{2,w_i^*}^*, c_{3,w_i^*}^*\}_{i \in [1, n]})$ ,  $K^* = \text{KDF}(\gamma^* || id^*)$ ; 随机选择  $b \in \{0, 1\}$ , 设定  $K_b^* = K^*$ ; 从封装密钥空间中随机选取  $K_{1-b}^*$ ; 返回  $(C_{id^*}^*, K_0^*, K_1^*)$  给  $\mathcal{A}$ .

- **询问阶段 2.**  $\mathcal{A}$  继续进行询问阶段 1 中的询问.

- **猜测.**  $\mathcal{A}$  输出猜测  $b'$ . 若  $b' = b$ , 则  $\mathcal{A}$  赢得游戏.

类似于引理 1 分析, 若  $\mathcal{A}$  以优势  $\epsilon$  赢得 IND-sID-CPA-Or 游戏, 则  $\mathcal{B}$  解  $q$ -DBDHI 问题优势  $\text{Adv}_{\mathcal{B}}^{q\text{-DBDHI}} = \epsilon$ .

**引理 4** 假定存在敌手  $\mathcal{A}$  能够以不可忽略的优势  $\epsilon$  赢得 IND-sID-CPA-Re 游戏, 则存在算法  $\mathcal{B}$  能够以不可忽略的优势解  $q$ -DBDHI 问题.

**证明** 给定  $q$ -DBDHI 实例  $(P, Q, aQ, \dots, a^q Q, Z)$ ,  $\mathcal{B}$  的目标是判断  $Z = e(P, Q)^{\frac{1}{a}}$  是否成立. 与引理 2 相同, 首先证明当  $l = 1$  时, 若  $\mathcal{A}$  能够以不可忽略的优势  $\epsilon_1$  赢得 IND-sID-CPA-Re 游戏, 则  $\mathcal{B}$  能够通过调用  $\mathcal{A}$  来解  $q$ -DBDHI 问题.

- **初始化.**  $\mathcal{A}$  输出挑战标识集合  $R^* = \{id_1^*\}$  和条件集合  $W^* = \{w_1^*, \dots, w_n^*\}$ . 其它设置与引理 3 相同.

- **询问阶段 1.**  $\mathcal{A}$  能够适应性地进行随机谰言机  $H_1$  询问, 私钥询问和重加密密钥询问, 询问响应均与引理 3 相同.

- **挑战.**  $\mathcal{B}$  随机选择标识  $id$ ,  $\gamma^* \in \mathbb{G}_T$ ,  $r^*, \alpha^*, \beta \in \mathbb{Z}_N^*$ , 定义多项式  $\Phi(x) = x \cdot g(x) = \beta \cdot \kappa^* \cdot (f(x))^2 + \eta = \sum_{i=0}^{2q-2} \phi_i \cdot x^i$ , 则有  $\beta \cdot \kappa^* \cdot (f(x))^2 \cdot x^{-1} = g(x) - \eta \cdot x^{-1}$ , 其中  $\eta \in \mathbb{Z}_N^*$ ,  $g(x)$  为  $2q-3$  阶多项式且  $e(P, Q)^{g(a)}$  可计算. 随后,  $\mathcal{B}$  计算  $\theta^* = \frac{Z^{\eta \cdot e(P_1, P_2)^{\beta}}}{e(P, Q)^{g(a)}}$ ,  $C_1^* = \beta \cdot P_1 = (x_1^*, y_1^*)$ ,  $c_0'^* = \gamma^* \cdot e(r^* \cdot (P_{pub} + H_1(id || hid) \cdot P_1), \alpha^* \cdot H_3(\theta^*) \cdot P'_2)$ ,  $c_2'^* = e(\alpha^* \cdot (P_{pub} + H_1(id || hid) \cdot P_1), r^* \cdot P'_2)$ ,  $K^* = \text{KDF}(\gamma^* || id)$ , 设定  $c_1'^* = (v_{1,0}^* = x_1^*, v_{2,0}^* = y_1^*)$ ,  $C_{R^*}' =$

$(c_0^*, c_1^*, c_2^*)$ .  $\mathcal{B}$  随机选择  $b \in \{0, 1\}$ , 设定  $K_b^* = K^*$ , 从封装密钥空间中随机选取  $K_{1-b}^*$ , 并返回  $(C_{R^*}', K_0^*, K_1^*)$  给  $\mathcal{A}$ .

- 询问阶段 2.  $\mathcal{A}$  继续进行询问阶段 1 中的询问.
- 猜测.  $\mathcal{A}$  输出猜测  $b'$ . 若  $b' = b$ , 则  $\mathcal{A}$  赢得游戏.

类似于引理 2 分析, 若  $\mathcal{A}$  以优势  $\epsilon$  赢得 IND-sID-CPA-Re 游戏, 则  $\mathcal{B}$  解  $q$ -DBDHI 问题优势  $\text{Adv}_{\mathcal{B}}^{q\text{-DBDHI}} \geq \frac{\epsilon}{l}$ .

**定理 4** 令方案中的哈希函数  $H_1$  为随机谰言机, 若  $q$ -SDH 假设成立, 则 SM9-IB-CBPRES<sup>+</sup> 方案满足 LR-CA 安全性.

**证明** 假定存在敌手  $\mathcal{A}$  能够以不可忽略的优势  $\epsilon$  赢得 LR-CA 游戏, 则存在算法  $\mathcal{B}$  能够以不可忽略的优势解  $q$ -SDH 问题. 给定  $q$ -SDH 实例  $(P, Q, aQ, \dots, a^q Q)$ ,  $\mathcal{B}$  的目标是输出  $(\omega, \frac{1}{a+\omega} \cdot P) \in \mathbb{Z}_N^* \times \mathbb{G}_1$ .

• 初始化.  $\mathcal{A}$  输出挑战标识  $id^*$ .  $\mathcal{B}$  随机选择  $\kappa_1, \dots, \kappa_{q-1}, \kappa^*, \mu, \nu \in \mathbb{Z}_N^*$ , 计算  $\xi_i = \kappa^* - \kappa_i$ , 其中  $i \in [1, q-1]$ .  $\mathcal{B}$  生成多项式  $f(x) = \prod_{i=1}^{q-1} (x + \kappa_i) = \sum_{i=0}^{q-1} \vartheta_i \cdot x^i$ , 隐式设定  $s = a$ , 计算  $P_2 = f(a) \cdot Q = \sum_{i=0}^{q-1} \vartheta_i \cdot a^i Q$ ,  $P_1 = \varphi(P_2)$ ,  $P_2' = \mu P_2$ ,  $P_2'' = \nu P_2$ ,  $P_{pub} = \varphi(\sum_{i=0}^{q-1} \vartheta_i \cdot a^{i+1} Q) = \varphi(a \cdot P_2) = s \cdot P_1$ ,  $u = e(P_{pub}, P_2)$ .  $\mathcal{B}$  返回公共参数  $pp$  给  $\mathcal{A}$ .

• 询问阶段 1.  $\mathcal{A}$  能够适应性地进行随机谰言机  $H_1$  询问, 私钥询问和重加密密钥询问, 其中  $H_1$  询问和私钥询问的响应与引理 1 相同. 当  $\mathcal{A}$  对  $(id_i, R_i = \{id_{i_0}, \dots, id_{i_l}\}, W_i = (A_i, \rho_i))$  进行重加密密钥询问时,  $A_i$  是一个  $n_{i,1} \times n_{i,2}$  的矩阵,  $\rho_i$  映射  $A$  的第  $k$  行  $A_{i,k} = (A_{i,k,1}, \dots, A_{i,k,n_{i,2}})$  为一个条件值. 若  $id_i = id^*$ ,  $\mathcal{B}$  随机选择  $\beta, r_2, \dots, r_{n_{i,2}}, t_2, \dots, t_{n_{i,2}}, z_1, \dots, z_{n_{i,1}} \in \mathbb{Z}_N^*$ , 计算  $\theta = u^\beta$ , 隐式设定  $\alpha = \frac{-s}{H_3(\theta) \cdot \mu \cdot (s + \kappa^*)}$ ; 对于  $j \in [i_0, i_l]$ , 提取  $(id_j, \kappa_j) \in \mathcal{L}_{H_1}$ , 计算  $C_j = \beta \cdot (P_{pub} + \kappa_j \cdot P_1) = (x_j, y_j)$ ; 通过拉格朗日插值生成多项式  $F_1(x) = \sum_{j=i_0}^{i_l} x_j \cdot \prod_{0 \leq k \neq j \leq l} \frac{x - \kappa_k}{\kappa_j - \kappa_k} = \sum_{j=0}^{i_l} v_{i,1,j} \cdot x^j \in \mathbb{F}_p[x]$  和  $F_2(x) = \sum_{j=i_0}^{i_l} y_j \cdot \prod_{0 \leq k \neq j \leq l} \frac{x - \kappa_k}{\kappa_j - \kappa_k} = \sum_{j=0}^{i_l} v_{i,2,j} \cdot x^j \in \mathbb{F}_p[x]$ , 设定  $rk_0 = (v_{i,1,0}, \dots, v_{i,1,i_l}, v_{i,2,0}, \dots, v_{i,2,i_l})$ ; 计算  $rk_1 = \frac{-1}{H_3(\theta) \cdot \mu} \cdot P_{pub}$ ; 对于  $k \in [1, n_{i,1}]$ , 计算  $rk_{2,k} = \sum_{j=2}^{n_{i,2}} A_{i,k,j} \cdot t_j \cdot P_2 + \sum_{j=2}^{n_{i,2}} A_{i,k,j} \cdot r_j \cdot P_2' + z_k \cdot P_2''$ ,  $rk_{3,k} = z_k \cdot (P_2' + H_2(\rho(k)) \cdot P_2)$ ,  $rk_{4,k} = z_k \cdot (P_{pub} + \kappa^* \cdot P_1)$ ; 返回  $RK_{id^* \rightarrow R_i} = (rk_0, rk_1, \{rk_{2,k}, rk_{3,k}, rk_{4,k}\}_{k \in [1, n_{i,1}]})$  给  $\mathcal{A}$ . 若  $id_i \neq id^*$ , 当  $(id_i, sk_{id_i}) \notin \mathcal{L}_{sk}$ ,  $\mathcal{B}$  对  $id_i$  进行私钥询问. 随后,  $\mathcal{B}$  运行  $\text{Re-KeyGen}(id_i, sk_{id_i}, R_i, W_i) \rightarrow RK_{id_i \rightarrow R_i}$  并返回  $RK_{id_i \rightarrow R_i}$  给  $\mathcal{A}$ .

• 输出.  $\mathcal{A}$  输出私钥  $sk'_{id^*}$ . 若  $e(P_{pub} + \kappa^* P_1, sk'_{id^*}) = u$ , 则  $\mathcal{A}$  赢得游戏. 通过定理 2 中方法,  $\mathcal{B}$  输出  $q$ -SDH 实例的解.

类似于定理 2 分析, 若  $\mathcal{A}$  以优势  $\epsilon$  赢得 LR-CA 游戏, 则  $\mathcal{B}$  解  $q$ -SDH 问题优势  $\text{Adv}_{\mathcal{B}}^{q\text{-SDH}} = \epsilon$ .

## 6 性能分析

本节从理论和实验两方面对所提方案与相关方案 [7, 11, 13, 21] 的性能进行对比分析.

### 6.1 理论分析

本小节从理论方面分析 SM9-IB-CBPRES 和 SM9-IB-CBPRES<sup>+</sup> 方案的计算代价、通信开销和特性, 并与已有文献 [7, 11, 13, 21] 进行对比. 表 2 给出计算代价的比较结果. 令  $P$  表示双线性配对运算,  $E_T$  表示群  $\mathbb{G}_T$  上指数运算,  $SM_i (i = 1, 2)$  表示群  $\mathbb{G}_i$  上标量乘运算,  $H$  表示 Map-to-Point 哈希运算,  $Inv$  表示有限域  $\mathbb{F}_p$  或群  $\mathbb{Z}_N^*$  上模逆运算,  $Mul$  表示有限域  $\mathbb{F}_p$  或群  $\mathbb{Z}_N^*$  上模乘运算,  $n$  表示条件集合尺寸,  $l$  表示数据请求者数量,  $n_1$  表示授权策略矩阵尺寸,  $|I|$  表示满足授权策略的条件数量.

表 2 计算代价比较  
Table 2 Comparison of computation cost

| Schemes                    | Extract      | Encrypt                                    | Re-KeyGen                                                                            | Re-Encrypt  | Decrypt | Re-Decrypt                                                     |
|----------------------------|--------------|--------------------------------------------|--------------------------------------------------------------------------------------|-------------|---------|----------------------------------------------------------------|
| [7]                        | $SM_1 + Inv$ | $E_T + 5SM_1 + 2SM_2 + 3Mul + Inv$         | $E_T + 3SM_1 + (l+2)SM_2 + H + (\frac{1}{2}l^2 + 2)Mul + Inv$                        | $P$         | $P$     | $3P + E_T + (l-1)SM_2 + H + \frac{1}{2}(l^2 + l - 2)Mul + Inv$ |
| [11]                       | $SM_2 + Inv$ | $E_T + (n+2)SM_1 + Inv + (2n+4)SM_2 + Mul$ | $E_T + (l+n_1+2)SM_1 + (6n_1+1)SM_2 + Inv + \frac{1}{2}(l^2 + 2n_1n_2 + 2)Mul$       | $3 I P$     | $P$     | $3P + E_T + (l-1)SM_2 + H + \frac{1}{2}(l^2 + l - 2)Mul + Inv$ |
| [13]                       | $SM_2 + Inv$ | $2SM_1 + E_T$                              | —                                                                                    | —           | $P$     | —                                                              |
| [21]                       | $SM_2 + Inv$ | $E_T + 2SM_1 + SM_2$                       | $E_T + (l+2)SM_1 + 2SM_2 + (\frac{1}{2}l^2 + 1)Mul$                                  | $P$         | $P$     | $3P + l \cdot SM_1 + SM_2 + \frac{1}{2}(l^2 + l - 2)Mul + Inv$ |
| SM9-IB-CBPRES              | $SM_2 + Inv$ | $E_T + 2SM_1 + SM_2 + H + (n-1)Mul$        | $E_T + (l+3)SM_1 + 2SM_2 + H + (l+1)^2Inv + (l^3 + 6l^2 + 5l + n)Mul$                | $2P$        | $P$     | $P + E_T + 2(l+1)Mul$                                          |
| SM9-IB-CBPRES <sup>+</sup> | $SM_2 + Inv$ | $E_T + (n+2)SM_1 + (2n+2)SM_2$             | $E_T + (l+n_1+3)SM_1 + 6n_1SM_2 + (l+1)^2Inv + (l^3 + 6l^2 + 5l + 2n_1n_2 - n_1)Mul$ | $(2 I +2)P$ | $P$     | $P + E_T + 2(l+1)Mul$                                          |

表 3 通信开销及特性比较  
Table 3 Comparison of communication overhead and features

| Schemes                    | $ C $                                              | $ RK $                                                          | $ C' $                                                       | $F_1$ | $F_2$ | $F_3$ | $F_4$ | $F_5$ | $F_6$ | $F_7$ |
|----------------------------|----------------------------------------------------|-----------------------------------------------------------------|--------------------------------------------------------------|-------|-------|-------|-------|-------|-------|-------|
| [7]                        | $2 \mathbb{G}_1  +  \mathbb{G}_2 $                 | $2 \mathbb{G}_1  + 2 \mathbb{G}_2  + l id $                     | $2 \mathbb{G}_1  + 2 \mathbb{G}_2  +  \mathbb{G}_T  + l id $ | ×     | ✓     | ✓     | ×     | ×     | ×     | ×     |
| [11]                       | $(n+1) \mathbb{G}_1  + (n+2) \mathbb{G}_2 $        | $(n_1+1) \mathbb{G}_1  + (2n_1+1) \mathbb{G}_2  + l id $        | $2 \mathbb{G}_1  + 2 \mathbb{G}_2  +  \mathbb{G}_T  + l id $ | ×     | ✓     | ✓     | ✓     | ✓     | ×     | ×     |
| [13]                       | $ \mathbb{G}_1 $                                   | —                                                               | —                                                            | ✓     | ×     | ×     | ×     | ×     | ✓     | ✓     |
| [21]                       | $ \mathbb{G}_1  +  \mathbb{G}_2  +  \mathbb{G}_T $ | $2 \mathbb{G}_1  + 2 \mathbb{G}_2  + l id $                     | $2 \mathbb{G}_1  + 2 \mathbb{G}_2  +  \mathbb{G}_T  + l id $ | ×     | ✓     | ×     | ×     | ×     | ×     | ✓     |
| SM9-IB-CBPRES              | $ \mathbb{G}_1  +  \mathbb{G}_2 $                  | $ \mathbb{G}_1  +  \mathbb{G}_2  + 2l \mathbb{F}_p $            | $2 \mathbb{G}_T  + 2l \mathbb{F}_p $                         | ✓     | ✓     | ✓     | ✓     | ×     | ✓     | ✓     |
| SM9-IB-CBPRES <sup>+</sup> | $(n+1) \mathbb{G}_1  + (n+1) \mathbb{G}_2 $        | $(n_1+1) \mathbb{G}_1  + 2n_1 \mathbb{G}_2  + 2l \mathbb{F}_p $ | $2 \mathbb{G}_T  + 2l \mathbb{F}_p $                         | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     |

如表 2 所示, 所有方案中算法 Extract 和 Decrypt 计算代价均为恒定. 对于算法 Encrypt, SM9-IB-CBPRES 与文献 [7, 13, 21] 均取得恒定计算代价. 然而, 文献 [7] 仅支持单一条件嵌入, 文献 [13] 缺乏密文转换支持致使灵活性差, 且文献 [21] 未考虑细粒度授权需求. SM9-IB-CBPRES<sup>+</sup> 与文献 [11] 计算代价与  $n$  呈正相关. SM9-IB-CBPRES 与文献 [7, 21] 中算法 Re-KeyGen 的计算代价均与  $l$  相关且算法 Re-Encrypt 计算代价恒定. 由于考虑策略控制, SM9-IB-CBPRES<sup>+</sup> 与文献 [11] 中算法 Re-KeyGen 和 Re-Encrypt 计算代价还分别与  $n_1$  和  $|I|$  相关. 此外, 对于算法 Re-Decrypt, 尽管所有方案中计算代价均与  $l$  成正比, 但所提方案中效率远高于文献 [7, 11, 21]. 综上, 与已知文献相比, 本文方案在计算代价方面存在优势.

表 3 给出通信开销及特性比较结果. 令  $|\mathbb{G}_i| (i = 1, 2, T)$  表示群  $\mathbb{G}_i$  中元素长度,  $|\mathbb{F}_p|$  表示有限域  $\mathbb{F}_p$  中元素长度,  $|id|$  表示标识长度,  $|C|$  表示初始密文长度,  $|RK|$  表示重加密密钥长度,  $|C'|$  表示重加密密文长度,  $F_1$  表示数据请求者标识信息隐私保护,  $F_2$  表示一对多授权,  $F_3$  表示细粒度授权,  $F_4$  表示多条件控制,  $F_5$  表示策略控制,  $F_6$  表示数据请求者数量不受限,  $F_7$  表示支持国密算法.

由表 3 可知, 与文献 [7, 11, 13, 21] 相比, 所提方案不仅取得了相当的通信开销, 还具备更丰富的特性和更强的安全性. 具体来说, SM9-IB-CBPRES 和文献 [7, 13, 21] 均实现恒定初始密文长度, 而 SM9-IB-CBPRES 优于文献 [7, 21], 主要原因在于 SM9-IB-CBPRES 采用集合承诺将条件控制信息与传统标识广播代理重加密的重加密控制密文融合. 同时, 可以看出, 与原始 SM9 密钥封装机制<sup>[13]</sup> 相比, SM9-IB-CBPRES 仅以一个额外元素的代价即可实现一对多授权和多条件控制下的细粒度授权. 由于文献 [11] 和 SM9-IB-CBPRES<sup>+</sup> 需在初始密文和重加密密钥中附加条件控制信息以实现策略控制, 故其与  $n$  和  $n_1$  相关. 考虑到文献 [7, 11, 21] 中数据请求者标识集合会随重加密密钥/密文传输以辅助解密操作, 故本文将其视为部分重加密密钥/密文. 因此, 文献 [7, 11, 21]

表 4 算法 Extract 和 Decrypt 的运行时间 (ms)

Table 4 Running time of algorithms Extract and Decrypt (ms)

| Algorithms | [7]   | [11]  | [13]  | [21] | SM9-IB-CBPRES | SM9-IB-CBPRES <sup>+</sup> |
|------------|-------|-------|-------|------|---------------|----------------------------|
| Extract    | 0.94  | 1.44  | 1.46  | 1.45 | 1.39          | 1.42                       |
| Decrypt    | 22.77 | 23.48 | 20.52 | 21.3 | 22.02         | 21.86                      |

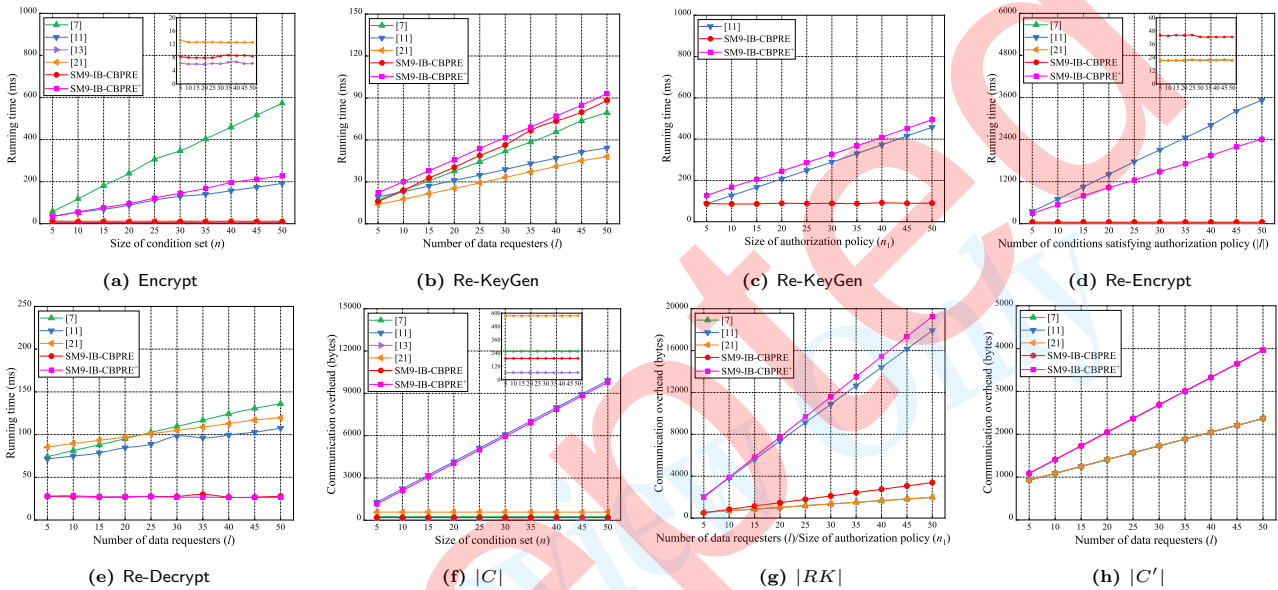


图 2 算法 Encrypt, Re-KeyGen, Re-Encrypt 和 Re-Decrypt 的运行时间以及初始密文, 重加密密钥和重加密密文的长度

Figure 2 Running time of algorithms Encrypt, Re-KeyGen, Re-Encrypt, and Re-Decrypt as well as size of original ciphertext, re-encryption key, and re-encrypted ciphertext

存在隐私泄露问题同时增加通信开销. 由上可知, 本文方案在功能性和通信开销方面取得更优的权衡, 更适用于实际场景.

## 6.2 实验分析

为准确评估方案性能, 本小节从实验方面对所提方案与文献 [7, 11, 13, 21] 进行对比. 测试环境为配有 8 核 Inter(R) Core(TM) i7-7700HQ@ 2.90 GHz 处理器、8GB 内存的 Linux 操作系统. 在 128-bit 安全性下, 基于 Python 语言和 Charm 密码学库, 使用 SM9 推荐曲线 (即 256-bit BN 曲线  $y^2 = x^3 + b$ ) 对所提方案与文献 [7, 11, 13, 21] 进行仿真实验.  $G_1, G_2, G_T$  和  $F_p$  中元素长度分别为 64、128、384 和 32 字节. 设定标识长度为 32 字节. 实验结果如表 4 和图 2 所示.

如表 4 所示, 所提方案中算法 Extract 和 Decrypt 的效率与文献 [7, 11, 13, 21] 相当. 根据图 2(a) 可得, 文献 [7, 11] 和 SM9-IB-CBPRES<sup>+</sup> 中算法 Encrypt 的计算代价同  $n$  正相关, 而文献 [13, 21] 与 SM9-IB-CBPRES 保持恒定. 主要原因在于 SM9-IB-CBPRES 采用集合承诺思想压缩多个条件值未引发额外开销, 文献 [13, 21] 密文中未包含条件信息. 相比之下, 文献 [7] 需重复执行  $n$  次算法以设定多个条件且文献 [11] 和 SM9-IB-CBPRES<sup>+</sup> 为实现策略控制须为每一个条件值生成相应控制密文. 具体来说, SM9-IB-CBPRES 生成包含 50 个条件值的初始密文需 8.39 ms, 而文献 [7, 11, 13, 21] 和 SM9-IB-CBPRES<sup>+</sup> 分别需要 572.95, 192.03, 6.21, 12.54, 和 227.72 ms. 图 2(b) 和图 2(c) 分别给出不同  $l$  和  $n_1$  下算法 Re-KeyGen 的运行时间. 由于文献 [7] 仅支持在重加密密钥中嵌入单个条件且文献 [21] 未考虑条件控制, 因此图 2(b) 和图 2(c) 中分别设定  $n_1 = 1$  和  $l = 50$ . 显然, 所提方案在算法 Re-KeyGen 上表现较弱, 这是因为所提方案需要利用拉格朗日插值技术生成多项式系数以保护数据请求者标识信息. 然而, 文献 [7, 11, 21] 中系统建立之后, 重加密密钥中数据请求者数量会受到限

制. 相比之下, 本文方案可支持任意规模数据请求者集合. 从图 2(d) 可以看出, 支持策略控制的文献 [11] 和 SM9-IB-CBPRE<sup>+</sup> 中算法 Re-Encrypt 的运行时间与  $n_1$  之间呈现正相关关系. 然而, SM9-IB-CBPRE<sup>+</sup> 效率优于文献 [11]. 具体来说, 当  $n_1 = 50$  时, SM9-IB-CBPRE<sup>+</sup> 执行算法 Re-Encrypt 需要 2412.19 ms, 而文献 [11] 需要 3522.53 ms, 即所提方案能够节约 31.52% 的计算代价. 此外, 文献 [7, 21] 和 SM9-IB-CBPRE<sup>+</sup> 中算法 Re-Encrypt 运行时间保持恒定. 图 2(e) 给出算法 Re-Decrypt 运行时间与  $l$  之间的关系. 可以明显看出, 相比于文献 [7, 11, 21] 中线性增长的解密开销, 所提方案取得恒定运行时间. 当  $l = 50$  时, 所提方案需要 27.93ms 解密重加密密文, 而文献 [7, 11, 21] 分别需要 136.01, 107.52 和 119.74 ms. 故所提方案分别降低了 79.46%, 74.02% 和 76.67% 的计算代价. 由图 2(f) 可知, SM9-IB-CBPRE 与文献 [7, 13, 21] 中初始密文长度均为恒定. 但是, SM9-IB-CBPRE 考虑多条件控制细粒度授权, 而文献 [7] 仅允许单条件控制且文献 [13, 21] 未考虑细粒度授权. 此外, SM9-IB-CBPRE<sup>+</sup> 初始密文长度优于文献 [11]. 如图 2(g) 和图 2(h) 所示, 所提方案中重加密密钥和重加密密文长度略高于文献 [7, 11, 21]. 具体而言, 当  $l = n_1 = 50$  (100) 时, 所提方案中重加密密钥为 3393 (6592) 和 19264 (38464) 字节, 而文献 [7, 11, 21] 分别为 1984 (3584), 17920 (35520) 和 1984 (3584) 字节; 所提方案中重加密密文长度为 3968 (7168) 字节, 而文献 [7, 11, 21] 为 2368 (3968) 字节. 主要原因在于所提方案包含两组多项式系数而非完整数据请求者标识集合. 故所提方案虽轻微增加了通信开销, 但避免了文献 [7, 11, 21] 中因数据请求者标识集合暴露所造成的隐私风险.

## 7 总结

针对 SM9 标识密码不支持一对多和细粒度授权、标识广播代理重加密面临的数据请求者隐私泄漏和实用性差等问题, 本文首先构建一个基于 SM9 的标识条件广播代理重加密方案 SM9-IB-CBPRE. 该方案中数据所有者能够嵌入条件集合至初始密文和重加密密钥结构中并隐式融入多个数据请求者信息, 实现隐私保护的一对多和细粒度授权同时增强系统实用性. 随后, 针对条件集合一致性匹配引发的授权灵活性受限问题, 本文提出扩展方案 SM9-IB-CBPRE<sup>+</sup>. 该方案将重加密密钥中的条件集合优化为表达能力更强的授权策略并采用单调张成方案分割用户私钥, 实现策略控制下的细粒度授权. 在随机谰言机模型下, 基于  $q$ -DBDHI 假设和  $q$ -SDH 假设, 证明所提方案能够满足 IND-sID-CPA 和 LR-CA 安全性. 性能分析结果表明, 与相关方案相比, 本文方案有效平衡计算代价和通信开销同时实现了更丰富的功能性.

## 参考文献

- 1 Kamara S, Lauter K. Cryptographic cloud storage. In: Proceedings of International Conference on Financial Cryptography and Data Security, Berlin: Springer, 2010. 136-149
- 2 Wei L, Zhu H, Cao Z, et al. Security and privacy for storage and computation in cloud computing. Inf Sci, 2014, 258: 371-386
- 3 Ming Y, Liu H, Wang C H, et al. Generic construction: Cryptographic reverse firewalls for public key encryption with keyword search in cloud storage. IEEE Trans Cloud Comput, 2024, 12: 405-418
- 4 Blaze M, Bleumer G, Strauss M. Divertible protocols and atomic proxy cryptography. In: Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques, Berlin: Springer, 1998. 127-144
- 5 Green M, Ateniese G. Identity-based proxy re-encryption. In: Proceedings of International Conference on Applied Cryptography and Network Security, Berlin: Springer, 2007. 288-306
- 6 Boneh D, Franklin M. Identity-based encryption from the weil pairing. In: Proceedings of Annual International Cryptography Conference, Berlin: Springer, 2001. 213-229
- 7 Xu P, Jiao T F, Wu Q H, et al. Conditional identity-based broadcast proxy re-encryption and its application to cloud email. IEEE Trans Comput, 2016, 65: 66-79
- 8 Huang Q L, Yang Y X, Fu J Y. Precise: Identity-based private data sharing with conditional proxy re-encryption in online social networks. Future Gener Comput Syst, 2018, 86: 1523-1533
- 9 Huang Q L, Yang Y X, Yue W, et al. Secure data group sharing and conditional dissemination with multi-owner in cloud computing. IEEE Trans Cloud Comput, 2021, 9: 1607-1618

- 10 Ge C P, Zhou L, Xia J Y, et al. A secure fine-grained identity-based proxy broadcast re-encryption scheme for micro-video subscribing system in clouds. In: *Proceedings of International Symposium on Security and Privacy in Social Networks and Big Data*, Singapore: Springer, 2019. 139–151
- 11 Deng H, Zhang J X, Qin Z, et al. Policy-based broadcast access authorization for flexible data sharing in clouds. *IEEE Trans Dependable Secure Comput*, 2022, 19: 3024–3037
- 12 Sun J F, Xu G W, Li H W, et al. Sanitizable cross-domain access control with policy-driven dynamic authorization. *IEEE Trans Dependable Secure Comput*, 2025, 22: 4126–4142
- 13 GM/T0044-2016. Identity-based cryptographic algorithm SM9. 2016 [GM/T0044-2016. SM9 标识密码算法. 2016] <http://www.gmbz.org.cn/main/postDetail.html?id=20180322410400>
- 14 Lai J C, Huang X Y, He D B. An efficient identity-based broadcast encryption based on SM9. *Chinese J Comput*, 2021, 44: 897–907 [赖建昌, 黄欣沂, 何德彪. 一种基于商密 SM9 的高效标识广播加密方案. *计算机学报*, 2021, 44: 897–907]
- 15 Lai J C, Huang X Y, He D B, et al. CCA secure broadcast encryption based on SM9. *J Softw*, 2023, 34: 3354–3364 [赖建昌, 黄欣沂, 何德彪, 等. 基于 SM9 的 CCA 安全广播加密方案. *软件学报*, 2023, 34: 3354–3364]
- 16 Cui Y, Huang X Y, Lai J C, et al. CCA anonymous broadcast encryption based on SM9. *J Cyber Secur*, 2023, 8: 15–27 [崔岩, 黄欣沂, 赖建昌, 等. 基于 SM9 的匿名广播加密方案. *信息安全学报*, 2023, 8: 15–27]
- 17 Liu X H, Huang X Y, Cheng Z H, et al. Fault-tolerant identity-based encryption from SM9. *Sci China Inf Sci*, 2024, 67: 122101
- 18 Shi Y, Ma Z Y, Qin R F, et al. Implementation of an attribute-based encryption scheme based on SM9. *Appl Sci*, 2019, 9: 3074
- 19 Liu X H, Huang X Y, Cheng Z H, et al. Key-policy attribute-based encryption based on SM9 and its fast decryption. *Chinese J Comput*, 2024, 47: 971–986 [刘晓红, 黄欣沂, 程朝辉, 等. 基于 SM9 的密钥策略属性基加密及快速解密. *计算机学报*, 2024, 47: 971–986]
- 20 Liu H, Ming Y, Wang C H, et al. Identity-based proxy re-encryption based on SM9. In: *Proceedings of International Conference on Information Security and Cryptology*, Singapore: Springer, 2023. 320–339
- 21 Liu H, Ming Y, Wang C H, et al. Verifiable and fair identity-based broadcast proxy re-encryption based on SM9. *Chinese J Comput*, 2025, 48: 721–737 [刘行, 明洋, 王晨豪, 等. 基于 SM9 的可验证公平标识广播代理重加密. *计算机学报*, 2025, 48: 721–737]
- 22 Cheung L, Newport C. Provably secure ciphertext policy ABE. In: *Proceedings of ACM Conference on Computer and Communications Security*, New York: ACM, 2007. 456–465
- 23 Maiti S, Misra S. P2B: Privacy preserving identity-based broadcast proxy re-encryption. *IEEE Trans Veh Technol*, 2020, 69: 5610–5617
- 24 Zhang J, Su S S, Zhong H, et al. Identity-based broadcast proxy re-encryption for flexible data sharing in VANETs. *IEEE Trans Inf Forensics Secur*, 2023, 18: 4830–4842
- 25 Sun J F, Xu G W, Zhang T W, et al. Verifiable, fair and privacy-preserving broadcast authorization for flexible data sharing in clouds. *IEEE Trans Inf Forensics Secur*, 2023, 18: 683–698
- 26 Shao J, Wei G Y, Ling Y, et al. Identity-based conditional proxy re-encryption. In: *Proceedings of IEEE International Conference on Communications*, New York: IEEE, 2011. 1–5
- 27 Weng J, Deng R H, Ding X H, et al. Conditional proxy re-encryption secure against chosen-ciphertext attack. In: *Proceedings of International Symposium on Information, Computer, and Communications Security*, New York: ACM, 2009. 322–332
- 28 Zhou D H, Chen K F, Liu S L, et al. Identity-based conditional proxy re-encryption. *Chin J Electron*, 2013, 22: 61–66
- 29 Waters B. Efficient identity-based encryption without random oracles. In: *Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Berlin: Springer, 2005. 114–127
- 30 Liang K T, Liu Z, Tan X, et al. A CCA-secure identity-based conditional proxy re-encryption without random oracles. In: *Proceedings of International Conference on Information Security and Cryptology*, Berlin: Springer, 2012. 231–246
- 31 Liang K T, Chu C K, Tan X, et al. Chosen-ciphertext secure multi-hop identity-based conditional proxy re-encryption with constant-size ciphertexts. *Theor Comput Sci*, 2014, 539: 87–105
- 32 Yao S M, Dayot R V J, Ra I H, et al. An identity-based proxy re-encryption scheme with single-hop conditional delegation and multi-hop ciphertext evolution for secure cloud data sharing. *IEEE Trans Inf Forensics Secur*, 2023, 18: 3833–3848
- 33 Li C, Chen R M, Wang Y, et al. REEDS: An efficient revocable end-to-end encrypted message distribution system for IoT. *IEEE Trans Dependable Secure Comput*, 2024, 21: 4526–4542
- 34 Ge C P, Susilo W, Wang J D, et al. Identity-based conditional proxy re-encryption with fine grain policy. *Comput Stand Interfaces*, 2017, 52: 1–9
- 35 Deng H, Qin Z, Sha L T, et al. A flexible privacy-preserving data sharing scheme in cloud-assisted IoT. *IEEE Internet Things J*, 2020, 7: 11601–11611
- 36 Cheng Z H. Security analysis of SM9 key agreement and encryption. In: *Proceedings of International Conference on Information Security and Cryptology*, Cham: Springer, 2018. 3–25
- 37 Lai J C, Huang X Y, He D B, et al. Security analysis of uppercaseSM9 digital signature and key encapsulation. *Sci Sin Inform*, 2021, 51: 1900–1913 [赖建昌, 黄欣沂, 何德彪, 等. 国密 SM9 数字签名和密钥封装算法的安全性分析. *中国科学: 信息科学*, 2021, 51: 1900–1913]
- 38 Zhang J L, Lai J C, Huang X Y, et al. Forward secure equality test based on SM9. *Sci Sin Inform*, 2025, 55: 1400–1418 [张健龙, 赖建昌, 黄欣沂, 等. 前向安全的 SM9 密文等值测试. *中国科学: 信息科学*, 2025, 55: 2002–2017]
- 39 Li C, Liang J K, Ding Y J, et al. Hierarchical identity-based broadcast inner product functional encryption based on SM9. *Sci Sin Inform*,

- 2024, 54: 1400–1418 [李聪, 梁俊凯, 丁煜甲, 等. 基于 SM9 的分层标识广播内积函数加密. 中国科学: 信息科学, 2024, 54: 1400–1418]
- 40 Fuchsbauer G, Hanser C, Slamanig D. Structure-preserving signatures on equivalence classes and constant-size anonymous credentials. *J Cryptol*, 2019, 32: 498–546
- 41 Lewko A, Waters B. Unbounded hibe and attribute-based encryption. In: *Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Berlin: Springer, 2011. 547–567
- 42 Bellare M, Boldyreva A, Micali S. Public-key encryption in a multi-user setting: Security proofs and improvements. In: *Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Berlin: Springer, 2000. 259–274

## Identity-based conditional broadcast proxy re-encryption based on SM9

Hang Liu, Yang Ming\*, Chenhao Wang & Yi Zhao

*School of Information Engineering, Chang'an University, Xi'an 710018, China*

\* Corresponding author. E-mail: yangming@chd.edu.cn

**Abstract** Identity-based conditional broadcast proxy re-encryption enables data owners to grant decryption rights of outsourced ciphertexts to a set of data requesters at a fine-grained level according to predefined conditions, with extensive applications in data trading, hierarchical data sharing, and service subscriptions. Nevertheless, existing solutions predefine the number of data requesters during system establishment and suffer from leakage of data requester identity privacy. SM9 identity-based encryption, as the identity-based cryptographic algorithm independently developed by China, has been deeply applied in critical fields such as finance, healthcare, and government affairs. However, it only supports one-to-one sharing and cannot meet the flexible and diversified requirements. To address the above problems, based on the SM9 identity-based encryption algorithm, this paper presents SM9-IB-CBPPE, an identity-based conditional broadcast proxy re-encryption scheme. Incorporating the idea of set commitments, this scheme embeds the condition set into the ciphertext and re-encryption key, realizing fine-grained authorization under multi-condition control. Also, it employs Lagrange interpolation polynomials to hide the information of data requesters, satisfying an arbitrary number of data requesters while eliminating privacy leakage risks. In response to the restricted authorization flexibility, an extended scheme SM9-IB-CBPPE<sup>+</sup> is put forward, drawing inspiration from key policy attribute-based encryption. This scheme leverages monotone span programs to split the user private key, optimizing condition set consistency matching into policy satisfiability verification, thus achieving fine-grained authorization under policy control. The security analysis demonstrates that the proposed schemes can resist the selective identity and chosen plaintext attacks and collusion attacks under the random oracle model. Performance analysis indicates that the proposed schemes are comparable to existing solutions in efficiency while significantly enhancing functionality and practicality.

**Keywords** SM9, conditional broadcast proxy re-encryption, fine-grained authorization, policy control, privacy-preserving