# 云存储环境下支持属性撤销的属性基加密方案

孙磊[1]，赵志远[2]，王建华[1]，朱智强[1]
（1. 战略支援部队信息工程大学三院，河南 郑州 450001；2. 61516 部队，北京 100062）

**摘 要**：属性基加密因其细粒度访问控制在云存储中得到了广泛应用。在属性基加密方案中，每个属性可能同时被多个用户共享，因此如何实现属性级用户撤销且能够抵抗用户合谋攻击是当前面临的重要挑战。针对上述问题，提出了一种支持属性撤销的属性基加密方案，所提方案可以有效地抵抗撤销用户与未撤销用户的合谋攻击，同时，将复杂的解密计算外包给具有强大计算能力的云服务商，减轻了数据用户的计算负担。在标准模型下，基于计算性 Diffie-Hellman 假设完成安全证明。最后从理论和实验 2 个方面对所提方案的效率与功能进行分析，结果表明所提方案可以安全地实现属性级用户撤销，并具有快速解密的能力。

**关键词**：云存储；属性基加密；合谋攻击；属性撤销；解密外包
**中图分类号**：TP309
**文献标识码**：A
**doi:** 10.11959/j.issn.1000−436x.2019116

# Attribute-based encryption scheme supporting attribute revocation in cloud storage environment

SUN Lei[1], ZHAO Zhiyuan[2], WANG Jianhua[1], ZHU Zhiqiang[1]
1. The Third Institute, Strategic Support Force Information Engineering University, Zhengzhou 450001, China
2. Troops 61516, Beijing 100062, China

**Abstract:** Attribute-based encryption (ABE) scheme is widely used in the cloud storage due to its fine-grained access control. Each attribute in ABE may be shared by multiple users at the same time. Therefore, how to achieve attribute-level user revocation is currently facing an important challenge. Through research, it has been found that some attribute-level user revocation schemes currently can't resist the collusion attack between the revoked user and the existing user. To solve this problem, an attribute-based encryption scheme that supported the immediate attribute revocation was proposed. The scheme could achieve attribute-level user revocation and could effectively resist collusion attacks between the revoked users and the existing users. At the same time, this scheme outsourced complex decryption calculations to cloud service providers with powerful computing ability, which reduced the computational burden of the data user. The scheme was proved secure based on computational Diffie-Hellman assumption in the standard model. Finally, the functionality and efficiency of the proposed scheme were analyzed and verified. The experimental results show that the proposed scheme can safely implement attribute-level user revocation and has the ability to quickly decrypt, which greatly improves the system efficiency.

**Key words:** cloud storage, attribute-based encryption, collusion attack, attribute revocation, outsourced decryption

## 1 引言

密码学可以保证信息的完整性、机密性、不可抵赖性、可控性及可用性[1]。属性基加密（ABE, attribute-based encryption）[2]通过用户属性的差异实现数据的细粒度访问控制及灵活共享[3]。目前，ABE

**收稿日期**：2018−01−18；**修回日期**：2019−04−22
**基金项目**：国家重点基础研究发展计划（“973”计划）基金资助项目（No.2013CB338000）；国家重点研发计划基金资助项目（No.2016YFB0501900）
**Foundation Items:** The National Basic Research Program of China (973 Program) (No.2013CB338000), The National Key Research and Development Program of China (No.2016YFB0501900)

方案依据访问结构位置的差异主要分为密钥策略属性基加密（KP-ABE, key-policy ABE）方案[4]和密文策略属性基加密（CP-ABE, ciphertext-policy ABE）方案[5]。KP-ABE 方案中，密文和属性相关联，私钥和访问结构相关联，当且仅当密文的属性满足密钥的访问结构时，用户才能解密密文以恢复出明文消息；CP-ABE 方案中，私钥和属性相关联，密文和访问结构相关联，当且仅当与私钥关联的属性满足与密文关联的访问结构时，用户才能解密密文，恢复出明文消息。CP-ABE 类似于传统访问控制中的基于角色的访问控制，指定具有某些属性的用户可以访问该密文，实现了“一对多”的加密模式，因此，CP-ABE 在云存储模式（大量用户、海量数据，且解密方未知）下能够发挥极大价值，受到学术界和产业界的广泛关注，成为当前密码理论的研究热点[6]。

云存储系统中大量用户共享部分相同属性导致撤销某一个用户的属性时往往会影响其他相关用户，因此研究如何撤销用户属性成为一个富有挑战且具有重要意义的课题[7]。Pirretti 等[8]第一次提出了属性可撤销的 ABE 方案，该方案为系统所有属性指定版本密钥，并定期更新属性的版本密钥，而被撤销的属性无法完成密钥更新以此达到属性撤销的目的。在这种撤销方法中，当未达到更新时刻时，即使撤销用户属性，也不能立刻实现属性撤销，这个时间间隙被称为脆弱性窗口，其影响方案的前向安全和后向安全[9]。

为解决上述问题，Ibraimi 等[10]和 Yu 等[11]分别提出了属性立即撤销的 ABE 方案，但这 2 种方案无法实现数据的细粒度访问控制。Hur 等[12]提出了一种支持属性级用户撤销的 ABE 方案，该方案能够实现实时撤销，不存在脆弱性窗口，但该方案无法抵抗用户合谋攻击。Yang 等[13]提出了一种支持属性级用户撤销的 ABE 方案，该方案中数据拥有者不需要实时在线参与撤销工作，且具有较高的计算效率，但该方案在随机预言机模型下完成安全性证明，而随机预言机模型是一种较弱的安全模型。Yang 等[14]提出了另外一种支持属性撤销的 ABE 方案中，属性授权机构需要更新密文，同时生成新版本的密钥、更新密钥和私钥，这些计算工作给属性授权机构带来严重的计算负担。马华等[15]提出了一种支持属性撤销的 ABE 方案，该方案基于密钥加密密钥树实现了密钥的更新，且在解密过程中，将部分解密运算外包给解密服务器，减少了用户的计算代价。马华等[15]声称该方案能够抵抗用户合谋攻击，但通过分析发现，该方案无法抵抗撤销用户与未撤销用户的合谋攻击。Shiraishi 等[16]提出了一种属性可撤销的 ABE 方案，但是其基于复杂假设完成安全证明导致安全性较弱。

目前，移动终端的弱计算能力与 ABE 方案解密过程中的复杂计算过程相矛盾。因此，将 ABE 方案的复杂计算外包给云服务商是一种切实可行的解决办法。Green 等[17]提出了一种计算外包 ABE 方案，该方案通过云服务商将原始密文转变成 ElGamal 型密文，数据用户通过一次指数运算就可获得明文。Lai 等[18]和 Li 等[19]分别提出了可验证外包解密的 ABE 方案。另外，Li 等[19]所提方案的密文长度与方案所采用的访问结构复杂度无关。

文献[12,15]中，一个群中的用户共享相同的属性群密钥，因此已被撤销的用户和未被撤销的用户可以发起合谋攻击。针对上述问题，本文提出了一种支持属性立即撤销且解密外包的 ABE 方案，该方案可以有效抵抗上述合谋攻击，采用外包技术，还可有效减少属性中心和用户的计算负担。本文在标准模型下基于计算性 Diffie-Hellman（CDH, computational Diffie-Hellman）假设完成安全证明。最后，实验表明所提方案具有更高的安全性，且提高了用户的解密效率。

## 2 理论基础知识

### 2.1 双线性映射

存在一个四元组 $(p,G,G_T,e)$。其中，$p$ 是大素数，$G$ 和 $G_T$ 是阶为素数 $p$ 的循环群。同时满足以下 2 个条件的映射 $e:G\times G\to G_T$ 为双线性映射。

1) 双线性：对于 $\forall u,v\in G$，$a,b\in Z_p$，有 $e(u^a,v^b)=e(u,v)^{ab}$。

2) 非退化性：$\exists g\in G$，使 $e(g,g)$ 在 $G_T$ 中的阶是 $p$。

3) 可计算性：对于 $\forall u,v\in G$，都能够计算 $e(u,v)$。

### 2.2 线性秘密共享方案

假设参与者集合为 $P=\{P_1,\cdots,P_n\}$，如果 $\prod$ 满足以下 2 个条件，则 $\prod$ 是定义在 $P$ 上的一个线性秘密共享方案（LSSS, linear secret sharing scheme）。

1) 对于每个参与者所持有的秘密份额都可以

构成 $Z_p$ 上的向量。

2) 每个 LSSS 的 $\prod$ 都对应着一个生成矩阵 $\boldsymbol{M}(l\times n)$，且映射 $\rho:\{1,2,\cdots,l\}\to P$ 把 $\boldsymbol{M}$ 的每一行 ($i=1,2,\cdots,l$)映射到参与者 $\rho(i)$，其中，$\rho$ 为单射函数。考虑向量 $\boldsymbol{v}=(s,y_2,\cdots,y_n)$，$s\in Z_p$ 是共享秘密值，选择随机数 $y_2,\cdots,y_n\in Z_p^*$ 隐藏共享秘密值 $s$。则共享秘密值 $s$ 的 $l$ 个秘密份额可以记为 $\boldsymbol{Mv}$，其中 $\lambda_i=(\boldsymbol{Mv})_i$ 是共享秘密值 $s$ 的第 $i$ 个秘密份额，并将其分配给 $\rho(i)$。

### 2.3 CDH 假设

给定三元组 $(g,g^a,g^b)\in G^3$，其中，$a,b\in Z_p^*$ 且未知，要求计算 $g^{ab}$ 的值。设敌手 $\mathcal{A}$ 成功输出 $g^{ab}$ 的概率为 $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{CDH}}=\left|\Pr[\mathcal{A}(g^a,g^b)=g^{ab}]\right|\leqslant\varepsilon$。其中 $\varepsilon$ 是可忽略的，则 CDH 问题是 $\varepsilon$−困难的。

### 2.4 密钥加密密钥树

密钥加密密钥（KEK, key encryption key）树[12]是一个完全二叉树，如图 1 所示。令系统中所有用户集合为 $U=\{u_1,u_2,\cdots,u_N\}$，系统中的所有属性集合为 $W=\{\mathrm{att}_1,\mathrm{att}_2,\cdots,\mathrm{att}_n\}$。设 $G_i\subset U$ 是拥有属性 $\mathrm{att}_i$ 的一个用户集合，被称为属性群。$G_i$ 则是可以正常访问属性 $\mathrm{att}_i$ 的访问列表。设 $\mathcal{G}=\{G_1,G_2,\cdots,G_n\}$ 是属性群集合。例如，若用户 $u_1$、$u_2$、$u_3$ 分别拥有属性集合 $\{\mathrm{att}_1,\mathrm{att}_2\}$、$\{\mathrm{att}_1,\mathrm{att}_2,\mathrm{att}_3\}$、$\{\mathrm{att}_2,\mathrm{att}_3\}$，那么 $G_1=\{u_1,u_2\}$、$G_2=\{u_1,u_2,u_3\}$、$G_3=\{u_2,u_3\}$。

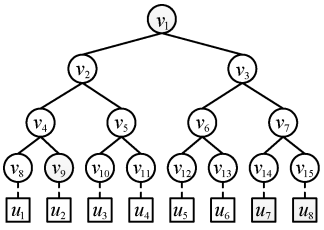


图 1　KEK 树示意

数据服务管理者（DSM, data service manager）按如下过程构建 KEK 树。

1) 二叉树的每一个叶子节点关联用户集合 $U$ 中的每一个用户 $u_k$。同时，每个内部节点 $v_j$ 存储一个随机值 $\theta_j$。

2) 路径节点生成算法 $\mathrm{Path}(u_k)$：从根节点到叶子节点上的所有节点被定义为用户 $u_k$ 的路径节点，如 $\mathrm{Path}(u_6)=\{v_{13},v_6,v_3,v_1\}$。

3) 最小覆盖集算法 $\mathrm{Mincs}(G_i)$：可以涵盖属性群 $G_i$ 中所有用户的最少节点集合为最小覆盖集。若 $G_i=\{u_1,u_2,u_4,u_6,u_7,u_8\}$，则 $\mathrm{Mincs}(G_i)=\{v_4,v_{11},v_{13},v_7\}$；若 $G_{i'}=\{u_1,u_4,u_7,u_8\}$，则 $\mathrm{Mincs}(G_{i'})=\{v_8,v_{11},v_7\}$。

4) 考虑 $\mathrm{Path}(u_k)$ 与 $\mathrm{Mincs}(G_i)$ 的交集，每一个用户 $u_k\in G_i$ 的路径节点 $\mathrm{Path}(u_k)$ 与 $\mathrm{Mincs}(G_i)$ 的交集至多有一个节点。例如，2)和 3)中的 $u_6$ 与 $\mathrm{Mincs}(G_i)$ 的交集为节点 $v_{13}$，$u_6$ 与 $\mathrm{Mincs}(G_{i'})$ 的交集为空。

## 3 文献[12,15]安全性分析

在 ABE 方案中，由于每个属性被多个用户共享，属性撤销是一个极其困难的问题，因此构建一个安全有效的属性撤销 ABE 方案至关重要。另外，ABE 方案一个重要的安全特点就是抵抗用户合谋攻击，但是在阅读分析文献[12,15]时发现，这 2 种方案是不安全的，且存在用户合谋攻击。下面分别对这 2 种方案进行安全性分析。

### 3.1 文献[12]安全性分析

文献[12]提出了属性群概念，并构建 KEK 树为用户分发属性群密钥，同时完成属性撤销后的密钥更新工作，但是该方案不能够抵抗撤销用户和未撤销用户的合谋攻击。

一个用户的密钥由两部分组成：属性集合关联的密钥 $\mathrm{sk}_1$（等同于基本 ABE 用户私钥）和基于 KEK 树的属性群密钥 $\mathrm{sk}_2$。$\mathrm{sk}_1$ 和 $\mathrm{sk}_2$ 是完全独立的，当一个用户从某个属性群撤销时，该用户将失去 $\mathrm{sk}_2$，但是该用户的 $\mathrm{sk}_1$ 仍然是可用的，因此该用户可以和其他用户合谋获得 $\mathrm{sk}_2$，完成最终密文解密。

攻击实例：假设消息 $m$ 用访问结构“教师 and 计算机”加密。用户 $u_1$ 的属性集合为“学生，计算机”，用户 $u_2$ 的属性集合为“教师，计算机”，则“计算机”的用户集合为 $G_j=\{u_1,u_2\}$，所以“计算机”的最小覆盖集为 $\mathrm{Mincs}(G_j)=\{v_4\}$，此时关联属性“计算机”的密文头文件用节点 $v_4$ 的随机值 $\theta_4$ 加密。$u_1$ 的路径节点是 $\mathrm{Path}(u_1)=\{v_8,v_4,v_2,v_1\}$，$u_2$ 的路径节点是 $\mathrm{Path}(u_2)=\{v_9,v_4,v_2,v_1\}$。

当没有属性撤销时，$u_2$ 能够通过 $L=(L')^{\lambda}$ 解密获得 $\mathrm{sk}_{2,u_2}$，通过属性集合获得 $\mathrm{sk}_{1,u_2}$，最终解密密文获得消息 $m$。

当 $u_2$ 改变行业从事密码学时，该用户的属性“计算机”将被撤销，则“计算机”的用户集合为 $G_j=\{u_1\}$，所以“计算机”的最小覆盖集为 $\mathrm{Mincs}(G_j)=\{v_8\}$，此时关联属性“计算机”的密

文头文件将通过用节点 $v_8$ 的随机值 $\theta_8$ 加密。即使用户 $u_2$ 仍然拥有关联属性集合“教师，计算机”的私钥 $\mathrm{sk}_{1,u_2}$，由于其没有 $\theta_8$，不能完成密文头解密，因此用户 $u_2$ 也不能完成最终密文解密。但是用户 $u_1$ 和用户 $u_2$ 合谋，$u_1$ 将随机值 $\theta_8$ 泄露给 $u_2$，$u_2$ 将通过 $\theta_8$ 完成对密文头的解密，再结合 $\mathrm{sk}_{1,u_2}$ 完成解密获得消息 $m$。

### 3.2 文献[15]安全性分析

文献[15]基于文献[12]构建，属性集合关联的密钥 $\mathrm{sk}_1$ 和 KEK 树分发的属性群密钥 $\mathrm{sk}_2$ 仍然是完全独立的，因此该方案也不能抵抗撤销用户和未撤销用户的合谋攻击。其分析过程如 3.1 节所述，这里不再赘述。

## 4 RO-CP-ABE 方案系统及安全模型

本节首先描述了支持属性撤销的属性基加密（RO-CP-ABE, CP-ABE with attribute revocation and outsourced decryption）方案的系统模型及其各组成部分的功能，然后对其进行形式化的描述，最后给出该方案的安全模型。

### 4.1 系统模型

本文提出了一种支持属性立即撤销的属性基加密方案，系统模型主要包括以下 4 类实体。

属性机构（AA, attribute authority）：AA 是一个完全可信的权威机构，主要负责生成系统公钥和系统主私钥，同时管控属性密钥分发等工作。

云服务商（CSP, cloud service provider）：CSP 主要是指第三方云存储提供商，本文定义的 CSP 包括 DSM、计算服务和存储服务。数据拥有者将加密的数据上传至 CSP，减少了用户的存储负担。为了减少用户（数据拥有者和数据用户）的计算负担，当撤销属性时，DSM 完成密文更新工作；当数据解密时，CSP 承担了解密过程中的部分计算。同时本文假设 CSP 是诚实并好奇的（honest but curious）。

数据拥有者（DO, data owner）：DO 在将数据上传至 CSP 之前需要用对称密钥 PK 加密数据，然后基于本文所提方案加密对称密钥 PK，通过对 PK 的安全共享完成数据的细粒度访问控制。

数据用户（DU, data user）：DU 即系统中的消费者，能够自由地访问云中的密文数据资源。属性机构根据其属性为其生成私钥并用于解密密钥密文。若其属性没有被撤销且满足访问结构，则用户能够计算出最终明文。

### 4.2 形式化定义

首先给出本文相关符号及其含义，如表 1 所示。

**表 1 相关符号及其含义**

| 符号 | 含义 |
|---|---|
| $S$ | 数据用户的属性集合 |
| $(\boldsymbol{M},\rho)$ | 数据拥有者定义的 LSSS 访问结构 |
| $m$ | 明文消息 |
| PK,MSK | 系统公钥和系统主私钥 |
| DPK,DSK | DSM 公钥和主私钥 |
| RK | 数据用户私钥 |
| SK | 数据用户转换密钥 |
| KEK′ | 属性群初始密钥 |
| KEK | 属性群密钥 |
| $\overline{\mathrm{KEK}}$ | 属性撤销后的属性群密钥 |
| CT′ | 中间密文 |
| CT | 密文 |
| $\overline{\mathrm{CT}}$ | 转换密文 |
| $\overline{\mathrm{CT}}$ | 属性撤销后的密文 |
| Hdr | 密文头 |
| $\overline{\mathrm{Hdr}}$ | 属性撤销后的密文头 |

RO-CP-ABE 方案包含以下 5 个阶段。

1) 系统初始化阶段

$\mathrm{AASetup}(1^{\lambda})\rightarrow\{\mathrm{PK},\mathrm{MSK}\}$：AA 运行该算法，输入安全参数 RK=$\lambda$，输出系统公钥 PK 和系统主私钥 MSK。

$\mathrm{DSMSetup}(\mathrm{PK})\rightarrow\{\mathrm{DPK},\mathrm{DSK}\}$：DSM 运行该算法，输入 PK，输出 DSM 的公钥 DPK 和主私钥 DSK。

2) 私钥生成阶段

$\mathrm{AAKeyGen}(\mathrm{id},\mathrm{PK},\mathrm{DPK},\mathrm{MSK},S)\rightarrow\{\mathrm{RK},\mathrm{SK},\mathrm{KEK}'\}$：AA 运行该算法，输入 PK、DPK、MSK 和属性集合 $S$，输出用户私钥 RK、转换密钥 SK 和属性群初始密钥 KEK′。

$\mathrm{DSMKeyGen}(\mathrm{KEK}',S)\rightarrow\mathrm{KEK}$：DSM 运行该算法，输入 KEK′ 和 $S$，输出用户属性群密钥 KEK。

3) 数据加密阶段

$\mathrm{Encrypt}(\mathrm{PK},(\boldsymbol{M},\rho),m)\rightarrow\mathrm{CT}'$：输入系统公钥 PK、访问结构 $(\boldsymbol{M},\rho)$ 和明文消息 $m$，输出中间密文 CT′。

$\mathrm{DSMEncrypt}(\mathrm{PK},\mathrm{DSK},\mathrm{CT}')\rightarrow\{\mathrm{Hdr},\mathrm{CT}\}$：输入 PK、DPK 和 CT′，输出密文头 Hdr 和最终密文 CT。

4) 数据解密阶段

OutDecrypt(PK,Hdr,CT,SK,KEK) $\to \overline{\mathrm{CT}}$：CSP 运行该算法，输入 PK、Hdr、CT 和 SK，输出转换密文 $\overline{\mathrm{CT}}$。

Decrypt(PK,$\overline{\mathrm{CT}}$,CT,RK) $\to m$：DU 运行该算法，输入 PK、$\overline{\mathrm{CT}}$、CT 和 RK，输出明文数据 $m$。

5) 用户属性撤销阶段

UpKEK(DSK,KEK,$\mathrm{att}_x$) $\to \overline{\mathrm{KEK}}$：DSM 运行该算法，输入 DSK、KEK 和被撤销属性 $\mathrm{att}_x$，输出新的属性群密钥 $\overline{\mathrm{KEK}}$。

ReEncryption(Hdr,CT,$\mathrm{att}_x$) $\to \{\overline{\mathrm{Hdr}},\overline{\mathrm{CT}}\}$：DSM 运行该算法，输入 Hdr、CT 和被撤销属性 $\mathrm{att}_x$，输出新的密文头 $\overline{\mathrm{Hdr}}$ 和密文 $\overline{\mathrm{CT}}$。

### 4.3 安全模型

为证明所提方案可以有效抵抗用户合谋攻击，定义敌手可以询问 2 种类型密钥：1) 已撤销用户的私钥询问，其中，$f(S,(\boldsymbol{M},\rho))=1$，但已撤销挑战属性；2) 未撤销用户的私钥询问，其中，$f(S,(\boldsymbol{M},\rho))\neq 1$，但 $S$ 包含挑战属性。证明过程如下。

**初始化**　$\mathcal{A}$ 选择挑战属性 Type-I 和挑战访问结构 $(\boldsymbol{M}^*,\rho^*)$ 并发送给 $\mathcal{B}$。其中，若 $\mathrm{att}^*\notin S$，则一定有 $f(S,(\boldsymbol{M}^*,\rho^*))\neq 1$。

**系统建立**　$\mathcal{B}$ 运行 AASetup 和 DSMSetup 后得到 PK、MSK、DPK 和 DSK。然后，$\mathcal{B}$ 更新关联属性 $\mathrm{att}^*$ 的密钥对 $\overline{\mathrm{DPK}}$ 和 $\overline{\mathrm{DSK}}$。最后，$\mathcal{B}$ 将 PK、DPK 和 $\overline{\mathrm{DPK}}$ 发送给 $\mathcal{A}$，自己保留 MSK、DSK 和 $\overline{\mathrm{DSK}}$。

**询问阶段 1**　$\mathcal{A}$ 可以询问以下 2 种类型密钥。

1) Type-I 私钥询问 $\langle u_{\mathrm{I}},S_{\mathrm{I}}\rangle$：用户 $u_{\mathrm{I}}$ 的属性集合 $S_{\mathrm{I}}$ 满足访问结构 $(\boldsymbol{M}^*,\rho^*)$，但是 $u_{\mathrm{I}}$ 的属性 $\mathrm{att}_x^*$ 已经被撤销。$\mathcal{B}$ 运行 AAKeyGen 和 DSMKeyGen 算法获得 $\mathrm{RK_I}$、$\mathrm{SK_I}$ 和 $\mathrm{KEK_I}$，然后将它们发送给 $\mathcal{A}$。

2) Type-II 私钥询问 $\langle u_{\mathrm{II}},S_{\mathrm{II}}\rangle$：用户 $u_{\mathrm{II}}$ 的属性集合 $S_{\mathrm{II}}$ 不满足访问结构 $(\boldsymbol{M}^*,\rho^*)$，但是 $u_{\mathrm{II}}$ 拥有属性 $\mathrm{att}_x^*$。$\mathcal{B}$ 运行 AAKeyGen 和 DSMKeyGen 算法获得 $\mathrm{RK_{II}}$、$\mathrm{SK_{II}}$ 和 $\mathrm{KEK_{II}}$，然后将它们发送给 $\mathcal{A}$。

**挑战阶段**　$\mathcal{A}$ 提交 2 个等长消息 $m_0$ 和 $m_1$。$\mathcal{B}$ 选择随机值 $b\in\{0,1\}$，并运行 Encrypt 和 DSMEncrypt 算法获得 Hdr* 和 $\mathrm{CT}_b^*$，最后将二者传递给 $\mathcal{A}$。

**询问阶段 2**　类似询问阶段 1。

**猜测阶段**　$\mathcal{A}$ 输出 $b'\in\{0,1\}$。若 $b'=b$，则 $\mathcal{A}$ 赢得游戏，攻破所提方案。$\mathcal{A}$ 攻破所提方案的优势定义为：$\mathrm{Adv}_{\mathcal{A}}=|\Pr[b'=b]-\frac{1}{2}|$。

**定义 1**　假设没有多项式时间的敌手能够以不可忽略的优势来攻破上述安全模型，则所提方案是选择安全的。

## 5 RO-CP-ABE 方案构造

本节给出 RO-CP-ABE 方案的具体构建方法，并基于 CDH 假设给出了方案的安全性证明。

### 5.1 方案构造

1) 系统初始化阶段

AASetup($1^\lambda$) $\to$ {PK,MSK}：该算法首先选择阶为素数 $p$ 的循环群 $G$ 和 $G_T$，$g$ 是群 $G$ 的生成元，存在映射 $e:G\times G\to G_T$。随机选取 $\alpha,a\in Z_p$，随机选取 $h_1,h_2,\cdots,h_n\in G$。输出系统主私钥 MSK=$g^\alpha$ 和系统公钥 PK=$(g,e(g,g)^\alpha,g^a,h_1,h_2,\cdots,h_n)$。

DSMSetup(PK) $\to$ {DPK,DSK}：DSM 为每一个属性 $\mathrm{att}_i$ $(1\leqslant i\leqslant n)$选择一个随机指数 $t_i\in Z_p$ 并计算 $T_i=g^{t_i}$，输出 DSM 的公钥 $\mathrm{DPK}=\{T_i|1\leqslant i\leqslant n\}$ 和主私钥 $\mathrm{DSK}=\{t_i|1\leqslant i\leqslant n\}$。

2) 私钥生成阶段

AAKeyGen(id,PK,DPK,MSK,$S$) $\to$ {RK,SK,KEK′}：该算法随机选择 $r_{\mathrm{id}}\in Z_p$，然后计算 $K'=g^{\alpha+ar_{\mathrm{id}}}$，$L'=g^{r_{\mathrm{id}}}$，对于任意 $\mathrm{att}_i\in S$，计算 $K_i'=h_i^{r_{\mathrm{id}}}$，$\mathrm{kek}_i'=T_i^{r_{\mathrm{id}}}$。然后随机选择 $\lambda\in Z_p$，计算 $K=(K')^\lambda$，$L=(L')^\lambda$，$K_i=(K_i')^\lambda$，$\mathrm{kek}_i=(\mathrm{kek}_i')^\lambda$。最后输出用户私钥 RK=$\lambda$，转换密钥 SK=$(K,L,\{K_i\})$ 和属性群初始密钥 KEK′=$\{\mathrm{att}_i,\mathrm{kek}_i\},\mathrm{att}_i\in S$。

DSMKeyGen(KEK′,$S$) $\to$ KEK：该算法按 2.4 节中 KEK 树为用户生成属性群密钥。对于每一个 $\mathrm{att}_i\in S$，DSM 计算 $\varphi_i$=Path($u_{\mathrm{id}}$)$\bigcap$Mincs($G_i$)。若 $\varphi_i=\varnothing$，DSM 停止计算；若 $\varphi_i\neq\varnothing$，DSM 计算 $\mathrm{KEK}_i=(\mathrm{kek}_i)^{\frac{1}{\theta_j}}=g^{\frac{t_i r_{\mathrm{id}}\lambda}{\theta_j}}$，其中随机值 $\theta_j$ 所对应节点 $v_j\in\varphi_i$。然后输出 $\mathrm{KEK}=\{\mathrm{att}_i,v_j,\mathrm{kek}_i,\mathrm{KEK}_i\},\mathrm{att}_i\in S$。

3) 数据加密阶段

Encrypt(PK,$(\boldsymbol{M},\rho)$,$m$) $\to$ CT′：该算法随机选择向量 $\boldsymbol{v}=(s,y_2,y_3,\cdots,y_n)\in Z_p^n$ 用于共享加密指数 $s$。对于 $1\leqslant i\leqslant l$，计算 $\lambda_i=\boldsymbol{v}\boldsymbol{M}_i$，其中 $\boldsymbol{M}_i$ 是 $\boldsymbol{M}$ 的

第 $i$ 行。然后计算 $C = me(g,g)^{\alpha s}$，$C' = g^s$，对于 $\forall i = 1,2,\cdots,l$，$C_i = g^{a\lambda_i} h_{\rho(i)}^{-s}$。最后输出中间密文 $\mathrm{CT}' = (C, C', \{C_i\}), 1 \leqslant i \leqslant l$。

DSMEncrypt(PK,DSK,CT′)→{Hdr,CT}：对于访问结构 $(\boldsymbol{M}, \rho)$ 中每一个属性 $\mathrm{att}_i$，DSM 随机选择 $k_i \in Z_p$ 并调用 Mincs($G_i$) 算法。然后重新加密中间密文 CT′ 获得 $\mathrm{CT} = (C, C', \{C_i g^{k_i}\}), 1 \leqslant i \leqslant l$，计算密文头 $\mathrm{Hdr}=\{v_j, E(k_i) = g^{\frac{k_i \theta_j}{t_i}}\}, v_j \in \mathrm{Mincs}(G_i), 1 \leqslant i \leqslant l$。最后 DSM 将 (CT,Hdr) 上传到云服务商进行存储。

4) 数据解密阶段

当数据用户的属性满足密文的访问结构且用户属性未被撤销时，可以通过以下过程计算获得明文。

OutDecrypt(PK,Hdr,CT,SK,KEK)→$\overline{\mathrm{CT}}$：云服务商根据转换密钥 SK 和属性群密钥 KEK 计算 $T'$、$T''$ 和 $\overline{\mathrm{CT}}$，如式(1)~式(3)所示，然后云服务商将 $\overline{\mathrm{CT}}$ 和 CT 发送给数据用户。

$$T' = \prod_{i \in I} \left( \frac{e(L, C_i g^{k_i}) e(K_i, C')}{e(\mathrm{KEK}_i, E(k_i))} \right)^{w_i} = \prod_{i \in I} \left( \frac{e(g^{r_{\mathrm{id}}\lambda}, g^{a\lambda_i} h_{\rho(i)}^{-s} g^{k_i}) e(h_i^{r_{\mathrm{id}}\lambda}, g^s)}{e(g^{\frac{t_i r_{\mathrm{id}} \lambda}{\theta_j}}, g^{\frac{k_i \theta_j}{t_i}})} \right)^{w_i} = \prod_{i \in I} \left( \frac{e(g^{r_{\mathrm{id}}\lambda}, g^{a\lambda_i}) e(g^{r_{\mathrm{id}}\lambda}, g^{k_i})}{e(g^{r_{\mathrm{id}}\lambda}, g^{k_i})} \right)^{w_i} = \prod_{i \in I} \left( e(g^{r_{\mathrm{id}}\lambda}, g^{a\lambda_i}) \right)^{w_i} = e(g,g)^{r_{\mathrm{id}} a \lambda s} \tag{1}$$

$$T'' = e(K, C') = e(g^{(\alpha + a r_{\mathrm{id}})\lambda}, g^s) = e(g,g)^{\alpha\lambda s} e(g,g)^{a r_{\mathrm{id}} \lambda s} \tag{2}$$

$$\overline{\mathrm{CT}} = \frac{T''}{T'} = \frac{e(g,g)^{\alpha\lambda s} e(g,g)^{a r_{\mathrm{id}} \lambda s}}{e(g,g)^{r_{\mathrm{id}} a \lambda s}} = e(g,g)^{\alpha\lambda s} \tag{3}$$

Decrypt(PK,$\overline{\mathrm{CT}}$,CT,RK)→$m$：数据用户接收到 $\overline{\mathrm{CT}}$ 后，用 RK=$\lambda$ 解密密文

$$m = \frac{C}{(\overline{\mathrm{CT}})^{\frac{1}{\mathrm{RK}}}} = \frac{me(g,g)^{\alpha s}}{(e(g,g)^{\alpha\lambda s})^{\frac{1}{\lambda}}} \tag{4}$$

5) 用户属性撤销阶段

UpKEK(DSK,KEK,$\mathrm{att}_x$)→$\overline{\mathrm{KEK}}$：当用户 $u_z$ 的属性 $\mathrm{att}_x$ 被撤销时，DSM 随机选择 $\sigma_x$ 并计算 $\overline{T_x} = T_x^{\sigma_x}$，$\overline{t_x} = t_x \sigma_x$，然后用 $\overline{T_x}$ 和 $\overline{t_x}$ 替代 DPK 和 DSK 中的 $T_x$ 和 $t_x$，获得新的 DSM 公钥 $\overline{\mathrm{DPK}}$ 和主私钥 $\overline{\mathrm{DSK}}$。DSM 更新属性群 $\overline{G_x}$ 并重新计算 Mincs($\overline{G_x}$)。例如，$G_x = \{u_1, u_2, u_5, u_6, u_7, u_8\}$，则 Mincs($G_x$)=$\{v_4, v_3\}$。当用户 $u_6$ 的属性 $\mathrm{att}_x$ 被撤销时，$\overline{G_x} = \{u_1, u_2, u_5, u_7, u_8\}$，则 $\mathrm{Mincs}(\overline{G_x}) = \{v_4, v_{12}, v_7\}$。对于每一个数据用户 $u_k \in \overline{G_x}$，DSM 计算 $\overline{\varphi_x}$=Path($u_k$)⋂Mincs($\overline{G_x}$)，然后计算 $\overline{\mathrm{kek}_x}=(\mathrm{kek}_x)^{\sigma_x}$ 和 $\overline{\mathrm{KEK}_x} = (\overline{\mathrm{kek}_x})^{\frac{1}{\overline{\theta_{j'}}}}$，其中随机值 $\overline{\theta_{j'}}$ 对应节点 $\overline{v_{j'}} \in \overline{\varphi_x}$。最后，DSM 用 $\{\mathrm{att}_x, \overline{v_{j'}}, \overline{\mathrm{kek}_x}, \overline{\mathrm{KEK}_x}\}$ 替换 KEK 中的 $\{\mathrm{att}_x, v_j, \mathrm{kek}_x, \mathrm{KEK}_x\}$。

ReEncryption(Hdr,CT,$\mathrm{att}_x$)→{$\overline{\mathrm{Hdr}}$,$\overline{\mathrm{CT}}$}：DSM 随机选择 $s', \overline{k_x} \in Z_p$，重加密密文：$\overline{C} = Ce(g,g)^{\alpha s'}$，$\overline{C'} = Cg^{s'}$，$\overline{C_x} = C_x h_{\rho(x)}^{-s'} g^{\overline{k_x} - k_x}$，$\{C_i g^{k_i} h_{\rho(i)}^{-s'}\}, 1 \leqslant i \leqslant l, i \neq x$。最后，$\overline{CT} = (\overline{C}, \overline{C'}, \overline{C_x}, \{C_i \ \ g^{k_i} h_{\rho(i)}^{-s'}\}), 1 \leqslant i \leqslant l, i \neq x$。

更新密文头为

$$\overline{\mathrm{Hdr}} = \begin{cases} \{\overline{v_{j'}}, E(\overline{k_x}) = g^{\frac{\overline{k_x}\overline{\theta_{j'}}}{\overline{t_x}}}\}, \overline{v_{j'}} \in \mathrm{Mincs}(\overline{G_x}) \\ \{v_j, E(k_i) = g^{\frac{k_i \theta_j}{t_i}}\}, v_j \in \mathrm{Mincs}(G_i), 1 \leqslant i \leqslant l, i \neq x \end{cases} \tag{5}$$

## 5.2 安全证明

**定理 1** 若 CDH 假设在群 $G$ 中成立，则没有多项式时间敌手能够攻破 RO-CP-ABE 方案，其中挑战矩阵为 $\boldsymbol{M}^*(l^* \times n^*)$。

**证明** 若 $\mathcal{A}$ 在 $q_{\mathrm{I}}$ 次 Type-I 询问和 $q_{\mathrm{II}}$ 次 Type-II 询问后，攻破所提方案的优势为不可忽略的值 $\varepsilon = \mathrm{Adv}_{\mathcal{A}}$。那么，可以创造一个 $\mathcal{B}$ 能够以不可忽略的优势 $\mathrm{Adv}_{\mathcal{B}} = \frac{\varepsilon}{q_1 q_{\mathrm{II}}}$ 攻破 CDH 假设。

**初始化** 挑战者将 $A = g^{z_1}$ 和 $B = g^{z_2}$ 发送给仿真者 $\mathcal{B}$，$\mathcal{A}$ 选择挑战访问结构 $(\boldsymbol{M}^*, \rho^*)$ 和挑战属性 $\mathrm{att}_x^*$ 并传递给 $\mathcal{B}$。其中，若 $\mathrm{att}^* \notin S$，则一定有 $f(S, (\boldsymbol{M}^*, \rho^*)) \neq 1$。

**系统建立** $\mathcal{B}$ 随机选取 $\alpha, a, e_1, e_2, \cdots, e_n \in Z_p$，并计算 $h_i = g^{e_i}$。输出公钥 PK=$(g, e(g,g)^{\alpha}, g^a, h_1, \cdots, h_n)$ 和系统主私钥 MSK=$g^{\alpha}$。对于每一个属性 $\mathrm{att}_i$ ($1 \leqslant i \leqslant n, i \neq x$)，$\mathcal{B}$ 选择一个随机指数 $t_i \in Z_p$ 并计算 $T_i = g^{t_i}$。对于 $\mathrm{att}_x^*$，$\mathcal{B}$ 随机选取 $t_x^* \in Z_p$ 计算 $T_x^* = g^{t_x^*}$。输出公钥 $DPK = \{T_i | 1 \leqslant i \leqslant n, i \neq x\} \cup \{T_x^*\}$ 和主私钥 $\mathrm{DSK} = \{t_i | 1 \leqslant i \leqslant n, i \neq x\} \cup \{t_x^*\}$。

然后 $\mathcal{B}$ 更新 $\text{att}_x^*$ 的密钥对 $\overline{T_x^*}=(T_x^*)^{z_1}=A^{t_x^*}$，设置 $\overline{t_x^*}=z_1 t_x^*$。$\mathcal{B}$ 更新 DSM 的公钥 $\overline{\text{DPK}}=\{T_i|1\leqslant i\leqslant n, i\neq x\}\cup\{\overline{T_x^*}\}$ 和 DSM 的主私钥 $\overline{\text{DSK}}=\{t_i|1\leqslant i\leqslant n, i\neq x\}\cup(\overline{t_x^*})$。注意：$\overline{t_x^*}$ 为理论值，实际情况下 $\mathcal{B}$ 不知道 $z_1$，因此也不能计算 $\overline{t_x^*}$。

**询问阶段 1**　$\mathcal{A}$ 可以询问 2 种类型密钥，$\mathcal{B}$ 设置 2 个列表 $L_{\text{I}}$ 和 $L_{\text{II}}$，并初始化 2 个列表为空。

1) Type - I 私钥询问 $\langle u_{\text{I}}, S_{\text{I}}\rangle$

用户 $u_{\text{I}}$ 的属性集合 $S_{\text{I}}$ 满足访问结构 $(\boldsymbol{M}^*,\rho^*)$，但是 $u_{\text{I}}$ 的属性 $\text{att}_x^*$ 已被撤销。$\mathcal{B}$ 首先查看 $L_{\text{I}}=\{u_{\text{I}}, r_{\text{I}}, \text{KEK}_{S_{\text{I}}}, \text{SK}_{\text{I}}, \text{RK}_{\text{I}}\}$ 中是否存在 $u_{\text{I}}$。若存在，则 $\mathcal{B}$ 将 $\{\text{KEK}_{S_{\text{I}}}, \text{SK}_{\text{I}}, \text{RK}_{\text{I}}\}$ 发送个敌手 $\mathcal{A}$；否则，$\mathcal{B}$ 随机选择 $r_{\text{I}},\lambda\in Z_p$，计算 $K=g^{\alpha\lambda}B^{ar_{\text{I}}\lambda}=g^{(\alpha+az_2r_{\text{I}})\lambda}$，$L=B^{r_{\text{I}}\lambda}=g^{z_2r_{\text{I}}\lambda}$，其隐含设置 $r_{\text{I}}^*=z_2r_{\text{I}}$。对于 $i\neq x$ 且 $\text{att}_i\in S_{\text{I}}$，计算 $K_i=h_i^{r_{\text{I}}\lambda}$，$\text{kek}_i=T_i^{r_{\text{I}}\lambda}$，$\mathcal{B}$ 产生 $\varphi_i=\text{Path}(u_{\text{I}})\cap\text{Mincs}(G_i)$ 并计算 $\text{KEK}_i=(\text{kek}_i)^{\frac{1}{\theta_j}}=g^{\frac{t_i r_{id}\lambda}{\theta_j}}$。其中，随机值 $\theta_j$ 与节点 $v_j\in\varphi_i$ 关联；针对 $\text{att}_x^*\in S_{\text{I}}$，$\mathcal{B}$ 计算 $K_x^*=h_x^{z_2r_{\text{I}}\lambda}=B^{e_xr_{\text{I}}\lambda}$ 和 $\text{kek}_x^*=(T_x^*)^{z_2r_{\text{I}}\lambda}=B^{t_x^*r_{\text{I}}\lambda}$。然后，$\mathcal{B}$ 随机选择值 $\theta^*\in\text{Path}(u_{\text{I}})$，计算获得 $\text{KEK}_x^*=(\text{kek}_x^*)^{\frac{1}{\theta^*}}=B^{\frac{t_x^*r_{\text{I}}\lambda}{\theta^*}}$。

$\mathcal{B}$ 令 $\text{RK}_{\text{I}}=\lambda$，$\text{SK}_{\text{I}}=(K,L,K_x^*,\{K_i\}),\text{att}_i\in S_{\text{I}},i\neq x$，$\text{KEK}_{S_{\text{I}}}=(\{\text{att}_x^*,v_j^*,\text{kek}_x^*,\text{KEK}_x^*\},\{\text{att}_i,v_j,\text{kek}_i,\ \text{KEK}_i\})$，$i\neq x$。然后，$\mathcal{B}$ 在 $L_{\text{I}}$ 中添加 $\{u_{\text{I}}, r_{\text{I}}, \text{KEK}_{S_{\text{I}}}, \text{SK}_{\text{I}}, \text{RK}_{\text{I}}\}$，再将 $\{\text{KEK}_{S_{\text{I}}}, \text{SK}_{\text{I}}, \text{RK}_{\text{I}}\}$ 传递给 $\mathcal{A}$。

2) Type - II 私钥询问 $\langle u_{\text{II}}, S_{\text{II}}\rangle$

用户 $u_{\text{II}}$ 的属性集合 $S_{\text{II}}$ 不满足访问结构 $(\boldsymbol{M}^*,\rho^*)$，但是 $u_{\text{II}}$ 拥有属性 $\text{att}_x^*$。$\mathcal{B}$ 首先查看 $L_{\text{II}}=\{u_{\text{II}}, r_{\text{II}}, \text{KEK}_{S_{\text{II}}}, \text{SK}_{\text{II}}, \text{RK}_{\text{II}}\}$ 中是否存在 $u_{\text{II}}$。若存在，则 $\mathcal{B}$ 将 $\{\text{KEK}_{S_{\text{II}}}, \text{SK}_{\text{II}}, \text{RK}_{\text{II}}\}$ 发送个敌手 $\mathcal{A}$；否则，$\mathcal{B}$ 随机选择 $r_{\text{II}},\lambda\in Z_p$，计算 $K=g^{(\alpha+ar_{\text{II}})\lambda}$，$L=g^{r_{\text{II}}\lambda}$。对于 $i\neq x$ 且 $\text{att}_i\in S_{\text{II}}$，仿真者 $\mathcal{B}$ 计算 $K_i=h_i^{r_{\text{II}}\lambda}$，$\text{kek}_i=T_i^{r_{\text{II}}\lambda}$，而后求交集 $\varphi_i=\text{Path}(u_{\text{II}})\cap\text{Mincs}(G_i)$。然后，$\mathcal{B}$ 根据交集结果计算 $\text{KEK}_i=(\text{kek}_i)^{\frac{1}{\theta_j}}=g^{\frac{t_i r_{\text{II}}\lambda}{\theta_j}}$，其中随机值 $\theta_j$ 所对应节点 $v_j\in\varphi_i$。对于 $\text{att}_x^*\in S_{\text{II}}$，计算 $K_x^*=h_x^{r_{\text{II}}\lambda}$，$\text{kek}_x^*=(\overline{T_x^*})^{r_{\text{II}}\lambda}=A^{t_x^*r_{\text{II}}\lambda}$，$\varphi_x^*=\text{Path}(u_{\text{II}})\cap\text{Mincs}(G_x)$ 和 $\text{KEK}_x^*=(\text{kek}_x^*)^{\frac{1}{\theta_j^*}}=A^{\frac{t_x^*r_{\text{II}}\lambda}{\theta_j^*}}$，其中随机值 $\theta_j^*$ 所对应节点 $v_j^*\in\varphi_x^*$。

$\mathcal{B}$ 设置 $\text{RK}_{\text{II}}=\lambda$，$\text{SK}_{\text{II}}=(K,L,\{K_i\}_{\text{att}_i\in S_{\text{II}}})$，$\text{KEK}_{S_{\text{II}}}=(\{\text{att}_x^*,v_j^*,\text{kek}_x^*,\text{KEK}_x^*\},\{\text{att}_i,v_j,\text{kek}_i,\text{KEK}_i\}_{i\neq x})$。最后，$\mathcal{B}$ 在 $L_{\text{II}}$ 中增加 $\{u_{\text{II}}, r_{\text{II}}, \text{KEK}_{S_{\text{II}}}, \text{SK}_{\text{II}}, \text{RK}_{\text{II}}\}$，并将 $\{\text{KEK}_{S_{\text{II}}}, \text{SK}_{\text{II}}, \text{RK}_{\text{II}}\}$ 发送给 $\mathcal{A}$。

**挑战阶段**　$\mathcal{A}$ 提交 2 个等长的消息 $m_0$ 和 $m_{\text{I}}$。$\mathcal{B}$ 随机选择 $b\in\{0,1\}$ 和向量 $\boldsymbol{v}=(s,y_2,y_3,\cdots,y_n)\in Z_p^n$，其用于共享加密指数 $s$。对于 $1\leqslant i\leqslant l$，计算 $\lambda_i=\boldsymbol{v}\boldsymbol{M}_i^*$，其中 $\boldsymbol{M}_i^*$ 是 $\boldsymbol{M}^*$ 的第 $i$ 行。然后，$\mathcal{B}$ 计算 $C=m_b e(g,g)^{\alpha s}$，$C'=g^s$ 和 $\{C_i=g^{a\lambda_i}h_{\rho(i)}^{-s}\},\forall i=1,2,\cdots,l$。

对于 $i\neq x$ 且 $\text{att}_i\in(\boldsymbol{M}^*,\rho^*)$，$\mathcal{B}$ 随机选择 $k_i\in Z_p$，并计算 $\{C_i^*=g^{a\lambda_i}h_{\rho(i)}^{-s}g^{k_i}\},1\leqslant i\leqslant l^*,i\neq x$；对于 $\text{att}_x^*\in(\boldsymbol{M}^*,\rho^*)$，计算 $C_x^*=g^{a\lambda_x}h_{\rho(x)}^{-s}g^{k_x^*}=g^{a\lambda_x}h_{\rho(x)}^{-s}A^{k_x}$，其意味着 $k_x^*=z_1k_x$。$\mathcal{B}$ 最终计算密文为 $\text{CT}_b^*=(C,C',C_x^*,\{C_i^*\}),1\leqslant i\leqslant l,i\neq x$。

对于 $\text{att}_i\in(\boldsymbol{M}^*,\rho^*)$，$\mathcal{B}$ 调用 $\text{Mincs}(G_i)$ 算法，并计算密文头

$$\text{Hdr}^*=\begin{cases}\{v_j,E(k_i)=g^{\frac{k_i\theta_j}{t_i}}\},v_j\in\text{Mincs}(G_i),1\leqslant i\leqslant l,i\neq x\\ \{v_j^*,E(k_x^*)=g^{\frac{z_1k_x\theta_j^*}{z_1t_x^*}}=g^{\frac{k_x\theta_j^*}{t_x^*}}\},v_j^*\in\text{Mincs}(G_x)\end{cases}\tag{6}$$

最后，$\mathcal{B}$ 将 $(\text{CT}_b^*,\text{Hdr}^*)$ 传递给 $\mathcal{A}$。

**询问阶段 2**　类似询问阶段 1。

**猜测阶段**　$\mathcal{A}$ 输出一个值 $b'\in\{0,1\}$ 作为对 $b$ 的猜测。假设 $\mathcal{A}$ 猜测 $b'=b$，且 $\text{Adv}_{\mathcal{A}}=|\Pr[b'=b]-\frac{1}{2}|=\varepsilon$。然后，仿真者 $\mathcal{B}$ 分别从 $L_{\text{I}}$ 和 $L_{\text{II}}$ 中选择 $\{u_{\text{I}}, r_{\text{I}}, \text{KEK}_{S_{\text{I}}}, \text{SK}_{\text{I}}, \text{RK}_{\text{I}}\}$ 和 $\{u_{\text{II}}, r_{\text{II}}, \text{KEK}_{S_{\text{II}}}, \text{SK}_{\text{II}}, RK_{\text{II}}\}$。对于 $\text{att}_x^*$，存在 $L_{\text{I}}$ 中的 $\{\text{SK}_{\text{I}}, \text{RK}_{\text{I}}\}$ 和 $L_{\text{II}}$ 中的 $\{\text{KEK}_{S_{\text{II}}}, \text{RK}_{\text{II}}\}$ 相结合，使等式(7)成立。

$$\begin{aligned}&\frac{(e(L,C_x^*)e(K_x^*,C'))^{\frac{1}{\text{RK}_{\text{I}}}}}{(e(\text{KEK}_x^*,E(k_x^*)))^{\frac{1}{\text{RK}_{\text{II}}}}}=\frac{e(B^{r_{\text{I}}},g^{a\lambda_x}h_{\rho(x)}^{-s}A^{k_x})e(B^{e_xr_{\text{I}}},g^s)}{e(A^{\frac{t_x^*r_{\text{II}}}{\theta_j^*}},g^{\frac{k_x\theta_j^*}{t_x^*}})}=\\ &\frac{e(B^{r_{\text{I}}},g^{a\lambda_x}A^{k_x})e(B^{r_{\text{I}}},g^{-e_xs})e(B^{e_xr_{\text{I}}},g^s)}{e(A^{r_{\text{II}}},g^{k_x})}=\\ &\frac{e(B^{r_{\text{I}}},g^{a\lambda_x})e(B^{r_{\text{I}}},A^{k_x})}{e(A^{r_{\text{II}}},g^{k_x})}=\\ &e(B^{r_{\text{I}}},g^{a\lambda_x})\end{aligned}\tag{7}$$

当且仅当 $A^{r_{\text{II}}}=g^{z_1z_2r_{\text{I}}}$ 时，等式(7)成立。$\mathcal{B}$ 计算 $g^{z_1z_2}=A^{\frac{r_{\text{II}}}{r_{\text{I}}}}=(\text{KEK}_x^*)^{\frac{\theta_j^*}{(r_{\text{I}}t_x^*RT_{\text{II}})}}$，其中，$\text{KEK}_x^*\in\text{KEK}_{S_{\text{II}}}$。

如果 $\mathcal{B}$ 没有中止游戏，那么 $\mathcal{A}$ 的视觉和真实的攻击视觉相同。假设敌手 $\mathcal{A}$ 进行了 $q_{\text{I}}$ 次 Type-I 询问和 $q_{\text{II}}$ 次 Type-II 询问，$\mathcal{B}$ 从 $L_{\text{I}}$ 和 $L_{\text{II}}$ 中正确地选中 $\{u_{\text{I}},r_{\text{I}},\text{KEK}_{S_{\text{I}}},\text{SK}_{\text{I}},\text{RK}_{\text{I}}\}$ 和 $\{u_{\text{II}},r_{\text{II}},\text{KEK}_{S_{\text{II}}},\text{SK}_{\text{II}},\text{RK}_{\text{II}}\}$ 的概率是 $\frac{1}{q_{\text{I}}q_{\text{II}}}$，因此，$\mathcal{B}$ 攻破 CDH 假设的优势为 $\text{Adv}_{\mathcal{B}}=\frac{\varepsilon}{q_{\text{I}}q_{\text{II}}}$。

## 6 方案分析及仿真

### 6.1 理论分析

#### 6.1.1 功能比较

表 2 表明对比方案的访问结构都具有强表达性，且可以灵活地表示属性的组合。所有方案都实现了属性级的用户撤销。文献[12,15]没有给出形式化的安全证明，相比较而言，文献[13,16]和本文方案给出了形式化安全证明，但只有本文方案基于弱假设 CDH 完成安全证明。另外，在解密过程中，文献[15]和本文方案将部分计算外包给 CSP，有效地减少了用户的计算量。

#### 6.1.2 通信成本

在进行通信成本对比之前，给出各符号所代表的含义，$|p|$、$|g|$、$|g_T|$分别代表 $Z_p$、$G$、$G_T$ 中元素的长度，$|C_k|$代表 KEK 的长度，$n_c$、$n_k$、$n_a$ 分别代表访问结构、私钥和系统中的属性数量，$n_u$ 代表系统中的用户数量。

通信成本主要由密钥和密文产生，本文方案与相关方案的通信成本对比情况如表 3 所示。

AA 与 DU 之间的通信成本主要由密钥产生。由于文献[15]和本文方案采用了解密外包技术，因此属性机构需要传送给数据用户一个最终解密密钥 RT。另外，本文方案需要属性机构传输 $n_k|g|$ 个 kek 密钥给数据用户，用于后续生成属性群密钥。

AA 与 DO 之间的通信成本主要由公钥产生。属性机构只需将公钥发送给 DO，然后 DO 使用公钥对明文消息加密。

CSP 与 DU 之间的通信成本主要由密文产生。文献[12,15]和本文方案使用了 KEK 树技术，所以 CSP 不仅要发送密文，还要发送密文头和 KEK 密钥。文献[12,15]中，CSP 需要额外发送大小为 $\frac{n_cn_u}{2}|C_k|$的密文头和大小为 $(\text{lb}(n_u+1))|C_k|$的属性群密钥。本文方案中，CSP 需要额外发送大小为 $\frac{n_cn_u}{2}|g|+\frac{n_u}{2}|p|$的密文头和大小为 $2n_k|g|+n_k|p|$ 的属性群密钥，DU 需要发送 $n_k|g|$ 个 kek 密钥给云服务商。另外，文献[15]和本文方案采用了外包解密

**表 2 本文方案与相关方案的功能对比**

| 对比方案 | 访问结构 | 安全假设 | 安全模型 | 撤销粒度 | 外包解密 |
|---|---|---|---|---|---|
| 文献[12]方案 | Tree | — | 一般群模型 | 属性级用户撤销 | 不支持 |
| 文献[13]方案 | LSSS | q-parallel BDHE | 随机预言机模型 | 属性级用户撤销 | 不支持 |
| 文献[15]方案 | LSSS | — | 一般群模型 | 属性级用户撤销 | 支持 |
| 文献[16]方案 | LSSS | q-parallel BDHE | 标准模型 | 属性级用户撤销 | 不支持 |
| 本文方案 | LSSS | CDH | 标准模型 | 属性级用户撤销 | 支持 |

**表 3 本文方案与相关方案的通信成本对比**

| 对比方案 | AA 与 DU | AA 与 DO | CSP 与 DU | CSP 与 DO |
|---|---|---|---|---|
| 文献[12]方案 | $(2n_k+1)\|g\|$ | $2\|g\|+\|g_T\|$ | $(2n_c+1)\|g\|+\|g_T\|+(\frac{n_cn_u}{2}+1\text{b}(n_u+1))\|C_k\|$ | $(2n_c+1)\|g\|+\|g_T\|$ |
| 文献[13]方案 | $(n_a+4)\|p\|$ | $(2n_a+4)\|g\|+\|g_T\|$ | $(3n_c+1)\|g\|+\|g_T\|$ | $(3n_c+1)\|g\|+\|g_T\|$ |
| 文献[15]方案 | $(n_k+2)\|g\|+\|p\|$ | $(n_a+2)\|g\|+\|g_T\|$ | $(n_c+n_k+5)\|g\|+\|g_T\|+(\frac{n_cn_u}{2}+1\text{b}(n_u+1))\|C_k\|$ | $(n_c+3)\|g\|+\|g_T\|$ |
| 文献[16]方案 | $(n_k+2)\|g\|$ | $(n_a+2)\|g\|+\|g_T\|$ | $(2n_c+1)\|g\|+\|g_T\|$ | $(2n_c+1)\|g\|+\|g_T\|$ |
| 本文方案 | $(2n_k+2)\|g\|+\|p\|$ | $(n_a+2)\|g\|+\|g_T\|$ | $(n_c+\frac{n_cn_u}{2}+4n_k+2)\|g\|+\|g_T\|+(n_k+\frac{n_u}{2})\|p\|$ | $(n_c+1)\|g\|+\|g_T\|$ |

技术，因此 DU 需要将其大小为$(n_k+2)|g|$的外包密钥发送给 CSP，由 CSP 代为解密。

CSP 与 DO 之间的通信成本主要由 DO 生成的密文产生。

通过原理分析发现，本文方案与其他方案相比在存储成本与通信成本的开销方面基本持平，在某些方面开销略大。但是本文方案基于弱假设且在标准模型下完成了方案的安全性证明，能够抵抗用户的合谋攻击；本文方案将复杂的解密计算外包给 CSP，同时由 CSP 完成属性群密钥更新和密文更新操作，有效较少用户的计算量。另外，文献[12,15]无法抵抗撤销用户与未撤销用户之间的合谋攻击，而抵抗用户合谋攻击时 ABE 方案最基本的安全需求。综合分析，本文方案具有一定的优势，更适用于实际情况。

### 6.2　实验仿真

本文基于 Ubuntu 系统搭建实验环境，并基于 Charm 实现本文所提方案。首先本文用 10 个属性构建了访问结构，并分别执行上述 5 种对比方案，每种方案执行 10 次，然后取其平均值作为最终值。需要注意，本文给出的时间为属性机构、DO 和 DU 的计算时间，而云服务具有强大的计算能力，因此这里没有列出 CSP 的计算时间。5 种方案各个阶段执行时间对比如图 2(a)所示。

系统建立阶段文献[13]的执行时间大约是其他方案的 2 倍，这是因为文献[13]在系统初始化阶段需要为每个属性设置 2 个公共属性密钥。密钥生成阶段本文方案执行时间要大于其他方案，这是因为本文方案属性机构需要为每个属性设置一个 kek 密钥，同时本文方案采用外包技术，属性机构需要将密钥盲化。数据加密阶段文献[13]的执行时间同样是其他方案的 2 倍，这是因为进行密文加密时，文献[13]需要为每个属性额外计算 2 个用于撤销后更新密文的组件，而其他方案撤销计算由第三方执行。数据解密阶段由于文献[15]和本文方案采用了外包解密技术，因此需要较少的计算量，这对于资源有限的用户至关重要。

本文方案由 CSP 完成属性群密钥更新和密文更新计算，因此本节只仿真加解密计算。

如图 2(b)所示，加密时间与访问结构复杂度呈正相关。另外，文献[13]需要为每个属性额外计算 2 个用于撤销后更新密文的组件，而其他方案撤销计算由第三方执行，所以文献[13]所需执行时间大约是其他方案的 2 倍，这在上文中已经分析。而其他 4 种方案的加密时间大致相同。

如图 2(c)所示，解密时间与解密所需属性数量呈线性增长关系，由于文献[15]和本文方案采用了外包解密技术，其用户将复杂的计算外包给 CSP，只需要进行少量计算就能够完成解密任务。在解密计算中，文献[15]只需计算一个双线性对操作和一个 $G_T$ 中的指数运算，而本文方案只需计算一个 $G_T$ 中的指数运算，与属性数量无关。

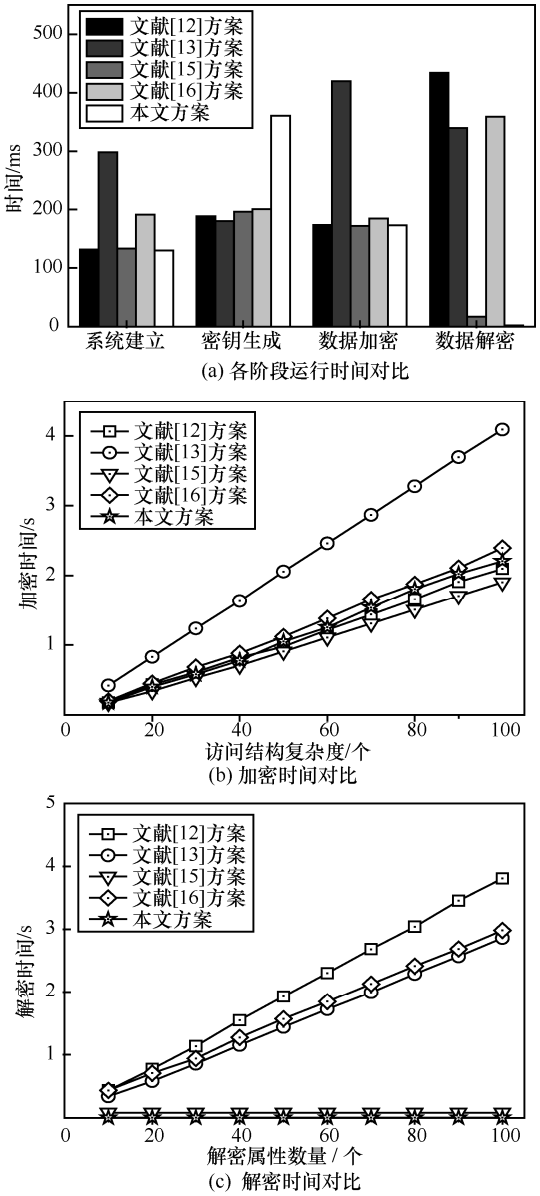


图 2　仿真时间对比

综合分析，本文方案对于属性机构的计算需求稍高于其他方案；由于采用外包解密技术，相对于其他方案，本文方案对于用户的计算需求明显小于其他方案；同时，由 DSM 完成属性撤销过程中的全部计算任务，有效较少了 AA 和用户的计算量，因此可

以得出本文方案在计算效率方面有较大优势。

## 7 结束语

属性级用户撤销是 ABE 方案的一个重点研究方向。本文研究现有方案发现文献[12,15]存在用户合谋攻击，其原因为 2 种方案中的 KEK 对于属性群中用户完全相同。基于此，本文提出了一种支持属性撤销的 ABE 方案，有效地解决了上述问题。所提方案可以有效抵抗撤销用户与未撤销用户的合谋攻击，同时，该方案将复杂的解密计算外包给 CSP，减轻了 DU 的计算负担。在标准模型下基于 CDH 假设完成安全证明。最后从理论和实验这 2 个方面对所提方案的效率与功能进行了分析，结果表明所提方案可以安全实现属性级用户撤销，并具有快速解密的能力。

## 参考文献：


[1] SUBASHINI S, KAVITHA V. A survey on security issues in service delivery models of cloud computing[J]. Journal of Network and Computer Applications, 2011, 34(1): 1-11.

[2] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//The 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2005: 457-473.

[3] 姚亮, 杨超, 马建峰, 等. 云端数据访问控制中基于中间代理的用户撤销新方法[J]. 通信学报, 2015, 36(11): 92-101.
YAO L, YANG C, MA J F, et al. New user revocation approach based on intermediate agency for cloud data access control[J]. Journal on Communications, 2015, 36(11): 92-101.

[4] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//The 13th ACM Conference on Computer and Communications Security. ACM, 2006: 89-98.

[5] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//IEEE Symposium on Security and Privacy. IEEE, 2007: 321-334.

[6] SOOKHAK M, YU F R, KHAN M K, et al. Attribute-based data access control in mobile cloud computing: Taxonomy and open issues[J]. Future Generation Computer Systems, 2017, 72(C): 273-287.

[7] 李勇, 曾振宇, 张晓菲. 支持属性撤销的外包解密方案[J]. 清华大学学报: 自然科学版, 2013, 53(12): 1664-1669.
LI Y, ZENG Z Y, ZHANG X F. Outsourced decryption scheme supporting attribute revocation[J]. Journal of Tsinghua University (Science & Technology), 2013, 53(12): 1664-1669.

[8] PIRRETTI M, TRAYNOR P, MCDANIEL P, et al. Secure attribute-based systems[C]//The 13th AMC conference on Computer and Communications Security. AMC, 2006: 99-112.

[9] RAFAELI S, HUTCHISON D. A survey of key management for secure group communication[J]. ACM Computing Surveys, 2003, 35(3): 309-329.

[10] IBRAIMI L, PETKOVIC M, NIKOVA S, et al. Mediated ciphertext-policy attribute-based encryption and its application[C]//The 10th International Workshop on Information Security Applications. 2009: 309-323.

[11] YU S, WANG C, REN K, et al. Attribute based data sharing with attribute revocation[C]//The 5th ACM Symposium on Information, Computer and Communications Security. ACM, 2010: 261-270.

[12] HUR J, NOH D K. Attribute-based access control with efficient revocation in data outsourcing systems[J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(7): 1214-1221.

[13] YANG K, JIA X, REN K. Attribute-based fine-grained access control with efficient revocation in cloud storage systems[C]//The 8th ACM SIGSAC Symposium on Information, Computer and Communications Security. ACM, 2013: 523-528.

[14] YANG K, JIA X. Security for cloud storage systems[M]. Berlin: Springer, 2014.

[15] 马华, 白翠翠, 李宾, 等. 支持属性撤销和解密外包的属性基加密方案[J]. 西安电子科技大学学报 (自然科学版), 2015, 42(6): 6-10.
MA H, BAI C C, LI B, et al. Attribute-based encryption scheme supporting attribute revocation and decryption outsourcing[J]. Journal of Xidian University (Science & Technology), 2015, 42(6): 6-10.

[16] SHIRAISHI Y, NOMURA K, MOHRI M, et al. Attribute revocable attribute-based encryption with forward secrecy for fine-grained access control of shared data[J]. IEICE Transactions on Information and Systems, 2017, 100(10): 2432-2439.

[17] GREEN M, HOHENBERGER S, WATERS B. Outsourcing the decryption of ABE ciphertexts[C]//The 20th USENIX Conference on Security. USENIX, 2011: 34.

[18] LAI J, DENG R H, GUAN C, et al. Attribute-based encryption with verifiable outsourced decryption[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(8): 1343-1354.

[19] LI J, SHA F, ZHANG Y, et al. Verifiable outsourced decryption of attribute-based encryption with constant ciphertext length[J]. Security and Communication Networks, 2017, 2017(2):1-11.


[作者简介]


**孙磊**（1973− ），男，江苏靖江人，博士，战略支援部队信息工程大学教授，主要研究方向为云计算、计算机网络、信息安全等。

**赵志远**（1989− ），男，吉林磐石人，61516 部队工程师，主要研究方向为云计算、信息安全和公钥密码等。

**王建华**（1962− ），男，北京人，博士，战略支援部队信息工程大学教授，主要研究方向为密码学、信息安全、计算机网络等。

**朱智强**（1961− ），男，吉林长春人，博士，战略支援部队信息工程大学教授，主要研究方向为云计算、网络与信息安全、密码学等。