具有可撤销功能的属性协同访问控制方案

彭长根[1,2,3]，彭宗凤[1,2]，丁红发[1,4]，田有亮[1,2,3]，刘荣飞[5]

（1. 贵州省公共大数据重点实验室(贵州大学)，贵州 贵阳 550025；2. 贵州大学计算机科学与技术学院，贵州 贵阳 550025；
3. 贵州大学密码学与数据安全研究所，贵州 贵阳 550025；4. 贵州财经大学信息学院，贵州 贵阳 550025；
5. 云上贵州大数据产业发展有限公司，贵州 贵阳 550025）

摘 要：针对属性协同访问控制面临更复杂的权限动态更新问题，提出了具有属性即时撤销、属性级用户撤销和协同策略撤销的属性协同访问控制方案。所提方案给出了形式化定义与安全模型，以分组属性组内成员列表信息的变化反映用户权限的动态更新，进一步设计高效的重加密算法实现属性即时撤销和用户撤销。在协同策略撤销方面，利用转移节点的转移值特性，快速更新协同属性对应的密文以实现细粒度的协同策略撤销。安全证明表明，所提方案在选择明文攻击下能保证数据机密性，前向、后向安全性，并能抵抗共谋攻击。与已有方案相比，所提方案具有更完备的细粒度撤销功能以及更高的撤销运行效率。

关键词：属性协同访问控制；基于密文策略的属性加密；撤销；转移节点；属性组

中图分类号：TP309

文献标识码：A

DOI: 10.11959/j.issn.1000−436x.2021058

Attribute-based revocable collaborative access control scheme

PENG Changgen[1,2,3], PENG Zongfeng[1,2], DING Hongfa[1,4], TIAN Youliang[1,2,3], LIU Rongfei[5]

1. Guizhou Provincial Key Laboratory of Public Big Data (Guizhou University), Guiyang 550025, China
2. College of Computer Science and Technology, Guizhou University, Guiyang 550025, China
3. Institute of Cryptography and Data Security, Guizhou University, Guiyang 550025, China
4. College of Information, Guizhou University of Finance and Economics, Guiyang 550025, China
5. Yunshang Guizhou Big Data Industry and Development Co., Ltd., Guiyang 550025, China

Abstract: To solve the dynamic update of access rights in attribute-based collaborative access control, a novel scheme was proposed with the revocation of attribute, user and collaborative policy. A formal definition and a security model were presented, the group-based attribute group were changed to reflect the update of rights, and further, an efficient re-encryption algorithm was used to realize the immediate revocation of attributes and users. The translation value was used to achieve the revocation of collaborative policy by update corresponding ciphertext. The security analysis shows the scheme can guarantee data confidentiality, forward/backward security, and resist collusion attack under chosen plain-text attack. Compared with the related works, the proposal achieved more complete and efficient revocation scheme.

Keywords: attribute-based collaborative access control, CP-ABE, revocation, translation node, attribute group

---

收稿日期：2020−08−26；**修回日期**：2020−11−20

基金项目：国家自然科学基金资助项目（No.U1836205, No.61772008）；贵州省科技计划基金资助项目（黔科合支撑 No.[2018]2159, 黔科合支撑 No.[2019]2004, 黔科合平台人才 No.[2020]5017, 黔科合重大专项字 No.[2018]3001）；贵州省高等学校创新人才基金资助项目（黔教合人才 No.[2013]09）；“十三五”国家密码发展基金资助项目（No.MMJJ20170129）

Foundation Items: The National Natural Science Foundation of China (No.U1836205, No.61772008), The Science and Technology Program of Guizhou Province (Qian-Science-Contract-Support No.[2018]2159, Qian-Science-Contract-Support No.[2019]2004, Qian-Science-Contract-Platform-Talent No.[2020]5017, Qian-Science-Contract-Major-Program No.[2018]3001), The Project of Innovative Group in Guizhou Education Department (Qian-Education-Contract-Talent No.[2013]09), The 13th Five-Year National Cryptography Development Foundation (No.MMJJ20170129)

1 引言

云存储服务的广泛应用使数据所有者失去对外包数据的管控能力，因此外包数据的访问控制变得越来越重要[1]。自 Sahai 和 Waters[2]提出属性加密（ABE, attribute-based encryption）的概念以来，基于属性加密的访问控制方案得到广泛深入的研究[3-5]。其中，Bethencourt 等[4]提出的基于密文策略的属性加密（CP-ABE, ciphertext policy attribute-based encryption）方案，因其访问结构具备安全、高效、灵活的访问控制特性，迅速成为访问控制领域的重要研究分支。然而，近年的云存储访问控制研究[6-8]只考虑了单个用户的属性集合与访问结构进行匹配，在匹配过程中，往往把多个用户组成的属性集合当作共谋攻击。但是，在实际应用场景中，如医院联合诊疗场景，信息资源访问往往需要多个用户分别利用各自的属性相互协作，并利用多用户多属性协同访问。可见，经典 CP-ABE 方案无法满足协同场景下多个用户的协同访问控制需求。

属性协同访问控制是近年来提出的一种能解决多个用户协同掌握访问权限的新型访问控制技术[9]，可以看作对经典 CP-ABE 方案的扩展。类似的协同思想最早可以追溯到秘密共享方案[10-11]，但该方案无法动态调整协同访问权限，难以满足实际协同需求。在协同访问控制方案设计方面，已有不少学者针对特定协同场景中基于任务、社区、扩展访问策略、面向用户组的属性协同等[9,12-13]展开研究，并试图寻求能够灵活地表达协同访问策略复杂性的方法。协同访问控制方案中的数据安全和隐私依赖多个参与者的协同防护[14]，面临更加困难的挑战，现有方案大多没有很好地解决该问题[9,12-13]，即使 Xue 等[13]基于特定属性和转移节点特性实现了安全可控的属性协同方案，但针对权限动态更新问题，并未给出具体的权限撤销方案。可见，属性协同访问控制依然存在诸多有待深入研究和思考的问题，特别是协同过程中由于授权不足、过度授权、权限更新不及时等，可能造成严重的隐私泄露问题[9]。基于此，本文提出了一种具有属性即时撤销、属性级用户撤销和协同策略撤销功能的属性协同访问控制方案。

1.1 更复杂的撤销需求——协同策略撤销

撤销是访问控制中的难点问题[15]。通常，访问控制中会涉及属性撤销和用户撤销问题，但在协同场景下，当协同功能完成时，除上述 2 种撤销需求外，还需及时撤销协同用户的协同权限。例如，医院内多学科联合诊疗就是一种常见的跨科室访问数据的协同场景。针对同时患有疾病 a 和疾病 b 的患者 1，从数据访问的角度来讲，A 科室医生需要从 B 科室获取该患者的临床诊疗数据，以制定更科学、合理的诊疗方案。实际上，每个科室的临床数据只有该科室的医务人员才有权限访问，此时 A 科室医生就需要 B 科室医生参与协同，协同过程相当于 B 科室医生将患者 1 在 B 科室的诊疗结果共享给 A 科室医生的过程，使 A 科室医生能够全面掌握该患者的诊疗数据，有助于提高诊疗质量。尤其在急诊情况中，高效的协同能进一步保障患者生命安全和数据安全。为便于表述，假设各自的属性集合如下。

患者 1：P={“疾病 a 病情 1” and “疾病 b 病史” and “疾病 a 病情 2”}

A 科室主治医生：S_1={“A 科室” and “主治医生 D_1”}

B 科室主治医生：S_2={“B 科室” and “主治医生 D_2”}

协同访问策略：S={{“A 科室” and “主治医生 D_1”} and {“B 科室” and “主治医生 D_2”}}

综上可知，{ S_1 and S_2} = S，并把子集 S_2 中“B 科室”和“主治医生 D_2”称作协同属性。诊疗结束后，若不及时撤销协同策略 S，会导致 B 科室的主治医生一直拥有该协同权限，则他可能与 A 科室医生共谋后获取非法的数据访问权限，造成协同权限的滥用，并对医疗数据安全造成威胁。在执行协同策略撤销时，不能影响具有相同属性的其他用户和被撤销协同属性的用户的正常访问，即上例中，从 S 中撤销访问子集 S_2 后，包含属性集合 S_2 的医生在 B 科室仍具有合法的访问权限。

在现有的撤销方案中，直接撤销存在属性撤销粒度较粗的问题[16-17]。间接撤销能实现灵活的属性撤销，但只针对一般属性的撤销问题[18-20]。然而，在属性协同访问控制中往往同时涉及协同属性和一般属性的撤销问题。已有的直接或间接撤销方案中[16-20]，尚没有根据属性的不同功能特性考虑更完备的撤销方案，且云服务器执行撤销操作时可能对数据安全造成威胁。因此，亟须一种安全、高效且具有细粒度属性撤销功能的属性协同访问控制技术。

1.2　本文工作

本文基于 Xue 等[13]提出的属性协同访问控制方案构造了一种具有属性即时撤销、属性级用户撤销以及协同策略撤销功能的属性协同访问控制方案。本文方案以用户组[21]为基础，引入属性组[20]模型，从而弥补了属性组在协同场景中的缺陷。一方面，通过属性组中成员列表信息的变化反映权限的动态更新，借鉴重加密的方法更新密文，实现属性即时撤销和属性级用户撤销；另一方面，利用转移节点[13]的转移值特性来撤销属性的协同功能，以实现协同策略的撤销。当某个属性被撤销时，只需在属性组中更新该属性对应的密文，进而有效提升了撤销运行效率。在安全性方面，基于改进后的组密钥更新树形结构，有效解决了密钥安全性问题。具体而言，本文的主要贡献如下。

1) 实现属性撤销和用户撤销。通过更新分组属性组中成员列表信息反映实际情景中用户加入、离开系统或用户属性的变更，进一步设计高效的重加密算法实现属性即时撤销和属性级用户撤销，其中，当一个用户的全部属性都被撤销时，意味着该用户被撤销，即属性级用户撤销。

2) 实现协同策略撤销。当某个协同功能被撤销时，更新协同属性对应的协同属性组信息，并结合转移节点的转移值特性快速更新协同属性对应的密文，只需删除协同属性对应的转移值信息，即可实现细粒度的协同策略撤销功能。

3) 构建了安全且高效的细粒度属性撤销方案。基于离散对数难解问题，改进密钥加密密钥树形结构，增强了密钥更新的安全性，并在标准模型下证明所提方案是选择明文的不可区分安全性，同时，保证数据机密性、前向后向安全性以及抗共谋攻击。由云服务器执行与撤销相关的复杂计算，只需更新撤销所影响的属性组中的组密钥参数等，大大缩小了单次密文更新范围，有效提升了撤销运行效率。

2　相关工作

协同场景广泛存在于日常生活中，例如协同编辑系统、在线社交网络以及医疗资源信息库等商业协同系统。Paci 等[9]根据协同的不同类型将协同访问控制分为以任务为导向的协同和以社区为导向的协同，前者旨在为不同的用户分配不同的权限，如协同编辑系统[22-23]中的可读、可写权限等；后者常见于在线社交网络领域。文献[24]通过设置信任级别，只有当请求访问的用户获得多个关联朋友的许可时，才能获得访问权限。Susilo 等[12]通过合法用户扩展访问策略来实现协同功能，需要额外的加密来保证协同前后的数据完整性。Huang 等[25]引入有效的策略扩展框架来实现数据协同。Li 等[26]基于二进制编码将单个访问控制策略合并成一个全局策略集来实现协同。此外，也有研究[13,21]从改进和扩展原始 ABE 或 CP-ABE 方案的角度来实现协同。Li 等[21]提出面向组的属性加密方案，允许同一组中多个用户合并后的私钥属性集合满足协同访问策略，进而在协同后获得解密权限，但该方案无法对协同能力进行灵活控制。Bobba 等[27]引入转移节点实现了基于密文策略的属性集合加密，增强了属性表达的灵活性。Xue 等[13]结合文献[21,27]的思想，提出了一种属性协同可控的访问控制方案，即访问策略中规定具有协同属性的用户能在指定属性上进行协同，以共享其访问权限，实现协同访问功能，该方案提到协同的撤销问题，但与已有协同方案一样，均未给出具体的撤销方案。

ABE 中的权限撤销管理可分为 3 类：用户级撤销、用户属性级撤销和系统属性级撤销[15]。根据不同的撤销执行者，撤销方法分为直接撤销和间接撤销。前者由数据加密者执行撤销操作，后者主要由系统权威执行撤销操作。有学者基于截止时间[16]、撤销列表[17]等方式实现直接撤销，但直接撤销方案难以适应大规模场景。在间接撤销中，存在由撤销操作引发的密钥更新和密文更新问题。因此，需要平衡撤销方案的效率与安全问题。Yeh 等[18]和 Hao 等[19]基于代理重加密分别实现了属性撤销和用户撤销，但都缺乏严格的安全性证明。Hur 等[20]基于属性组和二叉树，提出支持细粒度属性即时撤销的 CP-ABE 方案，但该方案中不可信的第三方可能对用户密钥安全造成威胁。王光波等[28]将属性撤销的相关操作托管给云存储服务器执行，减轻了中心权威的计算负载。

已有的研究工作分别考虑了协同场景下的访问控制问题[12-13,22-25]，以及访问控制中的细粒度撤销问题[16-20]，但尚无具体方案考虑协同访问控制中的细粒度撤销问题。此外，若直接将现有撤销机制与协同访问控制结合，不仅会带来更大的密钥和密文更新代价，也无法实现更有效的协同策略撤销。

3 背景知识

3.1 相关定义

定义 1 访问结构。令 $\{P_1,P_2,\cdots,P_n\}$ 是参与者集合，一个访问结构 A 是参与者集合的非空子集，即 $A\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}\setminus\{\varnothing\}$。若集合 $A\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}\setminus\{\varnothing\}$ 是单调的，则 $\forall B,C$；若 $B\in A$ 且 $B\subseteq C$，则 $C\in A$，在访问结构 A 中的集合称为授权集合，不在访问结构 A 中的集合称为非授权集合。本文方案中参与者集合指的是参与者的属性集合。

定义 2 令 T 表示访问结构的访问树，树中非叶节点代表门限。num_x 表示节点 x 的孩子节点总数，k_x 表示其门限值，则 $0\leqslant k_x\leqslant \text{num}_x$，且节点 x 可表示为 (k_x,num_x)。树中每个叶子节点用来刻画属性，令 $\text{att}(x)$ 表示树中叶子节点所刻画的属性，$\text{parent}(x)$ 表示树中节点 x 的父节点，父节点的每个子节点从 $1\sim\text{num}_x$ 以任意方式进行排序（从左至右），函数 $\text{index}(y)$ 返回子节点 y 的索引值。

定义 3 双线性映射。设置 2 个阶为素数 q 的乘法循环群 G 和 G_T，g 是 G 的一个生成元。存在一个双线性映射 $e:G\times G\to G_T$，满足以下 3 个性质。

1) 双线性。$\forall g_1,g_2\in G,\forall a,b\in {}_RZ_p$，都有 $e(g_1^a,g_2^b)=e(g_1,g_2)^{ab}$。

2)非退化性。$\exists g_1,g_2\in G$，有 $e(g_1,g_2)\neq 1$。

3)可计算性。$\forall g_1,g_2\in G$，计算 $e(g_1,g_2)$ 是有效函数。

3.2 困难问题

定义 4 判定双线性 Diffie-Hellman（DBDH, decisional bilinear Diffie-Hellman）问题。给定 2 个阶为 q 的循环加法群 G 和循环乘法群 G_T、一个双线性映射 $e:G\times G\to G_T$，G 的生成元为 g。DBDH 问题就是给定一个四元组 (g,g^a,g^b,g^c)，$a,b,c,z\in Z_p$，判断这个四元组是 DBDH 四元组 $(g,g^a,g^b,e(g,g)^{abc})$，还是随机四元组 (g,g^a,g^b,g^z)。如果在多项式时间内解决 DBDH 的概率是可忽略的，则 DBDH 问题是困难的。

3.3 用户组

Li 等[21]首先给出用户组的概念，其核心思想是只允许同一个用户组内的用户参与协同。用户组是根据实际需求对用户进行分类所形成的用户集合。例如，可将医院内同一个科室的医生分在一个用户组内，从而使多个用户合并后的属性集合可以满足访问策略，打破了 ABE 方案只允许单个用户的属性集合与访问策略进行匹配的局限性。

3.4 属性组

Hur 等[20]提出属性组的概念，其构造原则是将系统中拥有某个相同属性的用户分为一组，即属性组是拥有某属性的全部用户的集合。

4 算法形式化定义及模型定义

4.1 算法形式化定义

本文方案模型由 6 个算法构成。

1) 参数设置算法 $\text{Setup}(\partial,m)\to(\text{PK},\text{MSK})$。输入安全参数 ∂、用户组总数 m，输出系统公钥 PK 和主密钥 MSK。

2) 解密密钥（DK, decryption key）生成算法。由用户私钥生成算法和组密钥加密密钥生成算法两部分组成，分别为 $\text{SKeyGen}(\text{MSK},S)\to\text{SK}$，$\text{KEKGen}(\text{Gr})\to\text{KEKs}$。SKeyGen 输入主密钥 MSK、属性集合 S，输出用户私钥 SK；KEKGen 输入用户组 Gr，输出组密钥加密密钥 KEKs。

3) 加密算法 $\text{Enc}(\text{PK},M,A)\to\text{CT}$。在访问结构 A 下，输入公钥 PK、明文消息 M，输出密文 CT。

4) 重加密算法 $\text{ReEnc}(\text{CT},\text{Gr})\to(\text{CT}',\text{Hdr})$。假设云服务器是诚实且好奇的，输入密文 CT、属性组 Gr，输出重加密密文 CT′、头部信息 Hdr。只有当用户标识符在 Gr 中且未被撤销时才能获得解密权限。

5) 解密算法 $\text{Dec}(\text{CT}',\text{SK},K_\lambda)\to M$。输入重加密密文 CT′、私钥 SK、属性组密钥 K_λ，输出明文 M。

6) 更新算法 $\text{KeyUpdate}(\text{Gr}_{\lambda,\theta_m})\to K'_\lambda$。输入更新后的属性组 $\text{Gr}_{\lambda,\theta_m}$，输出由云服务器更新后的属性组密钥 K'_λ；然后，返回执行重加密算法，实现密文更新。

4.2 方案模型

图 1 给出本文所提具有可撤销功能的属性协同访问控制（AB-R-CAC, attribute-based revocable collaborative access control）方案模型。其中，数据拥有者（DO, data owner）将加密数据存储到云服务提供商（CSP, cloud service provider）处，CSP 中的数据服务管理器（DSM, data server manager）是诚实且好奇的，负责管理属性组和执行撤销相关操作；中心权威（CA, central authority）是可信的属

性权威，负责管理、分发密钥并将属性组发送至 DSM；数据使用者（DU, data user）根据 CSP 返回的密文头部信息 Hdr 更新自己的私钥，可解密得到明文。

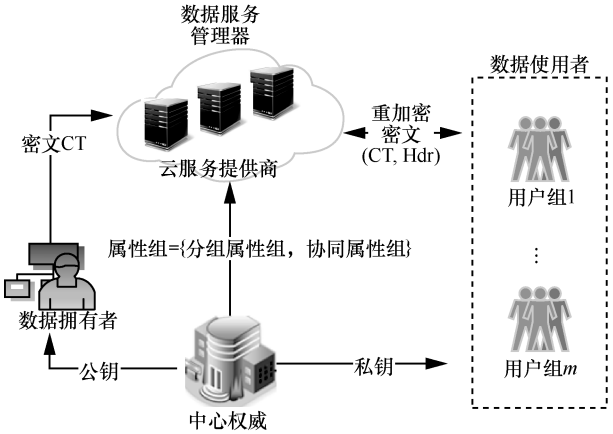

图 1　AB-R-CAC 方案模型

4.3　安全模型

本文方案算法的安全性基于可选择安全，其形式化定义如下。

1) 初始化。敌手选择要挑战的一个访问结构 A^* 发送给挑战者。

2) 系统建立。挑战者运行参数设置 Setup 算法，利用安全参数生成公钥 PK 和主密钥 MSK，将 PK 发送给敌手，挑战者自己保存 MSK。

3) 询问阶段 1。敌手可以询问关于属性集合 S_i 的私钥和组密钥加密密钥 KEKs，且 $S_i \notin A^*$，用户标识符存在于用户组 $U \in \mathrm{Gr}$。

4) 挑战。敌手向挑战者发送消息 M_0和M_1，挑战者随机投掷一枚硬币 $b \in \{0,1\}$，在所挑战的访问结构 A^* 下对 M_b 进行加密，并将结果返回给敌手。

5) 询问阶段 2。重复询问阶段 1。

6) 猜测。敌手输出对 b 的猜测 b'，若 $b'=b$，则敌手赢得游戏。

定义 5　IND-CPA 安全。若多项式时间敌手拥有可忽略的优势攻破上述游戏，则所提 AB-R-CAC 方案是 IND-CPA 安全的，且敌手优势为 $\mathrm{ADV}=\left|\Pr[b=b']-1/2\right|$。

4.4　分组属性组和协同属性组模型

考虑协同场景下撤销方案安全性以及撤销效率，本文方案将属性组和用户组巧妙地融合在一起，依据 Hur 等[20]提出的属性组构造原则，在用户组内构造属性组，并将一般属性的分类结果称作分组属性组（GAG, group-based attribute group），协同属性的分类结果称作协同属性组（CAG, collaborative attribute group）。在实际生成属性组的过程中，可以通过对属性的 Hash 值建立平衡二叉树结构，进而提高 CA 对属性的查找、增加、删除操作的执行效率。分组属性组树的具体构建过程如下。

例如，来自用户组 $\theta_j(1<j<m)$ 的 3 个用户 $\{u_1,u_2,u_3\}$ 属性分别为 $\{\lambda_1,\lambda_2,\lambda_3\}$、$\{\lambda_2,\lambda_3\}$、$\{\lambda_1,\lambda_3\}$，令属性 λ_2 是协同属性。首先，CA 在用户组 θ_j 内按照属性 λ_1、λ_2、λ_3 对这 3 个用户进行分类， GAG 记作 $\mathrm{Gr}_{\lambda,\theta_j}$，表示用户组 θ_j 中拥有一般属性 λ 的用户集合；同理，CAG 记作 $\mathrm{Co}_{\lambda_2,\theta_j}$。综上可知，$\mathrm{Gr}_{\lambda,\theta_j}$ 和 $\mathrm{Co}_{\lambda_2,\theta_j}$ 中的成员列表信息分别为 $\mathrm{Gr}_{\lambda_1,\theta_j}=\{u_1,u_3\}$、$\mathrm{Gr}_{\lambda_2,\theta_j}=\{u_1,u_2\}$、$\mathrm{Gr}_{\lambda_3,\theta_j}=\{u_1,u_2,u_3\}$ 和 $\mathrm{Co}_{\lambda_2,\theta_j}=\{u_1,u_2\}$，将属性组和每个用户组组密钥相关的秘密值 g^{θ_j} 发送给云服务器。当云服务器接收到属性组信息时，为每个属性组随机选取唯一的 $K_\lambda \in Z_p^*$ 作为属性组密钥。同时，DSM 根据分组属性组中所有用户的标识符集合生成一个分组属性组树，如图 2 所示。分组属性组树中每个叶子节点表示唯一的用户，黑色的根节点表示用户组秘密信息 g^{θ_j}。若用户 u_1 的属性 λ_1 被撤销，则更新的 $\mathrm{Gr}'_{\lambda_1,\theta_j}=\{u_3\}$，其对应的组密钥和密文也将被更新。本文方案中转移节点即协同属性，当协同属性 λ_2 被撤销时，直接删除转移节点对应的转移值即可撤销该协同属性对应的协同策略。值得注意的是，CSP 并未直接存储或执行与用户属性有关的隐私信息。本文方案在撤销协同策略时，不需要更新被撤销属性所影响的用户私钥成分。因此，不需要构建协同属性组树。

5　AB-R-CAC 方案构造

本文方案从 3 个层面实现撤销。首先，从数据拥有者的角度，在不需要协同功能时，需要及时撤销协同属性，即协同策略撤销，且撤销属性的协同功能时，不影响该属性除协同能力以外的访问权限；然后，从属性被撤销的角度，当用户的某个属性被撤销时，需要及时撤销该属性，且不能影响具有相同属性的其他用户的正常访问；最后，从用户撤销的角度，当某个用户的全部属性都被撤销时，意味着该用户被撤销，即属性级用户撤销。

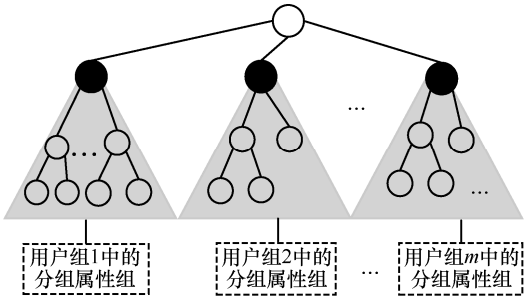

图 2 分组属性组树

算法 1 Setup(∂, m)。CA 执行参数设置算法，输入安全参数 ∂、用户组总数 m。G和G_T 是 2 个阶为素数 p 的乘法循环群，群 G 的随机生成元为 g，定义双线性映射 $e: G\times G\to G_T$，抗碰撞哈希函数 $H:\{0,1\}^*\to G$。随机选取 $\alpha,\beta_1,\beta_2\in Z_p$，组密钥 $\theta_m\in Z_p$，用户唯一标识符 $u_i\in Z_p$。输出系统公钥 $\mathrm{PK}=\{G,G_T,H,g,\ h_1=g^{\beta_1},h_2=g^{\beta_2},e(g,g)^{\alpha}\}$，系统主密钥 $\mathrm{MSK}=\{g^{\alpha},\beta_1,\beta_2,g^{\theta_1},\cdots,g^{\theta_m}\}$。

算法 2 解密密钥生成算法包含用户私钥生成算法和组密钥加密密钥生成算法。

SKeyGen(MSK,S)。CA 执行私钥生成算法，定义属性集合 $S_i=\{a_{i,1},\cdots,a_{i,n_i}\}$，$a_{i,j}$ 为 S_i 中的第 j 个属性，n_i 为 S_i 的属性总数。CA 检查用户 u_i 属于哪一个用户组，并且生成用户组密钥 θ_m；然后，CA 分别为用户 u_i 和属性 $a_{i,j}$ 随机选择 $r_i\in Z_p$ 和 $r_{i,j}\in Z_p$，$1<j<n_i$；最后，生成用户私钥为

$$\mathrm{SK}_i=\left\{D_i=g^{\frac{\alpha+\theta_m}{\beta_1}},\forall j\in[1,n_i]:D_{i,j}=g^{r_i}H(a_{i,j})^{r_{i,j}},\right.$$
$$\left.D'_{i,j}=g^{r_{i,j}},E_{\ i}=g^{\frac{\theta_m+r_i}{\beta_2}}\right\}$$

其中，E_i 为转移节点的转移密钥。本文方案中，转移节点表示协同属性[13]，转移节点在协同者参与协同解密及协同策略撤销过程中必不可少。简单起见，将多个用户的属性集合记作 γ，属性 $a_{i,j}$ 记作 λ_j，即 $\lambda_j\in\gamma$。

KEKGen(Gr)。由 CSP 执行，输入属性组 Gr，假设 $\mathrm{Gr}=\{u_1,u_2,u_3,u_4,u_5,u_6,u_7,u_8\}$，DSM 根据接收到的属性组信息，通过 KEKGen(Gr) 为分组属性组中每个用户 u_i 生成 KEKs。改进后的密钥加密密钥（IKEK, improved key encryption key）树如图 3 所示，每个节点 v_j 拥有一个密钥加密密钥值 KEK_j，从叶子节点到根节点的 KEK_j 的路径密钥（PK, path key）集合即组密钥加密密钥。只有 KEKs 满足重加密密文中 Hdr 的用户，才能解密得到分组属性组密钥。构造 IKEK 树的具体步骤如下。

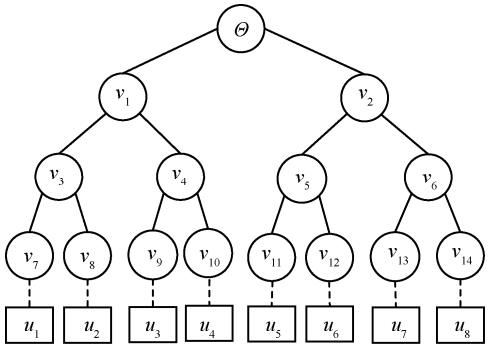

图 3 IKEK 树

步骤 1 分组属性组中用户成员与 IKEK 树中的叶节点一一对应，DSM 为树中每个叶节点和内部节点随机分配密钥。其中，每个节点的密钥分配是相互独立且随机的[29]。根节点的密钥为 $\Theta=g^{\theta_m}$，由于群上的离散对数问题是困难的，因此诚实且好奇的 DSM 在多项式时间内仍无法计算得到用户组密钥 θ_m。

步骤 2 分组属性组中每个用户成员 u_i 接收路径密钥 PK_i 作为 KEKs，DSM 用 PK_i 来加密分组属性组密钥。例如，用户 u_1 的组密钥加密密钥为 $\mathrm{KEKs}=\mathrm{PK}_1=\{\mathrm{KEK}_7,\mathrm{KEK}_3,\mathrm{KEK}_1,\Theta\}$。

算法 3 Enc(PK,M,A)。数据拥有者运行加密算法，输入访问结构 A、公钥 PK 和明文消息 M，接着选择随机密钥 $\kappa\in Z_p$ 作为对称加密密钥对明文进行加密，密文为 $E_{\kappa}(M)$。令 X 为访问树 T 中转移节点集合，Y 为访问树 T 中叶子节点集合，转移节点即访问策略中允许协同的属性。输出密文为

$$\begin{aligned}\mathrm{CT}=\{&T,\tilde{C}=\kappa e(g,g)^{\alpha s},C=h_1^s,\overline{C}=h_2^s,\\&\forall y\in Y:C_y=g^{q_y(0)},C'_y=H(\mathrm{att}(y))^{q_y(0)},\\&\forall x\in X:\hat{C}_x=h_2^{q_x(0)}\}\end{aligned}$$

数据拥有者将密文外包给 CSP 进行存储。其中，$\hat{C}_x$ 为转移节点的转移值。

算法 4 ReEnc(CT,Gr)。DSM 接收到密文后，执行重加密算法。输入密文 CT、属性组 Gr，重加密过程如下。

1) 对 $\forall\mathrm{Gr}_{y,\theta_1}\in\mathrm{Gr}$，随机选取分组属性组密钥

$K_{\lambda_y} \in Z_p^*$，输出密文为

$$\mathrm{CT}'=\{T,\tilde{C}=\kappa e(g,g)^{\alpha s},C=h_1^s,\overline{C}=h_2^s,$$
$$\forall y\in Y:C_y=g^{q_y(0)},C_y'=(H(\mathrm{att}(y))^{q_y(0)})^{K_{\lambda_y}},$$
$$\forall x\in X:\hat{C}_x=h_2^{q_x(0)}\}$$

2) 在 IKEK 树中选择能覆盖 Gr_{y,θ_1} 中用户的最小覆盖集合，$\mathrm{KEK}(\mathrm{Gr}_{y,\theta_1})$ 表示 Gr_{y,θ_1} 中用户的最小覆盖集合。当属性组 $\mathrm{Gr}_{y,\theta_1}=\{u_1,u_2,u_3,u_4,u_7,u_8\}$，其最小覆盖集合 $\mathrm{KEK}(\mathrm{Gr}_{y,\theta_1})=\{\mathrm{KEK}_1,\mathrm{KEK}_6\}$，即以节点 v_1 和 v_6 为根节点时，其子树包含 Gr_{y,θ_1} 中所有用户。$\mathrm{KEK}(\mathrm{Gr}_{y,\theta_1})$ 中有且仅有存在于 Gr_{y,θ_1} 中的用户。若 $\exists u_i\notin \mathrm{Gr}_{y,\theta_1}$，输出错误符号 $\mathrm{KEK}(\mathrm{Gr}_{y,\theta_1})=\perp$。

3) 生成头部信息。在步骤 2)的基础上，计算 $\mathrm{Hdr}=(\forall y\in Y:E_K(K_{\lambda_y})_{K\in\mathrm{KEK}(\mathrm{Gr}_{y,\theta_1})})$。当收到来自用户的数据访问请求时，DSM 返回(Hdr,CT′)信息作为响应，只要用户没有从任意属性组中撤销，就能从 Hdr 中解密得到 K_{λ_y}，然后解密密文。由于 DSM 无法解密用户组密钥 θ_m，故 DSM 无法解密得到有效明文信息。

算法 5　$\mathrm{Dec}(\mathrm{CT}',\mathrm{SK},\mathrm{K}_\lambda)$。用户运行分组属性组密钥解密算法。输入私钥 SK，若用户 $\mathrm{KEK}_i\in(\mathrm{KEK}(\mathrm{Gr}_{y,\theta_m})\cap\mathrm{PK}_i)$，计算得到属性组密钥 K'_λ，计算更新后用户私钥为

$$\mathrm{SK}_i=\left\{D_i=g^{\frac{\alpha+\theta_m}{\beta_1}},\forall j\in[1,n_i]:D_{i,j}=g^{r_i}H(a_{i,j})^{r_{i,j}},\right.$$
$$\left.D'_{i,j}=(g^{r_{i,j}})^{\frac{1}{K_{\lambda_j}}},E_{\ i}=g^{\frac{\theta_m+r_i}{\beta_2}}\right\}$$

用户执行密文解密算法。输入重加密密文 CT′、私钥及属性组密钥，属性集合包含单个用户的属性集合和多个用户协同后的属性集合，定义协同后的属性集合为 γ，即联合属性集合。对访问树中每个节点 x，树满足算法 $T_x(\gamma)$ 返回其标识符总集合 U_x，并将每个递归调用的结果存储在访问树中。若 $u_i\in U_x$，则意味着用户 u_i 能够解密节点 x。若 γ 满足访问树，则用户的标识符将被包含在 U_r 中，且用户执行解密算法 $\mathrm{DecryptNode}(\mathrm{CT}',\gamma,x,u_i)$；否则，$U_r=\varnothing$ 时，解密算法返回 $\perp$。

当 $x\in Y$ 时，若 $u_i\notin U_x$，$\mathrm{att}(x)\notin S_i$，则有 $\mathrm{DecryptNode}(\mathrm{CT}',\gamma,x,u_i)$；否则，解密算法返回值为 $\mathrm{att}(x)=a_{i,j}\in S_i$，计算 $\mathrm{DecryptNode}(\mathrm{CT}',\gamma,x,u_i)$ 为

$$\mathrm{DecryptNode}(\mathrm{CT}',\gamma,x,u_i)=\frac{e(D_{i,j},C_x)}{e(D'_{i,j},C'_x)}=$$
$$\frac{e(g^{r_i}H(a_{i,j})^{r_{i,j}},g^{q_x(0)})}{e\left((g^{r_{i,j}})^{K_{\lambda_x}},(H(a_{i,j})^{q_x(0)})^{\frac{1}{K_{\lambda_x}}}\right)}=e(g,g)^{r_iq_x(0)}$$

当 $x\notin Y$，x 是一个非叶节点时，则计算 $\mathrm{DecryptNode}(\mathrm{CT}',\gamma,x,u_i)$，用 z 表示 x 的 k_x 个子节点，并将结果存储到集合 B_x 中。若 z 不是转移节点，则令节点 z 与用户 u_i 相关联；若 z 是转移节点，则令转移节点 z 与用户 $u_{i'}$ 相关联，且 $i'\neq i$。

因此，对 $\forall z\in B_x$，z 不是转移节点时，算法调用 $\mathrm{DecryptNode}(\mathrm{CT}',\gamma,z,u_i)$，并将计算结果存储到变量 F_z；对 $\forall z\in B_x$，z 是转移节点时，即 $u_{i'}\in U_z$ 且 $i'\neq i$，算法调用 $\mathrm{DecryptNode}(\mathrm{CT}',\gamma,z,u_{i'})$，并将计算结果存储到变量 F'_z。这意味着，除数据请求者之外的用户 $u_{i'}$（协同者）能够协同解密节点 z，接着，协同者将其输出结果 F'_z 转移到变量 F_z，计算

$$F_z=e\left(\hat{C}_z,\frac{E_i}{E_{i'}}\right)F_{z'}=$$
$$e\left(g^{\beta_2q_z(0)},g^{\frac{\theta_m+r_i-(\theta_m+r_{i'})}{\beta_2}}\right)e(g,g)^{r_{i'}q_z(0)}=e(g,g)^{r_iq_z(0)}$$

基于转移密钥 E_i，把秘密值 F'_z 转移到 F_z，用户 u_i 获得节点 x 的 k_x 个子节点 z 的秘密，因此，能够解密节点 x。协同者 $u_{i'}$ 将秘密值转移给用户 u_i 等价于用户 u_i 独立拥有能满足节点 x 的谓词表达式的所有属性集合。然后，用户 u_i 使用拉格朗日多项式插值方法计算 F_x，具体为

$$F_x=\prod_{z\in B_x}F_z^{\Lambda_{k,B_z^{(0)}}},\mathrm{where}^{k=\mathrm{index}(z)}_{B_z'=\{i\mathrm{index}(z):z\in B_x\}}=$$
$$\prod_{z\in B_x}\left(e(g,g)^{r_iq_z(0)}\right)^{\Lambda_{k,B_z^{(0)}}}=\prod_{z\in B_x}\left(e(g,g)^{r_iq_{\mathrm{parent}(z)}(\mathrm{index}(z))}\right)^{\Lambda_{k,B_z^{(0)}}}=$$
$$\prod_{z\in B_x}\left(e(g,g)^{r_iq_x(k)}\right)^{\Lambda_{k,B_z^{(0)}}}=e(g,g)^{r_iq_x(0)}$$

其中，拉格朗日系数为 $\prod_{j\in B_x,j\neq k}\frac{x-j}{k-j}$。计算根节点的秘密值以及 F 分别为 $F_r=\mathrm{DecryptNode}(\mathrm{CT}',\gamma,r,u_i)=e(g,g)^{r_iq_r(0)}=e(g,g)^{r_is}$，$F=E(\overline{C},E_i)/F_r=e(g^{\beta_2q_r(0)},g^{\theta_m+r_i/\beta_2})/e(g,g)^{r_iq_r(0)}=e(g,g)^{\theta_ms}$。然后，计算

$$\kappa=\tilde{C}F/e(C,D_i)$$
$$\kappa e(g,g)^{\alpha s}e(g,g)^{\theta_m s}/e(g^{s\beta_1},g^{\theta_m+\alpha/\beta_1})$$

当用户获得对称密钥 κ 后，能解密出明文消

息 M。

算法 6 KeyUpdate($\mathrm{Gr}_{\lambda,\theta_m}$)。CA 根据用户的加入、退出请求，将更新后的属性组成员信息发送给 DSM。假设更新后的分组属性组和协同属性组分别为 $\mathrm{Gr}'_{j,\theta_1}$ 和 $\mathrm{Co}'_{\mathrm{CA}_j,\theta_1}$。针对 $\mathrm{Gr}'_{j,\theta_1}$，DSM 重新选择 $s'\in Z_p^*$ 和组密钥 $K'_{\lambda_j}\in Z_p^*$，若 $K'_{\lambda_j}\neq K_{\lambda_j}$，则重加密更新后的组密钥；针对 $\mathrm{Co}_{\mathrm{CA}_j,\theta_1}$，设置组密钥为 $K_{\mathrm{CA}_j,\theta_1}=\perp$，输出转移值 $\hat{C}_{\mathrm{CA}_j}=\perp$，即删除协同属性的转移值信息，撤销协同属性 CA_j 的协同功能。输出更新后的密文为

$$\begin{aligned}&\mathrm{CT}''=\left\{T,\tilde{C}=\kappa e(g,g)^{\alpha(s+s')},C=h_1^{(s+s')},\overline{C}=h_2^{(s+s')},\right.\\&C_j=g^{q_j(0)+s'},C'_j=\left(H(\mathrm{att}(y))^{q_j(0)}\right)^{K'_{\lambda_j}},\\&\forall y\in Y\setminus\{j\}:C_y=g^{q_y(0)},C'_y=\left(H(\mathrm{att}(y))^{q_y(0)}\right)^{K_{\lambda_y}},\\&\left.\forall x\in X\setminus\{j\}:\hat{C}_x=h_2^{q_x(0)+s'}\right\}\end{aligned}$$

因此，只需要更新被撤销属性所在属性组的组密钥，进行密文更新。DSM 根据更新后的 $\mathrm{Gr}'_{j,\theta_1}$ 重新选择最小覆盖集合，该集合包含拥有属性 λ_j 的新用户（保证后向安全性）或删除属性 λ_j 后的用户（保证前向安全性）。生成新的头部消息为

$$\begin{aligned}&\mathrm{Hdr}=(E_K(K'_{\lambda_j})_{K\in\mathrm{KEK}(\mathrm{Gr}_{j,\theta_m})},\\&\forall y\in Y\setminus\{j\}:E_K(K_{\lambda_y})_{K\in\mathrm{KEK}(\mathrm{Gr}_{y,\theta_m})})\end{aligned}$$

当用户请求访问外包数据时，DSM 返回 (Hdr,CT″) 给用户。

更新算法有效保证了细粒度访问控制。一旦 DSM 收到更新后的属性组信息列表，DSM 可直接执行算法 6，更新被撤销属性对应的密文，同时保证了属性级撤销粒度。

6 方案分析

6.1 安全性分析

6.1.1 数据机密性

定理 1 在 DBDH 假设下，本文所构造的 AB-R-CAC 方案具有选择明文攻击（IND-CPA, indistinguishable chosen-plaintext attack）的不可区分性。

证明 本文方案的安全性证明受到 Xue 等[13]在不同的威胁模型下的启发。在训练阶段考虑敌手询问私钥的 3 种可能的情况。其中，模型 1 表示敌手全部来自同一个用户组；模型 2 表示敌手来自不同用户组（即任意 2 个用户都属于不同的用户组）。组合模型即模型 1、模型 2 的组合，更接近现实情形。

若敌手能以不可忽略的优势在 IND-CPA 安全模型下选择性地攻破本文方案，那么就存在挑战者 B 能在多项式时间内以不可忽略的优势解决 DBDH 问题。假设挑战者随机翻转一枚硬币，硬币的正反 2 种情况用 $u=\{0,1\}$ 表示。当 $u=0$ 时，四元组为 $(A=g^a,B=g^b,C=g^c,Z=e(g,g)^{abc})$；否则，四元组 $(A=g^a,B=g^b,C=g^c,Z=e(g,g)^z)$，其中 $a,b,c,z\in Z_p$，挑战者输出 b' 作为 b 的猜测结果。

1) 初始化。敌手向挑战者发送挑战访问结构 A^*。

2) 参数设置。挑战者随机选取 $t,\alpha'\in Z_p$，设置 $\beta_1=\beta,\beta_2=t\beta,\alpha=\alpha'+ab,Z=e(g,g)^{\alpha}=e(g,g)^{\alpha'}\cdot e(g,g)^{ab}$，随机选取 $s_i\in Z_p,i\in I,H=g^{s_i}$，$h_1=g^{\beta},h_2=g^{t\beta}$，并将公钥发送给敌手 $\mathrm{PK}=\{H,h_1,h_2,Z\}$。

3) 训练阶段 1。训练阶段分别在模型 1、模型 2 以及组合模型下分情况讨论。

在模型 1 中的数据机密性分析如下。

① 私钥和组密钥询问阶段

当敌手询问的属性集合全部来自同一个用户组，且在这之前没有发生撤销操作时，敌手向挑战者询问属性集合 S_i 的私钥，$1<i<q_1$，$\{a_{i,j}\}$ 是 S_i 中的属性，i 表示与 S_i 相关的私钥询问，j 表示 S_i 中的第 j 个属性，挑战者随机选取 $r\in Z_p$，计算 $D_i=g^{\alpha'+ab+r/\beta}$，令 $r^*=t_i,r''=t_{i,j},t_i,t_{i,j}\in Z_p$。对任意 $a_{i,j}\in S_i$，计算 $D_{i,j}=g^{r^*}H(a_{i,j})^{r''},D'_{i,j}=g^{r''}$。挑战者选取 $K^*_{\lambda}\in {}_RZ_p^*$ 作为属性组密钥，并根据 KEKGen(u^*) 算法得到每个敌手询问的组密钥加密密钥 KEKs′。将私钥成分和 KEKs′ 发送给敌手。敌手得到有效私钥 KEKs、$\mathrm{SK}_i^*=\left(D_i=g^{\alpha'+ab+\frac{r}{\beta}},\right.$ $\left.\forall a_{i,j}\in S_i:D_{i,j}=g^{r^*},D'_{i,j}=g^{r''}H(a_{i,j})^{r''},E_i^*=g^{r^*+\frac{r}{t\beta}}\right)$。

当敌手获得属性组密钥加密密钥后，即可得到属性组密钥 K^*_{λ}。r 相当于用户组密钥，假设敌手是诚实且好奇的云服务提供商，一方面 Gr^* 中仅存放用户的标识信息，并没有直接包含用户属性集合；另一方面，即使获得私钥成分 $D_i=g^{\alpha'+ab+r/\beta}$，对于求解用户组密钥 r 仍然是困难问题。在原始 CP-ABE 方案的安全性证明基础上，没有与属性信

息相关的私钥时，访问无法满足访问结构，无法解密得到明文信息。当敌手询问的属性或协同功能被撤销时，挑战者检查敌手是否具有有效属性，若 $u^* \notin \mathrm{Gr}$，则敌手无法获取有效私钥成分。

② 私钥更新询问

当敌手询问的属性未被撤销，但同组中其他拥有相同属性的成员发生撤销，导致属性组密钥被更新时，敌手发出更新密钥请求，挑战者为原来的属性组 Gr 重新设置属性组密钥 K'_λ，将 Gr 更新为属性组 Gr^*，其中不包含被撤销用户。根据 Gr^* 的更新生成组密钥加密密钥 $\mathrm{KEKs}^* \in Z_p$，并将更新结果发送给敌手。敌手可以得到更新私钥成分如下。

$$\forall j \in [1, n_i]: D_{i,j} = g^{r^*} H(a_{i,j})^{r''}, D'_{i,j} = (g^{r''})^{\frac{1}{K'_{\lambda_j}}}$$

即更新私钥为

$$\mathrm{SK}^{**}_i = \left\{ D_i = g^{\frac{\alpha' + ab + r}{\beta}}, \forall j \in [1, n_i]: D_{i,j} = g^{r^*} H(a_{i,j})^{r''}, D'_{i,j} = (g^{r''})^{\frac{1}{K'_{\lambda_j}}}, E_i = g^{\frac{r + r^*}{t\beta}} \right\}$$

在模型 2 中的数据机密性分析如下。

① 私钥和组密钥询问阶段

当敌手均来自不同用户组且未被撤销时，敌手的私钥询问过程如下。假设 2 个来自不同组的敌手 A_a, A_b 分别询问属性集合 S_a, S_b 的私钥，$q_1 + 1 \leqslant a, b \leqslant q$，$u_a^* \in \mathrm{Gr}_a^*$，$u_b^* \in \mathrm{Gr}_b^*$，挑战者随机选取 $r_a, r_b, r_a^*, r_b^* \in Z_p, r_a'', r_b'' \in {}_R Z_p$，计算后得到部分私钥成分为

$$\mathrm{SK}^*_a = \left(D_i = g^{\frac{\alpha' + ab + r_a}{\beta}}, \forall a_{a,j} \in S_a: D_{a,j} = g^{r_a^*} H(a_{a,j})^{r_a''}, D'_{a,j} = g^{r_a''} E_a = g^{\frac{r_a^* + r_a}{t\beta}} \right)$$

$$\mathrm{SK}^*_b = \left(D_i = g^{\frac{\alpha' + ab + r_b}{\beta}}, \forall a_{b,j} \in S_b: D_{b,j} = g^{r_b^*} H(a_{b,j})^{r_b''}, D'_{b,j} = g^{r_b''} E_b = g^{\frac{r_b^* + r_b}{t\beta}} \right)$$

对于 Gr_a^* 中的私钥询问，当 $u_a^* \in \mathrm{Gr}_a^*$ 时，设置 $\mathrm{KEKs}_a^* \in {}_R Z_p$，同理，当 $u_b^* \in \mathrm{Gr}_b^*$，$\mathrm{KEKs}_b^* \in {}_R Z_p$。挑战者将私钥询问结果 SK_a^*、KEKs_a^* 和 SK_b^*、KEKs_b^* 分别发送给敌手 a, b。当属性被撤销时，$u_a^* \notin \mathrm{Gr}_a^*$，$u_b^* \notin \mathrm{Gr}_b^*$，敌手无法正常询问已被撤销属性的相关私钥成分。由于组密钥 $r_a \neq r_b$，无法产生协同，故模型 2 不考虑协同功能的撤销问题。

② 私钥更新询问

当有敌手发出密钥更新询问，且用户未被撤销时，挑战者根据 $\mathrm{Gr}_a^*, \mathrm{Gr}_b^*$ 的更新重新生成唯一的 $\mathrm{KEKs}_a^*, \mathrm{KEKs}_b^* \in Z_p$，并将其发送给敌手。同时，敌手可分析得到更新后私钥成分为

$$\forall j \in [1, n_i]: D_{a,j} = g^{r_a^*} H(a_{i,j})^{r_a''}, D'_{a,j} = (g^{r_a''})^{\frac{1}{K'_{\lambda_{a,j}}}}$$

$$\forall j \in [1, n_i]: D_{b,j} = g^{r_b^*} H(a_{i,j})^{r_b''}, D'_{b,j} = (g^{r_b''})^{\frac{1}{K'_{\lambda_{b,j}}}}$$

可得私钥为

$$\mathrm{SK}^{**}_a = \left(D_i = g^{\frac{\alpha' + ab + r_a}{\beta}}, \forall a_{a,j} \in S_a: D_{a,j} = g^{r_a^*} H(a_{a,j})^{r_a''}, D'_{a,j} = (g^{r_a''})^{\frac{1}{K'_{\lambda_{a,j}}}}, E_a = g^{\frac{r_a^* + r_a}{t\beta}} \right)$$

$$\mathrm{SK}^{**}_b = \left(D_i = g^{\frac{\alpha' + ab + r_b}{\beta}}, \forall a_{b,j} \in S_b: D_{bj} = g^{r_b^*} H(a_{b,j})^{r_b''}, D'_{b,j} = (g^{r_b''})^{\frac{1}{K'_{\lambda_{b,j}}}}, E_b = g^{\frac{r_b^* + r_b}{t\beta}} \right)$$

综上，每一个属性 S_i 与产生的 SK_i 一一对应，最后，敌手的属性集合即所有被询问属性的集合 $\gamma = \{S_1, S_2, \cdots, S_i, \cdots, S_q\}$。

组合模型中的数据机密性分析如下。

在组合模型中，可将来源于不同用户组的敌手进行分组，将其看作单个用户，并依据上述 2 种安全性证明的特性证明其数据机密性。

4) 挑战。阶段 1 结束后，敌手将其要挑战的访问结构 A^* 和 2 个明文消息 $M_0, M_1 \in G$ 发送给挑战者。挑战者运行密文产生算法，将产生的密文 CT^* 返回给敌手。注意，敌手询问的属性集合不满足访问结构 A^*。

$$\mathrm{CT}^* = \{A^*, \tilde{C} = M_b Z^s, C = h_1^s, \overline{C} = h_2^s, \forall y \in Y: C_y = g^{q_y(0)}, C'_y = (H(\mathrm{att}(y))^{q_y(0)})^{K_{\lambda_y}}, \forall x \in X: \hat{C}_x = h_2^{q_x(0)}\}$$

$$\mathrm{Hdr} = (E_K(K_{\lambda_j}))_{K \in \mathrm{KEK}(\mathrm{Gr}_{j,r})}$$

5) 训练阶段 2。与训练阶段 1 操作相同。

6) 猜测。敌手输出猜测结果 $b' \in \{0, 1\}$，当 $b' = b$，挑战者输出 $u' = 0$ 时，表示 (A, B, C, Z) 是一个有效的 DBDH 四元组；否则，(A, B, C, Z) 是一个随机四元组。当 $u = 1$ 时，攻击者并没有得到任何有

用信息，因此 $\Pr[b' \neq b \mid u=1]=1/2$。当 $b \neq b'$ 时，挑战者随机猜测 $u'=1$，因此有 $\Pr[b'=b]=1/2$。当 $u=0$ 时，敌手能够获取到 M_b 的密文，其优势定义为 $\mathrm{ADV}_{\mathrm{CPA}}$，所以 $\Pr[b=b' \mid u=0]=1/2+\mathrm{ADV}_{\mathrm{CPA}}$。当 $b=b'$，挑战者猜测 $u'=0$ 时，$\Pr[u'=u \mid u=0]=1/2+\mathrm{ADV}_{\mathrm{CPA}}$。综上，在解决 DBDH 问题的游戏中挑战者总的优势为

$$\frac{1}{2}\left(\Pr[u'=u \mid u=0]+\Pr[u'=u \mid u=1]\right)-\frac{1}{2}=\frac{1}{2}\left(\frac{1}{2}+\mathrm{ADV}_{\mathrm{CPA}}\right)+\frac{1}{2}\times\frac{1}{2}-\frac{1}{2}=\frac{1}{2}\mathrm{ADV}_{\mathrm{CPA}}$$

若敌手在概率多项式时间内赢得上述游戏的优势为 $\mathrm{ADV}_{\mathrm{CPA}}$，则挑战者能以不可忽略的优势 $\mathrm{ADV}_{\mathrm{CPA}}/2$ 解决 DBDH 困难问题。在安全模型中，敌手攻击本文方案的优势 $\mathrm{ADV}_{\mathrm{CPA}}$ 是可忽略的。因此，本文方案是 IND-CPA 安全的。

证毕。

6.1.2 抗共谋攻击

首先，CA 在私钥生成阶段使用随机化方法，使每个用户的属性都有唯一的随机参数，即使不同用户属性都满足访问策略，仍无法共同计算出 $e(g,g)^{\alpha s}$，故用户间无法产生共谋；其次，本文方案在密钥生成阶段为转移节点生成转移密钥，在加密阶段为转移节点生成转移值，只有同时具有相匹配的转移密钥和转移值的属性才可参与协同，因此，协同只能发生在转移节点上，故协同具有抗共谋性；最后，由于被撤销的用户所在属性组已被 CA 及时更新，即 $u_i \notin \mathrm{Gr}^*$，对应的属性组密钥和密文信息也被 DSM 及时更新，因此，被撤销用户无法解密更新后的密文，故被撤销的用户和现有用户之间无法实现共谋攻击。

6.1.3 前向安全性

基于改进后的 IKEK 树，对于被撤销的用户，其所在属性组的组密钥被及时安全地更新，被撤销用户无法更新其私钥，因此，被撤销的用户无法解密密文；当协同策略被撤销时，协同属性所在属性组的组密钥 $K_{\mathrm{CA}_j,\theta_i}=\perp$，在密文更新阶段 $\hat{C}_{\mathrm{co}}=\perp$，表示没有有效的密文信息，此时，被撤销的协同者即使拥有转移密钥也无法再参与协同。

6.1.4 后向安全性

当新用户加入系统时，DSM 根据更新后属性组信息更新相应的属性组密钥，此时，新加入的用户只能解密与 $e(g,g)^{\alpha(s+s')}$ 相关的更新后的密文，无法解密加入系统之前的密文关键项 $e(g,g)^{\alpha s}$，从而保证了新加入用户只能解密更新后的密文。

6.2 性能分析

表 1 从系统计算开销及功能特征方面将本文方案与已有协同访问控制研究[12-13]进行分析和比较。表 1 中，n_{u} 表示用户的平均属性数量，n_{c} 表示满足密文中访问树的平均属性数量，|tr| 表示密文中转移节点的平均数量，$|\mathrm{tr}_\gamma|$ 表示可解密密文的集合 γ 中转移节点的平均数量，$n_{\mathrm{c},\gamma}$ 表示属性集合 γ 的平均属性数量，|nl| 表示访问树中从叶节点到根节点的非叶节点数量，n_ρ 表示满足访问矩阵的平均属性数量，n_{l} 表示矩阵访问结构中有效属性的总行数，$|\mathrm{Gr}|$ 表示属性组中平均用户数量，$|\mathrm{Co}|$ 表示协同属性组数量，T_{p} 表示群上的配对运算时间，T_{e} 表示指数运算所需时间。

由表 1 可知，相比已有方案，本文方案实现了更加细粒度的撤销功能，仅增加了极少的计算开销。由 DSM 执行与撤销相关的操作，带来的额外密钥生成开销为 $\log 2|\mathrm{Gr}|+|\mathrm{Co}|$，重加密计算开销为 $n_{\mathrm{c}}T_{\mathrm{e}}$。

Susilo 等[12]通过增加访问策略实现协同，随着协同数量的增加，访问策略的冗余度增大，带来了更大的存储和计算负担。Xue 等[13]基于属性并利用

表 1 系统计算开销及功能特征比较

方案	密钥生成		加密(DO)	重加密(DSM)	解密	协同访问功能	属性即时撤销	用户撤销	协同策略撤销
	CA	DSM							
文献[12]方案	$(n_{\mathrm{u}}+4)T_{\mathrm{e}}$	—	$(3n_{\mathrm{c}}+4)T_{\mathrm{e}}$	—	$(2n_\rho+4)T_{\mathrm{p}}+(n_\rho+n_{\mathrm{l}})T_{\mathrm{e}}$	√	×	×	×
文献[13]方案	$(2n_{\mathrm{u}}+3)T_{\mathrm{e}}$	—	$(2n_{\mathrm{c}}+3+\lvert\mathrm{tr}\rvert)T_{\mathrm{e}}$	—	$(2n_{\mathrm{c},\gamma}+\lvert\mathrm{tr}_\gamma\rvert+2)T_{\mathrm{p}}+(n_{\mathrm{c},\gamma}+\lvert\mathrm{nl}\rvert)T_{\mathrm{e}}$	√	×	×	×
本文方案	$(2n_{\mathrm{u}}+3)T_{\mathrm{e}}$	$\log 2\lvert\mathrm{Gr}\rvert+\lvert\mathrm{Co}\rvert$	$(2n_{\mathrm{c}}+3+\lvert\mathrm{tr}\rvert)T_{\mathrm{e}}$	$n_{\mathrm{c}}T_{\mathrm{e}}$	$(2n_{\mathrm{c},\gamma}+\lvert\mathrm{tr}_\gamma\rvert+2)T_{\mathrm{p}}+(2n_{\mathrm{c},\gamma}+\lvert\mathrm{nl}\rvert+1)T_{\mathrm{e}}$	√	√	√	√

转移节点的特性在不增加访问策略的情况下，实现了较为高效的属性协同功能。但上述方案均未具体考虑增加了协同功能后所面临的更复杂的权限动态更新问题，尤其是同时达到协同策略撤销、属性撤销和用户撤销。本文方案在 Xue 等[13]的基础上实现了细粒度的属性即时撤销、属性级用户撤销和协同策略撤销。其中，属性即时撤销操作不需要等待一定的时间周期[16]，只要 DSM 收到被撤销属性对应的属性组信息，即可更新被撤销属性对应的密文信息。

文献[18-20]以及本文方案的撤销性能及安全性比较如表 2 所示。表 2 中，n_{user} 表示系统中所有用户数量，r 表示方案中被撤销的用户数量，被撤销的用户包含撤销属性、撤销协同属性，$|\text{Gr}|$ 表示属性组平均用户数量，T_{e} 表示指数运算所需时间。

由表 2 可知，本文方案不仅同时实现了细粒度的属性级撤销和协同策略撤销功能，还在标准模型下给出了严格的安全性证明。同类撤销方案[18-20]均未给出严格的安全性证明；Hao 等[19]实现了用户级撤销，但撤销粒度较粗；Yeh 等[18]和 Hur 等[20]都利用属性组实现细粒度属性级撤销，不同点是 Hur 等[20]将撤销操作交给云服务提供商执行，导致安全性较弱；Yeh 等[18]将撤销操作全部交给中心权威执行，虽增强了安全性，但中心权威计算负载太大。本文方案的撤销思想来源于文献[20]，但与之不同的是，本文方案在实现细粒度的属性撤销、用户撤销和协同策略撤销时，面向属性组实现更新，缩小了单次更新范围，进而提升了撤销运行效率，将密钥更新、密文更新的计算效率从 $O(n_{\text{user}}-r)$ 提升至 $O(|\text{Gr}|-r)$，并基于改进的密钥加密密钥树增强了方案安全性，在标准模型下证明本文方案是选择明文攻击安全的。本文方案假设 CA 能即时掌控用户的撤销信息，并能诚实地对相应的属性组信息进行更新。尚未考虑用户不诚实的情况下，如何即时发现不诚实用户，以实现更加细粒度的属性级撤销。

7　结束语

本文方案提出了一种具有可撤销功能的属性协同访问控制方案，实现了属性即时撤销、属性级用户撤销以及协同策略撤销功能，解决了协同访问控制中复杂的动态权限更新问题。该方案在属性组内执行密文和密钥更新，大大缩小了更新范围，有效提升了撤销运行效率。本文对协同场景下的协同策略撤销需求进行论述，定义了选择性安全模型。基于离散对数困难问题改进了组密钥更新树形结构，增强了密钥更新的安全性，同时，基于 DBDH 困难问题证明了该方案是 IND-CPA 安全的。下一步研究工作将考虑访问控制撤销方案中存在恶意用户的情况。

表 2　　**撤销性能及安全性比较**

方案	密钥更新		密文更新		撤销粒度	协同策略撤销	安全模型
	CA	DSM	CA	DSM			
文献[18]方案	$(n_{\text{user}}-r)T_{\text{e}}$	—	$4(n_{\text{user}}-r)T_{\text{e}}$	—	属性级	×	×
文献[19]方案	—	$(n_{\text{user}}-r)T_{\text{e}}$	—	$(n_{\text{user}}-r)T_{\text{e}}$	用户级	×	×
文献[20]方案	—	$(n_{\text{user}}-r)T_{\text{e}}$	—	$4(n_{\text{user}}-r)T_{\text{e}}$	属性级	×	×
本文方案	—	$(\|\text{Gr}\|-r)T_{\text{e}}$	—	$4(\|\text{Gr}\|-r)T_{\text{e}}$	属性级	√	标准模型

参考文献：

[1] DU M X, WANG Q, HE M Q, et al. Privacy-preserving indexing and query processing for secure dynamic cloud storage[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(9): 2320-2332.

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

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

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

[5] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[C]//International Workshop on Practice and Theory in Public Key Cryptography. Berlin: Springer, 2011: 53-70.

[6] XUE K P, XUE Y J, HONG J N, et al. RAAC: robust and auditable access control with multiple attribute authorities for public cloud storage[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(4): 953-967.

[7] LI W, XUE K P, XUE Y J, et al. TMACS: a robust and verifiable threshold multi-authority access control system in public cloud storage[J]. IEEE Transactions on Parallel and Distributed Systems, 2016, 27(5): 1484-1496.

[8] XUE K P, CHEN W K, LI W, et al. Combining data owner-side and

cloud-side access control for encrypted cloud storage[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(8): 2062-2074.

[9] PACI F, SQUICCIARINI A, ZANNONE N. Survey on access control for community-centered collaborative systems[J]. ACM Computing Surveys, 2018, 51(1): 1-38.

[10] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.

[11] TASSA T. Hierarchical threshold secret sharing[J]. Journal of Cryptology, 2007, 20(2): 237-264.

[12] SUSILO W, JIANG P, GUO F C, et al. EACSIP: extendable access control system with integrity protection for enhancing collaboration in the cloud[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(12): 3110-3122.

[13] XUE Y J, XUE K P, GAI N, et al. An attribute-based controlled collaborative access control scheme for public cloud storage[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(11): 2927-2942.

[14] HUMBERT M, TRUBERT B, HUGUENIN K. A survey on interdependent privacy[J]. ACM Computing Surveys, 2020, 52(6): 1-40.

[15] 房梁, 殷丽华, 郭云川, 等. 基于属性的访问控制关键技术研究综述[J]. 计算机学报, 2017, 40(7): 1680-1698.
FANG L, YIN L H, GUO Y C, et al. A survey of key technologies in attribute-based access control scheme[J]. Chinese Journal of Computers, 2017, 40(7): 1680-1698.

[16] ATTRAPADUNG N, IMAI H. Conjunctive broadcast and attribute-based encryption[C]//3rd International Conference on Pairing-Based Cryptography. Berlin: Springer, 2009: 248-265.

[17] LIU J K, YUEN T H, ZHANG P, et al. Time-based direct revocable ciphertext-policy attribute-based encryption with short revocation list[C]//16th International Conference on Applied Cryptography and Network Security. Berlin: Springer, 2018: 516-534.

[18] YEH L Y, CHIANG P Y, TSAI Y L, et al. Cloud-based fine-grained health information access control framework for lightweight IoT devices with dynamic auditing and attribute revocation[J]. IEEE Transactions on Cloud Computing, 2018, 6(2): 532-544.

[19] HAO J L, HUANG C, LIU J, et al. Efficient outsourced data access control with user revocation for cloud-based IoT[C]//2018 IEEE Global Communications Conference. Piscataway: IEEE Press, 2018:1-6.

[20] 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.

[21] LI M T, HUANG X Y, LIU J K, et al. GO-ABE: group-oriented attribute-based encryption[M]. Cham: Springer International Publishing, 2014.

[22] YEH S C, SU M Y, CHEN H H, et al. An efficient and secure approach for a cloud collaborative editing[J]. Journal of Network and Computer Applications, 2013, 36(6): 1632-1641.

[23] 史姣丽, 黄传河, 王晶, 等. 云存储下多用户协同访问控制方案[J]. 通信学报, 2016, 37(1): 88-99.
SHI J L, HUANG C H, WANG J, et al. Multi-user collaborative access control scheme in cloud storage[J]. Journal on Communications, 2016, 37(1): 88-99.

[24] ILIA P, CARMINATI B, FERRARI E, et al. SAMPAC: Socially-aware collaborative multi-party access control[C]//7th ACM on Conference on Data and Application Security and Privacy. New York: ACM Press, 2017: 71-82.

[25] HUANG Q L, LI N, YANG Y X. DACSC: dynamic and fine-grained access control for secure data collaboration in cloud computing[C]//2018 IEEE Global Communications Conference. Piscataway: IEEE Press, 2018: 1-7.

[26] LI C H, XIE W R, ZHOU K. Efficient binary-encoding access control policy combination for large-scale collaborative scenarios[C]//2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE) . Piscataway: IEEE Press, 2018: 560-566.

[27] BOBBA R, KHURANA H, PRABHAKARAN M. Attribute-sets: a practically motivated enhancement to attribute-based encryption[C]//14th European Conference on Research in Computer Security. Berlin: Springer, 2009: 587-604.

[28] 王光波, 刘海涛, 王晨露, 等. 云存储环境下可撤销属性加密[J]. 计算机研究与发展, 2018, 55(6): 76-86.
WANG G B, LIU H T, WANG C L, et al. Revocable attribute-based encryption in cloud storage[J]. Journal of Computer Research and Development, 2018, 55(6): 76-86.

[29] NAOR D, NAOR M, LOTSPIECH J. Revocation and tracing schemes for stateless receivers[C]//21st Annual International Cryptology Conference. Berlin: Springer, 2001: 41-62.

[作者简介]

彭长根（1963− ），男，贵州锦屏人，博士，贵州大学教授、博士生导师，主要研究方向为隐私保护、密码学和大数据安全。

彭宗凤（1995− ），女，贵州遵义人，贵州大学硕士生，主要研究方向为密码学与访问控制。

丁红发（1988− ），男，河南南阳人，贵州大学在站博士后，主要研究方向为隐私保护和大数据安全。

田有亮（1982− ），男，贵州六盘水人，博士，贵州大学教授、博士生导师，主要研究方向为算法博弈论、密码学与安全协议、大数据安全与隐私保护等。

刘荣飞（1987− ），男，云南宣威人，云上贵州大数据产业发展有限公司高级工程师，主要研究方向为大数据安全。