计算机科学
COMPUTER SCIENCE

# 多权威可撤销密文策略属性基加密数据共享方案

李莉, 陈介, 朱江文

引用本文

李莉, 陈介, 朱江文. 多权威可撤销密文策略属性基加密数据共享方案[J]. 计算机科学, 2025, 52(9): 388-395.

LI Li, CHEN Jie, ZHU Jiangwen. Multi-authority Revocable Ciphertext-policy Attribute-based Encryption Data Sharing Scheme [J]. Computer Science, 2025, 52(9): 388-395.

---

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.240700066

# 多权威可撤销密文策略属性基加密数据共享方案

李　莉[1]　陈　介[2]　朱江文[3]
1 北京电子科技学院电子与通信工程系　北京 102627
2 北京电子科技学院网络空间安全系　北京 102627
3 北京邮电大学网络空间安全学院　北京 100876
(laury_li@126.com)

**摘　要**　在数据安全保护与共享领域,密文策略属性基加密(CP-ABE)被认为是一种在保护数据保密性的同时,允许数据被分享给经过授权的访问者的方法。然而,用户的属性不是一成不变的,因此数据访问者的权限可能发生变化,一种实用的方法是数据所有者重新加密密文并将其上传到服务器,以确保被撤销的用户无法再次访问数据,但这种做法给服务器带来了较大的负担。为了解决这一问题,提出了一种无需更新云端密文的支持用户级和属性级撤销的CP-ABE方案,通过代理服务器对密文进行重加密和预解密,管理各用户的预解密密钥,撤销时只需更新预解密密钥。实验结果表明,在多属性权威机构的条件下,在无需更新云端密文的情况下即可实现细粒度的属性撤销,并且具有前向安全性,相较于同类方案具有较小的计算开销和密钥存储开销。在q-BDHE困难性问题下提供了安全性证明,证明该方案对选择明文攻击具有不可区分性。

**关键词**:属性基加密;访问控制;可撤销;前向安全;数据共享
**中图分类号**　TP309.7

## Multi-authority Revocable Ciphertext-policy Attribute-based Encryption Data Sharing Scheme

LI Li[1],CHEN Jie[2] and ZHU Jiangwen[3]
1 Department of Electronic and Communication Engineering,Beijing Electronic Science and Technology Institute,Beijing 102627,China
2 Department of Cyberspace Security,Beijing Electronic Science and Technology Institute,Beijing 102627,China
3 School of Cyberspace Security,Beijing University of Posts and Telecommunications,Beijing 100876,China

**Abstract**　In the field of data security protection and sharing,Ciphertext-Policy Attribute-Based Encryption(CP-ABE) is widely recognized as a method that ensures the confidentiality of data while allowing authorized users to access and share the data. However,users' attributes are not static,leading to potential changes in data access permissions. A practical approach is for data owners to re-encrypt ciphertext and upload it to the server to prevent revoked users from accessing the data. This practice imposes a significant burden on the server. To address this issue,a CP-ABE scheme supporting user-level and attribute-level revocation without updating cloud ciphertext is proposed,through proxy server re-encrypt and pre-decrypt ciphertext and managing the pre-decryption keys for each user,and updating only the pre-decryption keys during revocation. Experimental analysis demonstrates that under the conditions of multiple attribute authorities,this scheme achieves user-level and attribute-level revocation with forward security without updating cloud ciphertext,with lower computational and key storage overhead compared to similar schemes. Security proofs are provided under the q-BDHE hardness assumption,showing that the scheme is indistinguishable against chosen plaintext attacks.

**Keywords**　Attribute-based encryption,Access control,Revocable,Forward security,Data sharing

## 1　引言

现代社会信息的爆炸性增长使得数据的安全性保护与数据的共享成为研究热点。随着云存储的流行和个人数据量的增长,数据的保护与分享成为一个相对矛盾的问题,对于包含个人隐私、企业机密以及其他不想公开的数据,在上传到云服务器前,数据拥有者需要对其进行加密处理,以防止未经授权的用户或者云服务提供商窥探数据隐私,这造成了分享的困难。采用对称加密时,加密数据只有持有加密密钥的人才能访问,而加密密钥的安全传递在开放的互联网公开信道中是一个复杂的问题。公钥加密算法很好地解决了这个问题,加密者使用访问者的公钥进行加密,再将密态数据上传到开放

到稿日期:2024-07-10　返修日期:2024-09-30
基金项目:中央高校基本科研业务费(3282024007)
This work was supported by the Fundamental Research Funds for the Central Universities(3282024007).
通信作者:陈介(cj_workhub@163.com)

的网络环境中，只有持有相应私钥的访问者才能对加密的数据进行访问，这种方式省去了密钥传递的过程。

但传统的公钥加密（如 RSA，ECC 等）面临一个问题，即当一份数据有多个授权访问者时，需要使用多个用户的公钥对同一份数据进行多次加密，数据量和计算量会随着授权访问者的增加而线性增加。Sahai 等[1]提出的模糊 IBE 加密（Fuzzy Identity-Based Encrypted）很好地解决了这个问题，该方案是一种基于身份的加密方案，允许在一定的误差范围内使用模糊的身份信息来解密数据。基于模糊 IBE，有学者提出了属性基加密（Attribute-Based Encrypted，ABE），ABE 使用属性来描述用户身份，根据属性获得相应的属性密钥，密文也与属性相关联，当用户属性与密文属性的交集大于某一阈值时，对应的属性密钥就能正确解密密文[2]。2006 年，Goyal 等[3]提出了支持访问策略的 ABE 方案。根据访问策略的嵌入位置不同，ABE 可分为密文策略属性基加密（CP-ABE）和密钥策略属性基加密（KP-ABE）。在 CP-ABE 中，密钥与用户属性相关联，在密文中嵌入访问结构；在 KP-ABE 中，密文与用户属性相关联，在密钥中嵌入访问结构。现实的云数据共享，常用 CP-ABE，其允许数据拥有者定义复杂的访问策略，实现细粒度的权限管理，而用户使用者的属性只要满足访问策略即可访问数据而无须透露自己的身份信息。

在单权威的 CP-ABE 方案中，所有的属性密钥分发与管理全由一个机构控制，这个机构的安全责任和工作量很大，而且容易引起单点故障，导致整个系统瘫痪。多权威 CP-ABE 允许不同权威管理不同的属性集合，使得系统更加灵活，能够适应更复杂的访问控制需求，单个权威的工作量更小[4]。多权威 CP-ABE 还能通过多个权威之间的协作来增强系统的安全性，降低系统整体被攻破的风险。

用户的身份和权限不是一成不变的，当用户的身份或者权限发生改变时，就涉及属性撤销的问题。属性撤销按撤销方式可分为直接撤销和间接撤销。在直接撤销中，数据拥有者是执行者，其在加密文件时将被撤销用户的信息添加到撤销列表，并将该列表嵌入密文中，在撤销列表中的用户无法解密，但未被撤销的用户仍可解密。在间接撤销中，执行者是权威机构或第三方，其有权力动态发布撤销信息，为未撤销用户更新密钥，不再更新被撤销用户的密钥或为被撤销用户更新对应其撤销后属性集的密钥。无论是直接撤销还是间接撤销，都面临一个问题，即如何防止被撤销的用户利用过去持有的属性密钥来访问数据。在云存储的场景下，存储文件的云服务器难以对访问的用户进行属性鉴权，因此，需要重新加密数据形成新的密文来保证其不被已被撤销的用户访问，这带来了额外的计算开销和通信开销。本文方案解决了这一问题，当用户被撤销后，无需更新云端密文，仍可以保证数据不被之前具有访问权限但被撤销而不再满足访问条件的用户访问。

本文的贡献主要有：

1）提出了一种可撤销密文策略属性基加密数据共享方案，进行用户属性撤销后无需更新云端密文，具有前向安全性和更高的撤销效率。

2）支持多属性权威，将属性管理和密钥生成过程分散到多个权威机构中，具有更强的可扩展性，相较于单属性权威具有更高的安全性。

3）代理服务器完成解密过程的大部分计算并保存预解密密钥，用户端的计算开销和密钥存储开销较小。

## 2　相关工作

在可撤销 CP-ABE 方案的相关研究中，研究者致力于提出更安全、高效的访问控制方法和撤销方法。

直接撤销方面，Attrapadung 等[5]提出了广播 ABE 系统。广播 ABE 可用于构建具有可直接撤销功能的 ABE 系统，可以在不影响其他未被撤销用户的情况下进行用户撤销。但是该系统中的数据拥有者需要维护每个属性组的所有成员列表，以实现用户撤销，造成了额外的计算开销和存储开销，且只支持用户级别的撤销粒度。Wang 等[6]提出了一种支持细粒度撤销用户属性的 CP-ABE 方案，解决了 Atttrapadung 等提出的可撤销 ABE 方案只能实现用户级撤销的问题，可实现完全细粒度的属性撤销。该方案可以对用户撤销任意数量的属性，解决了撤销粒度过粗的问题，但该方案中公钥参数与系统用户数量线性相关，系统用户数量较大时会产生公钥过长的问题。Das 等[7]提出了支持细粒度撤销用户属性的 CP-ABE 方案，采用基于椭圆曲线密码的标量点乘法运算代替 ABE 方案中常用的双线性配对运算，将密钥生成过程分散到多个半可信属性权威中，减少了密钥生成开销，解决了密钥托管问题，提高了安全性，但该方案在初始化阶段的计算开销较大，基于椭圆曲线的方案在 ABE 领域也缺少广泛的安全性分析。Liu[8]等采用将撤销列表嵌入密文中的直接撤销方法实现了可撤销的 CP-ABE，并引入了密钥时间验证技术来管理密钥到期日期。被撤销的密钥可以在有效期结束后从撤销列表中删除，避免撤销列表冗长，但该方案只支持用户撤销，没有实现细粒度的属性撤销功能。Liu 等[9]提出了一种轻量级的密文策略属性加密方案，将车载终端的静态和动态属性分离，建立了基于路边单元和车载单元的双层解密架构，实现了直接属性撤销机制，但该方案使用椭圆曲线上的标量乘法代替双线性配对运算，缺少广泛的安全性分析。

间接撤销方面，Jiang 等[10]提出了一种支持属性撤销的全外包 CP-ABE 加密方案，利用计算外包将密钥生成以及加/解密过程中的复杂计算交由云服务器完成，减少了密钥生成中心和用户的计算开销。此外，通过属性密钥和密文的更新实现了对用户属性的细粒度撤销。但该方案需要更新云端密文以满足前向安全性，撤销的计算开销和通信开销较大。Wei 等[11]提出了一种可撤销的 ABE 方案，该方案支持动态用户撤销、公共密文更新和可扩展密钥委托等功能，用于在公共云存储中安全共享智能健康记录。该方案的计算开销较低，能够抵御实际密钥暴露攻击，但用户撤销是定时执行而非即时执行。Guo 等[12]提出了一个高效可追踪、可撤销的密文策略属性基加密方案，支持计算外包，通过更新用户的属性群密钥来实现用户撤销。但其需要通过重新加密密文来保证前向安全性，每个用户需要保存的密钥长度也较长。Zhou 等[13]将 CP-ABE 与单向函数树技术相结合，通过单向函数树共享属性组密钥，实现了可撤销的属性加密。通过多项式分

发版本密钥，当有用户属性发生变更时，更新版本密钥，只有被授权用户才能够正确更新密钥。但是，为了实现前向安全性，该方案仍需要更新密文。

## 3 预备知识

### 3.1 双线性映射

双线性映射可以用五元组$(p,g,G,G_1,e)$来表示，其中$G,G_1$均是阶为素数$p$的乘法循环群，$g$为$G$的生成元，$e:G\times G\rightarrow G_1$为双线性映射，其具有以下3个性质。

1)双线性：对于$\forall g_1,g_2\in G$和$a,b\in\mathbb{Z}_p$，有$e(g_1^a,g_2^b)=e(g_1,g_2)^{ab}$。

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

3)可计算性：对于$\forall g_1,g_2\in G$，存在多项式时间算法$\lambda$可以计算出$e(g_1,g_2)$。

### 3.2 访问策略

如果存在一个参与者的集合$P=\{p_1,p_2,\cdots,p_n\}$。对于集合$\Lambda\subseteq 2^{\{p_1,p_2,\cdots,p_n\}}$(其中$2^{\{p_1,p_2,\cdots,p_n\}}$表示集合$P$的所有可能子集的集合)和$\forall B,C\subseteq P$，如果$B\in\Lambda$且$B\subseteq C$，则有$C\in\Lambda$，那么$\Lambda$是单调的，$P$的非空单调子集构成的集合$\Lambda$是一个访问策略。$\Lambda$中的集合为授权集合，不在$\Lambda$中的集合为非授权集合。

### 3.3 线性秘密共享方案

1)加密过程：假设$\boldsymbol{M}$是根据访问策略$\Lambda$生成的一个$l$行$n$列的秘密分享矩阵。$\boldsymbol{M}$的每个行向量对应一个属性，即$l$个行向量与$l$个属性值形成一一映射的关系，$n$则反映了要重构秘密所需要的计算量。假设访问策略$\Lambda$的属性集合全集为$P$。对$i\in\{1,2,\cdots,l\}$，定义映射$\rho$，使得$P=\{\rho(i)\mid i=1,2,\cdots,l\}$。考虑列向量$\boldsymbol{y}=(s,y_2,\cdots,y_n)^{\mathrm{T}}$，其中$s\in\mathbb{Z}_q$表示要分享的秘密值，$y_2,\cdots,y_n\in\mathbb{Z}_q$是一组随机数。则$\boldsymbol{M}\cdot\boldsymbol{y}=(s_1,s_2,\cdots,s_l)\in\mathbb{Z}_q^{l\times 1}$是产生的$l$个秘密碎片，$s_j,j\in\{1,2,\cdots,l\}$对应属性$\rho(j)$。

2)解密过程：若用户的属性集合为$S=\{\rho(i)\in P\mid i\in\{1,2,\cdots,l\}\}$，则生成属性集合$S$对应秘密分享矩阵$\boldsymbol{M}$中行向量的矩阵$\boldsymbol{M}_S=\{\boldsymbol{M}_i\in\boldsymbol{M}\mid i\in\{1,2,\cdots,l\}\}$，其中$\boldsymbol{M}_i$表示$\boldsymbol{M}$的第$i$行。存在满足$\boldsymbol{M}_S^{\mathrm{T}}\cdot\boldsymbol{\lambda}=\boldsymbol{\varepsilon}=(1,0,\cdots,0)^{\mathrm{T}}$的向量$\boldsymbol{\lambda}$。最后，计算$s'=\boldsymbol{\lambda}^{\mathrm{T}}\cdot\boldsymbol{M}_S\boldsymbol{y}=\boldsymbol{\varepsilon}^{\mathrm{T}}\cdot\boldsymbol{y}$。若用户属性集$S$不满足访问策略$\Lambda$，则不能正确解出秘密值$s$，即$s'\neq s$；若满足，则$s'=s$。

### 3.4 判定性q双线性Diffie-Hellman假设

$G_1$和$G_2$均是阶为素数$p$的乘法循环群，$g$为$G_1$的生成元，$e:G_1\times G_1\rightarrow G_2$为双线性映射，随机选择$s,a,r\in\mathbb{Z}_p^*$，计算$\vec{y}=(g,g^s,g^a,g^{a^2},\cdots,g^{a^q},g^{a^{q+2}},\cdots,g^{a^{2q}})$和$Z=e(g,g)^{a^{q+1}s}$。

敌手$\mathcal{A}$的优势定义为：

$$Adv_{\mathcal{A}}^{\text{q-BDHE}}=|Pr[\mathfrak{B}(g,g^s,g^a,g^{a^2},\cdots,g^{a^q},g^{a^{q+2}},\cdots,g^{a^{2q}}),Z)=1]-Pr[\mathfrak{B}(g,g^s,g^a,g^{a^2},\cdots,g^{a^q},g^{a^{q+2}},\cdots,g^{a^{2q}}),e(g,g)^r)=1]|$$

若对所有的概率多项式时间算法都有$Adv_{\mathcal{A}}^{\text{q-BDHE}}\leqslant\varepsilon$且$\varepsilon$是可忽略不计的，则认为在多项式时间内解决判定性q-BDHE假设问题是困难的。

## 4 系统模型和安全模型

### 4.1 系统模型

本文方案中主要包含6种角色，中央权威(Central Authority，CA)、属性权威(Attribute Authorities，AA)、云服务提供商(Cloud Server Provider，CSP)、数据拥有者(Data Owner，DO)、数据使用者(Data User，DU)和代理服务器(Proxy Server，PS)。系统模型如图1所示。

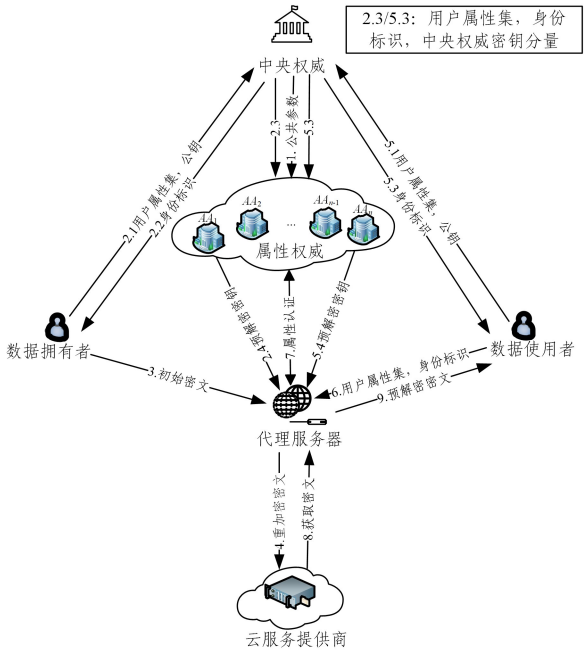


图1 系统模型

Fig. 1 System model

中央权威CA：负责系统初始化，生成公共参数，颁发系统主密钥。

属性权威AA：每个属性权威负责管理特定属性域的信息和相应的属性域的属性密钥分发，各属性权威管理的属性域不存在交叉。

云服务提供商CSP：负责提供存储服务，存储密文。

数据拥有者DO：负责设定数据的访问策略，并对数据进行初始加密，得到初始密文。

数据使用者DU：对代理服务器发起数据访问请求，接收到来自代理服务器的预解密密文后对其进行解密。

代理服务器PS：负责对初始密文进行重加密得到最终密文并将其上传到云服务提供商，对最终密文进行预解密并将其发送给数据使用者。

所提方案主要包含9个算法，方案的形式化定义为：

$\{Setup(),AASetup(),KeyGen(),Encrypt(),ReEncrypt(),AttCheck(),PreDecrypt(),Decrypt(),Revocation()\}$

$Setup(1^\lambda)\rightarrow(MK,PP)$：由中央权威CA执行。以安全参数$\lambda$作为输入，输出系统的主密钥$MK$和系统的公共参数$PP$，并发布公共参数$PP$。

$AASetup(PP,d)\rightarrow(SK_d,PK_d)$：由属性权威AA执行。系统中的属性权威集合为$\{AA_1,AA_2,\cdots,AA_m\}$。以公共参

数 $PP$ 和每个 $AA$ 的索引值 $d$ 作为输入，输出属性权威 $AA_d$ 的私钥 $SK_d$ 和公钥 $PK_d$。

$KeyGen(PP,id,pk_{\mathrm{id}},S)\rightarrow sk_{\mathrm{id,pre}}$：由属性权威 AA 执行。用户先自主生成公私钥对（$pk_{\mathrm{id}},sk_{\mathrm{id}}$），AA 以公共参数 $PP$、用户的 $id$，用户的公钥 $pk_{\mathrm{id}}$ 和用户的属性集 $S$ 作为输入，输出预解密密钥 $sk_{\mathrm{id,pre}}$，预解密密钥由代理服务器保存。

$Encrypt(PP,m,\Lambda)\rightarrow C_{m,\mathrm{pre}}$：由数据拥有者 DO 执行。以公共参数 $PP$、明文 $m$ 和访问策略 $\Lambda$ 作为输入，输出明文的初始密文 $C_{m,\mathrm{pre}}$。

$ReEncrypt(PP,C_{m,\mathrm{pre}})\rightarrow C_m$：由代理服务器 PS 执行。以公共参数 $PP$ 和初始密文 $C_{m,\mathrm{pre}}$ 作为输入，输出密文 $C_m$，将 $C_m$ 上传至 CSP 存储。

$AttCheck(id,S,K_3,K_4)\rightarrow(1/\perp)$：由中央权威、属性权威和代理服务器共同执行。输入用户的 $id$、用户的属性集 $S$ 和预解密密钥中的 $K_3$，$K_4$，输出真或假。

$PreDecrypt(PP,sk_{\mathrm{id,pre}},C_m)\rightarrow F$：由代理服务器 PS 执行。以公共参数 $PP$，预密钥 $sk_{\mathrm{id,pre}}$ 和密文 $C_m$ 作为输入，输出预解密密文 $F$。

$Decrypt(PP,sk_{\mathrm{id}},F,C_m)\rightarrow m$：由数据使用者 DU 执行。以预解密密文 $F$、私钥 $sk_{id}$、公共参数 $PP$ 和密文 $C_m$ 作为输入，输出明文 $m$。

$Revocation(PP,sk_{\mathrm{id,pre}},x_j)\rightarrow sk'_{id,pre}$：由属性权威 AA 执行。以公共参数 $PP$、预解密密钥 $sk_{\mathrm{id,pre}}$ 和待撤销属性 $x_j$ 作为输入，输出新的预解密密钥 $sk'_{\mathrm{id,pre}}$。

### 4.2　安全模型

下文讨论所提方案在明文攻击不可区分性（IND-CPA）安全模型下的安全性，考虑挑战者 $\mathcal{B}$ 和敌手 $\mathcal{A}$ 之间的博弈过程。

1）初始化：敌手 $\mathcal{A}$ 向挑战者 $\mathcal{B}$ 提交要攻击的访问策略 $\Lambda^*$。

2）建立：挑战者 $\mathcal{B}$ 以安全参数 $\lambda$ 作为输入，执行 Setup 算法生成公共参数 $PP$ 和主密钥 $MK$，并将公共参数 $PP$ 发送给敌手 $\mathcal{A}$。

阶段 1：敌手 $\mathcal{A}$ 向挑战者 $\mathcal{B}$ 询问属性集 $S^*=\{S_1,S_2,\cdots,S_q\}$ 对应的属性密钥，其中 $S^*$ 不满足访问策略 $\Lambda^*$。敌手 $\mathcal{A}$ 生成公私钥对（$pk_{\mathrm{id}},sk_{\mathrm{id}}$）并将 $pk_{\mathrm{id}}$ 发送给挑战者，挑战者 $\mathcal{B}$ 运行 KeyGen 算法生成预解密密钥并将其发送给敌手 $\mathcal{A}$。

4）挑战：敌手 $\mathcal{A}$ 选择两个长度相同的消息（$m_0,m_1$），运行 Encrypt 算法得到 $C_{m_0,\mathrm{pre}}$ 和 $C_{m_1,\mathrm{pre}}$ 并将其发送给挑战者 $\mathcal{B}$。挑战者 $\mathcal{B}$ 随机选择 $b\in\{0,1\}$，运行 ReEncrypt 算法加密 $m_b$ 得到密文 $C_{m_b}$，并将其发送给敌手 $\mathcal{A}$。

5）阶段 2：重复阶段 1，查询 $S^{*\prime}$ 对应的预解密密钥。

6）猜测：敌手 $\mathcal{A}$ 猜测一个值 $b'\in\{0,1\}$。如果 $b'=b$，则敌手赢得上述游戏。

敌手 $\mathcal{A}$ 赢得上述游戏的优势 $Adv=|Pr(b'=b)-1/2|$。

## 5　方案构造

1）$Setup(1^\lambda)$：中央权威运行一个以安全参数 $\lambda$ 为输入的群生成算法 $\mathcal{G}$，选择阶为素数 $p$ 的双线性群 $G$，$g$ 是 $G$ 的生成元。选择素数 $q$，使其满足 $\gcd(p,q)=1$，计算 $N=pq$。定义 $X$ 为包含 $h$ 个属性的全局属性集，$X=\{x_1,x_2,\cdots,x_h\}$。选择抗碰撞性哈希函数 $H:\mathbb{Z}_N\rightarrow\{0,1\}^*$ 和 $H_1:X\rightarrow G$。最后，随机选择 $\alpha,\beta\in\mathbb{Z}_N^*$，得到系统的公共参数 $PP$ 和主密钥 $MK$。

$$PP=(\beta,g,g^\alpha,e(g,g)^\alpha,H,H_1,N)$$

$$MK=(p,q,\alpha)$$

2）$AASetup(PP,d)$：每个属性权威都执行此算法，将公共参数和自己的权威索引 $d$ 作为输入。每个 $AA_d(1\leqslant d\leqslant m)$ 负责维护一个属性域 $\{x_{d_1},x_{d_2},\cdots,x_{d_n}\}$，$AA_d(1\leqslant d\leqslant m)$ 随机选择 $y_d,k_d\in\mathbb{Z}_N^*$ 作为其私钥 $SK_d$ 并为属性域计算相应的公钥 $PK_d=\{g^{y_d},g^{k_d}\}$。属性权威 $AA_d$ 为自己属性域中的每个 $x_{dj}$，$(1\leqslant j\leqslant n)$ 随机选择 $u_{dj}\in\mathbb{Z}_N^*$，并计算 $v_{dj}$，使其满足 $v_{dj}u_{dj}\equiv1(\mathrm{mod}\ N)$。

3）$KeyGen(PP,id,S)$：数据拥有者随机选择 $k\in\mathbb{Z}_N^*$ 作为自己的私钥，计算 $K=g^{\frac{1}{k}}$ 作为公钥，生成公私钥对（$pk_{\mathrm{id}}$，$sk_{\mathrm{id}}$）$=(K,k)$。将公钥 $pk_{\mathrm{id}}$、身份标识 $id$ 和数据拥有者的属性集合 $S=\{\rho(i)\in P\mid i\in\{1,2,\cdots,l\}\}$ 发送给中央权威。中央权威在接收到数据拥有者的请求后，随机选择一个 $c\in\mathbb{Z}_N^*$，计算：

$$K_1=K^\alpha g^{\beta c}$$

然后将 $c$ 发送给各属性权威 $AA_i$，各属性权威对自己管理的属性域中的 $\rho(i)$，$i\in\{1,2,\cdots,l\}$ 计算 $K_{2,d}=\{H_1(\rho(i))\}^c$ 和 $K_{3,d}=\begin{cases}g^{c\prod v_i/\rho(i)}, & d=1\\ K_{3,d}=(K_{3,d-1})^{c\prod v_i/\rho(i)}, & 2\leqslant d\leqslant m\end{cases}$。代理服务器计算 $K_2=\{K_{2,d}\mid d=1,2,\cdots,m\}$ 和 $K_3=K_{3,m}$。

输出预密钥 $sk_{\mathrm{id,pre}}=(K_1,K_2,K_3,K_4=c)$。

4）$Encrypt(PP,m,\Lambda)\rightarrow C_{m,pre}$：数据拥有者制定一个包含属性集合为 $P$ 的访问策略 $\Lambda$，并生成一个 $l$ 行 $n$ 列的秘密分享矩阵 $\boldsymbol{M}$ 和映射 $\rho$。将矩阵 $\boldsymbol{M}$ 中的每一行映射到一个参与者，则有 $P=\{\rho(i)\in X\mid i=1,2,\cdots,l\}$。选择一个秘密值 $s\in\mathbb{Z}_q$，根据线性秘密共享方案得到分享向量 $\boldsymbol{t}=(t_1,\cdots,t_l)$。然后，计算：

$$C_1=me(g,g)^{\alpha s},C_2=g^s,\{C_{i,1}=g^{t_i},C_{i,2}=H_1(\rho(i))\}_{1\leqslant i\leqslant l}$$

输出初始密文 $C_{m,\mathrm{pre}}=(C_1,C_2,C_{i,1},C_{i,2})$，并将 $C_{m,\mathrm{pre}}$ 发送给代理服务器。

5）$ReEncrypt(PP,C_{m,\mathrm{pre}})$：代理节点接收到来自数据拥有者的初始密文 $C_{m,\mathrm{pre}}$ 后，对初始密文进行重加密。随机选取 $r_1,r_2,\cdots,r_l\in\mathbb{Z}_N$，并计算

$$\{C_{i,3}=C_{i,1}^{\beta}C_{i,2}^{r_i},C_{i,4}=g^{-r_i}\}_{1\leqslant i\leqslant l}$$

输出密文 $C_m=(C_1,C_2,C_{i,1},C_{i,3},C_{i,4})$，并将 $C_m$ 上传至云服务提供商。

6）$AttCheck(id,S',K_3,K_4)\rightarrow(1/\perp)$：属性认证主要包括以下 5 个步骤。

（1）数据使用者将自己的属性集合 $S'=\{\rho(i)\in P\mid i\in\{1,2,\cdots,l'\}\}$、身份标识 $id$ 发送给代理服务器。

（2）代理服务器生成属性集合 $S'$ 对应的矩阵 $\boldsymbol{M}_{S'}=$

$\{\boldsymbol{M}_i \in \boldsymbol{M} | i \in \{1,2,\cdots,l'\}\}$，其中 $\boldsymbol{M}_i$ 表示 $\boldsymbol{M}$ 的第 $i$ 行，并计算满足 $\boldsymbol{w}\boldsymbol{M}_{s'}=(1,0,\cdots,0)$ 的向量 $\boldsymbol{w}$。将数据使用者的身份标识 $id$ 和属性集合 $S'$ 发送到中央权威。

(3)中央权威将 $S'$ 发送给各属性权威，各属性权威根据属性集合 $S'$，对属于自己管理的属性域中的 $x_j \in S'$，计算：

$$u_d' = \prod_{x_j \in S'} u_j, 1 \leqslant d \leqslant m$$

(4)中央权威计算：

$$u' = \prod_{d=1}^{m} u_d'$$

并将 $u'$ 发送给代理服务器。

(5)代理服务器下载数据密文 $C_m$，计算：

$$\prod_{i \in S} e(g^c, C_{i,1})^{w_i} \stackrel{?}{=} e(C_2', K_3)$$

是否成立，若成立，则说明数据使用者的属性集合满足密文中的访问策略，代理服务器为数据使用者执行预解密 $PreDecrypt$，并返回 1。否则返回 $\perp$，并终止验证过程。

7) $PreDecrypt(PP, sk_{id,pre}, C_m)$：代理服务器计算

$$F = \frac{e(K_1, C_2)}{\prod_{i \in S}(e(C_{i,3}, g^c)e(C_{i,4}, K_2))^{w_i}} = e(g,g)^{\frac{\alpha s}{k}}$$

并将预解密密文 $F$ 和初始密文中的组件 $C_1$ 发送给数据使用者。

8) $Decrypt(PP, sk_{id}, F, C_m)$：数据使用者收到预解密密文 $F$ 后，计算：

$$\frac{C_1}{F^{sk_{id}}} = \frac{C_1}{F^k} = \frac{me(g,g)^{\alpha s}}{e(g,g)^{\frac{\alpha s}{k} k}} = m$$

9) $Revocation(PP, sk_{id,pre}, x_j)$：

(1) 撤销某一用户 $id$ 的某个属性 $x_j$ 时，负责管理属性 $x_j$ 的属性权威计算：

$K_2' = K_2 / H_1(x_j)^{K_4}$，$K_3' = K_3 / g^{v_j}$

新的预解密密钥为 $sk'_{id,pre} = (K_1, K_2', K_3', K_4 = c)$

该属性权威为拥有该属性 $x_j$ 但未被撤销的用户重新计算预密钥中的 $K_3$。为属性 $x_j$ 重新生成 $u_j' \neq u_j$，并计算 $v_j'$ 使其满足 $v_j' u_j' \equiv 1 (\mathrm{mod}\ N)$，为未撤销的用户计算：

$K_3' = (K_3)^{v_j'} / g^{v_j}$

(2)撤销某一个用户 $id$ 时，代理服务器直接删除相应用户的预解密密钥 $sk_{id,pre}$ 即可。

## 6 方案分析

### 6.1 正确性

#### 6.1.1 解密正确性

下式成立，则说明数据使用者可以正确还原密文。

$$\begin{aligned}
F &= \frac{e(K_1, C_2)}{\prod_{i \in S}(e(C_{i,3}, g^c)e(C_{i,4}, K_2))^{w_i}} \\
&= \frac{e(g,g)^{\frac{\alpha s}{k}} e(g,g)^{\beta s c}}{\prod_{i \in S}(e(g^{\beta t_i} H_1(\rho(i))^{r_i}, g^c)e(g^{-r_i}, H_1(\rho(i))^c))^{w_i}} \\
&= \frac{e(g,g)^{\frac{\alpha s}{k}} e(g,g)^{\beta s c}}{\prod_{i \in S}(e(g,g)^{\beta t_i c} e(H_1(\rho(i)), g)^{r_i c} e(g, H_1(\rho(i)))^{-r_i c})^{w_i}} \\
&= \frac{e(g,g)^{\frac{\alpha s}{k}} e(g,g)^{\beta s c}}{\prod_{i \in S} e(g,g)^{\beta t_i c w_i}} \\
&= \frac{e(g,g)^{\frac{\alpha s}{k}} e(g,g)^{\beta s c}}{e(g,g)^{\beta s}} \\
&= e(g,g)^{\frac{\alpha s}{k}}
\end{aligned}$$

#### 6.1.2 属性验证正确性

属性验证过程中，若下面两个式子的计算结果相同，则说明数据使用者的属性满足密文中嵌入的访问策略。

$$\begin{aligned}
\prod_{i \in S} e(g^c, C_{i,1})^{w_i} &= \prod_{i \in S} e(g^c, g^{t_i})^{w_i} \\
&= e(g,g)^{\sum_{i \in S} c \cdot w_i t_i} \\
&= e(g,g)^{cs} \\
e(C_2', K_3) &= e(g^{s \prod_{x_i \in S} u_i}, g^{c \prod_{x_i \in S} v_i}) \\
&= e(g,g)^{cs \prod_{x_i \in S} u_i v_i} \\
&= e(g,g)^{cs}
\end{aligned}$$

### 6.2 安全性

#### 6.2.1 选择明文攻击不可区分性

**定理 1** 假定判定性 q-PBDHE 假设成立。则不存在概率多项式时间的敌手 $\mathcal{A}$ 在最多进行 $q$ 次询问的情况下，以不可忽略的优势 $\varepsilon$ 攻破多权威可撤销密钥策略属性基加密方案，且该方案是满足 IND-CPA 安全的。

证明：假设存在一个概率多项式时间的敌手 $\mathcal{A}$，能够以不可忽略的优势 $\varepsilon = Adv_{\mathcal{A}}$ 来区分随机元素的有效密文。挑战者 $\mathcal{B}$ 能够以不可忽略的优势 $\varepsilon$ 来解决判定性 q-BDHE 问题，并给定一个 q-BDHE 问题的实例 $\boldsymbol{y}$。模拟游戏的交互过程如下。

1)初始化：敌手 $\mathcal{A}$ 选择一个要挑战的访问策略 $\Lambda^*$ 来生成一个 $l^* \times n^*$，$n^* < q$ 的矩阵 $\boldsymbol{M}^*$ 和映射 $\rho^*$，并将其发送给挑战者 $\mathcal{B}$。

2)建立：挑战者 $\mathcal{B}$ 以安全参数 $\lambda$ 作为输入，执行 Setup 算法，生成公共参数 $PP$。

(1) 挑战者 $\mathcal{B}$ 随机选择 $\alpha' \in \mathbb{Z}_p$，并令 $\alpha = \alpha' + a^{q+1}$，则有

$$e(g,g)^{\alpha} = e(g,g)^{\alpha'} e(g,g)^{a^{q+1}}$$

(2) 对于每个属性 $x$，由属性权威随机选择 $z_x, u_x, v_x \in \mathbb{Z}_p^*$，并使得 $u_x v_x \equiv 1 \bmod N$。挑战者 $\mathcal{B}$ 按如下规则设计哈希函数 $H_1$：

$$H_1(x) = \begin{cases} g^{z_x} \prod_{i \in S} g^{\beta M_{i,1}^* / b_i} \cdot g^{\beta^2 M_{i,2}^* / b_i} \cdots g^{\beta^{n^*} M_{i,n^*}^* / b_i}, & X \neq \phi \\ g^{z_x}, & X = \phi \end{cases}$$

其中，$S$ 代表满足 $\rho^*(i) = x$ 的指数 $i$ 的集合。

(3) 随机选择一个 $\beta \in \mathbb{Z}_p$ 和一个抗碰撞随机函数 $H$。

最后，输出公共参数 $PP = (\beta, g, g^{\alpha}, e(g,g)^{\alpha}, H, H_1, N)$ 和主密钥 $MK = (p, q, \alpha)$，并将公共参数 $PP$ 发送给敌手 $\mathcal{A}$。

3)阶段 1：挑战者 $\mathcal{B}$ 响应敌手 $\mathcal{A}$ 的密钥询问。

(1) 挑战者 $\mathcal{B}$ 机选择 $k \in \mathbb{Z}_p$，并生成公私钥对 $(pk_{id}, sk_{id}) = (g^{1/k}, k)$。

(2) 由线性秘密共享方案可知，存在一个满足 $\boldsymbol{M}_i^* \cdot \boldsymbol{w} = 0$ 的向量 $\boldsymbol{w} = (w_1, \cdots, w_{n^*})^{\mathrm{T}} \in \mathbb{Z}_p^{n^*}$，其中 $\boldsymbol{M}_i^*$ 表示 $\boldsymbol{M}^*$ 的第 $i$ 行。挑战者 $\mathcal{B}$ 随机选择 $r \in \mathbb{Z}_p$，并定义：

$$c = r + w_1 a^q + w_2 a^{q-1} + \cdots + w_{n^*} a^{q-n^*+1}$$

(3) 根据 $c$ 的值,可以通过计算得到:

$$\begin{cases} g^{c} = g^{r+w_1 a^{q}+w_2 a^{q-1}+\cdots+w_{n^*} a^{q-n^*+1}} \\ \quad = g^{r} \prod_{1\leqslant i\leqslant n^*} (g^{a^{q+1-i}})^{w_i} \\ K_1 = K^{\alpha'} g^{\beta c} = g^{\frac{\alpha'}{k}} g^{\beta(r+w_1 a^{q}+w_2 a^{q-1}+\cdots+w_{n^*} a^{q-n^*+1})} \\ \quad = g^{\frac{\alpha'}{k}} g^{\beta r} \prod_{2\leqslant i\leqslant n^*} (g^{a^{q+2-i}})^{w_i} \\ K_3 = g^{c \prod_{1\leqslant i\leqslant n^*} v_i} = g^{r} \prod_{1\leqslant i\leqslant n^*} (g^{a^{q+1-i}})^{w_i v_i} \end{cases}$$

(4) 若访问策略中不包含属性 $x$,则设 $K_2 = K_1^{z_x}$。若包含属性 $x$,则设:

$$K_2 = g^{c\cdot z_x} \prod_{i\in S} \prod_{1\leqslant j\leqslant n^*} (g^{(a^{i}/b_i)r} \prod_{\substack{1\leqslant k\leqslant n^* \\ k\neq j}} (g^{a^{q+1+j-k}/b_i})^{w_k})^{M^*_{i,j}}$$

4)挑战:挑战者 $\mathcal{B}$ 为敌手 $\mathcal{A}$ 生成挑战密文。

(1) 敌手 $\mathcal{A}$ 选择两个长度相等的消息 $m_0$ 和 $m_1$,并发送给挑战者 $\mathcal{B}$。挑战者 $\mathcal{B}$ 随机选择 $b\in\{0,1\}$ 和 $Z$,计算:

$C_1 = Z\cdot m_b e(g,g)^{\alpha' s}$, $C_2 = g^{s}$

(2) 挑战者 $\mathcal{B}$ 随机选择 $y_2,\cdots,y_{n^*}\in\mathbb{Z}_p^*$,并计算 $v=(s, s\times a+y_2,\cdots,s\times a^{n-1}+y_{n^*})\in\mathbb{Z}_p^{n^*}$。

(3) 挑战者 $\mathcal{B}$ 随机选取 $r_1',r_2',\cdots,r_l'\in\mathbb{Z}_p^*$,定义 $R_i=\{i:\rho^*(i)=\rho^*(k),k\neq i\}_{i=1,\cdots,n^*}$,计算:

$$\begin{cases} C_{i,1} = \prod_{j=2,\cdots,n^*} g^{M^*_{i,j} y_j} \\ C_{i,3} = H_1(\rho^*(i)) - r_{i'}(\prod_{j=2,\cdots,n^*} (g^{a}) g^{M^*_{i,j} y_j}) \cdot \\ \qquad (g^{sb_i})^{z_{\rho^*(i)}} \cdot \prod_{k\in R_i} \prod_{j=1,\cdots,n^*} (g^{a_j\cdot s(\frac{b_i}{b_k})})^{M^*_{k,j}} \\ C_{i,4} = g^{r_i'} g^{sb_i} \end{cases}$$

并把挑战密文 $CT=(C_1,C_2,C_{i,1},C_{i,3},C_{i,4})$,$1\leqslant i\leqslant l$ 发送给敌手 $\mathcal{A}$。

5)阶段 2　重复阶段 1,查询 $S^*{}'$ 对应的预解密密钥。

6)猜测　敌手 $\mathcal{A}$ 输出一个猜测值 $b'\in\{0,1\}$。如果 $b=b'$,则挑战者 $\mathcal{B}$ 输出 0。如果 $b\neq b'$,则挑战者 $\mathcal{B}$ 输出 1。

当挑战者 $\mathcal{B}$ 输出 0 时,表明 $Z=e(g,g)^{a^{q+1}s}$,所以敌手 $\mathcal{A}$ 的优势为:

$$Pr[\mathcal{B}(y,Z=e(g,g)^{a^{q+1}s})=0]=\frac{1}{2}+Adv_{\mathcal{A}}$$

当挑战者 $\mathcal{B}$ 输出 1 时,表明 $Z$ 是 $G_2$ 中随机元素,无法获取到任何信息,所以敌手 $\mathcal{A}$ 的优势为:

$$Pr[\mathcal{B}(y,Z=e(g,g)^{r})=0]=\frac{1}{2}$$

由于判定性 q-PDBHE 问题是困难的,其优势 $\varepsilon=Adv_{\mathcal{A}}$ 可以被忽略,因此多权威可撤销密钥策略属性基加密方案是 IND-CPA 安全的。

### 6.2.2　抗合谋攻击

本方案具有抵御合谋攻击的能力,能确保数据的安全性。当多个用户串通访问加密数据时,由于本方案中的用户在申请属性密钥时需要提供其身份标识 id,而每个用户的身份标识 id 由用户在进行注册时分配并且各不相同,系统在生成各用户属性密钥时所使用的随机数也不同,因此,即使多个用户之间存在合谋,他们各自生成的属性密钥也是独立的,无法共同解密文件。

### 6.2.3　前向安全性分析

在本方案中,数据使用者若想正确解密密文,需要先经过代理服务器。代理服务器使用数据访问者的预解密密钥对密文进行预解密,得到预解密密文,并将其发送给数据使用者,数据使用者再利用自己持有的私钥对预解密密文进行最终解密,得到明文。当用户的部分属性被撤销时,代理服务器即时更新被撤销用户的预解密密钥,用户被撤销后再请求得到的预解密密文是使用更新后的预解密密钥进行预解密得到的,用户无法使用自己的私钥正确解密得到明文。当用户被撤销时,代理服务器将直接删除该用户的预解密密钥,不再响应该用户的请求,被撤销用户将丧失所有解密能力。综上所述,本方案具有前向安全性。

## 6.3　性能分析

本节将所提方案与相关工作中提到的其他现有方案进行比较,详细分析和讨论各方案的安全性能和计算性能。

功能对比如表 1 所列。可以看出,本方案在多权威机构的前提下实现了支持外包解密和属性级的即时撤销。

表 1　各方案的功能对比

Table 1　Functional comparison of each scheme

| 方案 | 数学难题 | 多权威 | 外包解密 | 撤销粒度 |
|---|---|---|---|---|
| 文献[5] | 双线性配对 | 支持 | 不支持 | 用户 |
| 文献[6] | 双线性配对 | 不支持 | 不支持 | 用户/属性 |
| 文献[7] | 椭圆曲线 | 支持 | 支持 | 用户 |
| 文献[8] | 双线性配对 | 不支持 | 不支持 | 用户 |
| 文献[10] | 双线性配对 | 不支持 | 不支持 | 用户 |
| 文献[11] | 双线性配对 | 不支持 | 支持 | 用户/属性 |
| 文献[12] | 双线性配对 | 不支持 | 支持 | 用户/属性 |
| Ours | 双线性配对 | 支持 | 支持 | 用户/属性 |

存储开销对比如表 2 所列。$U$ 表示系统属性数量,$T$ 表示访问树的深度,$T_L$ 表示访问结构中叶子节点的总数,$l$ 表示访问结构矩阵的行数,$S$ 表示用户属性的数量,$R$ 表示撤销用户的最大数量,$N$ 表示系统中的用户数量,$I$ 表示解密时涉及的属性数量,$D$ 表示时间段总数,$e$ 表示一次模指数运算的开销,$p$ 表示一次双线性对运算的开销。本方案中,用户端存储的密钥的长度并不会随着系统属性量的增长而增长,用户端的密钥存储开销也较小,私钥的长度仅为 1,即 $\mathbb{Z}_N^*$ 中一个随机数的长度。在密文长度方面,由于参与对比的方案都是 CP-ABE 方案,因此密文长度普遍会随着访问策略生成的矩阵行数的增加而增长,所提方案的密文长度随访问策略矩阵行数线性增长,与同类型方案相当。

表 2　存储开销对比

Table 2　Comparison of storage cost

| 方案 | 公钥 | 私钥 | 密文 |
|---|---|---|---|
| 文献[5] | $U+l+R+2$ | $U+2$ | $l+2$ |
| 文献[6] | $2N+2U+3$ | $2S+1$ | $6l+2$ |
| 文献[7] | $2U+1$ | $T$ | $2T_L+1$ |
| 文献[8] | $U+T+R+4$ | $S+3T+R+2$ | $l+4$ |
| 文献[10] | $U+T+\log D+3$ | $T\log N$ | $T(T+l+1)$ |
| 文献[11] | $S+1$ | $2S+3$ | $l+4$ |
| 文献[12] | $N$ | $2S+1$ | $2T_L+5$ |
| Ours | $S+4$ | 1 | $3l+2$ |

计算开销对比如表 3 所列，因为模乘运算的计算开销与模指数运算和双线性配对运算相比可忽略不计，因此不考虑模乘运算的计算开销。由于文献[7]方案使用椭圆曲线进行构造，因此不参与计算开销的比较。

表 3 中的撤销指为实现撤销和前向安全所进行的所有运算的开销之和。本方案初始化过程只需进行一次模指数运算和双线性配对运算。加密过程中，计算开销与访问策略生成的矩阵行数 $l$ 成正比例，优于同类方案。由于代理服务器完成了解密的大部分计算，因此用户端的解密计算开销较小，只需进行一次指数运算。在撤销时不涉及双线性配对运算，撤销计算量随系统中用户的数量线性增长，撤销开销小。

表 3 计算开销对比

Table 3 Comparison computation cost

| 方案 | 初始化 | 加密 | 用户解密 | 撤销 |
|---|---|---|---|---|
| 文献[5] | $e+(U+N)p+1$ | $(3l+1)e+l\cdot p$ | $(2l+2S+1)e+p\cdot l$ | $2e\cdot N$ |
| 文献[6] | $(2N+2U+1)e$ | $[2(U-R)l+3l+1]e+p$ | $Ie+[2I+2(U-R)+2]p$ | $2e\cdot N$ |
| Liu 等[8] | $(R+1)e+p$ | $(r+T+2l+3)e$ | $(I+1)e+(2I+4)p$ | $e\cdot T\cdot N$ |
| 文献[10] | $e+p$ | $eT(Ul+T)$ | $I(e+p)$ | $e\cdot T(lS+T)$ |
| 文献[11] | $(U+1)e+p$ | $4e\cdot l+e+p$ | $2(e+p)$ | $2e\cdot N$ |
| 文献[12] | $3e+p$ | $(2T_L+1)e+2p$ | $2e+S\cdot p$ | $(3+2N+2T_L)e$ |
| Ours | $e+p$ | $(3l+2)e+p$ | $e$ | $e\cdot N$ |

### 6.4 实验分析

使用 Charm-Crypto 库在 Python 3.10 的环境下实现了所提方案。选择 160 位素数阶的超奇异对称椭圆曲线群。在 Intel Core(TM) i5-8300H 和 4 GB RAM 的 Ubuntu20.04 系统的虚拟机上进行了实验，取 10 次实验的平均值。图 2 展示了所提方案的主要算法在不同用户属性数量下的运行时间，从中可知，密钥生成、加密的时间消耗随用户属性数量的增加大致呈线性增长；代理服务器预解密的时间消耗随用户属性数量的增加大致呈线性增长；用户解密的时间基本稳定且较短，并不会随用户属性数量的增加而增长；属性撤销的时间消耗随撤销属性数量的增多也大致呈线性增长。实验结果与理论分析一致。

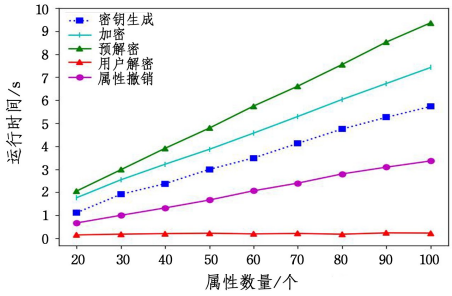


图 2 主要算法的时间消耗

Fig. 2 Time cost of main algorithm

**结束语** 本文提出了支持灵活且实时的用户和属性撤销的数据共享方案。该方案在进行撤销操作时，无需更新云端密文。方案中，用户属性由多个属性机构管理，有助于降低单个属性权威的工作量，同时提高系统整体的安全性。安全性分析表明，本方案在 q-BDHE 假设的前提下是 IND-CPA 安全的，并且能够有效抵御多个用户合谋获取密钥以解密数据的攻击。性能分析表明，相较于同类方案，该方案在用户端具有较小的计算开销和密钥存储开销，进一步提升了其实用性和效率。这些特点使得该方案在实际应用中具有显著的优势，为用户提供了更安全、高效的数据访问和管理方式。但是，代理服务器的引入，造成了额外的交互，导致本方案在解密时的通信开销与其他方案存在一定差距，这也是未来的工作方向之一，即减少以及简化系统各参与方之间的交互，减少整体的通信开销。

## 参 考 文 献

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

[2] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]// 2007 IEEE Symposium on Security and Privacy (SP'07). IEEE, 2007: 321-334.

[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. 2006: 89-98.

[4] YAN X, NI H, LIU Y, et al. Privacy-preserving multi-authority attribute-based encryption with dynamic policy updating in PHR [J]. Computer Science and Information Systems, 2019, 16(3): 831-847.

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

[6] WANG P P, FENG D G, ZHANG L W. CP-ABE Scheme Supporting Fully Fine-Grained Attribute Revocation [J]. Journal of Software, 2012, 23(10): 2805-2816.

[7] DAS S, NAMASUDRA S. MACPABE: Multi-Authority-based CP-ABE with efficient attribute revocation for IoT-enabled healthcare infrastructure [J]. International Journal of Network Management, 2023, 33(3): e2200.

[8] LIU J K, YUEN T H, ZHANG P, et al. Time-Based Direct Revocable Ciphertext-Policy Attribute-Based Encryption with Short Revocation List[C]// Applied Cryptography and Network

Security. Cham：Springer，2018：516-534.
[9] LIU Y L，XU S W，YUE Z Y. A Lightweight CP-ABE Scheme with Direct Attribute Revocation for Vehicular Ad Hoc Network[J]. Entropy，2023，25(7)：979.
[10] JIANG Y，SUSILO W，MU Y，et al. Ciphertext-policy attribute-based encryption with hidden access policy[J]. Mobile Networks and Applications，2018，23(4)：840-854.
[11] WEI J H，CHEN X F，HUANG X X，et al. RS-HABE：Revocable-Storage and Hierarchical Attribute-Based Access Scheme for Secure Sharing of e-Health Records in Public Cloud[J]. IEEE Transactions on Dependable and Secure Computing，2019，18(5)：2301-2315.
[12] GUO L F，XING X M，GUO H. An efficient traceable and revocable attribute-based encryption scheme in cloud storage[J]. Journal of Cryptologic Research，2023，10(1)：131-145.
[13] ZHOU X B，JIANG R. A fine-grained data encryption and sharing scheme in fog and cloud computing environments[J]. Journal of Cryptologic Research，2023，10(6)：1295-1318.

**LI Li**，born in 1974，Ph.D，professor，is a member of CCF（No. U9735M）. Her main research interests include network and system security and embedded system security application.

**CHEN Jie**，born in 2000，master. His main research interests include searchable encryption and attribute-based cryptography.

（责任编辑：何杨）

# 第 42 届 CCF 中国数据库学术会议（NDBC 2025）在长春举行

2025 年 8 月 1 日－3 日，由中国计算机学会（CCF）主办、CCF 数据库专委会和吉林大学共同承办的第 42 届 CCF 中国数据库学术会议（NDBC 2025）于吉林长春成功召开。

本次大会主要关注数据库领域所面临的新挑战、新问题和新方向，着力反映我国数据库技术研究的最新进展，为科研院所、科技企业的数据库研究、开发和应用相关人员搭建交流平台。大会由 5 个大会特邀报告、研究生学术辅导班、企业之夜、13 个分论坛报告、2 个大会论文分组报告、1 个萨师煊优秀论文报告、1 个系统演示等一系列活动组成，并邀请了国内外数据库领域著名专家到会作专题报告，来自国内各大高校、科研机构、公司企业的 680 余人注册参会。

8 月 2 日上午是开幕式，吉林大学副校长张国兴，NDBC2025 大会共同主席、浙江大学副校长陈刚，CCF 会士、常务理事、数据库专委会主任，华东师范大学教授周傲英先后致辞，NDBC2025 程序委员会主席、北京航空航天大学教授童咏昕介绍论文录用和会议工作相关情况，吉林大学计算机科学与技术学院院长杨博教授主持开幕式。

会议中，CCF 会士、中国科学院外籍院士、浙江大学黄铭钧教授，东京工业大学横田治夫教授，复旦大学薛向阳教授，清华大学李国良教授，腾讯云数据库研发负责人潘安群高工分别就“数据核心的系统与应用：从科研到转化”，“DATABASE TECHNOLOGIES FOR HEALTHCARE”，“大模型：当前数据塑造智能的一条成功路径”，“数据智能体：自主数据处理的新范式”，“从应用视角看数据库发展与未来”等题做了精彩的大会特邀报告，分享了他们的最新科研成果。

同时为了便于数据库领域的人才交流，NDBC 2024 大会于 8 月 1 日晚特设企业之夜活动环节。华为、达梦数据、OCEANBASE（海扬数据库）、腾讯云数据库、金篆信科、阿里云、TDENGINE、电科金仓、南大通用、移动云（大云海山数据库）、海量数据、百度、字节跳动、崖山数据库等数据库专委企业合作伙伴展示公司文化和招聘需求，与会者在友好愉快的氛围中实现各数据库企业、高校专家之间的行业探讨和技术探索，同时为学生身份的参会者提供与各名企面对面交流、简历快速投递等通道，将学术界与企业界相互融合交流。

另外，大会还组织了“第五生产要素背景下的数据技术论坛”、“大规模图数据管理与分析论坛”、“时序数据智能管理与分析论坛”、“数据库系统新技术论坛”、“ CCF－华为胡杨林基金数据库专项论坛”、“CCF－阿里云瑶池科研基金论坛”、“CCF－蚂蚁科研基金数据库专项论坛”、“数据库教育论坛”、“贝叶斯数据分析论坛”、“新一代数据库与数据赋能技术国际论坛”、“数据库开源技术论坛”、“移动云大云海山数据库合作生态论坛”等专题论坛，1 场研究生学术辅导班，1 场软件学报专刊报告会，1 场系统演示，2 个论文报告论坛，1 个萨师煊优秀学生论文汇报论坛。各位专家学者与同学们在报告中分享了最新的研究成果，并进行了热烈的讨论交流，为推动数据库技术的发展和创新作出了积极的贡献。

大会闭幕式上颁发了最佳系统演示、萨师煊优秀学生论文、优秀博士论文激励计划等奖项。同时，公布了新增执委名单。

最后，CCF 数据库专委会主任周傲英对整个 NDBC2025 大会做了总结，对大家的付出和参与表示了感谢。第 42 届 CCF 中国数据库学术会议取得圆满成功！

**据 CCF 专业委员会**