策略隐藏的可撤销属性基可搜索加密方案

刘晨旭[1]，曹素珍[1,2]，刘静洁[1]，庞新杰[1]，冯珍[1]

（1.西北师范大学计算机科学与工程学院，甘肃 兰州 730070；
2.西北师范大学密码学与数据分析重点实验室，甘肃 兰州 730070）

摘 要：数据隐私保护和密文可搜索性问题在云计算环境中的重要性与日俱增，针对传统 CP-ABE 方案中明文形式的访问策略可能会泄露敏感信息、恶意用户撤销繁琐等问题，提出一种具有前后向安全、可撤销和部分策略隐藏的属性基可搜索加密方案。通过公开用户属性名、隐藏用户属性值的方式实现部分策略隐藏，避免敏感信息泄露。将用户的身份信息与二叉树叶节点关联，用户撤销列表与密文绑定，使得恶意用户被可信中心添加到撤销列表后将无法访问撤销前后的密文，从而在满足前后向安全的情况下实现用户直接撤销。而云服务器仅需更新与撤销列表相关的密文，不需要执行密钥更新，提高了密文更新的效率。采用更新二叉树节点的随机值方式复用被撤销用户占用的二叉树节点，实现系统中用户数量的扩容。基于 q-BDHE 假设，证明所提出的方案在随机预言模型中满足选择明文攻击下的不可区分（IND-CPA）安全性。性能分析表明，相比传统 CP-ABE 方案，该方案在加密阶段的计算开销至少降低了 15.3%，在搜索验证和密文更新阶段计算开销较低。

关键词：策略隐藏；用户撤销；属性基加密；可搜索；二叉树

中图分类号：TP391 **文献标志码：**A **DOI：**10.19678/j.issn.1000-3428.0069806

Revocable Attribute-Based Searchable Encryption Scheme with Policy Hiding

LIU Chenxu[1], CAO Suzhen[1,2], LIU Jingjie[1], PANG Xinjie[1], FENG Zhen[1]

(1.College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, Gansu, China;
2.Key Laboratory of Cryptography and Data Analytics, Northwest Normal University, Lanzhou 730070, Gansu, China)

【Abstract】 The importance of data privacy protection and ciphertext searchability in cloud computing environments is increasing. Access policies in plain text in traditional CP-ABE schemes may leak sensitive information, and revoking malicious users is cumbersome. To address these issues, this study proposes an attribute-based searchable encryption scheme with forward and backward security, revocability, and partial policy hiding. This scheme achieves partial policy hiding by exposing user attribute names and hiding user attribute values to avoid sensitive information leakage. A user's identity information is associated with the leaves of a binary tree, and the user revocation list is bound to the ciphertext. Thus, malicious users cannot access the ciphertext before and after revocation once they are added to the revocation list by the trusted center, thereby achieving direct user revocation while meeting forward and backward security. After a malicious user is revoked, the cloud service provider only needs to update the ciphertext related to the revocation list, and no additional key update operation is required, which improves the computational efficiency of the ciphertext update. The binary tree nodes occupied by the revoked user are reused by updating the random value of the binary tree node, which increases the number of users in the system. Based on the q-Bilinear Diffie-Hellman Exponent (q-BDHE) assumption, the proposed scheme is proven to be Indistinguish ability under Chosen Plaintext Attack (IND-CPA) secure in the random oracle model. In performance analyses, computational burden reduces by at least 15.3% during the scheme's encryption stage, and the computational overhead is low in the search verification and ciphertext update phases.

【Key words】 policy hiding; user revocation; attribute-based encryption; searchable; binary tree

0 引言

5G 技术的飞速发展随之推动了工业物联网和云计算技术的应用[1]，多设备连接和高数据速率使人与物之间的联系愈发紧密，云服务器相应地为用户提供了计算资源和存储服务[2]。然而，面对海量的用户数据和近年频繁出现的众多信息安全事件，云服务器所提供的云计算和云存储服务中数据的隐私问题成为了云服务商亟需解决的问题[3-4]。

由于云服务器是半可信的，因此数据拥有者必

基金项目：国家自然科学基金（62262060，62362059）；甘肃省教育厅产业支撑计划项目（2022CYZC-17，2023CYZC-09）；甘肃省重点研发计划（23YFGA0081）。

作者简介：刘晨旭，男，硕士研究生，主研方向为网络与信息安全；曹素珍（通信作者），副教授；刘静洁、庞新杰、冯珍，硕士研究生。

收稿日期：2024-04-29 **修回日期：**2024-11-08 **E-mail：**caosuz@nwnu.edu.cn

须对上传的数据进行加密以保证数据的机密性，这又导致用户无法通过云服务器使用传统搜索技术进行搜索[5-6]。当面对社会海量的云上加密数据时，对加密数据的检索也变得越来越困难。加密数据通常是以“一对多”的模式分享给用户，因此需要细粒度访问控制的加密技术[7-8]与高效检索加密数据的搜索技术相结合。传统 CP-ABE 方案中与密文关联的访问策略存储在云服务器，属性满足访问策略的用户才可以检索密文并查看访问策略，然而这可能导致用户获得敏感信息并将其泄露。策略隐藏分为部分策略隐藏和完全策略隐藏，属性被分为属性名和属性值。属性名是不包含敏感信息的明文形式，属性值则不与属性相关联。

为解决加密数据的搜索问题，SONG 等[9]首次提出了可搜索加密(SE)的概念。BONEH 等[10]提出一种支持关键字检索的公钥加密(PEKS)技术，并在基于身份的加密电子邮件系统中得到应用[11]。但上述方案无法实现数据的细粒度访问控制。在云系统中，有两个功能是必不可少的，分别是细粒度访问控制和在密文中检索目标信息。属性基可搜索加密(ABSE)方案[12]不仅具备密文的安全搜索功能，还支持数据的细粒度访问控制。具备细粒度访问控制功能的 ABSE 方案还包括 CP-ABSE(Ciphertext-Policy ABSE)方案[13]。CP-ABSE 中密文包含访问策略，用户私钥关联属性集，只有当用户的属性集满足访问策略时才会成功解密。

在具有撤销机制的属性基加密体制中，被撤销的用户无法正确解密密文。撤销机制分为间接撤销和直接撤销，两者的区别在于撤销时是否更新未撤销用户的解密密钥。文献[14]采用二叉树结构存储秘密份额，用户获得从叶节点到根节点的路径节点上计算得到的解密密钥，从而将密钥更新的计算效率从线性关系减少到对数关系。文献[15]用属性组的方式实现了属性撤销，当恶意用户的属性被撤销时，属性组更新其他用户的密钥。然而，用户可能会故意泄露解密密钥，该恶意用户应立即被撤销。在上述间接撤销方案中仍需要进行密钥和密文更新，因此文献[16-17]提出了直接撤销的 CP-ABE 方案。文献[18]将撤销列表嵌入密文中，不再需要密钥更新，实现了可直接撤销。文献[19]根据用户的解密密钥和与用户信息关联的二叉树叶节点，实现了可追踪和可撤销的 CP-ABE 系统。在可撤销系统中，还需考虑两种安全属性：前向安全和后向安全[20]。前后向安全意味着被撤销用户无法正确解密撤销前后的密文。文献[21]提出 CP-ABE 方案具有密文更新、可追溯和可撤销功能，恶意用户被撤销后将无法访问撤销前后的加密数据，从而实现前后向安全。但方案中用户数量受限于叶节点的数量，无法应用到用户动态变化的环境。在文献[21]所提的方案中，访问策略包含用户隐私信息，可能导致敏感信息泄露。文献[22-23]提出的策略隐藏方案将敏感的属性值隐藏在密文中，属性名和密文一起发送，实现了部分策略隐藏，但这两个方案不具备关键字搜索功能。文献[24]结合智能合约技术提出一个灵活的可搜索属性基加密方案，有较高的密文搜索效率，但没有考虑用户撤销和密文更新问题。

结合上文提到的问题，本文提出一种策略隐藏的可撤销 CP-ABSE 方案，主要工作如下：

1)为提高直接撤销的效率，采用二叉树结构实现用户撤销。二叉树中叶节点的随机值随着用户的撤销而变化，通过节点复用提升系统中用户的数量上限，并且被撤销的用户无法再解密撤销前后的密文，合法用户则不受影响，保证了前后向安全。

2)二叉树的叶节点关联用户，撤销列表取决于二叉树。撤销用户后，被撤销用户无法正确解密密文，并且只需更新与撤销列表相关的密文，没有额外的密钥更新，降低了可信中心和用户间的通信开销。

3)采用线性秘密共享方案表示访问策略，将属性分为属性名和属性值。密文中的访问策略只包含属性名，属性值用于加密与访问策略相关的密文，用户无法得知具体的属性值。通过公开用户属性名、隐藏用户属性值来实现部分策略隐藏。

4)基于 q-BDHE(q-Bilinear Diffie-Hellman Exponent)困难问题，本方案满足选择明文攻击和选择性访问策略下的不可区分性以及关键字不可区分安全性。此外，本文方案可以抵抗共谋攻击。

1 预备知识

1.1 双线性映射

G_1，G_2 是素数 p 阶的循环群，g 是群 G_1 的生成元。双线性映射[25] $e:G_1\times G_1\rightarrow G_2$ 满足下列性质：

1)双线性：$\forall x,y\in G_1$ 和 $\forall a,b\in Z_p^*$，有 $e(x^a,y^b)=e(x,y)^{ab}$ 成立。

2)非退化性：$\exists x,y\in G_1$，使 $e(x,y)\neq 1$。

3)可计算性：对 $\forall x,y\in G_1$，可以计算 $e(x,y)$。

1.2 访问结构

设 $P=\{P_1,P_2,\cdots,P_n\}$是属性集合，则 $A\subseteq 2^P$ 单调。此外，对于 $\forall B,C\subseteq P$，如果 $B\in A$ 且 $B\subseteq C$，则 $C\in A$。若 A 是 $P=\{P_1,P_2,\cdots,P_n\}$的非空子

集，即 $A\subseteq 2^P\backslash\{\varnothing\}$。$A$ 中的集合称为授权集合，否则称为未授权集合。

1.3 线性秘密共享方案

定义 U 作为属性空间，每个属性包含属性名和属性值两部分。线性秘密共享方案通过$(\boldsymbol{M},\rho)$表示访问策略，$\boldsymbol{M}$ 是 $l\times n$ 的矩阵，ρ 为单射函数，将矩阵 $\boldsymbol{M}$ 的每一行映射为一个属性名，对于 $\boldsymbol{M}$ 中的每一行 $i=1,2,\cdots,l$，用 $\rho(i)$表示矩阵 $\boldsymbol{M}$ 中的第 i 行。线性秘密共享方案[26]包含如下特性：

1)令一个列向量 $\boldsymbol{v}=(s,v_2,\cdots,v_n)^{\mathrm{T}}$，$s\in Z_p$ 是共享秘密值，随机选择 $v_2,\cdots,v_n\in Z_p$。$\lambda_i=\boldsymbol{M}_i\times\boldsymbol{v}$ 是与 ρ_i 对应属性名的秘密 s 的份额，$\boldsymbol{M}_i$ 是矩阵 $\boldsymbol{M}$ 的第 i 行。

2)定义 $I=\{i:\rho(i)\in S\}\subseteq\{1,2,\cdots,l\}$，其中 S 表示授权集，存在 $\{\omega_i\in Z_p\}_{i\in I}$ 使 $\sum_{i\in I}\omega_i\boldsymbol{M}_i=(1,0,\cdots,0)$，计算可得 $\sum_{i\in I}\omega_i\lambda_i=s$。

1.4 二叉树

U 代表系统中用户的集合，$|U|$ 表示用户数量，R 为撤销列表。二叉树 UT 表示如下：

1)UT 的所有叶节点与系统中用户 u 相关联。UT 中节点数量为 $2|U|-1$，对每个节点使用广度优先搜索编号，根节点编号为 0，最后一个节点编号为 $2|Y|-2$。

2) path(u_{id})是一条从根节点到用户 u_{id} 的路径。

3)最小覆盖集合 cover(R)[27]是所有不在撤销列表 R 用户的最小节点集。

4)对于$\forall u\in R$，有 cover$(R)\cap$path$(u)=\varnothing$。对于 $u\notin R$，则只有一个节点 $j=$cover$(R)\cap$path(u)。

二叉树示意图如图 1 所示(彩色效果见《计算机工程》官网 HTML 版，下同)。从图 1 的二叉树中可得，撤销列表 $R=\{u_1,u_7,u_8\}$，所以 cover$(R)=\{4,5,8\}$。以非撤销用户 u_5 为例，path$(u_5)=\{0,2,5,11\}$。因此，唯一的相交节点为 $j=$cover$(R)\cap$path$(u_5)=\{5\}$。

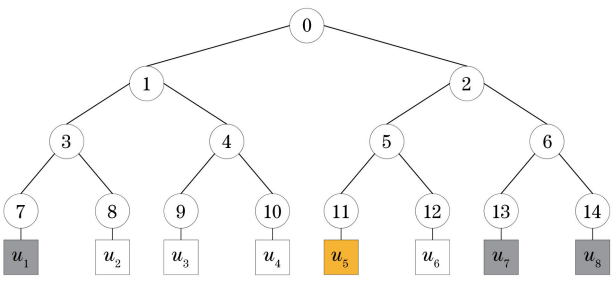

图 1 二叉树示意图

Fig.1 Schematic diagram of binary tree

1.5 困难性问题

1)q-BDHE 困难问题：G_1,G_2 是两个阶为素数 p 的循环群，g 是群 G_1 的生成元。随机选择 $a,b\in Z_p^*$，计算 $\boldsymbol{Y}=(g,g^b,g^a,\cdots,g^{a^q},g^{a^{q+2}},\cdots,g^{a^{2q}})$。如果存在一个多项式时间算法能以可忽略的优势 ε 区分 $e(g,g)^{a^{q+1}b}\in G_2$ 和 G_2 中随机元素 Z，则 q-BDHE 困难问题假设成立。

2)DL 困难问题：群 G_1 是阶为素数 p 的循环乘群。令 g 为群 G_1 的生成元，a 为 Z_p^* 中的一个随机数。给定元素$(g,g^a)\in G_1$，计算 a 是困难的。

2 方案模型

2.1 系统模型

本方案包括 4 类实体，系统模型如图 2 所示。

1)可信中心(TA)：是系统中完全受信任的实体，负责生成系统主密钥、发布公共参数、更新撤销列表，并为非撤销用户更新密钥。

2)云服务提供商(CSP)：是“诚实且好奇”的半可信机构，具备较强的计算和存储能力，负责存储数据拥有者加密的密文，并根据搜索陷门在密文中搜索。当撤销列表更新后，通过 TA 发来的参数相应地更新所存储的密文。

3)数据拥有者(DO)：制定密文的访问策略，并根据访问结构加密明文，将得到的密文上传到 CSP。此外，DO 还要在密文中设置关键字索引来完成密文搜索。

4)数据用户(DU)：从 TA 获得密钥来解密密文。如果用户属性满足访问策略且不在撤销列表中，则可以解密密文。为了完成密文搜索，DU 需要提供搜索关键字并以此生成搜索陷门。

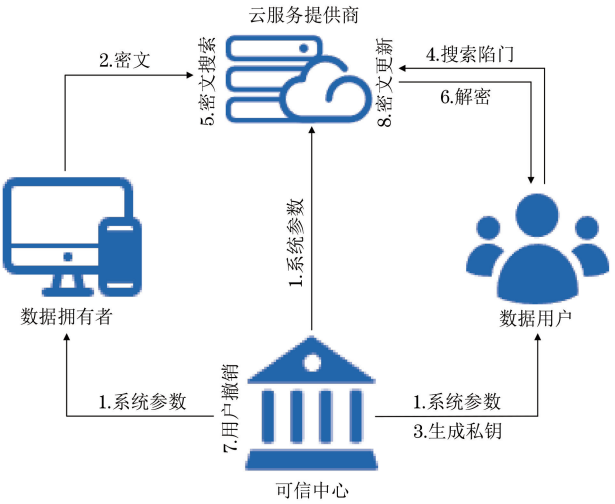

图 2 系统模型

Fig.2 System model

2.2 方案定义

本文方案由下列 8 个算法组成，描述如下：

1）Setup(λ,U,UT)→(K_{PK},K_{MSK})：TA 运行该算法。将安全参数 λ、属性空间 U 和二叉树 UT 作为输入，输出系统公共参数 K_{KP} 和系统主密钥 K_{MSK}。

2）Encryption(K_{PK},m,W,R,kw)→C_{CT}：DO 执行该算法，根据其制定的访问策略 W 加密明文消息 m，并发送带有不完整访问策略 $\overline{W}$ 的密文 C_{CT} 到 CSP，CSP 无法得知特定的属性值。输入为 K_{PK}、明文消息 m、访问策略 W、撤销列表 R 和关键字 kw，输出密文 C_{CT}。

3）KeyGen(K_{PK},K_{MSK},S,u)→K_{SK}：TA 运行该算法。输入 K_{PK}、K_{MSK}、属性集合 $S=(I_s,\zeta)$ 和用户身份 u，输出解密密钥 K_{SK} 并发送给 DU。

4）Trapdoor(K_{PK},K_{SK},skw)→s_{std}：DU 执行该算法，由用户设置的搜索关键字生成搜索陷门。输入为 K_{PK}、K_{SK} 和搜索关键字 skw，输出搜索陷门 s_{std}。

5）Test(C_{CT},s_{std})→1 or ⊥：CSP 执行该算法，用搜索陷门 s_{std} 和密文 C_{CT} 进行匹配。若匹配成功，输出 1，否则，输出⊥。

6）Decryption(K_{SK},C_{CT},UT)→m or ⊥：DU 执行该算法。输入为 K_{SK}、带有不完整访问策略 $\overline{W}$ 的密文 C_{CT} 和 UT。当用户属性满足访问策略且不在撤销列表中，才能解密得到 m，否则输出⊥。

7）Revoke(R,u,UT)→(R',UT′)：TA 运行该算法，把恶意用户加入撤销列表，维护新的撤销列表和二叉树。输入当前撤销列表 R、应被撤销的用户 u 和当前二叉树 UT，输出新的撤销列表 R' 和新的二叉树 UT′。

8）CTUpdate(K_{PK},C_{CT},R')→C'_{CT}：CSP 运行该算法，当恶意用户被撤销时，CSP 更新密文，但是不更改与访问策略相关的密文。输入 K_{PK}、密文 C_{CT} 和新的撤销列表 R'，输出更新后的密文 C'_{CT}。

2.3 安全模型

1）选择明文攻击下的不可区分安全性。

为证明选择明文攻击下的不可区分（IND-CPA）安全性，定义挑战者 C 和攻击者 A 之间的安全游戏。

（1）初始化：A 选择访问策略 $W^*=(\boldsymbol{M}^*,\rho^*,T)$ 和撤销列表 R^*，$\boldsymbol{M}^*$ 是 $l^*\times n^*$ 矩阵，ρ^* 把 $\boldsymbol{M}^*$ 中的行映射为属性名。$T=\{t_{\rho^*(i)}\}_{i\in[1,l^*]}$ 是 $(\boldsymbol{M}^*,\rho^*)$ 关联的属性值。

（2）系统建立：C 运行 Setup 算法，将生成的系统公共参数 K_{PK} 发送给 A。

（3）阶段 1：A 向 C 询问属性集合 $(u_1,S_1),\cdots,(u_n,S_n)$ 对应的解密密钥。如果 u_n 是未撤销用户且 S_n 满足访问策略，则算法终止。如果 u_n 是撤销用户且 S_n 满足访问策略，C 执行 KeyGen 算法生成 $(u_i,S_i)_{i\in[1,n]}$ 的解密密钥发送给 A。

（4）挑战阶段：A 向 C 提交明文 m_0、m_1，C 选择 $m_\eta(\eta\in\{0,1\})$ 并且将要挑战的访问策略 $W^*=(\boldsymbol{M}^*,\rho^*,T)$ 和撤销列表 R^* 作为参数输入，运行 Encryption 算法生成挑战密文 C_{CT_η} 发送给 A。

（5）阶段 2：攻击者 A 重复阶段 1 的询问。

（6）猜测阶段：A 返回猜测 $\eta'\in\{0,1\}$。如果 $\eta=\eta'$，A 赢得该游戏。

攻击者 A 在上述游戏中的优势为 $|\Pr[\eta=\eta']-1/2|$。

定义 1 若多项式时间攻击者 A 在上述游戏中的优势是可忽略的，则本文方案满足 IND-CPA 安全性。

2）选择关键字攻击下的不可区分安全性。

为证明选择模型下关键字不可区分安全性，定义了挑战者 C 和攻击者 A 之间的安全游戏。

（1）系统建立：挑战者 C 运行 Setup 算法，将生成的系统公共参数 K_{PK} 发送给攻击者 A。

（2）阶段 1：A 向 C 询问关键字，并向 C 提交属性集合 S、用户身份 u 和搜索关键字 skw。挑战者 C 运行 KeyGen 算法，输出解密密钥 K_{SK}，运行 Trapdoor 算法，生成搜索陷门 s_{std} 并返回给 A。

（3）挑战阶段：攻击者 A 向挑战者 C 提交等长的关键字 skw_1、skw_2。挑战者 C 随机选择 $skw_\gamma(\gamma\in\{0,1\})$，运行 KeyGen 算法和 Trapdoor 算法，得到搜索陷门 s_{std}。skw_1、skw_2 不能在阶段 1 中被询问。

（4）阶段 2：攻击者 A 重复阶段 1 的关键字询问，但不能询问 skw_1、skw_2。

（5）猜测阶段：攻击者 A 返回猜测 $\gamma'\in\{0,1\}$。如果 $\gamma=\gamma'$，攻击者 A 以 $|\Pr[\gamma=\gamma']-1/2|$ 的优势赢得该游戏。

定义 2 若攻击者 A 在多项式时间内能以可忽略的优势赢得该游戏，则本文方案满足选择关键字攻击下的不可区分安全性。

3 方案构造

为了实现细粒度的访问控制和可搜索功能，根据经典的 CP-ABE 方案[18]和可搜索加密方案[28]，本文提出一种具有前后向安全、可撤销和部分策略隐藏的属性基可搜索加密方案。由于明文形式的访问策略可能导致敏感信息泄露，因此对公开用户属性名、隐藏用户属性值的方式进行部分改进，从而实现部分策略隐藏。二叉树中叶节点的随机值会随着

用户的撤销而变化，通过节点复用提升系统中用户的数量上限。具体算法如下：

1）初始化 Setup(λ,U,UT)→(K_{PK},K_{MSK})。

G_1,G_2 是两个 p 阶循环群，g 是 G_1 的生成元，$e:G_1\times G_1\to G_2$ 是双线性映射。TA 随机选择 α,$\beta\in Z_p^*$,$h\in G_1$。对二叉树 UT 的每个节点，随机选择$\{v_i\}_{i=0}^{2|U|-2}\in Z_p^*$，计算$\{A_i=g^{v_i}\}_{i=0}^{2|U|-2}$，定义哈希函数 $H_0:\{0,1\}^*\to Z_p^*$。最终得到系统公共参数 $K_{\mathrm{PK}}=\langle g,h,e(g,g)^{\alpha},g^{\beta},\{A_i\}_{i=0}^{2|U|-2},H_0\rangle$，系统主密钥 $K_{\mathrm{MSK}}=\langle\alpha,\beta,\{v_i\}_{i=0}^{2|U|-2}\rangle$。

2）加密 Encryption(K_{PK},m,W,R,kw)→C_{CT}。

（1）随机选择一个向量 $\vec{\boldsymbol{v}}=(s,y_2,\cdots,y_n)^{\mathrm{T}}$，秘密值 $s\in Z_p^*$,$y_2,\cdots,y_n\in Z_p$。对 $i=1,2,\cdots,l$ 计算 $\lambda_i=\boldsymbol{M}_i\cdot\vec{\boldsymbol{v}}$。

（2）随机选择 $a\in Z_p^*$，计算以下密文：

$$C=m\cdot e(g,g)^{\alpha s}$$

$$C_0=g^{s/\beta}$$

$$\{C_i=g^{\lambda_i}h^{a},C_i'=g^{\lambda_i}g^{a\cdot t_{\rho(i)}},C_i''=g^{a}\}_{i\in[1,l]}\tag{1}$$

（3）令 cover(R)是关于撤销列表 R 的最小覆盖集，对每个 $j\in\mathrm{cover}(R)$，计算与撤销列表 R 相关的密文$\{Y_j=A_j^{s}\}_{j\in\mathrm{cover}(R)}$。最后计算关键字索引 $I_{\mathrm{Ind_{kw}}}=g^{s\cdot H_0(\mathrm{kw})}$。

算法最终得到密文 $C_{\mathrm{CT}}=\langle C,C_0,\{C_i,C_i',C_i''\}_{i\in[1,l]},\{Y_j\}_{j\in\mathrm{cover}(R)},R,\overline{W},I_{\mathrm{Ind_{kw}}}\rangle$，其中访问策略 $W=(\boldsymbol{M},\rho,T)$，$T=\{t_{\rho(i)}\}_{i\in[1,l]}$ 是关联$(\boldsymbol{M},\rho)$的属性值，$\overline{W}=(\boldsymbol{M},\rho)$是不包括属性值集的访问策略。

3）密钥生成 KeyGen(K_{PK},K_{MSK},S,u)→K_{SK}。

（1）属性集合 $S=(I_s,\zeta)$，其中 I_s 是用户属性名集合，$\zeta=\{s_i:i\in I_s\}$是用户属性值集合。随机选取 $r\in Z_p^*$，$\forall c\in I_s$，计算与用户属性相关的密钥 $\langle K=g^{\alpha\beta+r},L=g^{r},L_0=g^{r/\beta},\{K_c=g^{-r\cdot s_c/\beta}h^{-r}\}_{c\in I_s}\rangle$。

$$F_1=\prod_{i\in I}(e(L,C_i)e(L_0,C_i')e(K_{\rho(i)},C_i''))^{\omega_i}=$$

$$\prod_{i\in I}(e(g^{r},g^{\lambda_i}h^{a})e(g^{r/\beta},g^{\lambda_i}g^{a\cdot t_{\rho(i)}})e(g^{-r\cdot s_{\rho(i)}/\beta}h^{-r},g^{a}))^{\omega_i}=e(g,g)^{rs}e(g,g)^{rs/\beta}$$

$$F_2=e(K,C_0)=e(g^{\alpha\beta+r},g^{s/\beta})=e(g,g)^{\alpha s}e(g,g)^{rs/\beta}$$

$$F_3=\frac{F_2\cdot E}{F_1}=\frac{e(g,g)^{\alpha s}e(g,g)^{rs/\beta}e(g,g)^{rs}}{e(g,g)^{rs}e(g,g)^{rs/\beta}}=e(g,g)^{\alpha s}$$

$$\frac{C}{F_3}=\frac{m\cdot e(g,g)^{\alpha s}}{e(g,g)^{\alpha s}}=m\tag{2}$$

7）撤销 Revoke(R,u,K_{MSK},UT)→(R',UT')。

TA 运行该算法，输入撤销列表 R、被撤销用户 u、K_{MSK} 和二叉树 UT。随机选择 $v\in Z_p^*$，计算 $A=g^{v}$，将 K_{MSK} 中的 v_u 变为 v、二叉树 UT 中的 A_u 变为 A。TA 将用户 u 添加到撤销列表，输出新的撤销列表 $R'=R\cup u$ 和新的二叉树 UT'。

8）密文更新 CTUpdate(K_{PK},C_{CT},R')→C'_{CT}。

CSP 运行该算法，输入 K_{PK}、C_{CT} 和 R'。当 TA 撤销用户后，随机选择 μ 并计算 $Q=\{\mu\cdot v_i\}_{i=0}^{2|U|-2}$，然后通过秘密信道发送给 CSP，CSP 输出新的密文

（2）设 path(u)=$\{\mathrm{root},\cdots,u_{\mathrm{id}}\}$表示二叉树中从根节点到与用户 u 相关联的叶节点的路径，计算与撤销列表相关的密钥 $D_i=\{g^{r/v_{u_{\mathrm{id}}}}\}_{i\in\mathrm{path}(u)}$。

最终，以上两部分密钥组成完整密钥 $K_{\mathrm{SK}}=\langle K,L,L_0,\{K_c\}_{c\in I_s},\{D_i\}_{i\in\mathrm{path}(u)}\rangle$。

4）陷门构造 Trapdoor(K_{PK},K_{SK},skw)→s_{std}。

DU 运行该算法，输入 K_{PK}、K_{SK} 和搜索关键字 skw，输出搜索陷门 s_{std}。随机选取 $l\in Z_p^*$，$\tau\in Z_p^*$，计算 $td'=g^{l\cdot H_0(\mathrm{skw})/\tau}$，$td'_i=\{g^{l\cdot v_i/\tau}\}_{i\in\mathrm{path}(u)}$，得到搜索陷门 $s_{\mathrm{std}}=\langle td',\{td'_i\}_{i\in\mathrm{path}(u)}\rangle$。

5）陷门验证 Test(C_{CT},s_{std})→1 or ⊥。

CSP 运行该算法，输入 C_{CT} 和搜索陷门 s_{std}，若 $e(td',Y_j)=e(td'_i,I_{\mathrm{Ind_{kw}}})$，则算法输出 1，否则视为搜索失败，输出⊥。只有匹配成功，云服务器才会将 C_{CT} 发送到 DU 解密，如果用户在撤销列表 R 中，则无法搜索成功。

6）解密 Decryption(S_{SK},C_{CT},UT)→m or ⊥。

DU 运行该算法，输入 S_{SK}、C_{CT} 和 UT，算法存在以下 2 种情况：

（1）如果用户属性集 $S\notin(\boldsymbol{M},\rho)$或用户 $u\in R$，算法终止。

（2）如果 $S\in(\boldsymbol{M},\rho)$且 $u\notin R$，算法执行如下。

对于 $u\in R$，二叉树中有且仅有一个节点 $j\in\mathrm{cover}(R)\cap\mathrm{path}(u)$。令 path($u$)=$\{\mathrm{root},\cdots,u_{\mathrm{temp}(j)},\cdots,u_{\mathrm{id}}\}$，其中 $u_{\mathrm{temp}(j)}=j$，u_{id} 是二叉树中与用户 u 相关的叶节点的值，计算 $\theta=v_{u_{\mathrm{id}}}/v_j$ 以及 $E=e(D_i,Y_j)^{\theta}=e(g^{r/v_{u_{\mathrm{id}}}},g^{v_j s})^{\theta}=e(g,g)^{rs}$。

对于 $S\in(\boldsymbol{M},\rho)$，令 $I=\{i:\rho(i)\in S\}\subseteq[1,\cdots,l]$，存在$\{\omega_i\mid i\in I\}$满足 $\sum_{i\in I}\omega_i M_i=(1,0,\cdots,0)$，因此得到 $\sum_{i\in I}\omega_i\lambda_i=s$。Decryption 算法计算式如下：

C'_{CT}。令 cover(R')表示与新的撤销列表 R' 相关的最小覆盖集。对于 $j'\in$cover(R')存在以下情况。

(1)如果 $j\in$cover(R),使得 $j=j'$,则令 $Y_{j'}=Y_j$。

(2)如果 $j\in$cover(R)使 j 是 j' 的祖先节点,则 path(j')=path(j)$\cup\{i_{\text{temp}(j)+1},\cdots,i_{\text{temp}(j')}\}$,其中 $i_{\text{temp}(j)}=j$,$i_{\text{temp}(j')}=j'$。令 $X_j=Y_j$,并计算 $X_{i_{k+1}}=(X_{i_k})^{v'_{i_{k+1}}/v'_{i_k}}=y^{s}_{i_{k+1}}$,其中 $k=\text{temp}(j),\cdots,\text{temp}(j')$,则 $Y_{j'}=X_{j'}$。与访问策略相关的密文不变,最终更新得到的密文为 $C'_{CT}=\langle C,C_0,\{C_i,C'_i,C''_i\}_{i\in[1,l]},\{Y_{j'}\}_{j'\in\text{cover}(R')},R',\overline{W},I_{\text{Ind}_{kw}}\rangle$

4 安全性证明

4.1 选择明文的不可区分安全性

定理 1 若 q-BDHE 假设成立,则在选择性访问策略和选择明文攻击下,多项式时间攻击者攻破本方案的优势是可忽略的。

证明 如果存在一个多项式时间攻击者 A 能以优势 ε 攻破此方案,那么挑战者 C 就能以 $\varepsilon/2$ 的优势解决 q-BDHE。C 执行算法如下。

G_1,G_2 是素数 p 阶的循环群,g 是 G_1 的生成元。双线性映射 $e:G_1\times G_1\rightarrow G_2$。$C$ 选择 $\mu\in\{0,1\}$。令 $\vec{Y}=(g,g^s,g^{\alpha},\cdots,g^{\alpha^q},g^{\alpha^{q+2}},\cdots,g^{\alpha^{2q}})$。若 $\mu=1$,C 计算 $Z=e(g,g)^{\alpha^{q+1}s}$;否则 C 随机选择 $Z\in G_2$。

1)初始化:A 选择访问策略 $W^*=(\boldsymbol{M}^*,\rho^*,T)$ 和撤销列表 R^*,$\boldsymbol{M}^*$ 是 $l^*\times n^*$ 的矩阵且 $n^*\leqslant q$,ρ^* 映射矩阵 $\boldsymbol{M}$ 的每一行为一个属性名。$T=\{t_{\rho^*(i)}\}_{i\in[1,l^*]}$ 是关联($\boldsymbol{M}^*,\rho^*$)的属性值。

2)系统建立:挑战者 C 随机选择 $\alpha',\beta\in Z_p$,令 $e(g,g)^{\alpha}=e(g,g)^{\alpha'}e(g^d,g^{d^q})$,其中 $\alpha=\alpha'+d^{q+1}$。计算 g^{β},令 $h=g^d$。对撤销列表 R^*,存在 $I_{R^*}=\{i\in\text{path}(u)\mid u\in R^*\}_{i=0}^{2|U|-2}$。随机选择 $b_i\in Z_p^*$,如果 $i\in I_{R^*}$,令 $A_i=g^{b_i}g^{d^i}$,则 $v_i=b_i+d^i$;否则,令 $A_i=g^{b_i}g^{d^q}$,$v_i=b_i+d^q$。输出系统公共参数 $K_{\text{PK}}=\langle g,h,e(g,g)^{\alpha},g^{\beta},\{A_i\}_{i=0}^{2|U|-2},H_0\rangle$。

3)阶段 1:攻击者 A 请求用户属性集合(u,S)相关的解密密钥,其中 $S=(I_s,\zeta)$。

(1)如果 $S\in(\boldsymbol{M}^*,\rho^*)$ 且 $u\notin R^*$,算法终止。

(2)如果 $S\in(\boldsymbol{M}^*,\rho^*)$ 且 $u\in R^*$,令 $r=-d^{q+1}\beta+d^{q+1}\beta\cdot\frac{M^*_{i,1}}{M^*_{i,2}}$,计算 $K=g^{\alpha'\beta}(g^{d^{q+1}\beta})^{\frac{M^*_{i,1}}{M^*_{i,2}}}=g^{\alpha\beta+r}$,$L=(g^{d^{q+1}\beta})^{-1}(g^{d^{q+1}\beta})^{\frac{M^*_{i,1}}{M^*_{i,2}}}=g^r$,$L_0=(L)^{\frac{1}{\beta}}=g^{\frac{r}{\beta}}$,$K_c=\left(\prod_{k=1}^{n^*}g^{d^{q+k+1}\cdot M^*_{i,k}}\right)\cdot\left[\left(\prod_{k=1}^{n^*}g^{d^{q+k+1}\cdot M^*_{i,k}}\right)^{\frac{M^*_{i,1}}{M^*_{i,2}}}\right]^{-1}\cdot[(g^{d^{q+2}\cdot\beta})^{\frac{M^*_{i,1}}{M^*_{i,2}}}]^{-1}\cdot(g^{d^{q+2}})^{\beta}=g^{-r\cdot\frac{s_c}{\beta}}h^{-r}$。

假设 path(u)=$\{\text{root},\cdots,u_{\text{id}}\}$,root 表示根节点,$u_{\text{id}}$ 表示与用户 u 相关联的叶节点。因为 $u\in R^*$,所以 $u_k\in I_{R^*}$,$v_{u_k}=b_{u_k}+d^{u_k}$,$k\in\{0,\cdots,\text{id}\}$。挑战者 C 计算 $D_i=[(g^{d^{q+1}})^{-1}\cdot(g^{d^{q+1}})^{\frac{M^*_{i,1}}{M^*_{i,2}}}]^{\frac{\beta}{b_{u_k}+d^{u_k}}}$。

4)挑战阶段:攻击者 A 向挑战者 C 提交明文 m_0、m_1。

挑战者 C 掷币选择 $\eta\in\{0,1\}$ 并计算 $C=m_{\eta}\cdot e(g,g)^{\alpha s}$,$C_0=g^{s/\beta}$。挑战者 C 随机选择 $r'_2,\cdots,r'_n\in Z_p^*$,令 $\vec{\boldsymbol{v}}=(s,sd+r'_2,sd^2+r'_3,\cdots,sd^{n^*-1}+r'_n)\in Z_p^*$,并计算:

$$\begin{cases}C_i=\prod_{j=2}^{n^*}g^{M^*_{i,j}r'_j}\cdot g^{-\beta d^{i+1}}\\ C'_i=\prod_{j=2}^{n^*}g^{M^*_{i,j}r'_j}\cdot(g^{t_{\rho(i)}})^{-\beta d^i}\\ C''_i=g^{-\beta d^i}\end{cases}\tag{3}$$

对 $\forall j\in$cover(R^*),令 path(j)=$\{\text{root},\cdots,u_{\text{temp}(j)}\}$,其中 root 表示根节点,$u_{\text{temp}(j)}=j$。因为 $j\in$cover(R^*),所以 $v_j=b_j+d^q$,$A_j=g^{b_j+d^q}$,最终得到 $Y_j=(g^s)^{v_j}=A_j^s$。

挑战者 C 将密文 $C_{CT}=\langle C,C_0,\{C_i,C'_i,C''_i\}_{i\in[1,l]},\{Y_j\}_{j\in\text{cover}(R)},R,\overline{W},I_{\text{Ind}_{kw}}\rangle$ 发送给 A。

5)阶段 2:攻击者 A 重复阶段 1 的询问。

6)猜测阶段:A 输出 η 的猜想 η'。如果 $\eta'=\eta$,C 输出 $\mu'=1$,表示 $Z=e(g,g)^{\alpha^{q+1}s}$。否则,输出 $\mu'=0$,则 Z 是 G_2 中随机元素。

如上所示,对系统公共参数和私钥的模拟与本文方案完全相同。

如果 $\mu=0$,攻击者 A 无法获得关于 η 的信息。因此,$\Pr[\eta\neq\eta'\mid\mu=0]=\frac{1}{2}$。当 $\eta\neq\eta'$ 时,挑战者 C 选择 $\mu'=0$,则 $\Pr[\mu=\mu'\mid\mu=0]=\frac{1}{2}$。

如果 $\mu=1$,攻击者获得 m_{η} 的密文。假设攻击者 A 的优势为 ε,因此 $\varepsilon=\Pr[\eta=\eta'\mid\mu=1]-\frac{1}{2}$。当 $\eta=\eta'$ 时,挑战者 C 选择 $\mu'=1$,且 $\Pr[\eta=\eta'\mid\mu=$

$1]=\Pr[\mu=\mu'|\mu=1]=\varepsilon+\frac{1}{2}$。

挑战者 C 解决 q-BDHE 困难问题的优势为：

$$\Pr[\mu=\mu']=\Pr[\mu=\mu'|\mu=1]\cdot\Pr[\mu=1]+\Pr[\mu=\mu'|\mu=0]\cdot\Pr[\mu=0]-\frac{1}{2}=\left(\varepsilon+\frac{1}{2}\right)\cdot\frac{1}{2}+\frac{1}{2}\cdot\frac{1}{2}-\frac{1}{2}=\frac{1}{2}\varepsilon$$

4.2 关键字的不可区分安全性

定理 2 若 DL 困难问题成立，则方案在选择关键字攻击下满足不可区分安全性。

证明 如果存在一个概率多项式时间，攻击者 A 能以不可忽略的优势 ε 攻破此方案，那么可以构造一个多项式时间算法以优势 ε 解决 DL 困难问题。

1）系统建立：挑战者 C 运行 Setup 算法，随机选择 $\alpha,\beta\in Z_p^*$，$h\in G_1$。对二叉树 UT 的每个节点，随机选择 $\{v_i\}_{i=0}^{2|U|-2}\in Z_p^*$，计算 $\{A_i=g^{v_i}\}_{i=0}^{2|U|-2}$，定义哈希函数 $H_0:\{0,1\}^*\rightarrow Z_p^*$。输出系统公共参数 $K_{\mathrm{PK}}=\langle g,h,e(g,g)^{\alpha},g^{\beta},\{A_i\}_{i=0}^{2|U|-2},H_0\rangle$ 和系统主密钥 $K_{\mathrm{MSK}}=\langle\alpha,\beta,\{v_i\}_{i=0}^{2|U|-2}\rangle$。挑战者 C 保存系统主密钥 K_{MSK}，并将系统公共参数 K_{PK} 发给攻击者 A。

2）阶段 1：攻击者 A 向挑战者 C 提交属性集合 S、用户身份 u 和搜索关键字 skw。C 运行 KeyGen 算法。随机选取 $r\in Z_p^*$，$\forall c\in I_s$，计算 $\langle K=g^{\alpha\beta+r}$，$L=g^r$，$L_0=g^{r/\beta}$，$\{K_c=g^{-r\cdot s_c/\beta}h^{-r}\}_{c\in I_s}\rangle$。$C$ 计算用户 u 的相关密钥 $D_i=\{g^{r/v_{u_{\mathrm{id}}}}\}_{i\in\mathrm{path}(u)}$。输出解密密钥 $K_{\mathrm{SK}}=\langle K,L,L_0,\{K_c\}_{c\in I_s},\{D_i\}_{i\in\mathrm{path}(u)}\rangle$。随后 C 随机选取 $l\in Z_p^*$，$\tau\in Z_p^*$，计算 $td'=g^{l\cdot H_0(\mathrm{skw})/\tau}$，$td'_i=\{g^{l\cdot v_i/\tau}\}_{i\in\mathrm{path}(u)}$，输出得到搜索陷门 $s_{\mathrm{std}}=\langle td',\{td'_i\}_{i\in\mathrm{path}(u)}\rangle$。$C$ 将搜索陷门发送给 A。

3）挑战阶段：A 向 C 提交等长关键字 skw_1、skw_2。C 随机选择 $\mathrm{skw}_\gamma(\gamma\in\{0,1\})$，运行 KeyGen 算法和 Trapdoor 算法，生成搜索陷门 $s_{\mathrm{std}_\gamma}=\langle g^{l\cdot H_0(\mathrm{skw}_\gamma)/\tau},\{g^{l\cdot v_i/\tau}\}_{i\in\mathrm{path}(u)}\rangle$。$\mathrm{skw}_1$、$\mathrm{skw}_2$ 不能在阶段 1 中被询问。

4）询问阶段 2：A 重复阶段 1 的询问，但不能询问 skw_1、skw_2。

5）猜测阶段：A 输出一个猜测结果 $\gamma'\in\{0,1\}$。若 $\gamma=\gamma'$，则攻击者 A 赢得该游戏。在随机预言机模型下，关键字陷门的构造是基于 DL 困难问题完成的，由于解决离散对数问题是困难的，因此攻击者 A 无法以不可忽略的优势赢得该游戏。

4.3 抗共谋攻击

本方案中密钥 K_{SK} 被分为与用户属性相关和撤销列表相关的密钥 K_{SK}。对于抗共谋攻击，需要讨论撤销用户和非撤销用户间的共谋以及非撤销用户间的共谋两种情况。

当撤销用户和非撤销用户发生共谋时，通常会出现撤销用户满足解密所需的属性但没有解密资格，而非撤销用户不满足解密的属性但有解密资格的情况。因此，通常由撤销用户提供与用户属性相关的密钥，非撤销用户提供与撤销列表相关的密钥。而本方案中与用户属性相关的密钥为 $\langle K=g^{\alpha\beta+r}$，$L=g^r$，$L_0=g^{r/\beta}$，$\{K_c=g^{-r\cdot s_c/\beta}h^{-r}\}_{c\in I_s}\rangle$，与撤销列表相关的密钥为 $D_i=\{g^{r/v_{u_{\mathrm{id}}}}\}_{i\in\mathrm{path}(u)}$。$\alpha$、$\beta$、$r$ 是随机值，$c\in S$，$v_{u_{\mathrm{id}}}$ 关联用户身份。因为两部分密钥中都含有 r，所以为了使随机值保持一致，这两部分应当由一个用户生成。而且与用户属性相关的密钥 K_c 中的 s_c 代表用户身份，与撤销列表相关的密钥 D_i 中 $v_{u_{\mathrm{id}}}$ 也与用户身份相关。生成这两部分密钥时如果用户身份不同，会导致后续无法正确解密。

当非撤销用户发生共谋时，通常双方都不具备正确解密所需的属性权限。因此，非撤销用户的共谋是两方非撤销用户尝试合并各自的密钥来共同解密。本方案中与用户属性相关的密钥为 $\{K_c=g^{-r\cdot s_c/\beta}h^{-r}\}_{c\in I_s}$，$L_0=g^{r/\beta}$，其中，$s_c$ 与用户属性有关，β、r 都是随机值。即便属性相同的用户在密钥生成时也会生成完全不同的密钥，使得非撤销用户之间无法合并各自的密钥来解密。因此，本方案可以抵抗非撤销用户之间的共谋攻击。

4.4 前后向安全

因为在解密算法中二叉树有且仅有一个节点 $j\in\mathrm{cover}(R)\cap\mathrm{path}(u)$，数据使用者在得到 v_j 后才能计算 $\theta=v_{u_{\mathrm{id}}}/v_j$ 和 $E=e(D_i,Y_j)^{\theta}$，所以在该节点上与用户相关的随机值保证了前后向安全。当系统中恶意用户被撤销后，CSP 根据与新旧撤销列表相关的最小覆盖集合，更新与撤销列表相关的密文 $\{Y_j\}_{j\in\mathrm{cover}(R)}$。因此，即便被撤销用户存储了先前的部分解密结果，也无法正确计算 $E=e(D_i,Y_j)^{\theta}$，从而保证了本方案的前向安全性。TA 运行撤销算法时会随机选择 $\{v_i\}_{i=0}^{2|U|-2}\in Z_p^*$ 来替换 K_{MSK} 和 UT 中与被撤销用户相关的值，并输出新的撤销列表。对于在撤销列表中的用户，其无法找到额外满足 $\mathrm{cover}(R)\cap\mathrm{path}(u)$ 的节点，所持有的解密密钥也不再满足后续密文的访问控制策略，保证了后向安全性。

5 性能分析

表 1 将本文方案和文献[6,7,19,21]所提方案的计算开销进行对比。令 s 代表用户属性数量，l 代表访问策略中属性数量，r 代表 cover(R)的节点数量，n 代表密钥中属性数量，u 代表用户数量最大值，m 代表每条记录中关键字字段的数量，d 代表二叉树的深度，h 代表哈希运算，G 代表 G_1 和 G_2 上的指数运算，E 代表双线性配对运算。与乘法运算相比，指数运算和双线性配对运算的计算开销更大。因此，在计算开销分析中忽略乘法运算的时间开销。

在密钥生成阶段，本方案的计算开销为$(5+s)G$，优于文献[7]所提方案，略微优于文献[6,19,21]所提方案。但是随着用户属性的增加，文献[7,19]所提方案的计算开销会显著增加。在加密算法部分，本方案相比于其他方案都有明显的优势。在搜索验证阶段本方案仅需要两次双线性配对运算即可完成密文搜索，文献[6]所提方案的计算开销与搜索与访问策略中的属性个数有关，导致计算开销增大。而文献[7,19,21]所提方案不具备密文搜索功能。在解密阶段，本方案比文献[7]所提方案的计算开销有显著提升，与文献[19,21]所提方案的计算开销基本一致。文献[6]所提方案的解密算法开销略微优于本方案，但本方案提供了文献[6]所提方案不具备的用户撤销和密文更新功能，且在密钥生成、加密和搜索验证阶段的开销均优于文献[6]所提方案。在密文更新阶段，本方案和文献[19]所提方案的计算开销相同。与其他方案相比，本方案的计算开销会随着撤销用户在二叉树中的位置变化而变化。当处于理想情况时，计算开销为 0；最差情况时的计算开销为$((1+\text{lb}\ u)\cdot\text{lb}\ u)/2$。因此，本方案在密文更新时无需更新全部密文。而文献[7,21]所提方案需要更新全部密文，且计算开销中的指数运算基于访问策略中的属性个数，导致计算开销增加。

表 1 不同方案的计算开销比较

Table 1 Calculation costs comparison among different schemes

方案	KeyGen	Encryption	Test	Decryption	CTUpdate
文献[6]	$(7+s)G+h$	$(2l+6+m)G+2h$	$(2l+1)E+G$	$3E+2nG+h$	—
文献[7]	$(2+3s)G+2h$	$(5l+6)G+h$	—	$4nE+4nG+h$	$(5l+7)G$
文献[19]	$(4+2s)G$	$(4l+3+r)G$	—	$(2+3n)E+(4+2n)G$	0 or $((1+\text{lb}\ u)\cdot\text{lb}\ u)/2$
文献[21]	$(4+s+d)G$	$(3l+4+r)G$	—	$(2+2n)E+(2+3n)G$	$(3l+5+r)G$
本文方案	$(5+s)G$	$(2l+4+r)G+h$	$2E$	$(2+3n)E+(1+2n)G$	0 or $((1+\text{lb}\ u)\cdot\text{lb}\ u)/2$

本文的仿真实验使用 JPBC2.0.0 库，使用的软件环境为 JDK1.8.0 和 IntelliJ IDEA 2022.1.3，硬件环境为 Intel® Core™ i5-12500H @2.50 GHz。所有实验使用了 Type A 的素数阶双线性配对，在曲线 $y^2=x^3+x$ 上构造。本方案设置用户的属性数量和访问策略中的属性数量为 10～50。用户集合为 $U=\{u_1,u_2,u_3,u_4,u_5,u_6,u_7,u_8\}$，撤销列表 $R=\{u_1,u_7,u_8\}$，cover(R)$=\{4,5,8\}$。最终统计结果是 50 次实验的平均值。

不同方案在密钥生成阶段的时间如图 3 所示，本方案和文献[6,7,19,21]所提方案在密钥生成阶段的时间开销与用户属性数量呈线性关系，随着数据使用者的属性数量增加而增加。而本文方案只有 1 个指数运算随用户属性数量线性增长。因此，本文方案的计算开销显著优于文献[7,19]所提的方案，相比文献[6,21]所提方案的时间少了 5～10 ms。

图 4 所示为本方案和文献[6,7,19,21]所提方案在加密阶段的计算开销随着访问策略中的属性数

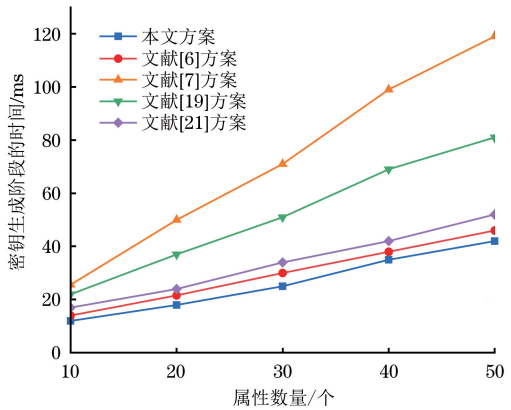

图 3 不同方案在密钥生成阶段的时间

Fig.3 Time among different schemes during the key generation phase

量增加。本方案和文献[19,21]所提方案的加密算法计算开销还与 cover(R)的节点数量相关，但文献[19,21]所提方案中加密用到了更多的访问策略数量，计算开销更高。文献[6]所提方案中访问策略的属性数量和本方案一致，但还需加密每条记录中关键字字段的数量，开销略高于本方案。

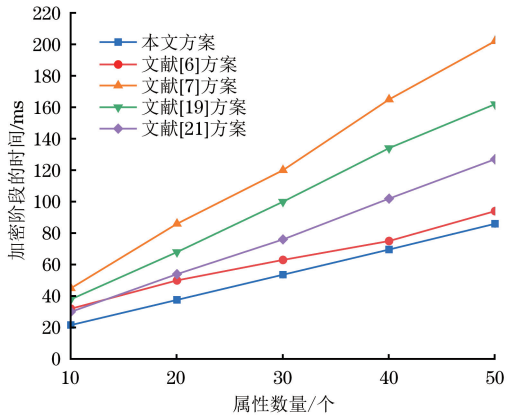

图 4 不同方案在加密阶段的时间

Fig. 4 Time among different schemes during the encryption phase

不同方案在搜索验证阶段的时间如图 5 所示。文献[7,19,21]所提方案不包含搜索验证阶段,因此在图 5 中只对比了本方案和文献[6]所提方案的效率。本方案的搜索验证与属性数量无关,计算开销大约保持在常数级水平,但文献[6]所提方案支持多关键字搜索,在搜索功能上较本方案更灵活。

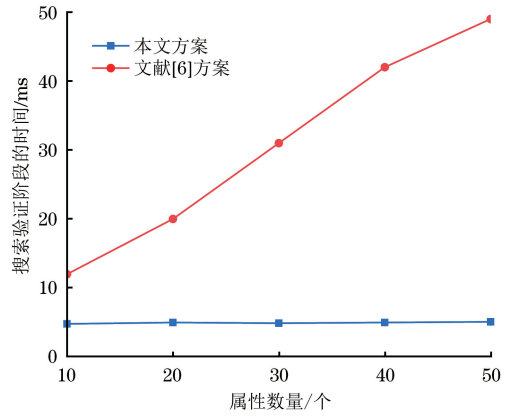

图 5 不同方案在搜索验证阶段的时间

Fig. 5 Time among different schemes during the search verification phase

不同方案在解密阶段的时间如图 6 所示。从图 6 可以看出,本方案在解密阶段的效率要优于文献[7]所提方案,与文献[19,21]所提方案的效率接近,但随着属性数量的增长,本方案的性能又优于这两个方案。由于文献[6]所提方案在做双线性配对运算时与密钥中属性数量无关,因此计算开销要低于本方案,但本方案在其他算法阶段的计算开销均优于文献[6]所提方案,且支持撤销恶意用户、密文更新和抗共谋攻击,在功能上更丰富。

不同方案在密文更新阶段的时间如图 7 所示。从图 7 可以看出,本方案和文献[19]所提方案的计算开销基本一致,明显优于文献[7,21]所提方案的

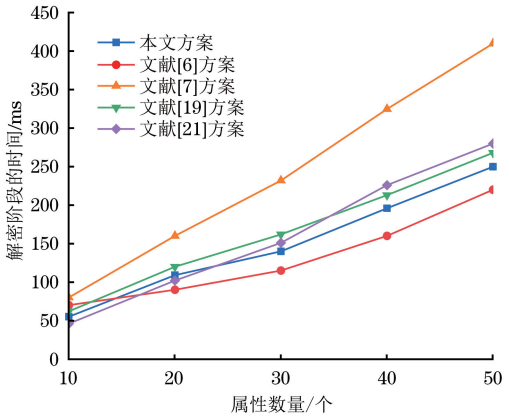

图 6 不同方案在解密阶段的时间

Fig. 6 Time among different schemes during decryption phase

计算时间开销。综上,本方案的仿真结果和计算开销分析基本保持一致。

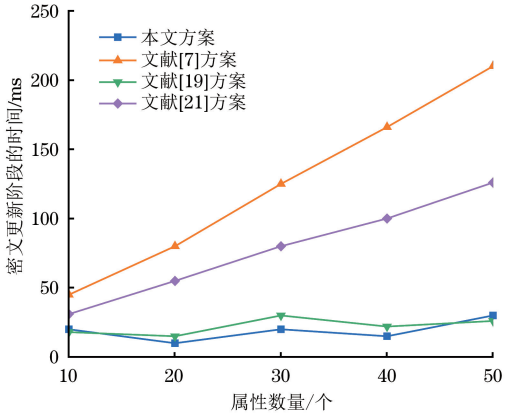

图 7 不同方案在密文更新阶段的时间

Fig. 7 Time among different schemes during the ciphertext update phase

6 结束语

本文提出策略隐藏的可撤销属性基可搜索加密方案,使用线性秘密共享方案作为访问策略,属性值用于加密,属性名则包含在密文中来实现部分策略隐藏。为提高撤销效率,采用二叉树结构来实现用户撤销,节点的可复用性又进一步提高了系统中的用户数量上限。此外,所提方案使用高效的密文搜索算法,在保持较高的搜索效率时防止已撤销用户搜索密文。本方案在随机预言模型下满足 IND-CPA 安全性。性能分析表明,本方案比同类方案在功能和计算效率上具有一定优势。下一步将在功能上实现完全策略隐藏和多关键字搜索,同时进一步提高方案的解密效率,将其运用于工业物联网场景中,增强方案的实用性。

参考文献

[1] SAI S, CHAMOLA V, CHOO K-K R, et al. Confluence of

blockchain and artificial intelligence technologies for secure and scalable healthcare solutions: a review[J]. IEEE Internet of Things Journal, 2022, 10(7): 5873-5897.
[2] WANG H Y, LIANG J L, DING Y, et al. Ciphertext-policy attribute-based encryption supporting policy-hiding and cloud auditing in smart health [J]. Computer Standards & Interfaces, 2023, 84: 103696.
[3] ZHANG G, DING Z, XU J, et al. Reasoning and tracing of information security events in the expressway networking system based on deep learning[J]. International Journal of Intelligent Systems, 2022, 37(11): 8988-9012.
[4] 蒋淇淇, 张亮, 彭凌祺, 等. 基于区块链的可问责可验证外包分层属性加密方案[J]. 计算机工程, 2025, 51(3): 24-33.
JIANG Q Q, ZHANG L, PENG L Q, et al. Accountable and verifiable outsourced hierarchical attribute encryption scheme based on blockchain [J]. Computer Engineering, 2025, 51(3): 24-33. (in Chinese)
[5] GOPALA M, SRIRAM G. Edge computing vs. cloud computing: an overview of big data challenges and opportunities for large enterprises[J]. International Research Journal of Modernization in Engineering Technology and Science, 2022, 4(1): 1331-1337.
[6] ZHANG Y H, ZHU T, GUO R, et al. Multi-keyword searchable and verifiable attribute-based encryption over cloud data [J]. IEEE Transactions on Cloud Computing, 2021, 11(1): 971-983.
[7] SETHI K, PRADHAN A, BERA P. PMTER-ABE: a practical multi-authority CP-ABE with traceability, revocation and outsourcing decryption for secure access control in cloud systems[J]. Cluster Computing, 2021, 24: 1525-1550.
[8] LI H, YU K P, LIU B, et al. An efficient ciphertext-policy weighted attribute-based encryption for the Internet of health things [J]. IEEE Journal of Biomedical and Health Informatics, 2021, 26(5): 1949-1960.
[9] SONG D X, WAGNER D, PERRIG A. Practical techniques for searches on encrypted data [C]// Proceeding of IEEE Symposium on Security and Privacy. Washington D. C., USA: IEEE Press, 2000: 44-55.
[10] BONEH D, DI CRESCENZO G, OSTROVSKY R, et al. Public key encryption with keyword search[C]// Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Germany: Springer, 2004: 506-522.
[11] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing [EB/OL]. [2024-03-21]. https://link.springer.com/content/pdf/10.1007/3-540-44647-8_13.pdf?pdf=core.
[12] YU Y, SHI J B, LI H L, et al. Key-policy attribute-based encryption with keyword search in virtualized environments [J]. IEEE Journal on Selected Areas in Communications, 2020, 38(6): 1242-1251.
[13] YIN H, ZHANG J X, XIONG Y Q, et al. CP-ABSE: a ciphertext-policy attribute-based searchable encryption scheme[J]. IEEE Access, 2019, 7: 5682-5694.
[14] BOLDYREVA A, GOYAL V, KUMAR V. Identity-based encryption with efficient revocation [C]//Proceedings of the 15th ACM Conference on Computer and communications Security. New York, USA: ACM Press, 2008: 417-426.
[15] LI J G, YAO W, HAN J G, et al. User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage [J]. IEEE Systems Journal, 2017, 12(2): 1767-1777.
[16] LIAN H J, WANG Q X, WANG G B. Large universe ciphertext-policy attribute-based encryption with attribute level user revocation in cloud storage[J]. The International Arab Journal Information Technology, 2020, 17(1): 107-117.
[17] BOUCHAALA M, GHAZEL C, SAIDANE L A. Trak-CPABE: a novel traceable, revocable and accountable ciphertext-policy attribute-based encryption scheme in cloud computing [J]. Journal of Information Security and Applications, 2021, 61: 102914.
[18] LIU Z H, DUAN S H, ZHOU P L, et al. Traceable-then-revocable ciphertext-policy attribute-based encryption scheme [J]. Future Generation Computer Systems, 2019, 93: 903-913.
[19] HAN D Z, PAN N N, LI K-C. A traceable and revocable ciphertext-policy attribute-based encryption scheme based on privacy protection[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(1): 316-327.
[20] ZHANG Y H, DENG R H, XU S, et al. Attribute-based encryption for cloud computing access control: a survey[J]. ACM Computing Surveys, 2020, 53(4): 1-41.
[21] YANG F, LIU L, YOU W, et al. You are revoked and out: towards directly revocable ciphertext-policy attribute-based encryption [J]. Security and Communication Networks, 2022, 41: 1-17.
[22] ZHANG Y H, ZHENG D, DENG R H. Security and privacy in smart health: efficient policy-hiding attribute-based access control[J]. IEEE Internet of Things Journal, 2018, 5(3): 2130-2145.
[23] MOHD SATAR S D, HUSSIN M, HANAPI Z M, et al. Towards virtuous cloud data storage using access policy hiding in ciphertext policy attribute-based encryption [J]. Future Internet, 2021, 13(11): 279.
[24] CHAUDHARI P, DAS M L. KeySea: keyword-based search with receiver anonymity in attribute-based searchable encryption[J]. IEEE Transactions on Services Computing, 2022, 15(2): 1036-1044.
[25] RASORI M, LA MANNA M, PERAZZO P, et al. A survey on attribute-based encryption schemes suitable for the Internet of things [J]. IEEE Internet of Things Journal, 2022, 9(11): 8269-8290.
[26] HE Y, WANG H Y, LI Y, et al. An efficient ciphertext-policy attribute-based encryption scheme supporting collaborative decryption with blockchain [J]. IEEE Internet of Things Journal, 2022, 9(4): 2722-2733.
[27] 王经纬, 宁建廷, 许胜民, 等. 面向可变用户群体的可搜索属性基加密方案[J]. 软件学报, 2023, 34(4): 1907-1925.
WANG J W, NING J T, XU S M, et al. Searchable attribute-based encryption scheme for dynamic user groups [J]. Journal of Software, 2023, 34(4): 1907-1925. (in Chinese)
[28] MIAO Y B, MA J F, LIU X M, et al. Attribute-based keyword search over hierarchical data in cloud computing[J]. IEEE Transactions on Services Computing, 2017, 13(6): 985-998.

文字编辑 薛晋栋
栏目编辑 赖玉玲