山西大学学报(自然科学版)48(5):933—945,2025
Journal of Shanxi University(Nat. Sci. Ed.)

DOI:10.13451/j.sxu.ns.2024029

智慧医疗中具有策略完全隐藏的属性基加密方案

郭丽峰[1*],徐卓恒[1],刘华[2]
(1.山西大学 计算机与信息技术学院,山西 太原 030006;
2.山西因弗美讯科技有限公司,山西 长治 047500)

摘 要:随着物联网和云计算技术的快速发展,智慧医疗的医疗质量已经得到显著提高,但是医疗系统仍然存在数据安全和用户隐私泄露问题。基于密文策略的属性加密(Ciphertext-Policy Attribute Based Encryption, CP-ABE)被认为是目前最有效的解决方案之一。然而在大多数的CP-ABE方案中攻击者可以从访问策略中获取用户隐私信息,而且由于解密密钥仅与属性相关联,与用户身份无关,所以当密钥泄露时无法准确确认用户的身份。针对上述问题,本文提出了一种策略完全隐藏的可追踪可撤销的CP-ABE方案,使用隐匿集合求交(Private Set Intersection, PSI)技术隐藏策略中的属性值和属性名称,采用与用户相关联的二叉树来追踪和撤销用户。为了提高该方案在加解密阶段的速度,引入离线/在线加密和外包解密技术。最后基于q-BDHE(q-Bilinear Diffie-Hellman Exponent)假设,证明了该方案的安全性,实验结果表明该方案加密和解密算法花费时间呈常量级,相比其他方案,效率有显著提升。

关键词:策略完全隐藏;隐匿集合求交;可追踪;可撤销;在线/离线加密;外包解密
中图分类号:TP309 **文献标志码**:A **文章编号**:0253-2395(2025)05-0933-13

Attribute-based Encryption Scheme with Policies Fully Hidden in Smart Health

GUO Lifeng[1*], XU Zhuoheng[1], LIU Hua[2]
(1. *School of Computer and Information Technology, Shanxi University, Taiyuan* 030006*, China;*
2. *Shanxi Yinfumeixun Technology Co., Ltd., Changzhi* 047500*, China*)

Abstract: With the rapid development of the Internet of Things and cloud computing technologies, the quality of healthcare in smart health has been significantly improved, but the healthcare system still has the problems of data security and user privacy leakage. Ciphertext-Policy Attribute Based Encryption (CP-ABE) is considered to be one of the most effective solutions at present. However, in most CP-ABE schemes attackers can obtain user privacy information from access policies. Since the decryption key is only associated with attributes and not with the user's identity, it is impossible to accurately confirm the user's identity when the key is leaked. To resolve the above problems, this paper proposes a traceable and revocable CP-ABE scheme with policies fully hidden by using Private Set Intersection (PSI) technology to hide the attribute values and attribute names in the policy. Furthermore, this paper adopts binary tree associated with information to track and revoke users. In order to enhance the speed of the scheme in the encryption and decryption phases, this paper introduces the skill of offline/online encryption and outsourced decryption techniques. Finally, based on the q-BDHE assumption, the security of the scheme is proved. The experiment results show that the encryption and decryption algorithms of this scheme take a constant amount of time, which is a significant improvement in efficiency compared to other schemes.

Key words: policy fully hidden; private set intersection; traceability; revocation; online/offline encryption; outsourced decryption

收稿日期:2023-10-13;**接受日期**:2024-01-30
基金项目:山西省自然科学基金(202203021221012)
* **通信作者**:郭丽峰(1975—),女,山西忻州人,博士,教授,主要研究方向为密码学与网络安全。E-mail:lfguo@sxu.edu.cn
引文格式:郭丽峰,徐卓恒,刘华.智慧医疗中具有策略完全隐藏的属性基加密方案[J].山西大学学报(自然科学版),2025,48(5):933-945. DOI:10.13451/j.sxu.ns.2024029.

0 引言

智慧医疗是一个新兴领域,它将人工智能与数据科学相结合,以科学的方式将数据转化为知识,并应用于医疗和精准健康领域,以改善人们的健康和福祉。随着物联网和云计算技术的快速发展[1],基于云计算的智慧医疗有望提供理想的健康服务,但是在实际应用中仍有许多问题需要解决[2],特别是数据安全和用户隐私泄露。例如病人希望自己的电子健康记录只能由授权的专业医疗人员访问,如果使用传统的访问控制技术,要么会违反数据安全,要么只允许粗粒度的访问策略。

在密码学领域中,基于属性的加密[3](Attribute-Based Encryption, ABE)被视为实现细粒度访问控制的重要工具。这种加密方法主要分为密文策略的属性基加密[4]和密钥策略的属性基加密[5]两大类。在属性加密方案中由于访问策略与密文一起存储在云服务器中,因此任何能检索到密文的人都可以使用相关访问策略,但是访问策略中可能包含敏感信息。例如访问策略"Neurology AND (Doctor OR Nurses)"通过医疗记录可以看出患者有神经系统疾病。对于部分策略隐藏,例如访问策略"(PN:* OR Doctor:*)AND (Hospital:*)",攻击者仍然可以看出数据和健康相关。因此具有策略完全隐藏的CP-ABE方案具有重要的研究意义。

由于解密密钥与属性紧密相关,所以发生密钥泄露事件时无法确认泄露源。例如,Alice和Bob他们共同拥有属性"Neuropathy AND Nurses",二者均可以访问"Neurology AND (Doctor OR Nurses)"密钥加密的病历,如果解密密钥泄露,无法确切地判断是Alice还是Bob成了泄露源。为解决解密密钥泄漏和追踪恶意用户的问题,ABE系统对基于可追踪性的撤销机制提出了很高的要求。

针对访问策略会泄露用户敏感信息的问题,Nishide等[6]第一次提出访问策略隐藏的概念,但是该方案计算开销较大。Zhang等[7]提出的方案通过解密测试实现了解密前访问权限的验证,但其在权限验证阶段存在隐私泄露。Yang等[8]利用bloom filter实现了一种具有全隐藏LSSS(Linear Secret Sharing Scheme)访问控制的CP-ABE方案,但其bloom filter有出现假阳性的概率。Zhang等[9]利用隐藏向量加密技术(Hidden Vector Encryption,HVE)实现了完全策略隐藏的CP-ABE方案,同时提供可信验证和解密正确性的验证。Yang等[10]基于PSI实现了大宇宙策略完全隐藏的CP-ABE方案,并使用外包可验证技术来提高解密速度,但其不支持身份的追踪和恶意用户撤销。Xue等[11]提出一种具有可追踪可撤销的完全隐藏策略方案,结合LSSS和HVE实现全隐藏策略。Luo等[12]提出一种基于ROBDD(Reduced Ordered Binary Decision Diagram)访问控制的CP-ABE方案,该结构具有更灵活的表达能力,利用Path Bloom Filter隐藏访问策略,降低解密成本,加快解密速度。

为了追踪恶意用户,Liu等[13]提出了一种基于属性的白盒可跟踪CP-ABE方案。Ning等提出了一种支持灵活属性的白盒可跟踪CP-ABE方案[14]和一种基于白盒的大宇宙CP-ABE方案[15],可以支持对恶意用户的追踪。Ning等[16]还设计了一种白盒可追踪的CP-ABE方案,能够有效地追踪恶意泄露解密密钥的用户。

尽管一些ABE方案支持可追踪机制,但是追踪后用户不能被撤销。Liu等[17]提出了一种先追踪后撤销的CP-ABE方案,但是它无法抵抗反串通攻击。Wang等[18]提出的CP-ABE方案利用与用户信息相关的二叉树实现属性撤销和用户跟踪。Lian等[19]提出了一种完全安全的追踪可撤销存储ABE方案,该方案只需要在撤销后更新部分密钥。Han等[20]提出了一种策略部分隐藏的可撤销可追踪的CP-ABE方案,但是该方案不支持外包解密。文献[21-24]中提出了一种可以支持外包解密的CP-ABE方案,将大部分的解密工作交给云服务器,在本地用户只需要少量计算即可解密。文献[25-26]中提出了一种基于在线/离线技术的CP-ABE方案,在离线阶段进行复杂的加密计算,在线阶段只需要进行轻量级处理,提升了加密速度。

综合上述分析,以上方案都只从某一方面进行解决问题,因此本文提出了一种策略完全隐藏的可撤销可追踪的属性基加密方案,实现了隐藏策略、在线/离线加密、外包解密、可追溯性和可撤销性的全部功能。本文主要贡献如下:

(1)本文通过引入隐匿集合求交(PSI)技术实现完全隐藏访问策略,且方案是在大范围下实现。

(2)本方案提供了一种有效的方法来计算密钥和密文之间的映射,通过设计标签向量来定位最小授权集的属性在用户属性集中的确切位置,以便正确解密。

(3)引入一种白盒追踪方法,解密密钥可被验证格式正确与否,从而可有效地追踪恶意用户,该方法无须存储用户标识列表,可以直接输出用户标识。

(4)引入一种基于二叉树的撤销方法,该结构可以在不更新用户私钥的情况下实现用户撤销。

(5)为了提高效率,本文使用离线/在线加密技术和外包解密技术实现轻量级处理。

1 预备知识

1.1 双线性映射

G和G_T是两个乘法循环群,g是G的生成元,双线性映射[3]$e: G \times G \rightarrow G_T$有以下性质:

(1)对于$\forall a, b \in Z_p$,有$e(g^a, g^b) = e(g, g)^{ab}$;

(2)$e(g, g) \neq 1$;

(3)存在多项式时间算法能够计算$e(g, g)$。

1.2 线性秘密共享

$\boldsymbol{M}$是一个$l \times n$的矩阵,ρ是一个单射函数。有以下两个算法[4]:

(1)秘密值分享:$\boldsymbol{M}$共享秘密值$s \in Z_p$,设向量$\boldsymbol{v} = \{s, v_2, v_3, \cdots, v_n\}^{\mathrm{T}}$,其中$v_2, v_3, \cdots, v_n \in Z_p$。在该算法中,$\lambda_i = M_i \cdot v$表示属性名索引$\rho(i)$所持有的共享秘密值。

(2)秘密值重构:$S \in A$是一个授权集合,其中$I \subset \{1, 2, \cdots, l\}$定义为$I = \{i | \rho(i) \in S\}$,存在一组常数$\{\omega_i \in Z_p\}_i \in I$,使$\sum_{i \in I} \omega_i M_i = (1, 0, \cdots, 0)$,因此有$\sum_{i \in I} \omega_i \lambda_i = s$。

1.3 二叉树

设$|U|$是系统中的用户数,R是撤销列表。密钥加密密钥树(Key-Encryption-Key, KEK)[18]T描述为:

(1)path(i)是根结点到节点i的路径集合;

(2)最小覆盖集cover(R)是覆盖R中未列出的所有用户的最小节点集;

(3)根据cover(R)$\cap$path(u),一个不在R中的用户u,只有一个节点j = cover(R)$\cap$path(u)。

如图1所示的密钥加密密钥树T,$R = \{u_3, u_5\} = \{9, 11\}$,则cover($R$)$= \{3, 10, 12, 6\}$。$u_7$的路径:path($u_7$)$= \{0, 2, 6, 13\}$。因此唯一节点$j$ = cover(R)$\cap$path(u_7)$= \{6\}$,利用二叉树的特征来实现撤销。

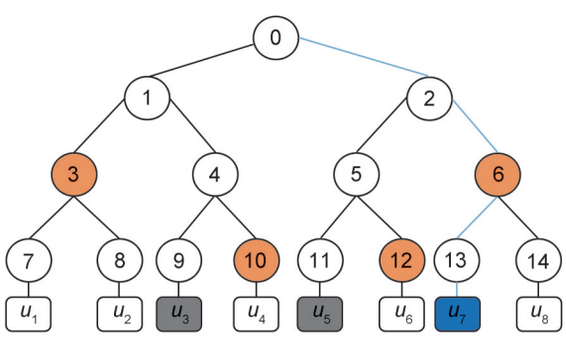

图1 密钥加密密钥树T

Fig. 1 Key-Encryption-Key tree T

1.4 隐匿集合求交

PSI[10]指双方在不泄露任何信息的情况下,一方拥有数据集A,另一方拥有数据集B,它们可以通过交集来获取两个数据集的共同部分,即$A \cap B$。A方从B方获得的信息仅为A和B的交集,

同理B方从A方获得的信息仅为A和B的交集。

1.5 困难问题假设

定义1 q-BDHE(q-Bilinear Diffie-Hellman Exponent)困难假设[18]是指在任意多项式时间内算法都无法以不可忽略的优势ε将$e(g,g)^{\alpha^{q+1}\cdot s}$和$G_T$中的一个随机的元素区分开来。

2 系统模型和算法定义

2.1 系统模型

系统模型如图2所示,由5个实体组成,每个实体负责的任务如下:

(1)授权中心(Central Authority ,CA):CA是完全可信的,它负责生成主密钥和公开参数,为用户生成解密密钥SK。此外,CA维护一个撤销列表R,并执行密钥检测算法来跟踪恶意用户。同时将更新密钥X'由CA发送到云端,实现可追溯和撤销。

(2)数据拥有者(Data Owner ,DO):通常为病人。DO指定访问策略,并根据访问策略对消息进行加密。

(3)数据用户(Data User ,DU):通常是医生。如果DU的属性满足访问策略,则能解密密文CT,获得明文消息。

(4)云服务器(Cloud Server ,CS):假设CS是半可信的,它负责存储密文并使用更新的密钥SK′来更新密文,实现恶意用户在系统中的撤销。

(5)云代理服务器(Cloud Proxy Server ,CPS):CPS为用户实现解密部分密文CT′,并将中间结果MD返回给解密用户。

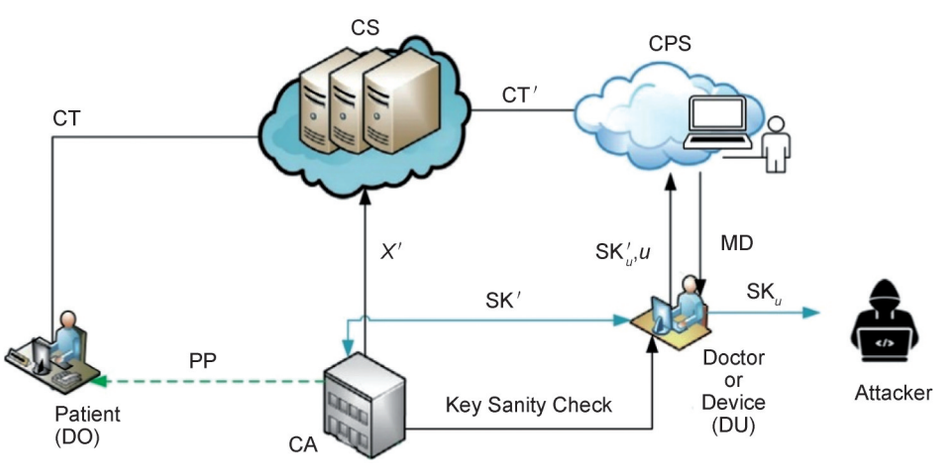

图2 系统模型图

Fig. 2 System model diagram

2.2 算法定义

基于策略完全隐藏的可追踪可撤销的属性基加密方案由以下算法组成:

(1)Setup($1^\lambda, T$)→(pp, msk):权威中心执行该算法,输入KEK树T和参数λ,输出公开参数pp和主密钥msk,CA保留撤销列表R。

(2)KeyGen(pp, msk, u, S)→SK:权威中心执行该算法,输入pp、身份u、属性集S和主msk,输出解密密钥SK,并将其发送给用户。其中SK由解密密钥DK和转换密钥TK组成。

(3)Enc.Off(pp)→IT:数据所有者执行该算法,输入公开参数pp,输出中间密文IT。

(4)Enc.On(m, pp, (M,ρ), IT, R)→CT:数据所有者执行该算法,输入pp、消息m、访问策略(M,ρ)、中间密文IT和撤销列表R,输出密文CT。

(5)PolicyHide(pp, policy)→(CP, L, V):数据所有者执行该算法,输入公开参数pp、访问策略

policy。输出密文策略CP、标签矩阵L和标签向量V。

(6)DecTest(pp,S,CP,L,V,S')→(True/False,Map):数据用户执行该算法,输入公开参数pp、属性集S、密文策略CP以及一些标签。通过计算用户属性集与策略的每个最小授权集之间的交集来确定授权关系。当用户的属性集包含它们的交集,该用户获得授权,如果用户的属性集不包含它们的交集,则用户是未授权的。当S是一个授权集时,输出True和密钥与密文之间的映射,否则输出False,算法终止。

(7)DecOut(TK,CT,Map,CP)→C_{Tout}:云代理服务器执行该算法,输入转换密钥TK、密文CT、映射关系Map和密文策略CP,输出部分密文C_{Tout},并发送给DU。

(8)Dec(pp,C_{Tout},DK)→m:数据用户执行该算法,以公共参数pp、密文C_{Tout}和解密密钥DK作为输入,输出消息m。

(9)KeySanityCheck(pp,msk,SK)→0/1:权威中心执行该算法,输入pp和SK,然后算法检查是否需要跟踪解密密钥SK,如果通过密钥检查,算法输出1,否则输出0。

(10)Trace(pp,SK,R)→u/$\perp$:权威中心执行该算法,输入pp、SK和R。如果SK通过KeySanityCheck,则输出u并更新撤销列表$R'=R\cup\{u\}$,否则算法终止,输出$\perp$。

(11)CTUpdate(CT,R',X')→CT':云服务器执行该算法,输入CT、R'和密钥X',输出更新密文CT'并保存到云端。

2.3 策略隐藏安全模型定义

策略隐藏的安全模型[10]:在策略隐藏方案中,有A和B两方,A希望隐藏访问策略中的属性,A的属性集为S_p,B的属性集为S。B计算授权和匹配关系。S_p和S之间的授权通过计算任意最小授权集与S之间的交集来判断,如果交集包含在S中,说明是授权集合。在求交中,双方在不暴露属性情况下计算授权。

设P表示一个策略隐藏方案,$f(x,y)$是一个用来计算x和y之间包含关系的函数。如果x包含y,则输出True,否则输出False。设X是S_p的最小授权集之一,设Y是仅包含S的一个元素集合,当且仅当存在X,使$f(S,X)$为True时,S是S_p的授权集。如果使$f(X,Y)$为True,并且Y的数量不小于$|X|$,则$f(X,S)$将为True。对于$\forall i\in A$,$f_i(X,Y)$表示参与者i的计算,$\text{view}_i(X,Y)$表示i的视图,$\text{op}_i(X,Y)$表示i的输出。P秘密计算$f(S,X)$相当于秘密计算$f(X,Y)$。

定义2 如果存在PPT模拟器S_1和S_2,P秘密计算交集,使以下两个方程同时成立:

$$\{(S_1(x,f_A(x,y)),f_B(x,y))\}=\{(\text{view}_A(x,y),\text{op}_B(x,y))\},\tag{1}$$

$$\{(f_A(x,y)),S_2(y,f_B(x,y))\}=\{(\text{op}_A(x,y)),\text{view}_B(x,y)\},\tag{2}$$

(其中=是不可区分的)。

2.4 选择安全模型定义

Init:攻击者A选定挑战访问策略(M^*,ρ^*)和撤销列表R^*之后将其发送给挑战者B。

Setup:B运行Setup算法,将pp发给A并保留主密钥msk。

Phase 1:A向B发起关于属性集$(u_1,S_1)(u_2,S_2)\cdots(u_q,S_q)$的密钥的询问。

1)如果属性集S是一个授权集并且用户$u\notin R^*$,游戏终止。

2)如果属性集S不是一个授权集并且用户$u\in R^*$,挑战者B运行KeyGen算法生成密钥$\{\text{SK}_{u,Si},u_i\}_i\in[1,q]$发给攻击者$A$。

Challenge:A向B提交两个等长的消息m_0和m_1。B随机选取m_b,其中$b\in\{0,1\}$。然后B运行Enc.on(m,pp,(M^*,ρ^*),IT,R^*)生成密文CT,并将其发送给A。

Phase 2:同Phase 1,A继续向B询问私钥。

Guess:A输出值$b'\in\{0,1\}$,如果$b'=b$,则称A赢得该游戏。攻击者A在该游戏的优势定义为

$\varepsilon=|\Pr[b=b']-1/2|$。

定义3 如果攻击者无法在多项式时间内以不可忽略的优势ε攻破上述安全游戏,则称本文提出的CP-ABE方案是选择明文安全的。

3 方案构造

(1)Setup$(1^\lambda)\to(\mathrm{pp},\mathrm{msk})$。CA选取随机数$\alpha\in Z_p$,$h,u,v,w\in G$,关于$T$中每个节点,随机选取$\{x_i\}_{i=0}^{2|U|-2}\in Z_p$并计算$\{y_i=g^{x_i}\}_{i=0}^{2|U|-2}$,公共参数pp和主密钥msk如下:

$$\mathrm{pp}=(g,e(g,g)^\alpha,h,u,v,w)\mathrm{msk}=(\alpha,g^\alpha)。$$

(2)KeyGen$(\mathrm{pp},\mathrm{msk},S)\to\mathrm{SK}$。CA选取随机数$z\in Z_p$,选取$k+1$个随机数$(r,r_1,r_2,\cdots,r_k)\in Z_p$。假设$\mathrm{path}(i_d)=\{i_0,\cdots,i_d\}$,其中$i_0=\mathrm{root}$,$i_d$是与用户$u$相关联的二叉树叶子节点的值,计算与用户$u$相关联的解密密钥组件$K_u=g^{r/x_{i_d}}$。解密密钥DK和转换密钥TK如下:

$$\mathrm{DK}=z,\mathrm{TK}=(K=g^{\alpha/z+r}w^r,L=g^r,K_u=g^{r/x_{i_d}},\forall i\in[k],K_{1,i}=g^{ri},K_{2,i}=(u^{A_i}h)^{r_i}v^{-r})。$$

最后,输出密钥$\mathrm{SK}=\{\mathrm{DK},\mathrm{TK}\}$。

(3)Enc.Off$(\mathrm{pp})\to\mathrm{IT}$。在离线加密阶段,生成中间密文IT,由两个模块组成。其中主模块计算方法:DO选择一个随机数$s\in Z_p$,计算$\tilde{C}=e(g,g)^{\alpha s}$和$\tilde{C}_0=g^s$,DO设置$\mathrm{IT}_{\mathrm{main}}=(\tilde{C},\tilde{C}_0)$为主模块。此外,属性模块的计算方法如下:DO选择一个随机数$x_i,t_i,\lambda_i'\in Z_p$,计算$\tilde{C}_{1,i}=w^{\lambda_i'}v^{t_i}$,$\tilde{C}_{2,i}=(u^{x_i}h)^{-t_i}$,$\tilde{C}_{3,i}=g^{t_i}$,其中$i\in J$,$J$表示中间密文池的大小,用于临时存储中间密文,DO设置$IT_{\mathrm{att}}=\{x_i,t_i,\lambda_i',\tilde{C}_{1,i},\tilde{C}_{2,i},\tilde{C}_{3,i}\}_i\in J$。最后DO定义$\mathrm{IT}=\{\mathrm{IT}_{\mathrm{main}},\mathrm{IT}_{\mathrm{att}}\}$作为中间密文。

(4) Enc.On$(m,\mathrm{pp},(\boldsymbol{M},\rho),\mathrm{IT},R)\to\mathrm{CT}$。DO随机选取$v_2,v_3,\cdots,v_n\in Z_p$,设置向量$\boldsymbol{v}=\{s,v_2,v_3,\cdots,v_n\}^{\mathrm{T}}$,并且计算$M\cdot\boldsymbol{v}=(\lambda_1,\lambda_2,\cdots,\lambda_l)^{\mathrm{T}}$作为$s$的有效共享向量。DO选择一个主模块$\mathrm{IT}_{\mathrm{main}}=(\tilde{C},\tilde{C}_0)$和属性模块$\mathrm{IT}_{\mathrm{att}}=\{x_i,t_i,\lambda_i',\tilde{C}_{1,i},\tilde{C}_{2,i},\tilde{C}_{3,i}\}_i\in l$,DO设置

$$C=m\cdot\tilde{C}=m\cdot e(g,g)^{\alpha s},C_0=\tilde{C}_0=g^s,C_{1,i}=\tilde{C}_{1,i},C_{2,i}=\tilde{C}_{2,i},C_{3,i}=\tilde{C}_{3,i}。$$

并且计算如下密文:$\{C_{4,i}=\lambda_i-\lambda_i',C_{5,i}=-t_i(\rho(i)-x_i)\}_i\in[l]$因此,密文$CT=\{R,C,C_0,\{C_{1,i},C_{2,i},C_{3,i},C_{4,i},C_{5,i}\}_i\in[l],\{T_j=y_j^s=g^{x_j\cdot s}\}_j\in\mathrm{cover}(R)\}$。

(5)PolicyHide$(\mathrm{pp},\mathrm{policy})\to(\mathrm{CP},\boldsymbol{L},\boldsymbol{V})$。计算标签矩阵$\boldsymbol{L}$,$\boldsymbol{L}$中的每一行就对应一个最小授权集,$\boldsymbol{L}$中的每一列都与相同属性相关。$\boldsymbol{L}$是一个$N\times|\boldsymbol{P}|$大的矩阵,其中$\boldsymbol{L}$中每个元素$\boldsymbol{L}_{i,j}$是布尔值,当$\boldsymbol{L}_{i,j}=1$时,说明属性$A_j$包含在$Y_i$中。同时DO生成一个有序映射行向量$\boldsymbol{V}=\{\boldsymbol{V}_0,\boldsymbol{V}_1,\cdots,\boldsymbol{V}_{l-1}\}$在属性集相同的访问矩阵和$\boldsymbol{P}'$之间。当$\rho(j)=A_i$时,$\boldsymbol{V}_i=j$。

最小授权集Y_i对应多项式$f_i(x)$,设$Y_i=\{A_{i,0},A_{i,1},\cdots,A_{i,n-1}\}$,$|Y_i|=n$,然后计算每个最小授权集的策略密文,如下所示:

$$\forall i\in[N]:f_i(x)=(x-A_{i,0})(x-A_{i,1})\cdots(x-A_{i,n-1})=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,$$

$$\mathrm{cp}_i=cp_{i|Yi|}\|cp_{i,|Yi|-1}\|\cdots\|cp_{i,0},$$

$$\mathrm{CP}=cp_1\|cp_2\|\cdots\|cp_N\|LM\|LV。$$

(6)DecTest$(\mathrm{pp},S,\mathrm{CP},\boldsymbol{L},\boldsymbol{V},LS')\to(\mathrm{True/False},\mathrm{Map})$。

举个例子:假设访问策略为"$\{A_1\vee A_2\}\wedge\{A_3\vee A_4\}$",则最小授权集为$\{\{A_1,A_3\},\{A_1,A_4\},\{A_2,A_3\},\{A_2,A_4\}\}$,排序后的策略属性集$\boldsymbol{P}'=\{A_1,A_2,A_3,A_4\}$,访问控制结构中的映射函数$\rho$,$\{\rho(1)=A_3,\rho(2)=A_4,\rho(3)=A_2,\rho(4)=A_1\}$。用户$u_1$的属性集$S=\{A_5,A_3,A_6,A_1\}$,则排序后的属性集$S'=\{A_1,A_3,A_5,A_6\}$。因为S包含最小授权集合$\{A_1,A_3\}$,可以得出$\boldsymbol{S}=\{1,1,0,0\}$。$\boldsymbol{S}'$表示密钥中的属性顺序与排序后的属性集$S''$中的属性顺序之间的关系,所以$\boldsymbol{S}'=\{3,1,0,2\}$。根据$\boldsymbol{L}$和$\boldsymbol{S}$,可以建立策略的排序属性集与排序用户属性集的对应关系。然后,通过LV和LS'可以知道密文和密钥之间的映射关系。映射关系如图3所示。

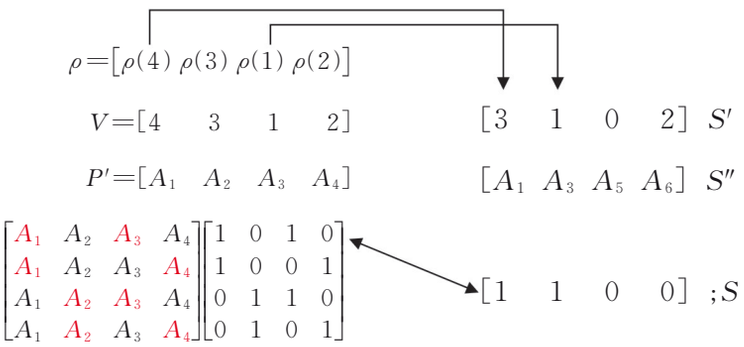

图3 映射关系图

Fig. 3 An example of the map diagram

根据L和S'关系可以得出密文和密钥之间的映射关系如下所示:

$$[C_{1,4}, C_{2,4}, C_{3,4}]\Leftrightarrow[K_{1,3}, K_{2,3}],$$
$$[C_{1,1}, C_{2,1}, C_{3,1}]\Leftrightarrow[K_{1,1}, K_{2,1}]。$$

(7)DecOut(TK, CT, Map, CP)$\rightarrow C_{\text{Tout}}$。CPS接收到密文后,通过转换密钥TK输出密文一部分C_{Tout}。存在以下两种情况:

Case1:如果$u\in R$,算法终止,输出$\perp$。

Case2:如果$u\notin R$,然后执行如下算法:

① 对于$u\notin R$,存在一个节点$j\in\text{cover}(R)\cap\text{path}(u)$,假设$\text{path}(u)=\{i_0, i_{\text{dept}(j)}, \cdots, i_d\}$,其中$i_{\text{dept}(j)}=j$,并且$i_d$是二叉树中与用户$u$相关的叶节点值,算法计算$\theta=\frac{x_{id}}{x_j}$,然后计算$B=e(K_u, T_j)^{\theta}=e(g,g)^{rs}$。

② 让$I\subset\{1,2,\cdots,l\}$定义为$I=\{i|\rho(i)\in S\}$,存在一组常数$\{\omega_i\in Z_p\}_i\in I$,使$\sum_{i\in I}\omega_i\boldsymbol{M}=(1,0,\cdots,0)$,因此有$\sum_{i\in I}\omega_i\lambda_i=s$。然后计算:

$$P=\prod_{i\in I}(e(C_{1,i}w^{C_{4,i}}, L)\cdot e(C_{2,i}u^{C_{5,i}}, K_{1,i})\cdot e(C_{3,i}, K_{2,i}))^{\omega_i}=e(g,w)^{rs},$$

$$A=e(K, C_0)=e(g,g)^{\frac{\alpha s}{z}}e(g,w)^{rs}e(g,g)^{rs},$$

$$C_{\text{Tout}}=\frac{A}{B\cdot P}=e(g,g)^{\frac{\alpha s}{z}}。$$

(8)Dec(pp, C_{Tout}, DK)$\rightarrow m$。DU收到云代理服务器输出的C_{Tout}后,通过解密密钥DK对消息m进行解密。$m=\frac{C}{(C_{\text{Tout}})^{z}}$。

(9)KeySanityCheck(pp, msk, SK)$\rightarrow$0/1。$z\in Z_p, K, L, K_u, K_{1,i}, K_{2,i}\in G$。

如果$e(K, g^z)=e(g,g)^{\alpha}e(L^z, w)e(L^z, g)\neq 1$,KeySanityCheck算法返回1。否则返回0。

(10)Trace(pp, SK, R)$\rightarrow u/\perp$。如果密钥SK不能通过KeySanityCheck,算法将终止,并输出$\perp$。否则,算法执行如下:

① 二叉树中如果不存在与i_d相关联的用户节点,算法中止,输出$\perp$。

② 如果$u\notin R$,将u添加到R中,更新后的列表$R'=R\cup\{u\}$。

(11)CTUpdate(CT, R', X')$\rightarrow CT'$。CA随机选择$\eta\in Z_p$,计算$X'=\{\eta\cdot x_i\}_{i=0}^{2|U|-2}$,设cover($R'$)为最新撤销列表$R'$相关联的最小覆盖集。给定$j'\in\text{cover}(R')$,有以下两种情况:

① 如果$j=j'$,则$T_j=T_j'$。

② 如果 j 是 j' 的祖先,则 path(j')=path(j)∪{$i_{\mathrm{dept}(j)+1},\cdots,i_{\mathrm{dept}(j')}$},其中 $i_{\mathrm{dept}(j)}=j$,$i_{\mathrm{dept}(j')}=j'$。让 $Y_j=T_j$ 并计算 $Y_{i\,k+1}=(Y_{i_k})^{\frac{x'_{i_{k+1}}}{x'_{ik}}}=y^s_{i_{k+1}}$,其中 $k=\mathrm{dept}(j),\cdots,\mathrm{dept}(j')$。

最后更新的密文 $CT'=\{R',C,C_0,\{C_{1,i},C_{2,i},C_{3,i},C_{4,i},C_{5,i}\}_i\in[l],\{T_{j'}=y^s_{j'}=g^{x'_{j'}\cdot s}\}_{j'}\in\mathrm{cover}(R')\}$。

4 安全性证明

定理1 如果q-BDHE假设成立,则在选择明文攻击的条件下,任何攻击者都无法在多项式时间内以不可忽略的优势攻破本文方案。

证明 如果攻击者 A 在 q 次询问后,能够以不可忽略的优势 ε 攻破本文方案,那么我们可以构造一个挑战者 B,该挑战者 B 能够以不可忽略的优势 $\varepsilon/2$ 攻破该假设。

Init:攻击者 A 将要挑战的策略(M^*,ρ^*)和撤销列表 R^* 发送给挑战者 B。

Setup:B 必须向 A 提供系统的公共参数。为了做到这一点,B 隐式地将方案的主密钥设置为 $\alpha=a^{q+1}+\tilde{\alpha}$,挑战者 B 随机选取 $\tilde{\alpha}\in Z_p$,其中 a,q 是在假设中设置,α 为正确分布,a 是理论上对 A 隐藏的信息。然后 B 选择随机指数 $\tilde{u},\tilde{v},\tilde{h}\in Z_p$,使用假设给 A 提供以下公共参数:

$$g=g,w=g^a,$$

$$v=g^{\tilde{v}}\cdot\prod_{(j,k\in[l,n])}(g^{\frac{a^k}{b_j}})^{M^*_{j,k}},u=g^{\tilde{u}}\cdot\prod_{(j,k\in[l,n])}(g^{\frac{a^k}{b^2_j}})^{M^*_{j,k}},$$

$$h=g^{\tilde{h}}\cdot\prod_{(j,k\in[l,n])}(g^{\frac{a^k}{b_j}})^{-\rho^*(j)M^*_{j,k}}\ e(g,g)^{\alpha}=e(g^a,g^{a^q})\cdot e(g,g)^{\tilde{\alpha}}。$$

Phase 1:攻击者 A 向挑战者 B 发起属性集$(u_1,S_1)(u_2,S_2)\cdots(u_q,S_q)$的密钥询问。

如果 S 不满足访问策略并且 $u\in R^*$,A 随机选取向量 $\boldsymbol{w}=\{w_1,w_2,w_3,\cdots,w_n\}^{\mathrm{T}}\in Z_p$,其中 $w_1=-1$ 和 $M^*_i\cdot\boldsymbol{w}=0$。对于所有的 $i\in I=\{i|\rho(i)\in S\}$,随机选取 $\tilde{r},z\in Z_p$,隐式定义如下:

$$r=\tilde{r}+w_1a^q+w_2a^{q-1}+\cdots+w_na^{q+1-n}=\tilde{r}+\sum_{i\in[n]}w_ia^{q+1-i},$$

$$K_0=g^{\frac{\alpha}{z}}g^rw^r=g^{\frac{\tilde{\alpha}}{z}}(g^a)^{\tilde{r}}\prod_{i=2}^{n}(g^{\frac{a^{q+1-i}}{z}})^{wi}g^{\tilde{r}}\prod_{i=2}^{n}(g^{a^{q+1-i}})^{wi}L=g^r=g^{\tilde{r}}\prod_{i\in[n]}(g^{a^{q+1-i}})^{w_i}。$$

假设 path(i_d)=$\{i_0,\cdots,i_d\}$,因为 $u\in R^*$,所以 $i_d\in I_{R^*}$,$x_{i\,d}=v_{i\,d}+d^{i_d}$。

接下来,B 计算 $K_u=(g^t\prod_{i=1}^{n^*}g^{w_i\,d^{q+1-i}})^{\frac{1}{(v_{id}+d^{id})\cdot(a+c)}}=g^{\frac{r}{x_{id}}}$。

此外,对于所有 $i\in[|S|]$,计算 $K_{1,i}=g^{r_i}$ 和 $K_{2,i}=(u^{A_i}h)^{r_i}v^{-r}$。

$$v^{-r}=v^{-\tilde{r}}(g^{\tilde{v}}\prod_{(j,k\in[l,n])}g^{a^kM^*_{j,k}/b\,j})^{-\sum w_ia^{q+1-i}}=\underbrace{v^{-\tilde{r}}\prod_{i\in[n]}(g^{a^{q+1-i}})^{-\tilde{v}wi}\cdot\prod_{(i,j,k\in[n,l,n])}(g^{a^{q+1-i}/bj})^{-wiM^*_{j,k}}}_{\Delta}\cdot\prod_{(i,j)\in[n,l]}g^{-wiM^*_{j,k}a^{q+1}/bj}=$$

$$\Delta\cdot\prod_{j\in[l]}g^{-<\vec{w},M^*_j>a^{q+1}/bj}=\Delta\cdot\prod_{\substack{j\in[l]\\ \rho^*(j)\notin S}}g^{-<\vec{w},M^*_j>a^{q+1}/bj}。$$

计算$(u^{A_i}h)^{r_i}$,对于每个属性 $A_i\in S$ 进行隐式定义:

$$r_i=\tilde{r}_i+r\cdot\sum_{\substack{i'\in[l]\\ \rho^*(i')\notin S}}\frac{b_{i'}}{A_i-\rho^*(i')}=\tilde{r}_i+r\cdot\sum_{\substack{i'\in[l]\\ \rho^*(i')\notin S}}\frac{b_{i'}}{A_i-\rho^*(i')}+\sum_{\substack{(i,i')\in[n,l]\\ \rho^*(i')\notin S}}\frac{w_ib_{i'}a^{q+1-i}}{A_i-\rho^*(i')}。$$

计算 $K_{2,i}=(u^{A_i}h)^{r_i}v^{-r}$。

$$(u^{A_i}h)^{r_i}=(u^{Ai}h)^{\tilde{r}_i}\cdot(g^{\tilde{u}Ai+\tilde{h}}\prod_{(j,k)\in[l,n]}g^{(Ai-\rho^*(j))M^*_{j,k}a^k/b^2_j})^{\tilde{r}\cdot\sum\limits_{\substack{i'\in[l]\\ \rho^*(i')\notin S}}\frac{b_{i'}}{Ai-\rho^*(i')}}\cdot(g^{\tilde{u}Ai+\tilde{h}}\prod_{(j,k)\in[l,n]}g^{(Ai-\rho^*(j))M^*_{j,k}a^k/b^2_j})^{\sum\limits_{(i,i'\in[n,l]}\frac{wib_{i'}a^{q+1-i}}{Ai-\rho^*(i')}}_{\rho^*(i')\notin S}=$$

$$\Psi\cdot\prod_{\substack{(i,j)\in[n,l]\\ \rho^*(j)\notin S}} g^{(Ai-\rho^*(j))w_iM^*_{j,k}b_ia^{q+1-i+k}/(Ai-\rho^*(j))b_j^2}=\Psi\cdot\prod_{\substack{j\in[l]\\ \rho^*(j)\notin S}} g^{<\vec{w},M^*_j>a^{q+1}/bj},$$

其中

$$\Psi=(u^{Ai}h)^{\tilde{r}_i}\cdot(K_{i,1}/g^{\tilde{r}i})^{\tilde{u}Ai+\tilde{h}}\cdot\prod_{\substack{(i',j,k\in[l,l,n])\\ \rho^*(i')\notin S}}(g^{b_ia^k/b_j^2})^{\tilde{r}(Ai-\rho^*(j))M^*_{j,k}/(Ai-\rho^*(i'))}\cdot\prod_{\substack{(i,i',j,k\in[n,l,l,n])\\ \rho^*(i')\notin S}}(g^{b_ia^{q+1+k-i}/b_j^2})^{(Ai-\rho^*(j))w_iM^*_{j,k}/(Ai-\rho^*(i'))}$$

$$K_{1,i}=g^{r_i}=g^{\tilde{r}i}\cdot\prod_{\substack{i'\in[l]\\ \rho^*(i')\notin S}}(g^{b_{i'}})^{\tilde{r}/(Ai-\rho^*(i'))}\cdot\prod_{\substack{(i,i')\in[n,l]\\ \rho^*(i')\notin S}}(g^{b_ia^{q+1-i}})^{w_i/(Ai-\rho^*(i'))}。$$

$(u^{A_i}h)^{r_i}$的第二部分恰好与v^{-r}有问题的部分抵消。因此挑战者可以为所有的$A_i\in S$计算$K_{1,i}$和$K_{2,i}$,并将密钥$sk=\{K,L,K_u,K_{1,i},K_{2,i}\}$发送给攻击者A。

Challenge:攻击者将输出一对相同长度的消息(m_0,m_1)。在此阶段,挑战者抛出随机硬币$b\in\{0,1\}$并构造$C=m_b\cdot T\cdot e(g,g)^{\tilde{\alpha}s}$,$C_0=g^s$,其中$T$是挑战项,$g^s$是假设的对应项。

挑战者设置$\boldsymbol{y}=(s,sa+\tilde{y}_2,sa^2+\tilde{y}_3,\cdots,sa^{n-1}+\tilde{y}_n)^{\perp}$,其中$(\tilde{y}_2,\tilde{y}_3,\cdots,\tilde{y}_n)\in Z_p$。由于$\boldsymbol{\lambda}=\boldsymbol{M}\cdot\boldsymbol{y}$,本文有$\lambda_T=\sum_{i\in[n]}M^*_{T,i}sa^{i-1}+\sum_{i=2}^{n}M^*_{T,i}\tilde{y}i=\sum_{i\in[n]}M^*_{T,i}sa^{i-1}+\tilde{\lambda}_T$。$\tilde{\lambda}_T=\sum_{i=2}^{n}M^*_{T,i}\tilde{y}i$挑战者已知,对于每一行$T\in[l]$,挑战者$B$隐式设置$t_T=-sb_T$,利用以上,$B$可以计算出:

$$C_{1,T}=w^{\lambda'_T}v^{t_T}=w^{\tilde{\lambda}'_T}\cdot\prod_{i\in[n]}g^{M^*_{T,i}sai}\cdot(g^{sb_T})^{-\tilde{v}}\cdot w^{\tilde{\lambda}'_T}\cdot\prod_{(j,k)\in[l,n]}g^{-M^*_{j,k}a^ksb_T/b_j}=w^{\tilde{\lambda}'_T}\cdot(gsb_T)^{-\tilde{v}}\cdot\prod_{\substack{(j,k)\in[l,n]\\ j\neq T}}(g^{sa^kb_T/b_j})^{-M^*_{j,k}}$$

$$C_{2,T}=(u^{\rho^*(T)}h)^{-t_T}=(g^{sb_T})^{-(\tilde{u}\rho^*(T)+\tilde{h})}\cdot(\prod_{(j,k)\in[l,n]}g^{(\rho^*(T)-\rho^*(j))M^*_{j,k}a^k/b_j^2})^{-sb_T}=$$

$$(g^{sb_T})^{-(\tilde{u}\rho^*(T)+\tilde{h})}\cdot\prod_{\substack{(j,k)\in[l,n]\\ j\neq T}}(g^{sa^kb_T/b_j^2})^{-(\rho^*(T)-\rho^*(j))M^*_{j,k}},$$

$$C_{3,T}=g^{t_T}=(g^{sb_T})^{-1}。$$

此外,挑战者B随机选取$\beta_T,\varepsilon_T\in Z_p$,挑战者$B$计算:$C_{4,T=}\beta_T$,$C_{5,T=}\varepsilon_T$。

$\forall j\in\mathrm{cover}(R^*)$,有$x_j=v_j+d^q$和$y_j=g^{v_j}+d^q$,然后$B$计算出$T_j=(g^s)^{v_j+d^q}=y_j^s$。

注意,通过使用$t_T=-sb_T$,与$w^{\lambda'_T}$的未知次幂相抵消。因此挑战者B将密文$CT=(C,C_0,\{C_{1,i},C_{2,i},C_{3,i},C_{4,i},C_{5,i}\}_i\in[l],\{T_j\}_j\in\mathrm{cover}(R))$交给攻击者$A$。

Phase2:与查询阶段1相同。

Guess:攻击者为挑战位输出一个猜测b'。如果$b'=b$,挑战者B输出0,即它声称挑战项是$T=e(g,g)^{sa^{q+1}}$,否则输出1。

如果$T=e(g,g)^{sa^{q+1}}$,则A进行了安全游戏,即可计算$C=m_b\cdot T\cdot e(g,g)^{\tilde{\alpha}s}=m_b\cdot e(g,g)^{\alpha s}$。如果攻击者$A$以不可忽略的优势攻破了方案,那么挑战者$B$就能以不可忽略的优势攻破q-BDHE假设。因此证明了定理1。

定理2　对于任何PPT敌手来说,本文方案的PolicyHide算法是安全的。

证明　通过构造一个满足方程1和2的模拟器来证明该定理。在此场景中,DO为A,DU为B。A在模拟器中计算相关参数,B得到最终结果,在这个场景中不会出现公式2。在交集中有如下两种情况:假设构建了模拟器S_1,$f_A(x,y)=f_B(x,y)=(Y\subset X)$,并让$(X,f_A(X,Y))$作为输入:

$$f_A(X,Y)=f_B(X,Y)=(Y\subset X),f_A(X,Y)=f_B(X,Y)=(Y\not\subset X)。$$

(1)S_1取$(X,Y\subset X)$作为输入。首先它随机选择持有$f_A(X,Y)=f_A(X,\bar{Y})$的集合$\bar{Y}=\bar{y}_1,\bar{y}_2,\cdots,\bar{y}_m$。然后$S_1$为$X$传导多项式$f(x)$,其中$A=(a_0,a_1,\cdots,a_n)$为$f$的系数集。

(2)S_1选择一个较大的随机元素$r'\in Z_p$。它根据A来计算$\vec{A}'=(g^{r'a_0},g^{r'a_1},\cdots,g^{r'a_n})$。然后,它计算$\vec{B}=(m,(\bar{y}_1+\bar{y}_2+\cdots\bar{y}_m),\cdots,(\bar{y}_1^{-n}+\bar{y}_2^{-n}+\cdots+\bar{y}_m^{-n}))$。实体$A$也选择一个较大的随机元素

$r\in Z_p$进行计算$\vec{A}=(g^{ra_0},g^{ra_1},\cdots,g^{ra_n})$。

(3)S_1的计算如下:$C'=g^{r'a_0m}\cdot g^{r'a_1(\bar{y}_1+\bar{y}_2+\cdots+\bar{y}_m)}\cdot(\cdots)\cdot g^{r'a_n(\bar{y_1}^n+\bar{y_2}^n+\cdots+\bar{y_m}^n)}=g^{r'[f(\bar{y}_1)+\cdots+f(\bar{y}_m)]}$,实体$B$的计算如下:$C=g^{ra_0m}\cdot g^{ra_1(\bar{y}_1+\bar{y}_2+\cdots+\bar{y}_m)}\cdot(\cdots)\cdot g^{ra_n(\bar{y_1}^n+\bar{y_2}^n+\cdots+\bar{y_m}^n)}=g^{r[f(\bar{y}_1)+\cdots+f(\bar{y}_m)]}$。

然后,$\text{view}_A(X,Y)=\{X,A,\vec{A},r\}$,$S_1(X,Y)=\{X,A,\vec{A}',r',C'\}$,$f_B(X,Y)=\text{output}_B(X,Y)=\{C\}$。根据假设,我们得到$C'=C=(Y\in X)$。当$r'=r$,$\vec{A}'=\vec{A}$。因此公式1成立。

5 方案分析

5.1 功能对比

将本文提出的策略完全隐藏的可追踪可撤销的CP-ABE方案与其他基于策略隐藏、大宇宙、在线/离线、解密测试、外包解密、追踪和撤销功能的CP-ABE方案[10]和[20]进行比较,对比结果如表1所示。

表1 不同方案功能对比

Table 1 Comparison of functionals among different schemes

方案	策略隐藏	大宇宙	在线/离线	解密测试	外包解密	追踪和撤销
TR-CPABE[20]	半隐藏	×	×	×	×	√
FH-CPABE[10]	全隐藏	√	×	√	√	×
本方案	全隐藏	√	√	√	√	√

从表1中可以看出,TR-CPABE(Traceable and Revocable Ciphertext Policy Attribute-based Encryption)[10]和FH-CPABE(Fully Hidden Ciphertext Policy Attribute-based Encryption)[10]都不支持在线/离线加密技术,FH-CPABE[12]虽然支持外包解密,但不支持密钥的追踪和用户的撤销,因此该方案不具有实用性。TR-CPABE[20]支持追踪和撤销,但不支持策略完全隐藏和大宇宙,方案不具有可扩展性。本方案结合了TR-CPABE[20]和FH-CPABE[10]的优点,同时支持全隐藏、大宇宙、在线/离线、解密测试、外包解密、追踪撤销的功能,因此具有更强可用性。

5.2 存储成本对比

存储开销是访问控制方案中最重要的问题之一。令$|e_T|$为G_T中的元素大小,$|e|$为G和Z_p中的元素大小,l为策略中属性的个数,s为用户属性集中的属性个数,$|c|$为密文大小,M为客户端存储的数字对的平均个数,S_{ma}为最小授权集。

从表2中可以看出,本方案的密文分布在不同的服务器上。但在TR-CPABE[20]中,云服务器负责存储所有密文,当多个用户同时访问时,会有较大的延迟。同时,TR-CPABE[20]中的策略密文通常随着系统中属性集的增加而增加,而本方案的策略密文随着$\sum_{j=1}^{N}|S_{\text{ma}}|$的值而增加,$S_{\text{ma}}$的值取决于策略的复杂度。

5.3 实验分析

为了进一步评价本方案的性能,在PyCharm编译器中引入Charm库[27],用Python实现了本方案、TR-CPABE[20]和FH-CPABE[10]。实验运行环境如下:操作系统为Linux,镜像为Ubuntu 18.04.6,运行内存4 GB。访问策略中的属性数量从0增加到25,同时满足访问策略的用户属性数

表2 TR-CPABE方案和本方案存储成本对比

Table 2 Comparison of storage costs between TR-CPABE scheme and ours

方案	数据拥有者	代理服务器	云服务器
TR-CPABE[20]	$(4+s)\|e\|$	×	$\|e_T\|+(l+1)\|e\|+\|c\|$
本方案	$(M+3+2s)\|e\|$	$\|e_T\|+(3l+1+\sum_{j=1}^{N}\|MAS\|)\|e\|$	$\|c\|$

量也从0增加到25,实验一共进行50次,取均值为最终结果。

如图4所示,在初始化方面,文献[10]中FH-CPABE的初始化时间花费少,因为此方案没有追踪和撤销功能,而本方案和TR-CPABE[20]为了实现追踪和撤销,在初始化阶段需要初始化一个二叉树,因此消耗的时间比FH-CPABE[10]长。如图5所示,在密钥生成方面,三个方案密钥生成消耗的时间均与属性数量呈线性关系。如图6所示,在数据拥有者加密方面,TR-CPABE[20]和FH-CPABE[10]加密所需时间与属性数量呈线性关系,而本文方案呈常量级,因为本方案加密阶段把大量计算转移到离线阶段,在线阶段只需要执行轻量级操作。如图7所示,在数据用户解密方面,TR-CPABE[20]的解密时间与属性数量呈线性关系,而FH-CPABE[10]和本方案的解密时间呈常量级,因为大部分解密到外包到代理云服务器,用户只需要执行少量解密运算。在本方案中,有一个主要因素影响策略隐藏的时间,即策略的复杂性。实验中,本方案使用两个简单的值来表示复杂度:最小授权集的平均大小$|S_{ma}|$和最小授权集的数量N。从图8中可以看出,策略隐藏时间随着策略复杂度的增加而增加。

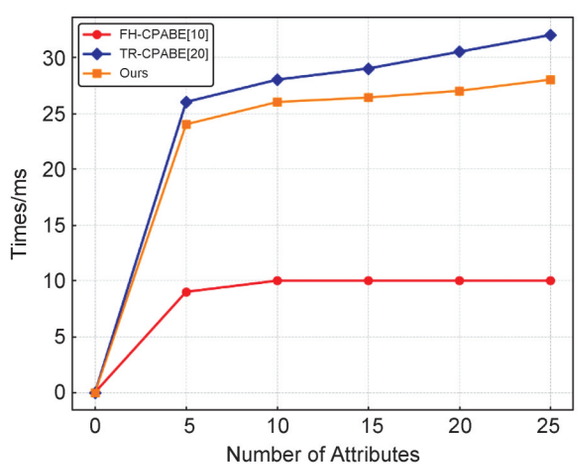

图4 授权中心初始化时间开销

Fig. 4 Time costs of CA initialization

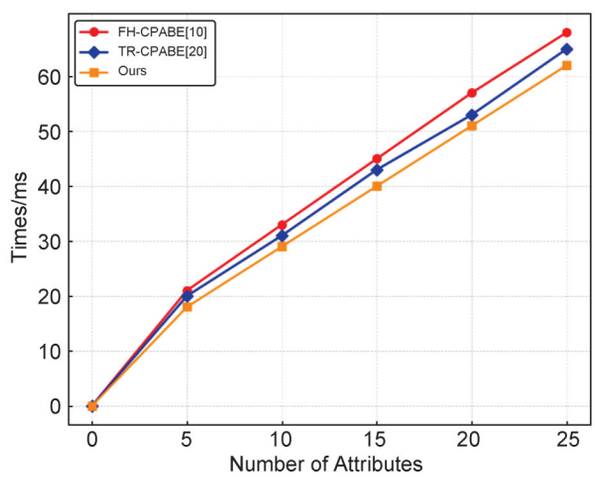

图5 授权中心密钥生成时间开销

Fig. 5 Time costs of CA keygeneration

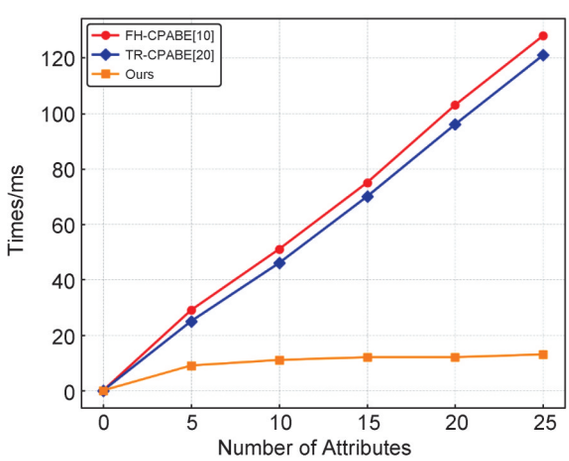

图6 数据拥有者加密时间开销

Fig. 6 Time costs of DO encryption

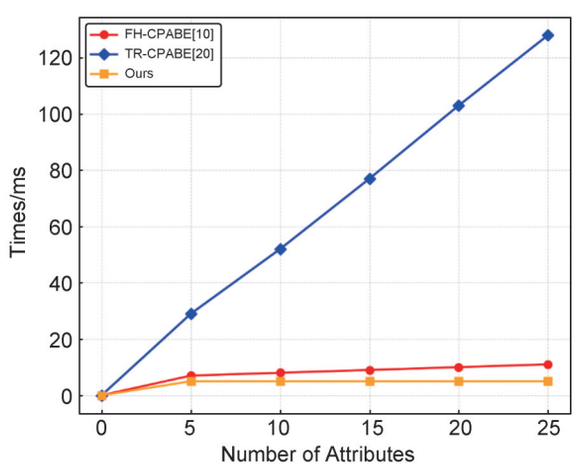

图7 数据用户解密时间开销

Fig. 7 Time costs of DU decryption

综上所述,本方案兼并了文献[20]TR-CPABE和文献[10]FH-CPABE的优点,功能更丰富,实用性更强,并且在加密和解密阶段所消耗时间达到了常量级。整体来看,本方案的表现力更强。

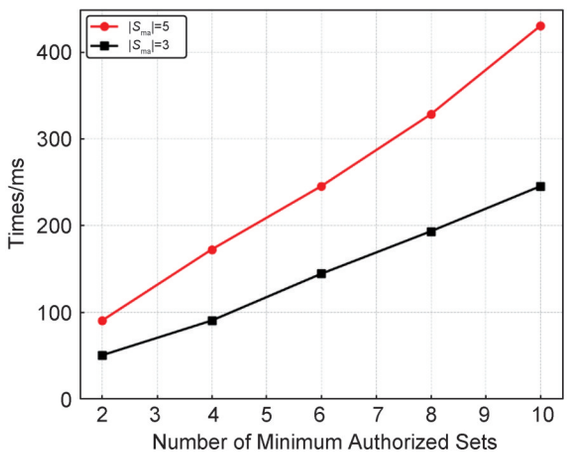

图 8 PolicyHide算法运行的时间开销

Fig. 8 Runtime costs of the PolicyHide

6 结论

本文提出了一个具有策略完全隐藏的属性基加密方案,有效地解决了医疗系统中数据所有者的隐私和数据安全性问题,在保护用户隐私的基础上增加了追踪和撤销功能,使方案更具有可用性。方案使用PSI技术实现了策略的完全隐藏,使用在线/离线技术提高了算法的加密速度,采用外包解密技术,将大部分密文给医疗云服务器计算,从而降低用户的计算开销。此外,本方案可以根据用户的解密密钥追踪用户,使用与用户信息相关联的二叉树的叶节点值来撤销用户。最后通过困难性假设证明了该方案的安全性。

参考文献:

[1] WANG C G, BI Z M, XU L D. IoT and Cloud Computing in Automation of Assembly Modeling Systems[J]. *IEEE Trans Ind Inform*, 2014, **10**(2): 1426-1434. DOI: 10.1109/TII.2014.2300346.

[2] XU B Y, XU L D, CAI H M, *et al*. The Design of an M-health Monitoring System Based on a Cloud Computing Platform[J]. *Enterp Inf Syst*, 2017, **11**(1): 17-36. DOI: 10.1080/17517575.2015.1053416.

[3] SAHAI A, WATERS B. Fuzzy Identity-based Encryption [C]//Proceedings of the 24th annual international conference on Theory and Applications of Cryptographic Techniques. New York: ACM, 2005: 457-473. DOI: 10.1007/11426639_27.

[4] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy Attribute-based Encryption[C]//2007 IEEE Symposium on Security and Privacy (SP '07). New York: IEEE, 2007: 321-334. DOI: 10.1109/SP.2007.11.

[5] 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, 2006: 89-98. DOI: 10.1145/1180405.1180418.

[6] NISHIDE T, YONEYAMA K, OHTA K. Attribute-based Encryption with Partially Hidden Encryptor-specified Access Structures[C]//Proceedings of the 6th international conference on Applied cryptography and network security. New York: ACM, 2008: 111-129. DOI: 10.5555/1788857.1788864.

[7] ZHANG Y H, CHEN X F, LI J, *et al*. Anonymous Attribute-based Encryption Supporting Efficient Decryption Test[C]//Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security. New York: ACM, 2013: 511-516. DOI: 10.1145/2484313.2484381.

[8] YANG K, HAN Q, LI H, *et al*. An Efficient and Fine-grained Big Data Access Control Scheme with Privacy-preserving Policy[J]. *IEEE Internet Things J*, 2017, **4**(2): 563-571. DOI: 10.1109/JIOT.2016.2571718.

[9] ZHANG Z Q, ZHANG J B, YUAN Y L, *et al*. An Expressive Fully Policy-hidden Ciphertext Policy Attribute-based Encryption Scheme with Credible Verification Based on Blockchain[J]. *IEEE Internet Things J*, 2022, **9**(11): 8681-8692. DOI: 10.1109/JIOT.2021.3117378.

[10] YANG L, LI C, CHENG Y T, *et al*. Achieving Privacy-preserving Sensitive Attributes for Large Universe

Based on Private Set Intersection[J]. *Inf Sci*, 2022, **582**: 529−546. DOI: 10.1016/j.ins.2021.09.034.

[11] XUE J, SHI L, ZHANG W, *et al*. Poly-ABE: A Traceable and Revocable Fully Hidden Policy CP-ABE Scheme for Integrated Demand Response in Multi-Energy Systems[J]. *J Syst Architect*, 2023, **143**: 102982. DOI: 10.1016/j.sysarc.2023.102982.

[12] LUO C, SHI J, XIE M, *et al*. A Lightweight Access Control Scheme Supporting Policy Hidden Based on Path Bloom Filter[C]//International Conference on Information Security and Cryptology. Singapore: Springer Nature Singapore, 2023: 433-451. DOI: 10.1007/978-981-97-0942-7_22.

[13] LIU Z, CAO Z F, WONG D S. White-box Traceable Ciphertext-policy Attribute-based Encryption Supporting any Monotone Access Structures[J]. *IEEE Trans Inf Forensics Secur*, 2013, **8**(1): 76−88. DOI: 10.1109/TIFS.2012.2223683.

[14] NING J T, DONG X L, CAO Z F, *et al*. White-box Traceable Ciphertext-policy Attribute-based Encryption Supporting Flexible Attributes[J]. *IEEE Trans Inf Forensics Secur*, 2015, **10**(6): 1274−1288. DOI: 10.1109/TIFS.2015.2405905.

[15] NING J T, CAO Z F, DONG X L, *et al*. Large Universe Ciphertext-policy Attribute-based Encryption with White-box Traceability[C]//Computer Security-ESORICS 2014. New York: ACM,: 55−72. DOI: 10.1007/978-3-319-11212-1_4.

[16] NING J T, CAO Z F, DONG X L, *et al*. White-box Traceable CP-ABE for Cloud Storage Service: How to Catch People Leaking Their Access Credentials Effectively [J]. *IEEE Trans Dependable Secure Comput*, 2018, **15**(5): 883−897. DOI: 10.1109/TDSC.2016.2608343.

[17] LIU Z H, DUAN S H, ZHOU P L, *et al*. Traceable-then-revocable Ciphertext-policy Attribute-based Encryption Scheme[J]. *Future Gener Comput Syst*, 2019, **93**(C): 903−913. DOI: 10.1016/j.future.2017.09.045.

[18] WANG S P, GUO K K, ZHANG Y L. Traceable Ciphertext-policy Attribute-based Encryption Scheme with Attribute Level User Revocation for Cloud Storage [J]. *PLoS One*, 2018, **13**(9): e0203225. DOI: 10.1371/journal.pone.0203225.

[19] LIAN H J, WANG G B, WANG Q X. Fully Secure Traceable and Revocable-storage Attribute-based Encryption with Short Update Keys via Subset Difference Method[C]//2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC). New York: IEEE, 2018: 1−8. DOI: 10.1109/SSIC.2018.8556734.

[20] 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 Trans Dependable Secure Comput*, 2022, **19**(1): 316−327. DOI: 10.1109/TDSC.2020.2977646.

[21] LIU Z C, JIANG Z L, WANG X, *et al*. Practical Attribute-based Encryption: Outsourcing Decryption, Attribute Revocation and Policy Updating[J]. *J Netw Comput Appl*, 2018, **108**: 112−123. DOI: 10.1016/j.jnca.2018.01.016.

[22] CUI H, WAN Z G, WEI X L, *et al*. Pay as you Decrypt: Decryption Outsourcing for Functional Encryption Using Blockchain[J]. *IEEE Trans Inf Forensics Secur*, 2020, **15**: 3227−3238. DOI: 10.1109/TIFS.2020.2973864.

[23] GREEN M, HOHENBERGER S, WATERS B. Outsourcing the Decryption of ABE Ciphertexts[C]//Proceedings of the 20th USENIX conference on Security. New York: ACM, 2011: 34. DOI: 10.5555/2028067.2028101.

[24] LI J, CHEN X F, LI J W, *et al*. Fine-grained Access Control System Based on Outsourced Attribute-based Encryption[C]//European Symposium on Research in Computer Security. Berlin, Heidelberg: Springer, 2013: 592−609.10.1007/978−3−642−40203−6_33

[25] HOHENBERGER S, WATERS B. Online/Offline Attribute-based Encryption[C]//International Workshop on Public Key Cryptography. Berlin, Heidelberg: Springer, 2014: 293−310.10.1007/978−3−642−54631−0_17

[26] DATTA P, DUTTA R, MUKHOPADHYAY S. Fully Secure Online/Offline Predicate and Attribute-based Encryption[C]//International Conference on Information Security Practice and Experience. Cham: Springer, 2015: 331−345.10.1007/978−3−319−17533−1_23

[27] AKINYELE J A, GARMAN C, MIERS I, *et al*. Charm: a framework for rapidly prototyping cryptosystems[J]. *J Cryptogr Eng*, 2013, **3**: 111−128. DOI: 10.1007/s13389-013-0057-3.