https://crad.ict.ac.cn
63(3): 735−751, 2026

数据空间中可比较属性的数据访问控制方案

余增文[1,3,4] 张嘉伟[2] 姜 奇[2,4] 杨 力[1,4] 方 志[3,4] 史润方[3]
[1](西安电子科技大学计算机科学与技术学院 西安 710071)
[2](西安电子科技大学网络与信息安全学院 西安 710071)
[3](北京计算机技术及应用研究所 北京 100854)
[4](大数据与决策实验室(国防科技大学) 长沙 410073)
(yuzengwen@stu.xidian.edu.cn)

Data Access Control Scheme with Comparable Attribute for Dataspace

Yu Zengwen[1,3,4], Zhang Jiawei[2], Jiang Qi[2,4], Yang Li[1,4], Fang Zhi[3,4], and Shi Runfang[3]
[1](*School of Computer Science and Technology*, *Xidian University*, *Xi'an* 710071)
[2](*School of Cyber Engineering*, *Xidian University*, *Xi'an* 710071)
[3](*Beijing Institute of Computer Technology and Application*, *Beijing* 100854)
[4](*Laboratory for Big Data and Decision* (*National University of Defense Technology*), *Changsha* 410073)

Abstract Dataspace is an important infrastructure for achieving effective data sharing and circulation. However, problems such as privacy leakage, data theft, and illegal abuse during the data sharing process bring big challenges to the implementation of industry dataspaces. Attribute-based encryption (ABE) can ensure the confidentiality and fine-grained access control of shared data, but there are still many problems when directly applied to dataspaces. For example, traditional ABE schemes have high computational overhead in user revocation, which cannot meet performance requirements if a lot of dynamic users join or leave the dataspace. Besides, many industry dataspaces need to exert flexible access control on shared data based on user attribute comparison and access time, and verify the decryption results. To overcome these problems, we propose a data access control approach based on comparable attributes in dataspaces, which realizes flexible and efficient user revocation to ensure forward security. The approach can make flexible decisions on access behavior based on access time and attribute comparison, and also support verification of the decryption process. Through formal security analysis, the approach has semantic security under chosen plaintext attacks. In addition, a large number of experimental analyses show that the approach is suitable for actual data sharing applications in dataspaces.

Key words dataspace; ABE; time-based access control; puncturable encryption; comparable attribute

摘 要 数据空间是实现数据有效共享和流通的重要基础设施。但是,数据共享过程中面临的隐私泄露、数据窃取和非法滥用等问题给行业数据空间落地带来巨大挑战。属性基加密能够确保共享数据的机密性和细粒度访问控制,但直接将其应用于数据空间还存在诸多问题。首先,传统属性基加密方案在用户撤销时计算开销较大,无法满足数据空间中大量动态用户加入或退出的场景。其次,许多行业数据空间

收稿日期: 2025-06-06; **修回日期**: 2025-10-27
基金项目: 国家自然科学基金项目(U24A20243, 62472337, 62125205, 62372350, 62572377); 中央高校基本科研业务费专项资金(ZYTS25066); 陕西省自然科学基础研究计划项目(2024JC-YBMS-544, 2025JC-JCQN-084)
This work was supported by the National Natural Science Foundation of China (U24A20243, 62472337, 62125205, 62372350, 62572377), the Fundamental Research Funds for the Central Universities (ZYTS25066), and the Natural Science Basic Research Program of Shaanxi Province (2024JC-YBMS-544, 2025JC-JCQN-084).
通信作者: 张嘉伟(jiaweizhang@xidian.edu.cn)

需要根据用户属性比较和访问时间对其共享数据进行灵活的访问控制,并且能够对解密结果进行验证。为解决上述问题,提出一种数据空间中基于可比较属性的数据访问控制方案,实现了灵活高效的用户撤销以确保前向安全性,能够根据访问时间和属性比较来对其访问行为进行灵活决策,并支持对解密过程的验证。经过形式化安全分析,所提方案在选择明文攻击下具有语义安全性。大量的实验分析表明所提方案适用于数据空间中数据的共享应用。

关键词 数据空间;属性基加密;基于时间访问控制;可穿刺加密;可比较属性

中图法分类号 TP311.13; TP309

DOI: 10.7544/issn1000-1239.202550411 **CSTR:** 32373.14.issn1000-1239.202550411

随着新一轮数字化转型浪潮的到来,5G、云计算、人工智能和物联网等技术得到广泛应用,推动了众多产业的深入变革和数字经济的蓬勃发展[1]。数据作为数字经济时代的关键生产要素,其价值日益凸显,已成为全球经济增长和价值创造的重要动力源泉[2]。数据的爆炸式增长和流通利用需求为数据组织管理、访问控制、挖掘分析等带来了新的挑战[3]。国家《"十四五"数字经济发展规划》①中明确提出到2025年初步建立数据要素市场体系,将数据流通作为数据要素市场体系构建的关键环节。数据空间作为一种新的数据组织管理模式[4],通过保护数据主权、确保数据安全、推动数据跨域流通,聚焦数据价值的挖掘分析和二次利用,促进数据在行业领域内统一标准和互操作,为实现数据要素价值有序释放提供了有效的解决方案,已成为数字经济时代的重要基础设施[5],数据空间架构图如图1所示。

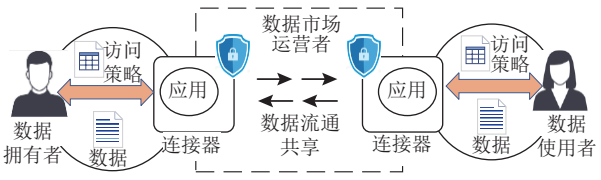


Fig. 1 Dataspace architecture diagram

图1 数据空间架构图

在数据空间中,数据拥有者与数据使用者共享数据的过程中,往往伴随着数据被窃取、篡改以及滥用的风险,从而导致数据主权丧失。数据访问控制[6-7]通过统一管理各参与主体数字身份以及数据访问策略,能够实现数据共享时的精准投递和访问管理,已成为数据空间中实现数据流通与可信共享的关键技术之一。2024年12月,美国电气电子工程师学会(Institute of Electrical and Electronics Engineers, IEEE)发布了可信数据空间系统架构(trusted data matrix system architecture, TDMSA)国际标准,明确将数据访问控制作为其功能视图、业务视图的重要组成部分[8]。

目前,各行业领域数据空间在实现数据机密性和访问控制时大量采用基于密文策略属性加密(ciphertext-policy attribute based encryption, CP-ABE)技术[9-15]。即数据提供者为其数据指定具体的访问策略并进行数据加密,只有权限符合访问策略的数据使用者才能够解密得到正确的明文数据。尽管CP-ABE能够对密文数据实现灵活的细粒度访问控制,但直接将其应用于数据空间实现安全的数据共享还面临许多问题。

首先,数据空间的数据使用者一般具有高度动态性,大量参与主体随时可能加入或离开,给数据访问控制造成困难。例如,在医疗数据空间中,医院将其健康医疗数据共享给用户 U_1 和 U_2。当 U_2 离开数据空间后,此时不应再拥有访问医院共享数据的权限。解决该问题的直接方法是使用可撤销CP-ABE来实现数据的动态访问控制。然而,当前大多数可撤销CP-ABE方案[16-19]要么需要大量计算和存储开销来管理用户,要么需要承担额外的通信开销且无法保证前向安全性,难以实现安全、高效和灵活的用户撤销。

其次,在许多行业数据空间中,共享数据的访问决策不再仅仅依赖于用户权限是否满足访问策略,还需要结合多种因素来对数据的访问进行自适应控制。例如,患者就医产生的医疗数据,需要被主治医师在较早的时间访问从而进行分析和诊断,再由医疗科研机构在之后的时间进行访问。同时,患者的数据需要由级别高于主治医师的副主任医师访问,该数据空间的数据访问控制需要根据用户的可比较属性和访问时间顺序进行访问决策。传统的CP-ABE方案大多无法根据时间顺序或者属性范围比较

① https://www.gov.cn/zhengce/content/2022-01/12/content_5667817.htm

来进行访问决策。虽然，Hong 等人[20]提出基于时间的 CP-ABE 方案，根据访问时间进行数据访问控制，Xue 等人[21]基于 0-1 编码机制设计了属性可比较的 CP-ABE 方案。但是，当前这些方案无法同时基于时序和属性比较实现对数据的访问控制。

为解决上述问题，本文提出一种数据空间中基于可比较属性的数据访问控制（comparable attribute based data access control, CADAC）方案。本文主要贡献体现在 3 个方面：

1）可验证的动态数据访问控制。本文设计了一种高效的可穿刺 CP-ABE 方法，该方法通过在 CP-ABE 中融入可穿刺加密技术对数据使用者解密指定密文的能力进行动态访问控制，确保前向安全性，即被撤销的数据使用者不再具有解密之前密文的能力。同时，方案支持当一部分数据使用者被撤销访问权限后，不再需要更新密文并给其他数据使用者分配新密钥，从而降低撤销过程中的计算和通信开销。此外，该方法结合 Pedersen 承诺实现了对解密结果的正确性验证。

2）基于可比较属性的访问策略。本文设计了一种基于时间的可比较访问策略。不同于传统 CP-ABE 方案只能根据用户属性集与策略属性的精确匹配或将时间因素嵌入密文来实现基于时间的访问决策方式，本文基于时间和属性比较实现了更加灵活的数据访问控制决策，并结合时释性加密和 0-1 编码对共享数据进行加密，满足了数据空间中对访问时序敏感和更细粒度的安全访问控制要求。

3）通过严格的安全性分析，证明 CADAC 方案在随机预言机模型上的选择明文攻击（chosen plaintext attack, CPA）的安全性。同时，大量的仿真实验性能评估表明该方案能够在实现更灵活的数据访问控制的同时具有安全性、高效性和实用性，具备应用于数据空间中的数据共享访问控制的能力。

1 相关工作

数据空间的概念由 Franklin 等人[22]于 2005 年提出，早期被认为是一种异构数据的组织管理和关联集成模式。直到 2016 年德国提出了工业数据空间[23]，此后逐渐被当作一种跨行业、跨领域的数据共享平台，或一个由治理框架定义的分布式系统，旨在创建一个安全可信的数据流通环境。在数据空间治理和技术体系中，访问控制技术已经成为确保数据安全流通和利用的关键基石。

目前，属性基加密已成为数据空间实现数据访问控制最有发展前景的技术，国内外学者提出了很多属性基加密方案来满足数据空间的数据拥有者对其数据的控制需求。Sahai 等人[24]提出了属性基加密机制以实现数据访问控制。之后，Bethencourt 等人[25]进一步提出 CP-ABE 机制，从而能够让数据拥有者灵活地对其密文指定访问策略。然而，对数据空间中数据的访问控制还需要考虑更多的实际场景需求。

为了基于时间进行数据访问控制，Androulaki 等人[26]基于 ElGamal 和标签加密实现了基于位置和时间的访问控制。但是，该方案无法实现针对数据的细粒度访问控制，其时间尺度和计算开销较大.Fan 等人[27]则结合谓词加密和 Rivest 等人[28]提出的时释性加密（time-release encryption, TRE）方法，设计了一种云计算环境下定时释放权限的数据访问控制方案。然而，该方案计算复杂度较高，也无法根据属性进行灵活的权限控制。Hong 等人[20]基于 CP-ABE 和 TRE 提出了一个时释性数据访问控制方案。通过在 CP-ABE 的访问策略中嵌入时间属性，以定时释放陷门的方式实现对数据的访问权限管理。只有当可信时间代理在某个时间点释放访问权限后，属性集合满足条件的授权用户才能够对数据进行访问。然而，该方案在性能上仍然有较大提升空间。

此外，基于属性比较的访问控制在数据空间的数据共享中也是需要考虑的重要因素。在传统的 CP-ABE 方案中，属性集合与访问策略的属性值比较操作只有“=”。然而，在操作系统和数据库等系统中，需要根据属性与访问策略之间的各种关系（如“=, <, >”）来进行访问控制。Attrapadung 等人[29]在布尔表达式基础上提出了一个基于属性范围的 CP-ABE 方案。然而，该方案拥有较高的访问策略复杂度。Xue 等人[21]基于百万富翁问题中的 0-1 编码技术提出了一个属性可比较的 CP-ABE 方案，通过将属性转换为 0-1 编码实现属性的灵活比较功能。在此基础上，Miao 等人[30]提出了属性可比较的基于属性的可搜索加密方案，在实现属性可比较访问控制的同时完成数据密文检索功能。但这些方案无法实现动态用户撤销。

在数据空间中实现数据的细粒度共享访问时，大规模灵活高效的用户撤销一直是 CP-ABE 方案长期面临的问题。学者们提出了大量用户可撤销 CP-ABE 方案。根据撤销执行者的不同，现有的用户撤销方案可分为直接撤销[18,31-35]和间接撤销[36-39]两类。直接撤销通过数据拥有者更新其所维护的撤销列表以及对应密文实现快速的直接用户撤销。然而，

数据拥有者需要承担较重的计算负担。间接撤销则通过权威机构与未撤销用户的交互更新其解密密钥，利用代理重加密更新密文实现灵活的用户间接撤销，但该方法会增加系统的复杂性和通信开销。近年来，有研究人员将 CP-ABE 与可穿刺加密结合构建可撤销 CP-ABE 方案[17,40-41]，不仅保留了基于属性基加密的访问控制能力，还能够确保前向安全性。同时，为了确保云端在用户撤销和解密过程中的不诚实行为，Miao 等人[42]提出了可验证的 CP-ABE 方案，利用可验证标签技术实现对于云端返回数据的正确性验证。而 Chen 等人[43]则提出可验证可撤销的 CP-ABE 方案。

然而，上述方案无法满足数据空间中多种因素叠加的灵活数据共享访问控制需求。因此，本文提出了 CADAC 方案。通过与相关方案的对比，CADAC 除了能够实现数据机密性和细粒度访问控制外，还支持面向数据空间中动态用户基于时间和属性比较的数据访问控制，确保数据拥有者能够对数据使用者的访问能力进行高效灵活的控制和撤销。本文所提 CADAC 方案和相关方案的对比结果见表 1。

Table 1 Function Comparison

表 1 功能对比

方案	细粒度访问控制	用户撤销	属性比较	访问时间	可验证性
文献 [18]	√	×	×	×	×
文献 [21]	√	×	√	×	×
文献 [26]	×	×	×	√	×
文献 [27]	√	×	×	√	×
文献 [28]	√	×	×	√	×
文献 [30]	√	×	√	×	×
文献 [31]	×	√	×	×	×
文献 [32]	√	√	×	×	×
文献 [33]	√	√	×	×	√
文献 [34]	√	√	×	×	×
文献 [35]	√	√	×	×	×
文献 [36]	√	√	×	×	×
文献 [37]	√	√	×	×	√
文献 [38]	√	√	×	×	×
文献 [39]	√	√	×	×	×
文献 [42]	√	×	×	×	√
CADAC（本文）	√	√	√	√	√

由表 1 可知，本文 CADAC 方案支持将属性比较、访问时间、可验证性以及用户撤销等多个因素结合，能够满足数据空间中数据拥有者对多种数据共享场景下灵活、高效的细粒度访问控制要求，且时间开销优于其他大部分方案。

2 基础知识

本节主要介绍本文方案 CADAC 所使用的符号和相关基础知识。

2.1 符号列表

令$\mathbb{N}$表示自然数集合。对于 $n\in\mathbb{N}$，$n\in\{1,2,\cdots,n\}$ 的集合。如果 x 和 y 分别是 2 个字符串，那么 $x\|y$ 代表 x 与 y 的串联。本文方案的常用符号见表 2。

Table 2 Notation Descriptions

表 2 符号说明

符号	说明
PK_K, MK_K	系统公钥和主密钥
SPK, SMK	数据市场的签名公钥和签名私钥
T_a	访问策略
DK_u	数据使用者的解密密钥
TS_x	节点 x 上未暴露状态的陷门
TS'_x	节点 x 上处于暴露状态的陷门
TK_t	时间令牌
F_T	统一时间格式

2.2 CP-ABE

密文策略属性基加密，即 CP-ABE[24]，是属性基加密的一个重要类别，允许数据拥有者定义访问控制策略，只有满足特定属性的用户才能解密数据。典型的 CP-ABE 方案主要包括 4 个算法：

1）初始化。输入安全参数 λ 和属性全集 U，输出系统主密钥 MK 和公共参数 PK。

2）密钥生成。输入系统主密钥 MK 和一组属性集，输出与输入属性集相关联的安全密钥 SK。

3）加密。输入公共参数 PK、消息 M 和对某些属性的访问策略 T_a，输出密文 CT。

4）解密。输入安全密钥 SK 和密文 CT，输出消息 M 或解密失败符号 $\perp$。

2.3 可穿刺加密

可穿刺加密[38]能够实现非交互的前向安全性，通过输入当前密钥和一个标签 t，计算得到一个新的密钥来解密未嵌入标签 t 的密文，确保密文的前向安全性。典型的可穿刺加密方案由 4 个算法组成：

1）密钥生成。$KeyGen(l,d)\rightarrow(pk,sk_0)$，输入安全参数 l 和密文最大的标签数 d，输出公钥 pk 和 sk_0。

2）加密。$Enc(pk, M,t_1,t_2,\cdots,t_d)\rightarrow(CT)$，输入公钥 pk、明文 M 以及标签集 $\{t_1,t_2,\cdots,t_d\}$，输出密文 CT。

3）穿刺。$Puncture(pk,sk_{i-1},t)\rightarrow(sk_i)$，输入公钥 pk、旧的密钥 sk_{i-1} 和标签 t，输出一个新的密钥 sk_i。

4）解密。$Dec(pk,sk_i, CT,t_1,t_2,\cdots,t_d)\rightarrow(M,\perp)$，输入公钥 pk、私钥 sk_i 和密文 CT 以及标签集 $\{t_1,t_2,\cdots,t_d\}$。解密成功，输出明文 M；解密失败，输出 $\perp$。

2.4 0-1 编码

0-1 编码[17]最初是为了解决百万富翁问题而提出的。设 $S=s_ns_{n-1}\cdots s_1\in\{0,1\}^n$ 是一个长度为 n 的二进制字符串，则 S 的 0 编码和 1 编码定义如式（1）所示。

$$\begin{aligned}S_s^0&=\{s_ns_{n-1}\cdots s_{i+1}1|s_i=0,1\leqslant i\leqslant n\},\\S_s^1&=\{s_ns_{n-1}\cdots s_i|s_i=1,1\leqslant i\leqslant n\}。\end{aligned}\tag{1}$$

具体地，S 的 1 编码是其所有奇数前缀子串的集合，0 编码是其所有修改后的偶数前缀子串的集合，其中最低有效位从 0 翻转为 1。

为了比较 2 个整数 x 和 y，用 1 编码表示 x，用 0 编码表示 y，当且仅当 x 的 1 编码和 y 的 0 编码中存在公共元素时，则 $x>y$。例如，x=6=110_2，y=2=010_2，则 x 的 1 编码是 $\{1, 11\}$，y 的 0 编码是 $\{1, 011\}$，二者有共同元素 1，因此，$x>y$。如果 x=2=010_2，y=6=110_2，则 x 的 1 编码是 $\{01\}$，y 的 0 编码是 $\{111\}$，二者没有共同元素，则 $x\leqslant y$。

2.5 密码学原语和复杂性问题假设

1）双线性映射[13]。设 G_0,G_1 是 2 个阶为素数 p 的乘法循环群，g 是群 G_0 的一个生成元。若映射 $\hat{e}:G_0\times G_0\rightarrow G_T$ 满足如下条件：

① 对于任意 $a,b\in\mathbb{Z}_p$，$v,w\in G_0$，$\hat{e}\left(v^a,w^b\right)=\hat{e}(v,w)^{ab}$；

② $\hat{e}(g,g)\neq 1_{G_1}$；

③ 存在一个有效的算法计算 $\hat{e}(v,w)$，则 $\hat{e}$ 被称为双线性映射。

2）判定性双线性 DH 假设（decisional bilinear Diffie-Hellman, DBDH）[39]。假设存在一个随机多项式时间（probabilistic polynomial-time, PPT）算法 A，给定阶为素数 p 的乘法群 G_0 和 G_1 以及 1 个双线性映射 $\hat{e}:G_0\times G_0\rightarrow G_1$。随机选择生成元 $g\in G_0$ 和 $a,b,c\in\mathbb{Z}_p$，将 $g,g^a,g^b,g^c,\hat{e}(g,g)^{abc}$ 和 $T\in G_1$ 发送给 A，判定 T 是否等于 $\hat{e}(g,g)^{abc}$。若相等，则输出 1；否则输出 0。

定义算法 A 解决上述问题的优势如式（2）所示。

$$\begin{aligned}Adv^{\mathrm{DBDH}}=&Pr\left[A\left(g,g^a,g^b,g^c,\hat{e}(g,g)^{abc}\right)=1\right]-\\&Pr\left[A\left(g,g^a,g^b,g^c,T\right)=1\right]。\end{aligned}\tag{2}$$

如果任何多项式算法 A 无法以一个不可忽略的优势解决上述问题，则 DBDH 假设成立。

3 方案模型

本节将展示 CADAC 的系统模型、威胁模型、设计目标、系统定义和安全模型。

3.1 系统模型

CADAC 的系统模型主要由 4 个实体组成，即密钥生成中心（key generation center, KGC）、数据拥有者（data owner, DO）、数据使用者（data user, DU）和数据市场（data marketplace, DM），如图 2 所示。

1）KGC。该实体负责管理整个系统的密钥及生成时间令牌，包括为系统生成公共参数，为 DU 生成解密密钥，而且充当时间代理完成时间令牌释放。

2）DO。该实体负责对其拥有的数据定义访问策略和穿刺策略，并进行加密外包，然后将数据密文发送至 DM 进行共享，以实现数据机密性和细粒度访问控制。

3）DU。该实体根据需求向 DM 发送访问请求并下载相应数据密文。当且仅当属性集合满足访问策略，访问时间符合时间令牌释放时间，且其标签不匹配密文穿刺策略时，DU 才能够解密数据密文得到明文。

4）DM。该实体负责对数据空间的数据资产进行共享和流通管理。一方面负责数据密文的外包存储并管理数据的访问、流通和共享；另一方面在收到时间令牌后负责访问权限释放，并在 DO 接收到穿刺策略时刺穿密文。

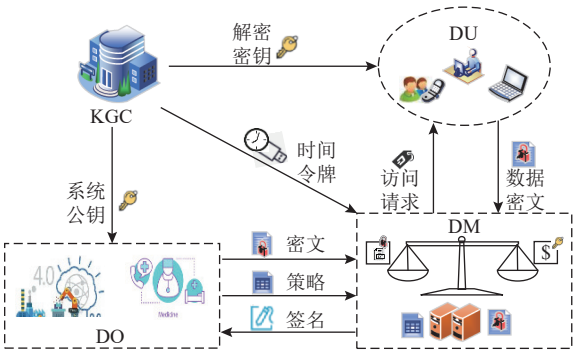


Fig. 2 System model of CADAC

图 2 CADAC 系统模型

3.2 威胁模型

在 CADAC 的系统模型中，KGC 被认为是可信的第三方，KGC 和 DO 将分别诚实地执行密钥生成和数据资产加密算法。KGC 无法获取 DM 的密文。DM 被认为是半诚实的，在执行预定协议并得到预定

执行结果的同时,试图从协议执行过程中获取或者推断隐私信息。DU 被认为是半诚实的,可能会试图通过合谋攻击获取未经授权的数据资产。同时,数据空间中的数据资产在应用中往往需要根据 DU 的访问时间进行访问控制。

3.3 方案设计目标

CADAC 方案的目标在于针对数据空间中数据共享所面临的安全问题,设计一种轻量级多因素数据访问控制方案,支持在数据空间应用中进行灵活安全的用户动态性配置。总体设计目标为:

1)基于可比较属性的访问控制。对于数据空间中的共享数据密文,只有拥有足够权限的 DU 才能够解密。对于未授权的 DU,即使通过合谋攻击也无法访问共享数据,而对于已授权的 DU,如果其访问时间不满足共享数据的访问时间策略,也无法访问数据。

2)数据机密性和一致性。由于 DO 需要将其数据以密文形式存储在 DM 中,数据使用权和所有权分离。为防止隐私和敏感信息泄露,DU 在数据解密过程能够被验证以防止 DM 伪造和攻击者篡改。

3)前向安全的灵活用户撤销。需要支持在数据共享过程中灵活、精确地撤销用户的访问权限。同时,确保数据的前向安全性,即被撤销的用户无法解密之前的密文,即使其属性和访问时间满足访问策略。

3.4 系统定义

CADAC 由 7 个算法构成,包括:*Setup*, *KeyGen*, *Encrypt*, *TokenGen*, *TrapdoorExposure*, *Puncture*, *Decrypt*。下面给出方案的形式化定义:

1)$Setup(1^{\lambda},d)\rightarrow(PK_K,MK_K),(SPK,SMK)$。在该算法中,输入安全参数 1^{λ} 和标签数 d,输出为系统公钥 PK_K 和系统主密钥 MK_K,以及 DM 签名公钥 SPK 和私钥 SMK。

2)$KeyGen(S,PK_K,MK_K,T)\rightarrow(DK_u)$。该算法用于生成 DU 解密密钥。输入系统公钥 PK_K 和私钥 MK_K,以及 DU 的属性集合 S 和一组标签 $T=\{l_1,l_2,\cdots,l_d\}$,KGC 生成解密密钥 DK_u。

3)$Encrypt(T_a,M,PK_K)\rightarrow(CT)$。在该算法中,输入访问策略 T_a、消息 M 和系统公钥 PK_K 后,DO 生成消息 M 对应的密文 CT。

4)$TokenGen(t,MK_K)\rightarrow(TK_t)$。在该算法中,输入系统主密钥和时间点 $t\in F_T$,KGC 生成相应的时间令牌 TK_t,并将其在系统中公开发布。

5)$TrapdoorExposure(TS_x,TK_t)\rightarrow(TS'_x)$。在该算法中,输入时间陷门 TS_x 及其相关的时间令牌 TK_t,DM 暴露陷门为 TS'_x。

6)$Puncture(PK_K,PP_K,SMK,CT)\rightarrow(CT',\zeta)$。在该算法中,输入系统公钥 PK_K、穿刺策略 PP_K、DM 签名私钥 SMK 和密文 CT 后,DM 对密文 CT 进行穿刺,输出穿刺后的密文 CT' 和穿刺结果签名 ζ。

7)$Decrypt(CT,DK_u,PK_K)\rightarrow(M\ \mathrm{OR}\ \perp)$。在该算法中,输入密文 CT,DU 解密密钥 DK_u 和系统公钥 PK_K,DU 解密得到明文 M 或 $\perp$。

3.5 安全模型

假设 CADAC 存在 3 种类型的敌手。类型 1:属性集合不满足访问策略 A^*,虽然已经到达了权限释放时间,但是其权限不满足访问策略。类型 2:属性集合满足访问策略 A^*,但是其访问时间并未达到相应的权限释放时间。类型 3:属性集合满足挑战访问策略 A^* 和访问时间 t_{A^*},且访问时间达到相应的权限释放时间。其中,类型 1 和类型 2 为基于时间的访问控制类型选手,类型 3 是基于穿刺策略类型的敌手。本节将以安全游戏的方式构建安全模型。

1)安全游戏 1。主要针对类型 1 和类型 2 敌手,该安全游戏的参与者包括挑战者$\mathbb{C}$和敌手$\mathbb{A}$。挑战者$\mathbb{C}$根据方案执行指定算法并接受敌手$\mathbb{A}$的挑战,即敌手$\mathbb{A}$能够申请询问挑战者$\mathbb{C}$的属性集合、解密密钥等信息,并根据这些先验知识对挑战者$\mathbb{C}$发起挑战。当收到挑战者$\mathbb{C}$对敌手$\mathbb{A}$挑战的响应后,敌手$\mathbb{A}$进行猜测,如果猜测成功,则敌手$\mathbb{A}$具备攻破方案的能力;否则,方案对于敌手$\mathbb{A}$来说是可区分的。形式化建模描述如下:

①系统建立。挑战者$\mathbb{C}$运行 *Setup* 算法,并将算法得到的系统公共参数交给敌手$\mathbb{A}$。

②询问 1。敌手$\mathbb{A}$适应性地向挑战者$\mathbb{C}$询问属性集合 S 对应的解密密钥,并声称访问时间 t_{A^*} 以及挑战访问策略 A^*。此时约定,属性集合 S 在时间 t_{A^*} 不满足策略 A^*。挑战者$\mathbb{C}$生成 S 对应的解密密钥以及一系列不晚于 t_{A^*} 的时间令牌,并将解密密钥和时间令牌交给敌手$\mathbb{A}$。

③挑战者应答。敌手$\mathbb{A}$提交 2 个等长消息 m_0 和 m_1 给挑战者$\mathbb{C}$。接着,挑战者$\mathbb{C}$抛掷随机硬币 $b\in\{0,1\}$,并用策略 A^* 加密消息 m_b 并将密文 CT_b 返回给敌手$\mathbb{A}$。

重复上述步骤扩充敌手私钥所对应的属性集合,并请求一个比 t_{A^*} 更迟的访问时间 t_B。然而,新的属性集合在 t_B 时依然不满足访问策略 A^*。

④猜测。敌手输出对 b 的猜测,记为 b'。

敌手$\mathbb{A}$在这个安全游戏中的优势定义如式(3)所示。

$$Adv = |Pr[b = b'] - 1/2|。 \quad (3)$$

定义 1. CADAC 方案在上述敌手模型下的机密性定义为对于所有 PPT 敌手在上述安全游戏中只能获得可忽略的优势。

2)安全游戏 2。针对类型 3 敌手，此时，敌手具有根据指定的访问策略和穿刺策略发起选择明文攻击挑战的能力。类似安全游戏 1，继续通过挑战者$\mathbb{C}$和敌手$\mathbb{A}$进行形式化建模描述。

①初始化。敌手$\mathbb{A}$提交一个挑战访问策略和穿刺策略对(A^*, PP_K)至挑战者$\mathbb{C}$。

②系统建立。挑战者$\mathbb{C}$运行 *Setup* 算法生成系统公钥和主密钥，并将公钥发送给敌手$\mathbb{A}$。

③询问 1。敌手$\mathbb{A}$适应性地向挑战者$\mathbb{C}$询问属性集合S和标签集合$T = (l_1, l_2, \cdots, l_d)$，其中，属性集合$S$和标签集合$T$与$(A^*, PP_K)$不匹配。挑战者$\mathbb{C}$计算解密密钥$DK_u$，并将其发送至敌手$\mathbb{A}$。

④挑战者应答。敌手$\mathbb{A}$提交 2 个等长消息m_0和m_1给挑战者$\mathbb{C}$。接着，挑战者$\mathbb{C}$随机选择$b \in \{0,1\}$，运行算法 $Encrypt(A^*, m_b, PK_K)$ 并将该算法输出的密文CT_b返回给敌手$\mathbb{A}$。

⑤询问 2。敌手$\mathbb{A}$重复询问 1。

⑥猜测。敌手$\mathbb{A}$输出对b的猜测b'，如果$b = b'$，则敌手$\mathbb{A}$赢得该安全游戏。其优势定义如式(4)所示。

$$Adv = |Pr[b = b'] - 1/2|。 \quad (4)$$

定义 2. 如果任意 PPT 敌手最多只能以 1 个可忽略的优势赢得上述安全游戏，则 CADAC 在选择明文攻击下是不可区分性安全的。

4 方案构造

本节将介绍 CADAC 的工作流程及具体构造。

4.1 工作流程

针对数据空间中大规模用户能实现高效可验证的灵活撤销，本文 CADAC 方案将可穿刺加密融入 CP-ABE，并结合 Pedersen 承诺进行设计和构造。具体地，DU 的密钥由大小不相关的访问属性集合和标签集合组成，并将 CP-ABE 和可穿刺加密进行关联，从而实现灵活的密钥穿刺。此外，在 CP-ABE 密文中，通过将嵌入可穿刺加密的密钥作为公共参数，在撤销某一 DU 对某个密文的解密能力时，DO 只需使用 1 组标签构造 1 个穿刺策略发送至 DM。DM 根据 De Morgan 定律将穿刺策略转换为访问策略，依此对密文进行穿刺，无需对密文本身进行重加密和更新操作，只需将 DU 密钥中的 1 组标签激活，即可实现用户撤销。例如，企业$\mathbb{E}$根据访问策略{“企业$\mathbb{E}$” AND {“用户”AND “$VIP > 1$”}}对其共享数据加密。数据使用者U_1的解密密钥中，属性集合为{“企业$\mathbb{E}$”，“用户”，“$VIP = 2$”}，标签集合设置为{“企业$\mathbb{E}$”，“用户”，“$ID=U_1$”}。如果企业$\mathbb{E}$要撤销用户U_1，可以使用相应的标签集合构造穿刺策略{“企业$\mathbb{E}$” AND “用户” AND “$ID=U_1$”}来穿刺密文。此时，U_1无法再次访问企业$\mathbb{E}$的共享数据。CADAC 方案整体工作流程包括 4 个阶段，即初始化、数据托管、数据访问和密文穿刺，如图 3 所示。

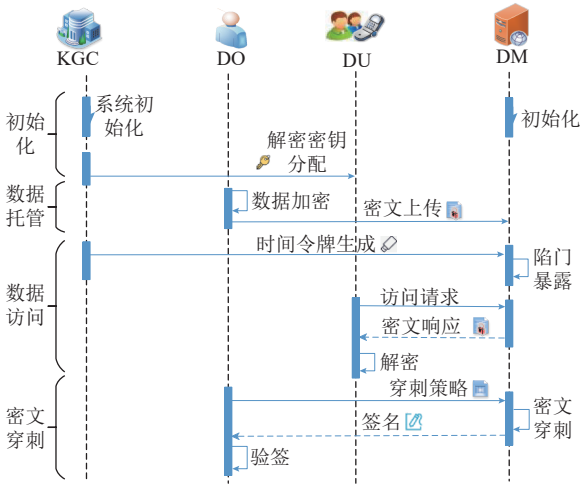


Fig. 3 Workflow of CADAC

图 3 CADAC 工作流程

1)初始化阶段。KGC 生成系统公钥和主密钥，为 DU 分发密钥。DM 生成其公私钥对。

2)数据托管阶段。DO 按照其数据运营托管需求，设定相应的数据访问策略，并根据该访问策略计算数据密文，并将该密文托管至 DM，以便其对 DU 提供共享、流通和运营等服务。

3)数据访问阶段。DU 根据其实际需求，向 DM 请求相关数据。DM 接到访问请求后，根据当前 DU 的属性集合判断是否满足访问策略并返回目标密文。为了实现基于时间的访问控制，KGC 周期性地向 DM 发布时间令牌，并由 DM 实现将相关密文的访问策略陷门暴露。

4)密文穿刺阶段。DO 根据上下文环境情况以及其需求变化，对其托管至 DM 的密文数据进行穿刺，以实现 DU 访问控制权限的更新。

4.2 具体构造

1)$Setup(1^\lambda, d) \rightarrow (PK_K, MK_K), (SPK, SMK)$。首先，KGC 生成 1 个双线性群，其包括 2 个阶为素数p的乘法循

环群G_0和G_1, 双线性映射$\hat{e}: G_0 \times G_0 \to G_1$, 和$G_0$的生成元$g$。此时, 定义2个抗碰撞哈希函数$H: \{0,1\}^* \to \mathbb{Z}_p, H_1: \{0,1\}^* \to G_0, H_2: G_1 \to \mathbb{Z}_p$, 属性全集$U=\{1,2,\cdots,n\}$和统一的时间格式$F_{\mathrm{T}}$, 以及标签$l_0$。标签$l_0$是唯一不会用到的标签, 用于标记穿刺前后的初始密钥是否一致。

其次, KGC随机选择$\tilde{a},\alpha,\beta,\gamma \in \mathbb{Z}_p$, 计算$g_1=g^{\tilde{a}}$, $g_2=g^{\beta}, f=g^{\gamma}$, 定义多项式$q(x)$, 其中, $q(0)=\beta$, $Q(x)=g^{q(x)}$。同时, KGC随机选择$u,v \in G_0$, 选择一个输出长度为$\mathcal{L}$的密钥导出函数$KDF1$。

最后, KGC保存系统主密钥MK_K=$(\tilde{a},\gamma,g^{\alpha})$, 计算并公开系统公钥$PK_K$=$(g,u,v,g_1=g^{\tilde{a}}, g_2=g^{\beta}, f=g^{\gamma}, \hat{e}(g,g)^{\alpha}, l_0, \mathcal{L}, KDF1, F_{\mathrm{T}}, H, H_1, H_2)$。同时, DM随机选择$\delta \in \mathbb{Z}_p$, 计算其签名公钥和私钥$SPK=g^{\delta}$, $SMK=\delta$。

2) $KeyGen(S, PK_K, MK_K, T) \to (DK_{\mathrm{u}})$。KGC随机选择$r,z \in \mathbb{Z}_p$, 根据DU的属性集合$S$及其标签集$T=\{l_1,l_2,\cdots,l_d\}$生成解密密钥$DK_{\mathrm{u}}$, 如式(5)所示。

$$DK_{\mathrm{u}}=\left(G^{(1)},G^{(2)},G_y^{(3)},G_i^{(4)}\right), \tag{5}$$

其中$G^{(1)}=g^{\alpha}g^{\tilde{a}r+\tilde{a}\beta}$, $G^{(2)}=g^{r}$, $\{G_y^{(3)}=h_y^{r}\}_{y\in S}$, $\{G_i^{(4)}=Q(l_i)^{\tilde{a}}\}_{i\in[1,d]}h_x=g^{\varphi_x}$, 随机选择$\varphi_x \in \mathbb{Z}_p$。

3) $Encrypt(T_{\mathrm{a}}, M, PK_K) \to (CT)$。当DO对其消息$M \in \{0,1\}^*$加密时, 选择1个对称加/解密算法对$(E, D)$。随机选择$s,\rho \in \mathbb{Z}_p$计算$g_3=g^{s}, \hat{e}(g,g)^{\alpha s}$和$KDF1(\hat{e}(g,g)^{\alpha s}, \mathcal{L})=\bar{K}\|\vec{d}$, 得到对称密钥$\bar{K}$。计算$M$的对称加密密文$C_s=E_{\bar{K}}(M)$, 以及Pedersen承诺$\tilde{C}=u^{\bar{K}}v^{\vec{d}}$来验证对称密钥$\bar{K}$。

首先, DO随机选择$r_0 \in \mathbb{Z}_p$, 生成一个可穿刺加密的初始密钥$SK_0=\{l_0, D_0=g_1^{1+r_0}, F_0=g_3^{r_0}, Q_0=Q(l_0)^{r_0}\}$, 并将其嵌入到密文中。

其次, 对访问策略T_{a}的每个节点x关联3个参数, 即s_x^0, s_x^1和s_x^{τ}。其中, s_x^0参与父节点共享, s_x^1由其子节点共享, s_x^{τ}是节点x的时间相关参数。这3个参数的值根据T_{a}采用自顶向下的方式进行分配, 具体如下:

①如果x是根节点R, 则$s_R^0=s$;

②对于每一个具有s_x^0的节点x, 如果该节点x不存在时间陷门, 则$s_x^{\tau}=1$, $s_x^1=s_x^0$; 如果该节点x存在时间陷门, 则$s_x^{\tau} \in \mathbb{Z}_p$, $s_x^{\tau} \times s_x^1 = s_x^0$。

当时间陷门存在于非叶子节点时, 在未到达释放时间前, 该节点的子树都是被锁定的。对于和时间点$t \in F_{\mathrm{T}}$以及参数s_x^{τ}相关的时间陷门TS_x, 随机选择$r_t \in \mathbb{Z}_p$并计算$TS_x=(A_x=g^{r_t}, B_x=(s_x^{\tau}+H_2(\hat{e}(H_1(t),f)^{r_t})))$。

再次, 在访问策略T_{a}中, 每一个叶子节点x代表1个属性y, DO根据大小关系将x转换为0编码或者1编码的子树。对于“>”关系, 替换x为0编码, 否则, x为1编码, 用S_1代表扩充后的属性集。

最后, 计算消息M的密文CT, 如式(6)所示。

$$\begin{aligned} CT=&(SK_0, T_{\mathrm{a}}, \tilde{C}, C_s, C_1=g_1^{s}, C_2=g_2^{s}, C_3=g_3,\\ &\forall x \in S_1: C_x=g^{\tilde{a}s_x^1}h_x^{s}, TS_x=(A_x,B_x))。\end{aligned} \tag{6}$$

4) $TokenGen(t, MK_K) \to (TK_t)$。KGC作为时间代理, 在每个时间点$t \in F_{\mathrm{T}}$生成并公开发布1个时间令牌$TK_t=H_1(t)^{\gamma}$, 该令牌用于DM进行其共享密文关联的访问策略中相关时间陷门的释放。

5) $TrapdoorExposure(TS_x, TK_t) \to (TS_x')$: 当到达与时间陷门$TS_x$相关的释放时间点$t$时, DM获得1个由KGC发布的相应令牌$TK_t$查询访问策略中所有时间陷门。如果数据密文所关联的访问策略T_{a}中某节点x关联了1个时间陷门TS_x, 当该陷门未被释放时, 其值为$TS_x=(A_x=g^{rt}, B_x=(s_x^{\tau}+H_2(\hat{e}(H_1(t),f)^{rt})))$。此时, 对于1个拥有足够权限的DU, 即其属性集合S满足节点x所对应的访问策略子树, 由于无法获取节点x对应的值s_x^{τ}而无法完成解密计算。对于该陷门TS_x对应的释放时间点t, DM收到KGC发布的时间令牌TK_t后, 计算$TS_x'=B_x-H_2(\hat{e}(TK_t, A_x))$。若$TS_x'=s_x^{\tau}$, 则该陷门被成功暴露, 并在其相关的密文$CT$中用$TS_x'$代替$TS_x$。此时, 任何拥有足够权限的DU均可根据$s_x^{\tau}$完成$T_{\mathrm{a}}$解密计算。CADAC通过上述机制完成基于时间的访问控制。

6) $Puncture(PK_K, PP_K, SMK, CT) \to (CT', \zeta)$。当DM收到DO的穿刺策略$PP_K$后对密文进行穿刺, 不直接对CP-ABE密文进行其他操作。

首先, 将穿刺策略PP_K转换为访问策略AP_K。对于PP_K中的每个非叶子节点, 将OR门变为AND门, AND门变为OR门, (k,n)门则变为$(n-k+1,n)$门[41]。对于每个叶子节点, 与叶子节点相关的标签t变为否定形式NOT t(例如: 穿刺策略PP_K的第k层第j个节点t_{kj}, 转换为AP_K后记为$\neg t_{kj}$)。嵌入在密文中的初始密钥为$SK_{K-1}=\{sk_0, sk_1, \cdots, sk_{k-1}\}$, $sk_0=\{l_0, D_0, F_0, Q_0\}$。此时, DM随机选择$\lambda_k, r_k \in \mathbb{Z}_p$并计算新的密钥$sk_0'$, 如式(7)所示。

$$\begin{aligned} sk_0'=&(l_0, D_0'=D_0g_1^{r_k-\lambda_k}=g_1^{1+r_0+r_k-\lambda_k},\\ &F_0'=F_0g_3^{r_k}=g_3^{r_0+r_k},\\ &Q_0'=Q_0Q(l_0)^{r_k}=Q(l_0)^{r_0+r_k})。\end{aligned} \tag{7}$$

依此类推可得到第k次穿刺密钥。

其次, 将λ_k作为秘密值按照AP_K进行划分, 对于叶子节点标签$\neg t_{kj}$, λ_k在其上的秘密值为λ_{kj}, 随机选择

$r_{k,j}\in\mathbb{Z}_p$并计算 $sk_{k,j}=(l_{k,j},D_{k,j}=g_1^{\lambda_{k,j}+r_{k,j}},F_{k,j}=g_3^{r_{k,j}},Q_{k,j}=Q(l_{k,j})^{r_{k,j}})$，则穿刺后的密钥如式(8)所示。

$$SK_k=(\{PP_i,AP_i\}_{i\in\{1,2,\cdots,k\}},sk_0',sk_1,\cdots,sk_{k-1},sk_k)。\quad(8)$$

再次，DM使用其私钥生成对新密钥组件$N_k=sk_k$的签名$\zeta=g^{\frac{1}{\delta}\times H(N_k)}$发送至DO验证。

最后，DM将新的密钥SK_K嵌入到密文中，并输出穿刺后的密文CT'，如式(9)所示。

$$CT'=(SK_k,T_a,\tilde{C},C_s,C_1=g_1^s,C_2=g_2^s,C_3=g_3,$$
$$TS_x=(A_x,B_x),\forall x\in S_1:C_x=g^{\bar{a}s_x^1}h_x^s)。\quad(9)$$

此时，通过穿刺密文可实现共享数据密文的前向安全性。需要注意的是，DO收到DM进行穿刺操作时生成的签名ζ，需使用签名公钥SPK根据穿刺策略计算验证其密文是否被正确穿刺，验证方法如式(10)所示。

$$\hat{e}\left(SPK\times g^{H(N_k)},\zeta\right)=\hat{e}(g,g),\quad(10)$$

若相等，则验证成功。

7) $Decrypt(CT,DK_u,PK_K)\rightarrow(M\ \text{OR}\ \perp)$。在收到DU的访问请求后，DM首先判断其属性集$S$是否与$CT$的访问策略匹配，若匹配，则将密文$CT$返回。收到密文后，DU检查标签集$\{l_1,l_2,\cdots,l_d\}$是否为$DK_u$中所有，若标签不相同，则执行如下步骤。

对于访问策略T_a的叶子节点$x\in S$，如果节点x上的陷门已暴露，则执行DecryptNode算法，如式(11)所示。

$$DecryptNode(CT,TK_u,x)=\left(\frac{\hat{e}\left(C_x,G^{(2)}\right)}{\hat{e}\left(C_3,G_x^{(3)}\right)}\right)^{s_x^\tau}=$$
$$\frac{\hat{e}\left(g^{\bar{a}s_x^1}h_x^s,g^r\right)^{s_x^\tau}}{\hat{e}(g^s,h_x^r)^{s_x^\tau}}=\hat{e}(g,g)^{\bar{a}rs_x^0},\quad(11)$$

否则，$DecryptNode(CT,TK_u,x)=\perp$。

对于非叶子节点x，递归执行DecryptNode算法，如式(12)所示。

$$F_x=\left(\prod_{z\in S_x}F_z^{\Delta_{i,s_z'}(0)}\right)^{s_x^\tau}=\left(\prod_{z\in S_x}\left(\hat{e}(g,g)^{\bar{a}rq_z(0)s_z^0}\right)^{\Delta_{i,s_x'}(0)}\right)^{s_x^\tau}=$$
$$\left(\prod_{z\in S_x}\hat{e}(g,g)^{\bar{a}rq_{\text{parent}}(z)\times(index(z))\times s_z^0}\right)^{s_x^\tau}=\hat{e}(g,g)^{\bar{a}rs_x^1s_x^\tau}=\hat{e}(g,g)^{\bar{a}rs_x^0}。\quad(12)$$

依此类推，对于访问策略T_a的根节点R可以得到$W=DecryptNode(CT,DK_u,R)=\hat{e}(g,g)^{\bar{a}rs_R^0}=\hat{e}(g,g)^{\bar{a}rs}$。接着计算，如式(13)所示。

$$A=\frac{\hat{e}\left(C_3,G^{(1)}\right)}{W}=\frac{\hat{e}\left(g^s,g^\alpha g^{\bar{a}r+\bar{a}\beta}\right)}{\hat{e}(g,g)^{\bar{a}rs}}=$$
$$\frac{\hat{e}(g,g)^{\alpha s}\hat{e}(g,g)^{\bar{a}sr}\hat{e}(g,g)^{\bar{a}s\beta}}{\hat{e}(g,g)^{\bar{a}rs}}=\hat{e}(g,g)^{\alpha s}\hat{e}(g,g)^{\bar{a}s\beta}。\quad(13)$$

对于AP_i中的叶子节点$\neg t_{i,j}$，找寻一组拉格朗日系数$\{w_1,w_2,\cdots,w_d,w^*\}$，使得$\sum_{n=1}^{d}(w_n\times q(l_n))+w^*\times q\left(l_{i,j}\right)=q(0)=\beta$，计算如式(14)所示。

$$J_{i,j}=\frac{\hat{e}(D_{i,j},C_2)}{\hat{e}\left(F_{i,j},\prod_{n=1}^{d}(G_n^{(4)})^{w_n}\right)\hat{e}(Q_{i,j},C_1)^{w^*}}=$$
$$\frac{\hat{e}(g,g)^{\bar{a}s\beta(\lambda_{i,j}+r_{i,j})}}{\hat{e}(g,g)^{\bar{a}r_{i,j}s\prod_{n=1}^{d}(w_n\times q(l_n))}\hat{e}(g,g)^{\bar{a}r_{i,j}sw^*q(l_{i,j})}}=\hat{e}(g,g)^{\bar{a}s\beta\lambda_{k,j}}。\quad(14)$$

根据$\{J_{i,j}\}_{i,j\in[1,2,\cdots,k]}$恢复$AP_i$根值$J_i=\hat{e}(g,g)^{\bar{a}s\beta\lambda_i}$。而对于$SK_K$中的$sk_0'$，找寻一组拉格朗日系数$\{\tau_1,\tau_2,\cdots,\tau_d,\tau^*\}$，使得$\sum_{n=1}^{d}(\tau_n\times q(l_n))+\tau^*\times q(l_0)=q(0)=\beta$，计算如式(15)所示。

$$J_0=\frac{\hat{e}\left(D_0',C_2\right)}{\hat{e}\left(F_0',\prod_{n=1}^{d}(G_n^{(4)})^{w_n}\right)\hat{e}(Q_0',C_1)^{\tau^*}}=\hat{e}(g,g)^{\bar{a}s\beta(1-\lambda_k)}。\quad(15)$$

此时，DU计算如式(16)所示。

$$B=\prod_{i=0}^{k}J_i=\hat{e}(g,g)^{\bar{a}s\beta}。\quad(16)$$

最后，DU计算得到数据密文CT的对称密钥$\overline{K}$，并对其进行验证，如式(17)所示。

$$\frac{A}{B}=\frac{\hat{e}(g,g)^{\alpha s}\hat{e}(g,g)^{\bar{a}s\beta}}{\hat{e}(g,g)^{\bar{a}s\beta}}=\hat{e}(g,g)^{\alpha s},$$
$$KDF1(\hat{e}(g,g)^{\alpha s},\mathcal{L})=\overline{K}\|\overline{d}。\quad(17)$$

如果$u^{\overline{K}}v^{\overline{d}}=\tilde{C}$，则$\overline{K}$验证成功，计算$M=D_{\overline{K}}(C_s)$并返回消息明文$M$；否则，返回$\perp$。

5 方案分析

本节主要对CADAC方案的安全性和性能进行分析，通过严格的形式化分析来证明方案的安全性，以及通过大量仿真实验和应用分析展示方案的高效性和实用性。

5.1 安全性分析

针对CADAC面临的3种类型敌手，通过下面的定理来证明针对CADAC的安全性。

定理 1. 如果DBDH假设成立，那么不存在多项式时间的类型1敌手能够以不可忽略的优势攻破本文方案CADAC的基于时间数据访问控制。

证明. 假设存在敌手$\mathbb{A}$以不可忽略的优势Adv威胁CADAC的安全性。此时，安全游戏可以为敌手$\mathbb{A}$

提供足够的时间令牌。然而，解密过程会因为不充足的属性集合而无法完成。在这种限制下，可以构建模拟器$\mathbb{B}$，以不可忽略的优势破解 DBDH 难题。以下为构建方式。

1)初始化。DBDH 的挑战者$\mathbb{C}$设置群G_0和G_1以及双线性映射函数$\hat{e}$，生成元$g\in G_0$。挑战者$\mathbb{C}$抛掷随机硬币$\mu\in\{0,1\}$。如果$\mu=0$，挑战者$\mathbb{C}$设置元组$(A,B,C,Z)=(g^a,g^b,g^c,\hat{e}(g,g)^{abc})$；否则，元组设置为$(A,B,C,Z)=(g^a,g^b,g^c,\hat{e}(g,g)^z)$，其中，元组$(A,B,C,Z)$对应的随机数$a,b,c,z\in\mathbb{Z}_p^*$。模拟器$\mathbb{B}$获得元组$(A,B,C,Z)$。

2)建立。模拟器$\mathbb{B}$重复使用挑战者$\mathbb{C}$生成的群$G_0,G_1,\hat{e},g$，随机选择$\bar{a},\alpha,\beta,\gamma\in\mathbb{Z}_p$，定义时间格式$F_{\mathrm{T}}$，计算$g_1=g^{\bar{a}},g_2=g^{\beta},f=g^{\gamma}$，定义哈希函数$H$和$H_2$设置预言机$H_1$。随后，$\mathbb{B}$将公共参数$PK=\{g_1=g^{\bar{a}},g_2=g^{\beta},f=g^{\gamma},\hat{e}(g,g)^{\alpha},F_{\mathrm{T}},H,H_1,H_2\}$发送至敌手$\mathbb{A}$。

3)询问 1。此阶段中，敌手$\mathbb{A}$申请关联属性集合$S=\{A_1,A_2,\cdots,A_l\}$的解密密钥以及访问时间点t_{A^*}。同时，确定挑战访问策略A^*，S的任何子集无法在访问时间t_{A^*}之前满足A^*。令S_A为A^*中所含的属性集合。收到该请求后，模拟器$\mathbb{B}$获取集合Γ，满足$\Gamma\cap S=\varnothing$，$\Gamma\subset S_A$且集合$S_A-\Gamma$不能在t_{A^*}以及之前满足A^*。模拟器$\mathbb{B}$随机选择$r\in\mathbb{Z}_p$，计算$G^{(1)}=g^{\alpha}C^{\beta}$，$G^{(2)}=C$。对于$S$中每个属性$A_i$，构建$G_y^{(3)}=H(A_i)$。模拟器$\mathbb{B}$返回解密密钥至敌手$\mathbb{A}$。

4)挑战者应答。敌手$\mathbb{A}$提交 2 个等长的消息m_0和m_1给模拟器$\mathbb{B}$。$\mathbb{B}$抛掷硬币$\upsilon\in\{0,1\}$。对于每个属性$A_i\in S_A$，若$A_i\notin\Gamma$，则$C_i=B^{q_i(0)}$；否则，$C_i=g_1^{q_i(0)}$。对于每个时间陷门TS_x，如果关联的权限释放时间满足$t\leqslant t_{A^*}$，那么直接用s_x^{τ}作为释放状态下的陷门。相应地，若$t>t_{A^*}$时，陷门在未释放状态，模拟器$\mathbb{B}$运行算法来产生陷门。此时，模拟器$\mathbb{B}$根据υ输出m_{υ}完整的密文，其结构如式(18)所示。

$$CT=\left(A^*,\frac{\hat{e}\left(C^{\beta}g^{\alpha},A\right)}{Z},A^{\beta},\{C_x\}_{x\in S_A},\{A_x,B_x\},\cdots\right)。\tag{18}$$

从敌手$\mathbb{A}$的视角观察密文，密文中的每个元素与真实方案中的分布是一致的。若$\mu=1$，则$Z=\hat{e}(g,g)^{abc}$，模拟的CT在这种情况下是m_{υ}的合法密文；反之，$Z=\hat{e}(g,g)^z$只是 1 个随机元素，此时CT不包含任何有关m_{υ}的信息。

5)询问 2。重复询问 1 以获得关联更大属性集合的解密密钥，但仍然无法满足挑战策略A^*。此处只关心类型 1 敌手的属性集合不充足的情况，因此，在本阶段不考虑访问时间修改的情况。本阶段中，在敌手$\mathbb{A}$很有可能申请解密密钥所关联的属性中，存在$A_i\in S-\Gamma$。此时，模拟器$\mathbb{B}$因无法继续而终止模拟过程；否则继续。令q表示模拟终止事件不发生的概率，该概率会随着属性集合S和挑战策略A^*的选择而变化，更小的集合S或者更复杂的策略A^*会引起更大的概率q。限制访问策略的复杂程度，存在常数$q_{\mathrm{D}}>0$，使得$q>q_{\mathrm{D}}$。

6)猜测。敌手$\mathbb{A}$提交对υ的猜测υ'。如果$\upsilon=\upsilon'$，模拟器$\mathbb{B}$输出自己对μ的猜测$\mu'=0$来表明所参与的 DBDH 挑战中的元组为合法的 DBDH 元组；否则，如果$\upsilon\neq\upsilon'$，$\mathbb{B}$输出$\mu'=1$来表明 DBDH 挑战中的元素只是一个随机的四元组。

假设μ和υ的选择是相互独立的。用符号χ表示模拟终止的事件。对于模拟器$\mathbb{B}$不中断模拟的情况。当$\mu=1$时，敌手$\mathbb{A}$无法获得关于υ的任何信息，因此，有$Pr\left[\upsilon\neq\upsilon'|\mu=1,\bar{\chi}\right]=\frac{1}{2}$。而当$\upsilon\neq\upsilon'$时，$\mu'=1$，此时$Pr\left[\mu=\mu'|\mu=1,\bar{\chi}\right]=\frac{1}{2}$。而当$\mu=0$时，敌手$\mathbb{A}$获得的是一个关于$m_{\upsilon}$的合法密文。根据假设，敌手$\mathbb{A}$具有$Adv$的优势，即$Pr\left[\upsilon=\upsilon'|\mu=0,\bar{\chi}\right]=\frac{1}{2}+Adv$。同样地，由于模拟器$\mathbb{B}$在$\upsilon=\upsilon'$时输出$\mu'=0$，因此，有$Pr\left[\mu=\mu'|\mu=0,\bar{\chi}\right]=\frac{1}{2}+Adv$。即在$\bar{\chi}$事件的前提下，其结果如式(19)所示。

$$\begin{aligned}&Pr\left[\mu=\mu'|\bar{\chi}\right]=Pr\left[\mu=\mu'|\mu=1,\bar{\chi}\right]\times Pr\left[\mu=1,\bar{\chi}\right]+\\&Pr\left[\mu=\mu'|\mu=0,\bar{\chi}\right]\times Pr\left[\mu=0,\bar{\chi}\right]=\\&\frac{1}{2}\times\frac{1}{2}+\frac{1}{2}\times\left(\frac{1}{2}+Adv\right)=\frac{1}{2}Adv+\frac{1}{2}。\end{aligned}\tag{19}$$

对于模拟器$\mathbb{B}$中断模拟的情况，此时，随机选择对μ的猜测μ'，因此，其正确率为$\frac{1}{2}$。此时，模拟器$\mathbb{B}$对 DBDH 挑战的整体优势如式(20)所示。

$$\begin{aligned}&Adv'=Pr\left[\mu=\mu'|\bar{\chi}\right]\times Pr\left[\bar{\chi}\right]+Pr\left[\mu=\mu'|\chi\right]\times Pr\left[\chi\right]-\\&\frac{1}{2}=\left(\frac{1}{2}+Adv\right)\times c+\frac{1}{2}\times(1-q_{\mathrm{D}})-\frac{1}{2}=\frac{q_{\mathrm{D}}}{2}Adv.\end{aligned}\tag{20}$$

从上述分析可知，如果 CADAC 存在概率多项式时间敌手的不可忽略优势Adv，那么就存在优势为$\frac{q_{\mathrm{D}}}{2}Adv$且不可忽略的 DBDH 难题的概率多项式敌手。因此，本文方案对于缺乏充足属性的选择明文攻击敌手(类型 1 敌手)是语义安全的。 证毕.

类型 2 敌手的证明与定理 1 证明类似。下面对类型 3 敌手进行分析和证明。

定理 2. 如果 DBDH 假设成立，那么不存在一个概率多项式时间的类型 3 敌手$\mathbb{A}$能够破坏 CADAC

在 IND-CPA 下的安全性。

证明. 与定理 1 中对于安全游戏 1 的证明原理相同，挑战者$\mathbb{C}$和敌手$\mathbb{A}$之间按照下面的交互进行博弈。假设存在一个挑战者$\mathbb{C}$，随机选择元素$a,b,c\in\mathbb{Z}_p$和生成元$g\in G_0$，计算得到(g^a,g^b,g^c)。挑战者$\mathbb{C}$的目标是能够区分$\hat{e}(g,g)^{abc}$和群G_1中的随机元素。因此，挑战者$\mathbb{C}$需要运行下面步骤：

1)初始化。敌手$\mathbb{A}$选择一个访问策略A^*和一个穿刺策略PP_K，并将其发送至挑战者$\mathbb{C}$。

2)系统建立。$\mathbb{C}$选择随机元素$\alpha'\in\mathbb{Z}_p$，使得$\alpha=ab+\alpha'$，从而得到$\hat{e}(g,g)^{\alpha}=\hat{e}(g,g)^{ab+\alpha'}=\hat{e}(g,g)^{ab}\hat{e}(g,g)^{\alpha'}=\hat{e}(g,g)^{a}\hat{e}(g,g)^{b}(g,g)^{\alpha'}=A\times B\times\hat{e}(g,g)^{\alpha'}$。接着，$\mathbb{C}$随机选择$\tilde{\alpha},\beta\in\mathbb{Z}_p$，并令$\tilde{\alpha}=a,\beta=b$。对于属性$i\in U$，$\mathbb{C}$定义如下：

如果$i\in S$，则$\mathbb{C}$随机选择元素$\eta_i\in\mathbb{Z}_p$并计算$\varphi_i=\eta_i,H_i=g^{\eta_i}$。否则，$\mathbb{C}$随机选择$\mu_i\in\mathbb{Z}_p$，并计算$\varphi_i=b\mu_i$，$H_i=g^{b\mu_i}=B^{\mu_i}$。$\mathbb{C}$随机选择$d+1$个值$\{\theta_{t_0},\theta_{t_1},\cdots,\theta_{t_d}\}\in\mathbb{Z}_p$。令$q(0)=\beta,q(t_i)=\theta_{t_i}$以及$Q(t_i)=g^{q(t_i)}=g^{\theta_{t_i}}$。$\mathbb{C}$生成公钥，如式(21)所示。

$$PK_K=(g,g_1=g^{\tilde{a}},g_2=g^{\beta},g^{q(1)},g^{q(2)},\cdots,g^{q(d)},h_1=g^{\varphi_1},h_2=g^{\varphi_2},\cdots,h_{|U|}=g^{\varphi_{|U|}},f=g^{\gamma},\hat{e}(g,g)^{\alpha},l_0,F_{\mathrm{T}})。\quad(21)$$

3)询问 1。敌手$\mathbb{A}$重复多次向$\mathbb{C}$询问属性集合S和标签集合$T=\{l_1,l_2,\cdots,l_d\}$。$\mathbb{C}$随机选择$r',z\in\mathbb{Z}_p$，同时，$\mathbb{C}$需要计算$G^{(1)}=g^{ab}g^{\alpha'}g^{a(r'+b)}g^{ab}=g^{\alpha}g^{a(r+\beta)}=g^{\alpha}A^{(r+\beta)}$。此处，$\mathbb{C}$使用$r'+b$来模拟随机数$r$。

接着，$\mathbb{C}$计算$G^{(2)}=g^{(r'+b)}=g^{r}$，以及$G_y^{(3)}=h_y^{(r'+b)}=h_y^{r}=(g^{\varphi})^{r}=(g_y)^{\eta_i r}$。对于标签集合$T=\{l_1,l_2,\cdots,l_d\}$，$\mathbb{C}$计算$G_i^{(4)}=Q(l_i)^{\tilde{a}}$。因此，$\mathbb{C}$可以通过设置解密密钥$DK_{\mathrm{u}}=(G^{(1)},G^{(2)},G_y^{(3)},G_i^{(4)})$进行模拟。

4)挑战者应答。敌手$\mathbb{A}$输出 2 个等长消息m_0和m_1给挑战者$\mathbb{C}$。接着，$\mathbb{C}$随机选择$r_0,\rho\in\mathbb{Z}_p$，并计算$SK_0=\{l_0,D_0=g_1^{r_0},F_0=g_3^{r_0},Q_0=Q(t_0)^{r_0}\}$。接着，$\mathbb{C}$随机选择$b\in\{0,1\}$，计算$C_1=g_1^{s}=g^{ac}=A^{c},C_2=g^{bc}=B^{c},C_3=g^{c}=C,\forall x\in S_1:C_x=g^{aq_x(0)s_x^{\mathrm{l}}}h_x^{s}=A_x^{q_x(0)}C^{\varphi_x}$。最终，$\mathbb{C}$发送密文$CT_b=(SK_0,T_a,\tilde{C},C_1,C_2,C_3,C_4,C_x)$返回给敌手$\mathbb{A}$。

5)询问 2。敌手$\mathbb{A}$按照询问 1 的方式对挑战者$\mathbb{C}$进行询问。

6)猜测。敌手$\mathbb{A}$输出对b的猜测$b'\in\{0,1\}$。如果$b'=b$，则挑战者$\mathbb{C}$输出c=1，否则输出c=0。

7)分析。敌手$\mathbb{A}$输出对b的猜测b'，如果$b'=b$，则挑战者$\mathbb{C}$输出对c的猜测$c'=1$，此时，$\mathbb{A}$得到合法的密文，其在该过程中的优势为$\epsilon=|Pr[b=b'|c=1]-1/2|$，也即$Pr[c=c'|c=1]=\epsilon+1/2$；否则，$\mathbb{C}$猜测$c'=0$，此时，$\mathbb{A}$得到一个随机密文，即$Pr[b\neq b'|c=0]=1/2$，此时$\mathbb{C}$输出$c'=1$，于是有$Pr[c\neq c'|c=0]=1/2$。因此，可以得到挑战者$\mathbb{C}$解决 BDHE 困难性问题的优势如式(22)所示。

$$\left|\frac{1}{2}Pr[c=c'|c=0]+\frac{1}{2}Pr[c=c'|c=1]-\frac{1}{2}\right|=\frac{1}{2}\epsilon。\quad(22)$$

因此，假设敌手$\mathbb{A}$能够以不可忽略的优势ϵ攻破 CADAC，则挑战者$\mathbb{C}$能够以同等优势赢得游戏并攻破 DBDH 假设，从而证明 CADAC 在选择明文攻击下是不可区分的。 证毕.

5.2 性能分析

本节将从理论分析、实验分析和应用验证 3 方面对 CADAC 的性能进行综合评估，并与当前 4 个相关的先进方案 ER-CP-ABE[18]，RABE-DI[43]，Pun-CP-ABE[40]，RS-HABE[38] 进行对比分析，验证其应用于数据空间的可行性和实用性。

5.2.1 理论分析

主要从 *Setup*，*KeyGen*，*Encrypt*，*Decrypt*，*Revocation* 的 5 个阶段进行计算复杂度的对比分析。分析过程主要考虑群元素的指数和乘法运算以及双线性运算，忽略哈希函数、对称加解密和拉格朗日差值等较小的计算开销。对比结果见表 3 所示。

1)在 *Setup* 算法方面，方案 ER-CP-ABE 由于需要生成与撤销二叉树相关参数，而方案 RS-HABE 则在此基础上要生成时间二叉树的相关参数，因此，RS-HABE 需要更多的双线性运算和群G_1的指数运算以生成直接撤销所需的参数。方案 RABE-DI 由于支持大规模属性空间，其系统初始化过程中的计算开销并未受到属性空间中全部属性数量的影响，因此拥有较小的计算开销。而 CADAC 和方案 Pun-CP-ABE 在双线性运算方面的开销较小，但是由于需要生成与标签集合相关的系统参数，需要更多的群G_0元素指数运算开销，但是，标签集合往往是固定值，在实际应用中计算开销不会显著增加。然而，CADAC 由于引入密钥封装技术而省去了 DM 对密文的加密操作，不需要初始化相关公钥和私钥，因此，相比 Pun-CP-ABE 而言，CADAC 在系统初始化阶段减少了$2E_{G_0}$的计算量，即是群G_0元素指数运算开销的 2 倍。

2)在 *KeyGen* 算法方面，CADAC 在解密密钥的生成过程中，不需要对密钥的每个元素进行隐蔽因子的指数运算，因此，其计算开销相比 Pun-CP-ABE 而言减少了大量群G_0元素的指数运算，具有更小的计算复杂度。具体而言，相比 Pun-CP-ABE，CADAC 在解密密钥生成阶段减少了$3E_{G_0}$的计算开销，即是群G_0元素指数运算开销的 3 倍，减少了对于密钥生

Table 3 Computational Complexity Comparison

表 3 计算复杂度对比

方案	*Setup*	*KeyGen*	*Encrypt*	*Decrypt*	*Revocation*
Pun-CP-ABE	$(u+n+6)E_{G_0}+E_{G_1}+P$	$(v+d+3)E_{G_0}+M_{G_0}$	$(2t+7)E_{G_0}+(t+2)M_{G_0}+E_{G_1}+2M_{G_1}+P$	$E_{G_0}+(nk(d+1)+t+2)E_{G_1}+2M_{G_1}+(2t+3)P$	$3E_{G_0}+3M_{G_0}+9nM_{G_1}+3E_{G_1}$
ER-CP-ABE	$(u+n_p+2)E_{G_0}+2E_{G_1}+2P$	$(9v+12)E_{G_0}+3E_{G_1}$	$(7t+4)E_{G_0}+2E_{G_1}+(7t+2)M_{G_0}+M_{G_1}$	$(4t+1)E_{G_0}+E_{G_1}+(3t+2)M_{G_1}+(4t+1)P$	$(7t+n_d)n_pE_{G_0}+2n_pE_{G_1}+2n_pM_{G_1}$
RABE-DI	$5E_{G_0}+2E_{G_1}+P$	$(8v+15)E_{G_0}$	$((18n_2+12)t+12)E_{G_0}+2E_{G_1}$	$(12t+2)E_{G_0}+12P$	$((18n_2+18)t+12)E_{G_0}+2E_{G_1}$
RS-HABE	$(u+n_p+n_d+1)E_{G_0}+E_{G_1}+P$	$n_u(4v+8)E_{G_0}$	$(4t+n_d+1)n_pE_{G_0}+n_pE_{G_1}+(tn_p+n_d)M_{G_0}+n_pM_{G_1}$	$2tE_{G_1}+(2t+3)M_{G_1}+(3t+2)P$	$(4t+n_d+1)n_pE_{G_0}+n_pE_{G_1}+(4tn_p+n_d)M_{G_0}+n_pM_{G_1}$
CADAC（本文）	$(u+n+4)E_{G_0}+E_{G_1}+P$	$(v+d)E_{G_0}+M_{G_0}$	$(2t+6)E_{G_0}+tM_{G_0}+2M_{G_1}+2P$	$2E_{G_0}+(nk(d+1)+t)E_{G_1}+2M_{G_1}+(2t+1)P$	$3E_{G_0}+3M_{G_0}+9nM_{G_1}+3E_{G_1}$

注：E_{G_0}和E_{G_1}表示循环群G_0和G_1中的指数运算，M_{G_0}和M_{G_1}表示群G_0和G_1中的乘法运算，P表示双线性映射$\hat{e}$的双线性运算。t表示与密文相关的访问策略属性数，n_2表示与密文相关的访问策略属性的划分数，v表示与用户密钥相关的属性集合数，k表示密文的穿刺数，n表示与穿刺策略相关联的标签数，d表示与密钥相关联的标签数，u表示属性空间中全部的属性数，m表示系统中已撤销的用户数，n_p表示撤销二叉树的节点数，n_u表示与未撤销用户相关联的节点数，而n_d则表示撤销二叉树的深度。

成中心的计算负担。而 ER-CP-ABE 和 RS-HABE 则由于利用二叉树对用户和时间进行管理，其密钥组成元素不仅与用户的属性集合数量相关，而且还与二叉树的深度相关，因此，其解密密钥需要更多的层级密钥元素生成，导致其计算开销较大。RABE-DI 则由于其属于双系统加密，在解密密钥生成过程中需要更多元素，因此其密钥生成时间也较长。

3）在 *Encrypt* 算法方面，CADAC 由于取消 DM 的重复加密，其计算开销相比 Pun-CP-ABE 减少了相应的指数运算。具体而言，相比 Pun-CP-ABE，CADAC 无需 DO 和 DM 之间进行密钥协商，同时，不需要对密文验证部分进行大量计算，因此，其对于 DO 的整体加密开销较 Pun-CP-ABE 方案减少了$E_{G_0}+E_{G_1}+tM_{G_0}-P$的计算量，减轻了 DO 的加密计算负担。而 ER-CP-ABE 和 RS-HABE 涉及到了与二叉树相关的密文元素计算，RABE-DI 则涉及双系统数据加密运算，因此，这几个相关先进方案的加密计算开销相对更大。

4）在 *Decrypt* 算法方面，CADAC 在解密验证部分，相比 Pun-CP-ABE，无需进行更多的指数运算和更加耗时的双线性运算，同时，还减少了对于 DM 解密部分的计算过程，其整体解密计算的开销相比 Pun-CP-ABE 减少了$2E_{G_1}+2P-E_{G_0}$，减轻了 DU 设备的解密计算开销，进一步增强了在数据空间中应用的实用性。而 ER-CP-ABE，RABE-DI，RS-HABE 尽管无需在解密过程中对密文的穿刺部分进行计算，但是其所需要的与访问策略复杂度数量相关的指数和耗时的双线性运算量要远大于 CADAC，因此，这 3 个方案在解密计算中需要更大的开销。

5）在 *Revocation* 方面，ER-CP-ABE 由于使用直接撤销，用户需要完成对用户撤销列表的维护和密文的更新，因此，其计算量较大，RABE-DI 和 RS-HABE 使用了间接撤销机制，用户撤销过程中包括密文更新和未撤销用户密钥更新的计算，其撤销计算开销较高且与访问策略复杂度成正比。而 Pun-CP-ABE 和 CADAC 则使用穿刺加密算法实现用户撤销，其计算开销与用户属性数或用户数量无关，也不需要进行复杂的密文重加密计算，仅与标签数量相关，因此，能够以较小的开销实现更灵活的用户撤销和前向安全性。

5.2.2 实验分析

为了实现方案原型，本文构建了仿真实验环境，包含一台配置了 Intel Core i5-6500 3.20 GHz 处理器、16 GB 内存和 Windows Server 2022 操作系统的服务器用于模拟 DM，以及一台配置了 Intel Core i7-1260P 3.20 GHz 处理器、32 GB 内存和 Windows11 操作系统的 ThinkPad T14 笔记本电脑用以模拟 DU 的终端设备。此外，采用 JDK64-17 和 Java 双线性对密码库(Java pairing-based cryptography, jPBC)[44]，并使用 Java 编程语言实现了 CADAC 以及相关先进方案 ER-CP-ABE，Pun-CP-ABE，RS-HABE 的原型，并将这些原型部署在仿真实验环境中，收集汇总各项指标数据并对实验结果进行对比和评估。

CADAC 与相关先进方案 ER-CP-ABE，RABE-DI，Pun-CP-ABE，RS-HABE 在系统初始化阶段的运行时间对比，如图 4 所示。

该实验中，按照实际场景设置 n=10，n_p=15，n_d=5，控制属性空间大小在 [1,10] 区间递增。由图 4 可知，CADAC 与 Pun-CP-ABE 相比在系统初始化中的运行时间开销略小，这表明 CADAC 基于时间和属性可比较访问控制等新增因素在实际运行中并未增加系统初始化过程中的计算开销。ER-CP-ABE 则因其直接撤销机制需要与二叉树相关的变量开销，导致其系

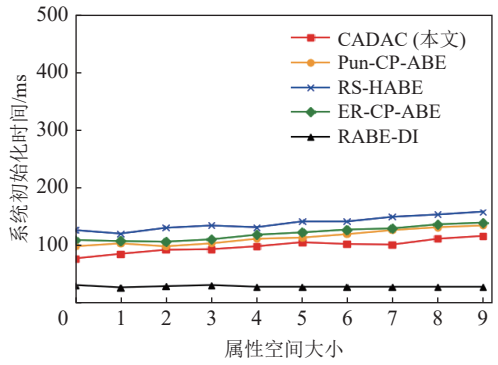


Fig. 4 Time for system initialization

图 4 系统初始化时间

统初始化计算开销较大。RABE-DI 则因支持大规模属性全集，其系统初始化时间开销不随属性空间大小变化。而 RS-HABE 则由于实现了层级用户的间接撤销，需要对层级用户管理、时间管理以及间接撤销所需维护的状态变量在实际运行中带来了更多的额外计算开销。

CADAC 与另外 4 个相关方案在密钥生成阶段的计算开销对比，如图 5 所示。

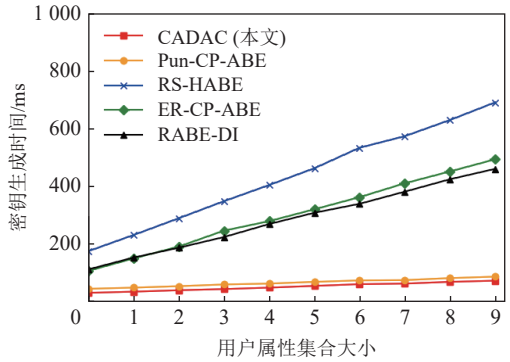


Fig. 5 Time for key generation

图 5 密钥生成时间

在该实验中，设置 d=5, n_u=3，并控制用户属性集合大小在 [1,10] 范围内递增。可以看出，由于 CADAC 和 Pun-CP-ABE 在用户解密密钥生成过程中不需要生成额外的二叉树相关密钥元素以及层级用户相关密钥元素，因此，其计算开销随着用户属性大小缓慢变化，而且远低于 RS-HABE 的计算开销。与此同时，CADAC 的密钥生成时间相比 Pun-CP-ABE 更小，这是由于后者需要为每个密钥元素计算执行更多的指数运算，说明在密钥生成算法上，CADAC 并未带来额外的密钥生成负担。由图 5 可知，随着属性集合大小的增加，RS-HABE 和 ER-CP-ABE 的密钥生成时间增长速度要比 RABE-DI 更快，其中，RS-HABE 的密钥生成时间增长率取决于 n_u 和属性集合大小的乘积，因此，其时间开销在所有 5 个方案中最大。

CADAC 与 4 个相关方案在数据加密方面的时间开销对比，如图 6 所示。

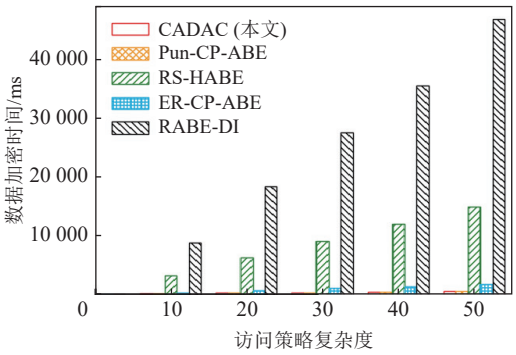


Fig. 6 Time for data encryption

图 6 数据加密时间

图 6 中横轴表示访问策略复杂度，是一个公差等于 10 的等差数列。设置 n_2 = 10，可以看出随着访问策略复杂度的增加，RS-HABE, RABE-DI, ER-CP-ABE 的加密运行时间增加较快，CADAC 和 Pun-CP-ABE 的加密时间随着访问策略复杂度的增加而缓慢增长，但相较于 Pun-CP-ABE, CADAC 加密计算时间更少。这是由于 CADAC 在加密过程中虽然增加了基于时间和属性对比的访问控制策略，需要额外的时间陷门计算，但是减少了对于 DM 加密的计算开销，整体加密时间开销相比 Pun-CP-ABE 有所减少。此外，由于采用直接撤销方式，ER-CP-ABE 在加密数据过程中需要大量的计算，而 RS-HABE 则由于需要计算更多的时间二叉树和撤销二叉树的密文元素，因此，其数据加密时间开销更大。

CADAC 与 4 个相关方案在数据解密阶段的时间开销对比，如图 7 所示。

在该实验中，设置 d=5, k=3，随着访问策略复杂度的增加，RS-HABE, RABE-DI, ER-CP-ABE 解密时间开销增长较快。而在标签数量和时间陷门数量均固

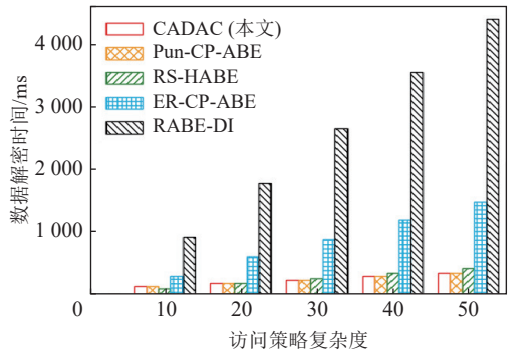


Fig. 7 Time for data decryption

图 7 数据解密时间

定的情况下, CADAC 和 Pun-CP-ABE 的解密时间开销增长较慢。其中, 由于 CADAC 方案优化了数据验证机制, 其数据解密过程减少了指数运算和耗时的双线性运算, 相比 Pun-CP-ABE 具有更少的解密时间。

此外, 图 8 进一步验证 CADAC 相比 Pun-CP-ABE, RABE-DI, RS-HABE, ER-CP-ABE 在用户撤销过程中的性能优势。

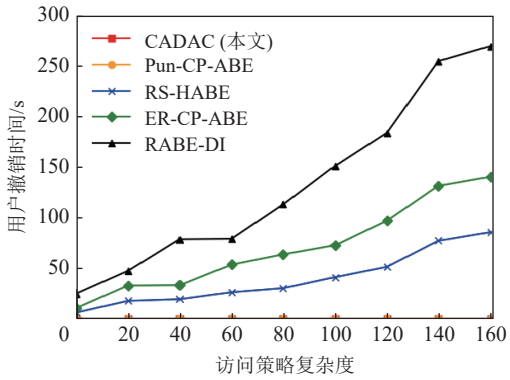


Fig. 8 Time for user revocation

图 8 用户撤销时间

其中, ER-CP-ABE 使用直接方式进行用户撤销, Pun-CP-ABE 与 CADAC 使用可穿刺加密实现了灵活的用户撤销, RS-HABE 则使用传统的间接用户撤销方式完成动态用户管理, 而 RABE-DI 同时实现了间接用户撤销和可验证的访问控制。由图 8 可知, RS-HABE 和 RABE-DI 采用了间接用户撤销方法, 在用户撤销过程中, 一方面需要更新未撤销用户密钥, 另一方面需要更新密文以实现前向安全性, 因此, 其用户撤销计算开销随着访问策略复杂度的增加而快速增大。而 ER-CP-ABE 则采用直接撤销机制, 在用户撤销过程中, 需要维护撤销列表和用户二叉树, 并根据该用户管理结构进行密文更新, 其用户撤销时间开销也随着访问策略复杂度的增加而快速增大。相比之下, 由于 CADAC 和 Pun-CP-ABE 采用了可穿刺加密技术, 在数据解密和用户撤销过程中实现了较低的计算开销, 且不受访问策略复杂度影响。充分表明本文基于时间和属性比较的访问控制机制在实际运行中未明显增加用户撤销的时间开销。

综上, 与相关先进方案相比, CADAC 由于不需要密文代理重加密和密钥更新操作, 降低了用户撤销过程中的计算开销, 可通过较小的计算成本实现灵活的用户撤销和前向安全性。同时, 该方案还能够同时实现基于时间和属性对比的动态数据访问控制, 并支持解密运算的一致性验证, 在数据空间的落地应用中更具优势。

5.2.3 应用验证

为了进一步探索 CADAC 在行业数据空间中的实用性, 本节以医疗数据空间中个人健康记录(personal health record, PHR)的共享流通过程为场景搭建了测试平台, 验证 CADAC 在保护 PHR 共享时的安全和实际性能。

在医疗数据空间中, 患者就医时会产生大量 PHR 信息, 并在主治医生和医护人员之间共享流通, 用于医疗诊断和康复护理, 同时, 科研人员也需要大批患者的 PHR 信息进行相关科学研究。然而, 由于 PHR 中包含大量患者隐私和敏感信息, 直接共享会带来安全隐患。因此, 医疗数据空间需支持患者以密态形式进行 PHR 流转, 同时确保 PHR 在共享过程中能够对不同角色的人员进行细粒度访问控制, 保护患者个人隐私数据安全。

1)场景设置。在医疗数据空间中, 每天都有大量的患者加入或者退出, 大量的 PHR 信息和复杂的访问控制需求, 会给 PHR 信息共享和流转带来巨大挑战, 场景设置如图 9 所示。

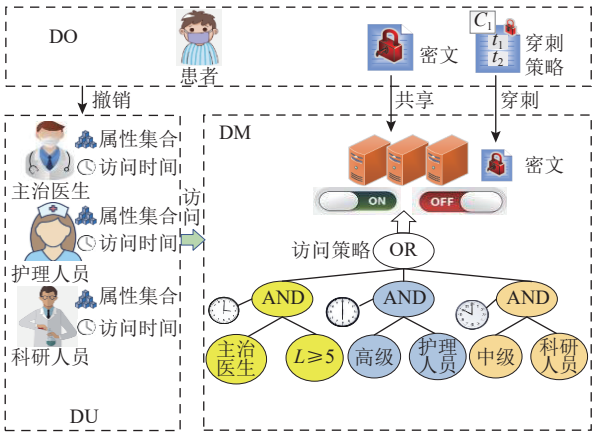


Fig. 9 Application example of CADAC in the medical dataspace

图 9 CADAC 在医疗数据空间中的应用示例

在图 9 中, 患者作为 PHR 的 DO 实体, 在其 PHR 共享过程中存在非法访问和隐私泄露的担忧。主治医生、医护人员、科研人员作为 PHR 的 DU 实体, 其越权访问以及离开系统后的恶意访问都可能造成 PHR 的隐私泄露, 同时, DU 对于 PHR 的访问具有时间先后顺序。通常, 根据患者就医的紧急性, PHR 首先应由主治医生进行访问, 其次是护理人员, 最后是科研人员。特别地, 根据患者的病情, 一些诊疗工作需要高级别的主治医生来会诊。

因此, 针对 PHR 共享过程中的机密性和访问控制, 首先, CADAC 方案支持在共享前对 PHR 信息进

行加密。其次，在访问策略中，可灵活设置访问策略。例如：支持设置只有级别高于 5 的主治医师才能够访问该患者的 PHR 进行诊疗，在患者就医的时候即可对该节点的事件陷门进行释放，以支持主治医生最早访问该患者信息。最后，当一些 DU 离开系统后，CADAC 能够根据穿刺策略实现高效及时的用户撤销，确保 PHR 信息的前向安全。例如：一些临时安排参加某项科学研究的科研人员，在结束任务后，CADAC 支持通过用户撤销，使其立即失去对于患者 PHR 的访问权限。

2）测试平台搭建。搭建了包含 2 台主机、1 台笔记本电脑、1 台智能手机的测试平台，用于验证 CADAC 在实际应用时的真实性能，如图 10 所示。

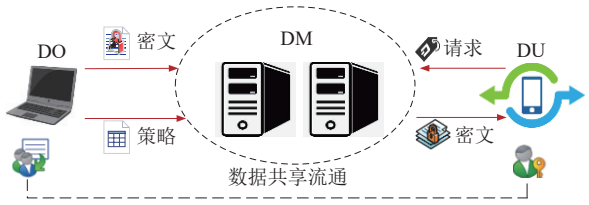


Fig. 10 System architecture of test platform

图 10 测试平台系统架构

2 台主机分别配置了 Intel Core i5-6500 3.20 GHz 处理器、16 GB 内存和 Intel Core i7-13600K 3.5 GHz 处理器、32 GB 内存来模拟 DM 实体。1 台笔记本电脑配置了 Intel Core i7-1260P 3.20 GHz 处理器、32 GB 内存，用于模拟 DO 实体的终端设备。1 部 Android OS 6.0 操作系统的华为 P20 智能手机，用于模拟 DU 实体的终端设备，各设备分别部署了数据共享应用。

3）实际测试。为了验证方案的实用性，设定 DU 的属性集合大小$|S|$=10，穿刺策略标签数 n=10，访问策略复杂度为 15。分别运行 CADAC 以及 ER-CP-ABE，Pun-CP-ABE，RS-HABE 中的密钥生成（*KeyGen*）、数据加密（*Encrypt*）、数据解密（*Decrypt*）和用户撤销（*Revocation*）算法 1 000 次，取其算术平均值，结果如表 4 所示。

Table 4 Comparison of Practical Performance Testing Results

表 4 实际性能测试结果对比 ms

方案	*KeyGen*	*Encrypt*	*Decrypt*	*Revocation*
Pun-CP-ABE	86	186	165	19
ER-CP-ABE	689	4 868	129	6 275
RABE-DI	459	13 768	1 329	24 912
RS-HABE	492	516	451	10 672
CADAC（本文）	72	175	148	18

由表 4 可知，测试平台的运行结果与仿真测试结果一致。其中，在 *KeyGen* 算法中，CADAC 相比 Pun-CP-ABE 有较高的密钥生成效率，对密钥生成中心的计算开销较小，而 ER-CP-ABE，RABE-DI，RS-HABE 的密钥生成时间则远超 CADAC。在 *Encrypt* 算法中，CADAC 不仅能够支持基于属性比较和访问时间的控制策略，其数据加密时间相比 Pun-CP-ABE 节省了约 10 ms 的计算开销，相比其他 3 个方案其加密时间降低更多。对于 *Decrypt* 算法，CADAC 优化了密文验证机制，因此，其在 DU 设备的密文解密开销有所下降，相比 Pun-CP-ABE 降低了大约 20 ms，比 RABE-DI 和 RS-HABE 则分别降低约 1 200 ms 和 300 ms。在 *Revocation* 算法中，CADAC 与 Pun-CP-ABE 都采用了穿刺加密技术，用户撤销性能接近且均超过其他 3 个方案。综合对比可知，CADAC 与 Pun-CP-ABE 相比有更低的密钥生成、数据加密和数据解密开销，且用户撤销性能相近。表明 CADAC 在安全性、执行效率和鲁棒性上更具优势，能够更好地支持行业数据空间构建。

6 结　论

数据访问控制是实现数据空间中数据安全流通的关键技术之一，然而，现存的基于属性加密方案难以满足用户高度灵活动态性的细粒度数据访问控制需求。因此，本文提出了一种基于可比较属性动态可验证的数据访问控制方案（CADAC），能够同时支持基于访问时间、属性比较和动态用户撤销等多因素的可验证访问控制。具体地，CADAC 通过设计一个可验证的可穿刺 CP-ABE 密码原语，不仅实现了共享数据的机密性和访问控制的细粒度，还保证了用户撤销的灵活性和前向安全性，且支持解密过程的可验证性。此外，该方案结合时释性加密和 0-1 编码技术，设计并实现了一种基于时间和属性比较的可比较访问控制策略。严格的安全分析证明了 CADAC 在随机预言机模型上是 CPA 安全的。大量实验结果、对比分析和应用验证证明了其在数据空间构建中的实用性。

作者贡献声明：余增文、张嘉伟、姜奇负责方案整体设计并撰写论文；杨力、方志负责部分算法思路和实验方法设计，并提供实验环境；史润方参与修改论文。

参　考　文　献

[1] Xu Jing, Wang Zhan, Yuan Guojun, et al. A survey on fine-grained

flow control for artificial intelligence data centers[J]. Journal of Computer Research and Development, 2025, 62(11): 2806−2825 (in Chinese)
(许晶, 王展, 元国军, 等. 面向智算中心的细粒度流量控制技术综述[J]. 计算机研究与发展, 2025, 62(11): 2806−2825)

[2] Tao Xiaoming, Peng Jieyang, Wang Yue, et al. Information metrics for data components based on information entropy: Data pricing and its application analysis for electric energy statistics[J]. SCIENTIA SINICA Informationis, 2025, 55(3): 654−680 (in Chinese)
(陶晓明, 彭劼扬, 王钺, 等. 基于信息熵的数据元件信息计量——以数据定价及其电能统计应用分析为例[J]. 中国科学: 信息科学, 2025, 55(3): 654−680)

[3] Li Fenghua, Li Hui, Niu Ben, et al. Research category and future development trend of data elements circulation and security[J]. Journal on Communications, 2024, 45(5): 1−11 (in Chinese)
(李凤华, 李晖, 牛犇, 等. 数据要素流通与安全的研究范畴与未来发展趋势[J]. 通信学报, 2024, 45(5): 1−11)

[4] Fan Shuhuan, Hou Mengshu. Dataspace: A new data organization and management model[J]. Computer Science, 2023, 50(5): 115−127 (in Chinese)
(范淑焕, 侯孟书. 数据空间: 一种新的数据组织和管理模式[J]. 计算机科学, 2023, 50(5): 115−127)

[5] Deepa N, Pham Q V, Nguyen D C, et al. A survey on blockchain for big data: Approaches, opportunities, and future directions[J]. Future Generation Computer Systems, 2022, 131: 209−226

[6] Roy S, Nandi S, Maheshwari R, et al. Blockchain-based efficient access control with handover policy in IoV-enabled intelligent transportation system[J]. IEEE Transactions on Vehicular Technology, 2024, 73(3): 3009−3024

[7] Parkinson S, Khan S. A survey on empirical security analysis of access-control systems: A real-world perspective[J]. ACM Computing Surveys, 2022, 55(6): 1−28

[8] IEEE Computer Society. IEEE Standard for Trusted Data Matrix System Architecture [S/OL]. 2024 [2025-04-15]. https://xplorestaging.ieee.org/document/10797717

[9] Liu Xiaohong, Huang Xinyi, Cheng Zhaohui, et al. Key-policy attribute-based encryption based on SM9 and its fast decryption[J]. Chinese Journal of Computers, 2024, 47(5): 971−986 (in Chinese)
(刘晓红, 黄欣沂, 程朝辉, 等. 基于 SM9 的密钥策略属性基加密及快速解密[J]. 计算机学报, 2024, 47(5): 971−986)

[10] Li Teng, Zhang Jiawei, Shen Yulong, et al. Hierarchical and multi-group data sharing for cloud-assisted industrial Internet of things[J]. IEEE Transactions on Services Computing, 2023, 16(5): 3425−3438

[11] Zhang Jiawei, Yang Yanbo, Liu Ximeng, et al. An efficient blockchain-based hierarchical data sharing for healthcare Internet of things[J]. IEEE Transactions on Industrial Informatics, 2022, 18(10): 7139−7150

[12] Zhang Jiawei, Li Teng, Ying Zuobin, et al. Trust-based secure multi-cloud collaboration framework in cloud-fog-assisted IoT[J]. IEEE Transactions on Cloud Computing, 2022, 11(2): 1546−1561

[13] Zhang Jiawei, Ma Jianfeng, Yang Yanbo, et al. Revocable and privacy-preserving decentralized data sharing framework for fog-assisted Internet of things[J]. IEEE Internet of Things Journal, 2021, 9(13): 10446−10463

[14] Zhang Jiawei, Li Teng, Obaidat M S, et al. Enabling efficient data sharing with auditable user revocation for IoV systems[J]. IEEE Systems Journal, 2021, 16(1): 1355−1366

[15] Ning Jianting, Huang Xinyi, Wei Lifei, et al. Tracing malicions insider in attribute-based cloud data sharing[J]. Chinese Journal of Computers, 2022, 45(7): 1431−1445 (in Chinese)
(宁建廷, 黄欣沂, 魏立斐, 等. 支持恶意用户追踪的属性基云数据共享方案[J]. 计算机学报, 2022, 45(7): 1431−1445)

[16] Li Xiaoguo, Yang Guoming, Xiang Tao, et al. Make revocation cheaper: Hardware-based revocable attribute-based encryption[C]// Proc of the 2024 IEEE Symp on Security and Privacy (SP). Los Alamitos, CA: IEEE Computer Society, 2024: 3109−3127

[17] Yang Mengxue, Wang Huaqun, He Debiao, et al. PM-ABE: Puncturable bilateral fine-grained access control from lattices for secret sharing[J]. IEEE Transactions on Dependable and Secure Computing, 2025, 22(2): 1210−1223

[18] Zhang Qingyang, Xu Chang, Zhong Hong, et al. Revocable and efficient blockchain-based fine-grained access control against EDoS attacks in cloud storage[J]. IEEE Transactions on Computers, 2024, 73(8): 2012−2024

[19] Luo Fucai, Wang Haiyan, Yan Xingfu, et al. Key-policy attribute-based encryption with switchable attributes for fine-grained access control of encrypted data[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 7245−7258

[20] Hong Jianan, Xue Kaiping, Xue Yingjie, et al. TAFC: Time and attribute factors combined access control for time-sensitive data in public cloud[J]. IEEE Transactions on Services Computing, 2017, 13(1): 158−171

[21] Xue Kaiping, Hong Jianan, Xue Yingjie, et al. CABE: A new comparable attribute-based encryption construction with 0-encoding and 1-encoding[J]. IEEE Transactions on Computers, 2017, 66(9): 1491−1503

[22] Franklin M, Halevy A, Maier D. From databases to dataspaces: A new abstraction for information management[J]. Association for Computing Machinery, 2005, 34(4) : 27-33

[23] Guo Jingwei, Cheng Ying, Wang Dongxu, et al. Industrial dataspace for smart manufacturing: Connotation, key technologies, and framework[J]. International Journal of Production Research, 2023, 61(12): 3868−3883

[24] Sahai A, Waters B. Fuzzy identity-based encryption[C]// Proc of the 24th Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2005: 457−473

[25] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]// Proc of the 2007 IEEE Symp on Security and Privacy (SP'07). Piscataway, NJ : IEEE, 2007: 321−334

[26] Androulaki E, Soriente C, Malisa L, et al. Enforcing location and time-based access control on cloud-stored data[C]// Proc of the 34th Int Conf on Distributed Computing Systems. Piscataway, NJ: IEEE, 2014: 637−648

[27] Fan Chun-I, Huang Shiyuan. Timed-release predicate encryption and its extensions in cloud computing[J]. Journal of Internet Technology, 2014, 15(3): 413−425

[28] Rivest R L, Shamir A, Wagner D A. Time-lock puzzles and timed-release Crypto[J/OL]. Massachusetts Institute of Technology, [2025-05-10]. https://dl.acm.org/doi/abs/10.5555/888615

[29] Attrapadung N, Hanaoka G, Ogawa K, et al. Attribute-based

encryption for range attributes[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2018, 101(9): 1440−1455

[30] Miao Yinbin, Ma Jianfeng, Liu Ximeng, et al. Practical attribute-based multi-keyword search scheme in mobile crowdsourcing[J]. IEEE Internet of Things Journal, 2017, 5(4): 3008−3018

[31] Meng Lei, Xu Haitao, Tang Runze, et al. Dual hybrid CP-ABE: How to provide forward security without a trusted authority in vehicular opportunistic computing[J]. IEEE Internet of Things Journal, 2023, 11(5): 8800−8814

[32] Hao J, Tang W, Huang C, et al. Secure data sharing with flexible user access privilege update in cloud-assisted IoMT[J]. IEEE Transactions on Emerging Topics in Computing, 2021, 10(2): 933−947

[33] Yang Mengxue, Wang Huaqun, Wan Zhiguo, et al. PUL-ABE: An efficient and quantum-resistant CP-ABE with policy update in cloud storage[J]. IEEE Transactions on Services Computing, 2024, 17(3): 126−1139

[34] Guo Yuyan, Lu Zhenhua, Ge Hui, et al. Revocable blockchain-aided attribute-based encryption with escrow-free in cloud storage[J]. IEEE Transactions on Computers, 2023, 72(7): 1901−1912

[35] Ruan Conghao, Hu Chunqiang, Li Xingwang, et al. A revocable and fair outsourcing attribute-based access control scheme in metaverse[J]. IEEE Transactions on Consumer Electronics, 2024, 70(1): 3781−3791

[36] Xiong Hu, Qu Zheng, Huang Xin, et al. Revocable and unbounded attribute-based encryption scheme with adaptive security for integrating digital twins in Internet of things[J]. IEEE Journal on Selected Areas in Communications, 2023, 41(10): 3306−3317

[37] Zhang Leyou, Li Xinmin, Wu Qing, et al. Blockchain-aided anonymous traceable and revocable access control scheme with dynamic policy updating for the cloud IoT[J]. IEEE Internet of Things Journal, 2023, 11(1): 526−542

[38] Wei Jianghong, Chen Xiaofeng, Huang Xinyi, 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, 2021, 18(5): 2301−2315

[39] Phuong T V X, Ning Rui, Xin Chunsheng, et al. Puncturable attribute-based encryption for secure data delivery in Internet of things[C]// Proc of the 2018 IEEE Conf on Computer Communications. Piscataway, NJ : IEEE, 2018: 1511−1519

[40] Ghopur D, Ma Jianfeng, Ma Xindi, et al. Puncturable ciphertext-policy attribute-based encryption scheme for efficient and flexible user revocation[J]. Science China Information Sciences, 2023, 66(7): 172104

[41] Yang Mengxue, Wang Huaqun, He Debiao, et al. Puncturable attribute-based encryption from lattices for classified document sharing[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 4028−4042

[42] Miao Yinbin, Li Feng, Li Xinghua, et al. Verifiable outsourced attribute-based encryption scheme for cloud-assisted mobile e-health system[J]. IEEE Transactions on Dependable and Secure Computing, 2024, 21(4): 1845−1862

[43] Chen Shaobo, Li Jiguo, Zhang Yicheng, et al. Efficient revocable attribute-based encryption with verifiable data integrity[J]. IEEE Internet Things Journal, 2024, 11(6): 10441−10451

[44] De Caro A, Iovino V. jPBC: Java pairing based cryptography[C]// Proc of the 2011 IEEE Symp on Computers and Communications (ISCC). Piscataway, NJ : IEEE, 2011: 850−855



Yu Zengwen, born in 1985. PhD candidate, senior engineer. Student member of CCF. His main research interests include data analysis and data security.

余增文, 1985 年生。博士研究生，高级工程师。CCF 学生会员。主要研究方向为数据分析、数据安全。



Zhang Jiawei, born in 1985. PhD, lecturer. His main research interests include data security, wireless network security, blockchain, and cloud security.

张嘉伟, 1985 年生。博士，讲师。主要研究方向为数据安全、无线网络安全、区块链、云安全。



Jiang Qi, born in 1983. PhD, professor. Senior member of CCF. His main research interests include security protocols, Internet of things security, and data security.

姜　奇, 1983 年生。博士，教授。CCF 高级会员。主要研究方向为安全协议、物联网安全、数据安全。



Yang Li, born in 1977. PhD, professor. Senior member of CCF. His main research interests include applied cryptography, cloud security, and trusted computing.

杨　力, 1977 年生。博士，教授。CCF 高级会员。主要研究方向为应用密码学、云安全、可信计算。



Fang Zhi, born in 1979. PhD, professor. His main research interests include big data, AI, and data analysis.

方　志, 1979 年生。博士，研究员。主要研究方向为大数据、人工智能、数据分析。



Shi Runfang, born in 1990. Master, engineer. His main research interests include data governance and data security.

史润方, 1990 年生。硕士，工程师。主要研究方向为数据治理、数据安全。