密文长度固定的策略部分隐藏多授权机构CP-ABE方案

刘怡龙[1,2]，许盛伟[1,3]，岳梓岩[1,2]
（1.北京邮电大学网络空间安全学院，北京 100876；2.北京电子科技学院网络空间安全系，北京 100070；
3.北京电子科技学院信息安全研究所，北京 100070）

摘　要：针对现有访问策略隐藏的密文策略属性加密（CP-ABE）方案存在的安全性低、资源开销大的问题，提出了一种密文长度固定的策略部分隐藏多授权机构CP-ABE方案。首先，通过隐藏访问策略中的属性值，降低隐私数据泄露的风险；其次，通过固定密文长度和使用外包解密技术，减少用户的资源开销；最后，采用多授权机构管理机制，避免部署单一授权机构易产生的密钥托管问题。通过安全分析证明了方案在标准模型中满足选择明文攻击下的密文不可区分性，以及方案隐藏的访问策略和产生的外包密钥能够抵抗属性值猜测攻击。通过与已有方案的性能对比，证明了所提方案的总体资源开销更小。

关键词：密文策略属性加密；策略部分隐藏；密文长度固定；多授权机构；外包解密
中图分类号：TP393
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024142

Partially hidden policy multi-authority CP-ABE scheme with constant length ciphertext

LIU Yilong[1,2], XU Shengwei[1,3], YUE Ziyan[1,2]
1. School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
2. Department of Cyberspace Security, Beijing Electronic Science and Technology Institute, Beijing 100070, China
3. Institute of Information Security, Beijing Electronic Science and Technology Institute, Beijing 100070, China

Abstract: To solve the problems of low security and high resource overhead of existing hidden policy ciphertext policy attribute-based encryption (CP-ABE) schemes, a partially hidden policy multi-authority CP-ABE scheme with constant length ciphertext was proposed. Firstly, the values of the attributes in the access policy were hidden, enabling the proposed scheme to reduce the risk of private data leakage. Secondly, by fixing the ciphertext length and using outsourcing decryption techniques, the resource overhead for the user was reduced in the proposed scheme. Finally, the multi-authority management mechanism was used so that the proposed scheme avoided the key escrow problem that can easily arise when using a single authoritative authority. The security analysis proves that the proposed scheme satisfies the indistinguishability under chosen plaintext attack in the standard model, as well as the scheme's hidden access policy and the generated outsourcing key can resist attribute value guessing attack. The overall resource overhead of the proposed scheme is proven to be lower by comparing its performance with the existing schemes.

Keywords: CP-ABE, policy partially hidden, constant ciphertext length, multi-authority, outsourcing decryption

0　引言

云计算因其弹性存储和强大的计算能力，为计算模式带来了革命性的创新[1]。但随着物联网技术的发展，集中式云计算在面临持续且海量增长的数据量和数据处理需求时，无法满足用户低时延和高带宽需求[2-3]。边缘计算[4-5]作为一种去中心化计算

收稿日期：2024–04–08；修回日期：2024–07–08
通信作者：许盛伟，18510529691@163.com
基金项目：国家重点研发计划基金资助项目（No.2022YFB3104402）
Foundation Item：The National Key Research and Development Program of China (No.2022YFB3104402)

范例，因更靠近数据源使其相比于集中式云计算具有数据处理快和能源消耗低等优点，目前已被广泛应用于智能电网[6]、智慧交通[7]和智慧医疗[8]等领域。虽然边缘计算可有效解决数据传输时延和网络带宽瓶颈等问题，但仍面临着隐私保护、密钥管理和访问控制等数据安全问题。建立高效灵活的访问控制机制是保证网络数据安全的重要手段，可有效防止未经授权的用户恶意访问数据。相比于基于角色和标识的访问控制[9-10]，基于密文策略的属性加密（CP-ABE, ciphertext policy attribute-based encryption）方案可以提供更加灵活、动态的细粒度访问控制[11-13]。

传统的CP-ABE方案数据访问策略是以明文形式包含在密文中，攻击者可以通过窃听访问策略来获取用户部分隐私数据。为了保证用户隐私数据的整体安全性，研究者们提出了许多基于策略隐藏CP-ABE方案。现有的基于策略隐藏的CP-ABE方案主要分为策略全隐藏[14-16]和策略部分隐藏2种，其中策略全隐藏CP-ABE方案在密文中隐藏了策略包含的所有属性信息；策略部分隐藏CP-ABE方案将属性分为属性名和属性值两部分，且仅在密文中隐藏了属性值。在不暴露用户隐私数据的前提下，策略部分隐藏CP-ABE方案比策略全隐藏CP-ABE方案更高效且实用。文献[17]首次将策略隐藏的概念引入到CP-ABE方案中，提出了2种策略部分隐藏CP-ABE方案。文献[18]通过在数据解密前增加属性测试阶段来判断用户属性是否满足访问策略，提出了一种支持高效解密测试的策略部分隐藏CP-ABE方案，减少了在解密阶段给未授权用户带来的大量不必要的计算开销。文献[19]提出了一种支持策略部分隐藏与测试的CP-ABE方案，相比于文献[18]的方案进一步减少了属性测试阶段的计算开销。文献[20]提出了一种支持策略隐藏的关键字搜索CP-ABE方案，将策略隐藏嵌入到基于属性的关键字搜索中以抵御关键字猜测攻击。文献[21]提出了一种可实现用户撤销、白盒追踪和策略部分隐藏的CP-ABE方案。文献[22]为了抵抗“假策略”攻击提出了一种访问策略隐藏且可验证的CP-ABE方案。以上方案由于部署单一授权机构和隐藏的访问策略不能抵抗属性值猜测攻击，存在密钥托管和用户隐私数据泄露的安全问题，且由于密文长度与属性数量有关，存在资源开销大的问题。为了解决密钥托管问题，文献[23-24]分别提出了一种支持策略部分隐藏的多授权机构CP-ABE方案，但同样存在资源开销大和隐藏的访问策略不能抵抗属性值猜测攻击的问题。文献[25]利用双指数技术提出了一种策略部分隐藏的CP-ABE方案。文献[26]提出了一种可实现访问策略部分隐藏、直接撤销和可验证外包解密的CP-ABE方案。文献[27]提出了一种支持访问策略部分隐藏、恶意用户白盒追踪、用户直接撤销和大规模属性空间的CP-ABE方案。与文献[18-19]类似，文献[28-29]分别提出了一种基于测试−解密−验证的策略部分隐藏的CP-ABE方案。虽然在文献[25-29]提出的方案中隐藏的访问策略可以抵抗属性值猜测攻击，但仍存在密钥托管和资源开销大的问题。

传统CP-ABE方案中，密文长度与访问结构中属性数量成正比，从而产生的资源消耗大，为了减少这一问题，文献[30]提出了一种适用于物联网应用的轻量级全安全CP-ABE方案，在该方案中解密计算开销和密文长度不变。文献[31]基于有序二元决策图（OBDD, ordered binary decision diagram）访问结构提出了一种密钥长度保持不变且密文长度仅与访问结构中有效路径个数有关的CP-ABE方案。文献[32]提出了一种适用于云辅助物联网的密钥和密文长度均不变，且支持可验证外包解密的CP-ABE方案。文献[33]提出了一种支持密文长度固定、恶意用户追踪和代理重加密功能的CP-ABE方案。以上方案通过减少密文长度，有效降低了用户的资源消耗，但由于在方案中使用的是单一授权机构且访问策略以明文形式随密文进行传输，因此存在密钥托管和泄露隐私数据的安全问题。文献[34]针对边缘计算辅助物联网提出了一种支持密文长度固定、多属性授权机构和属性间接撤销等功能的轻量级CP-ABE方案。文献[35]提出了一种支持多属性授权机构和属性直接撤销的CP-ABE方案，该方案中的密文长度与访问结构中包含的属性数量无关，而与管理访问结构中属性的授权机构数量有关。文献[34-35]中的方案通过减少密文长度和使用多属性授权管理机制，降低了用户资源消耗，解决了密钥托管问题，但仍存在攻击者通过窃听访问策略获取用户隐私数据的风险。文献[36]提出了一种可同时支持密文长度固定、访问策略全隐藏和多属性授权机构的CP-ABE方案，但该方案在数据解密过程中存在漏洞，当某一用户拥有的属性与访问策

略中包含的属性属于同一属性授权机构管理时，即使该用户拥有的属性不满足密文中的访问策略也可解密获得正确的明文信息。

通过对现有文献的分析可知，目前对同时支持密文长度固定、访问策略隐藏和多属性授权机构功能的CP-ABE方案的研究仍较少。为此，本文提出了一种密文长度固定的策略部分隐藏多授权机构CP-ABE方案，主要工作如下。

1) 本文方案通过隐藏访问策略中的属性值，降低了攻击者通过窃听访问策略来获取用户隐私数据的风险，并通过少量运算即可在不暴露用户属性值的前提下，快速判断用户拥有的属性集合是否满足访问策略。

2) 本文方案的密文长度固定，减少了用户资源的消耗，并利用外包解密技术进一步减少了用户的解密计算开销。

3) 本文方案采用多授权管理机制，避免了部署单一授权机构易产生的密钥托管问题。另外，本文方案还实现了基于白名单的恶意用户可追踪和基于代理的属性直接撤销机制。

4) 基于判定性q-BDHE（decisional q-bilinear diffie-hellman exponent）假设证明了本文提出的多授权机构CP-ABE方案在标准模型中满足选择明文攻击下的不可区分性（IND-CPA, indistinguishability under chosen plaintext attack），并基于DBDH（decisional bilinear diffie-hellman）假设和离散对数（DL, discrete logarithm）假设证明了本文方案隐藏的访问策略和产生的外包密钥能够抵抗属性值猜测攻击。通过理论和仿真实验分析，证明了本文方案比已有方案所需的计算、存储和通信开销更小。

1 预备知识

1.1 双线性映射

令G_1和G_T表示以素数$p > 2^\lambda$为阶的2个乘法循环群，其中λ为安全参数。双线性映射$\hat{e}:G_1 \times G_1 \rightarrow G_T$满足以下3个性质。

1) 双线性：对于任意的$g,h \in G_1$和$a,b \in Z_p$，$\hat{e}(g^a,h^b) = \hat{e}(g,h)^{ab}$成立。

2) 非退化性：对于任意的$g,h \in G_1$，$\hat{e}(g,h) \neq 1$成立。

3) 可计算性：对于任意的$g,h \in G_1$，可简单计算$\hat{e}(g,h)$。

1.2 与门访问结构

令$U = \{\text{att}_1,\text{att}_2,\cdots,\text{att}_m\}$表示系统属性集合，其中，$m$为系统包含的属性总数，$\text{att}_i(i \in [1,m])$为属性名称。令$V_i = \{v_{i,1},v_{i,2},\cdots,v_{i,|V_i|}\}$表示属性$\text{att}_i$的取值集合，其中，$|V_i|$为属性$\text{att}_i$包含的属性值个数，$v_{ij}(j \in [1,|V_i|])$为属性值。令$S = \{a_1,a_2,\cdots,a_m\}$表示用户属性集合，$W = \{w_1,w_2,\cdots,w_m\} = \Lambda_{i \in I_W} w_i$表示访问结构，其中，$I_W = \{i|i \in [1,m]\}$为下标索引集合。对于$\forall i \in [1,m]$，如果$a_i = w_i$，则表示$S$满足$W(S| = W)$；否则，表示$S$不满足$W(S| \neq W)$。

1.3 困难问题假设

1.3.1 判定性q-BDHE假设

在以素数p为阶的双线性群$(\hat{e},G_1,G_T)$下，其中，G_1的生成元为g，随机选择指数$s,a \in Z_p^*$，判定性q-BDHE假设定义为：给定$y = (g^s,g^a,g^{a^2},\cdots,g^{a^q},g^{a^{q+2}},\cdots,g^{a^{2q}}) \in {G_1}^{2q}$和$T \in G_T$，判定$T = \hat{e}(g,g)^{sa^{q+1}}$是否成立。

如果$|\Pr[\mathcal{A}(g,y,\hat{e}(g,g)^{sa^{q+1}}) = 0] - \Pr[\mathcal{A}(g,y,T) = 0]| \geqslant \varepsilon$，则攻击者$\mathcal{A}$在解决判定性q-BDHE假设时具有优势$\varepsilon$。

定义1 如果不存在多项式时间算法以不可忽略的优势解决判定性q-BDHE问题，则判定性q-BDHE假设成立。

1.3.2 DBDH假设

在以素数p为阶的双线性群$(\hat{e},G_1,G_T)$下，其中，G_1的生成元为g，选择随机数$a,b,c \in Z_p^*$，DBDH假设定义为：给定(g,g^a,g^b,g^c)和$T \in G_T$，判定$T = \hat{e}(g,g)^{abc}$是否成立。

如果$|\Pr[\mathcal{A}(g,g^a,g^b,g^c,\hat{e}(g,g)^{abc}) = 0] - \Pr[\mathcal{A}(g,g^a,g^b,g^c,T) = 0]| \geqslant \varepsilon$，则攻击者$\mathcal{A}$在解决DBDH假设时具有优势$\varepsilon$。

定义2 如果不存在多项式时间算法以不可忽略的优势解决DBDH问题，则DBDH假设成立。

1.3.3 DL假设

假设G_1为以素数p为阶且生成元为g的循环群，选择随机元素$A \in G_1$，DL假设定义为：给定g和A，计算使得$A = g^\alpha$成立的$\alpha \in Z_p^*$。

定义3 如果不存在多项式时间算法以不可忽略的优势解决DL问题，则DL假设成立。

1.4 属性值猜测攻击

属性值猜测攻击（AVGA, attribute value guess-

ing attack）作为一种离线字典攻击，通常是针对隐藏访问策略和外包密钥发起的。假设系统属性集合中的每一个属性包含的属性值个数是多项式大小的，AVGA的攻击过程为：攻击者首先在多项式时间内找到某一个判别式，然后将属性值放入判别式中来检查判别式是否成立；如果某一个属性值可以使判别式成立，则攻击者可以从隐藏的访问策略或外包密钥中推断出访问策略或用户属性包含的属性值。

2　相关定义

2.1　系统模型

本文提出了一种可适用于边缘计算场景中密文长度固定的策略部分隐藏多授权机构CP-ABE方案，其系统模型如图1所示。

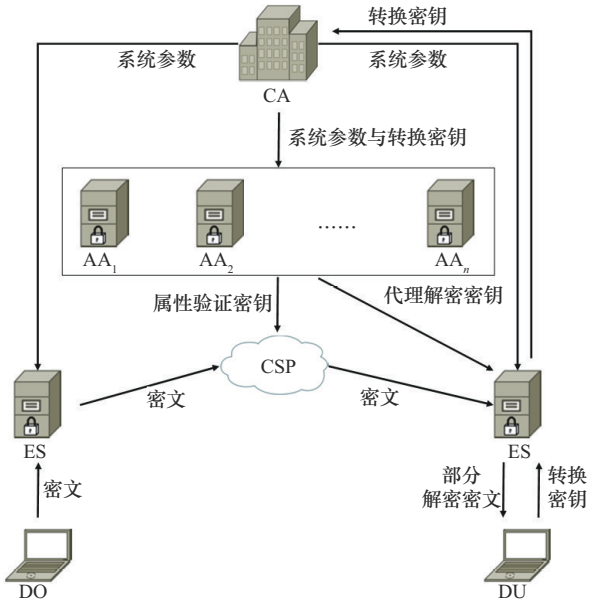

图1　系统模型

中央授权机构（CA, central authority）完全可信，其主要负责生成系统参数、维护恶意用户追踪列表、为用户生成全局唯一标识。

属性授权机构（AA, attribute authority）主要负责为不同的属性生成属性私钥和公钥；根据数据使用者发送的转换密钥，生成代理解密密钥和属性验证密钥，并将其分别发送给边缘服务器和云服务提供商。在本文方案设计中，假设系统中存在n个属性授权机构，不同的属性授权机构$\mathrm{AA}_i(i\in[1,n])$管理不同的属性集合U_i，令$U=\{U_1\cup U_2\cup\cdots\cup U_n\}=\bigcup_{i=1}^{n}U_i$表示系统属性集合。

云服务提供商（CSP, cloud service provider）主要负责存储数据拥有者上传的加密数据；利用属性验证密钥检查数据使用者拥有的属性集合是否满足密文的访问结构。在本文方案设计中，CSP被设定为诚实但好奇的，即CSP会诚实地执行相关任务，但会额外推断隐私数据。

边缘服务器（ES, edge server）主要负责将数据拥有者上传的加密数据发送给云服务提供商；利用代理解密密钥为数据使用者提供外包解密服务。在本文方案设计中，ES也被设定为诚实但好奇的。

数据拥有者（DO, data owner）根据定义的访问控制策略对明文信息进行加密，并发送给边缘服务器。

数据使用者（DU, data user）主要负责本地独立生成用户解密密钥和转换密钥，并将转换密钥发送给中央授权机构；利用用户解密密钥实现密文的完整性验证和完全解密。

2.2　算法定义

1) 系统初始化

该阶段包含由中央授权机构运行的CASetup和由属性授权机构运行的AASetup这2个多项式时间算法。

$\mathrm{CASetup}(\lambda)\rightarrow \mathrm{SP}$。该算法以安全参数$\lambda$作为输入，以系统参数SP作为输出。

$\mathrm{AASetup}(\mathrm{SP},U_i)\rightarrow(\mathrm{AAPK}_i,\mathrm{AASK}_i)$。该算法分别由系统中包含的$n$个属性授权机构独立运行，以系统参数SP和下标索引为$i(i\in[1,n])$的属性授权机构AA_i管理的属性集合$U_i=\{\mathrm{att}_{i,1},\mathrm{att}_{i,2},\cdots,\mathrm{att}_{i,|U_i|}\}$作为输入，其中，$|U_i|$为$U_i$中包含的属性个数，属性$\mathrm{att}_{i,j}\in U_i(j\in[1,|U_i|])$包含的属性值集合为$V_{i,j}=\{v_{i,j,1},v_{i,j,2},\cdots,v_{i,j,|V_{i,j}|}\}$，$|V_{i,j}|$为$\mathrm{att}_{i,j}$包含的属性值个数。以属性授权机构$\mathrm{AA}_i$的公钥$\mathrm{AAPK}_i$和主密钥$\mathrm{AASK}_i$作为输出。

2) 密钥生成

该阶段包含由用户运行的DUKeyGen和由属性授权机构运行的AAKeyGen这2个多项式时间算法。

$\mathrm{DUKeyGen}(\mathrm{SP})\rightarrow(\mathrm{USK},\mathrm{TSK})$。该算法以系统参数SP作为输入，以用户解密密钥USK和转换密钥TSK作为输出。

$\mathrm{AAKeyGen}(\mathrm{SP},\mathrm{AASK}_i,\mathrm{TSK},S_i,\mathrm{UID})\rightarrow(\mathrm{VSK}_{i,j},\mathrm{DSK}_{i,j})$。该算法以系统参数SP、属性授权机构$\mathrm{AA}_i$的主密钥$\mathrm{AASK}_i$、转换密钥TSK、用户属性集合$S$

中由AA_i管理的部分属性集合$S_i \in U_i$和用户身份标识UID作为输入，以属性验证密钥$VSK_{i,j}$和代理解密密钥$DSK_{i,j}$作为输出。

3) 数据加密

$Encrypt(SP,AAPK_i,M,W) \rightarrow CT$。该算法由数据拥有者运行，以系统参数SP、相关属性授权机构的公钥$AAPK_i$、明文数据M和访问结构W作为输入，以密文CT作为输出。

4) 数据解密

该阶段包含由云服务提供商运行的属性验证算法CSPVerify、由边缘服务器运行的外包解密算法ESDecrypt和由数据使用者运行的本地解密算法DUDecrypt这3个多项式时间算法。

$CSPVerify(SP,\{VSK_{i,j}\},CT) \rightarrow CT_{CSP}$。该算法以系统参数SP、属性验证密钥$VSK_{i,j}$和密文CT作为输入，如果用户属性集合$S$满足访问结构$W$，则验证成功，输出部分密文$CT_{CSP}$；否则，验证失败，输出⊥。

$ESDecrypt(SP,\{DSK_{i,j}\},CT_{CSP}) \rightarrow CT_{ES}$。该算法以系统参数SP、代理解密密钥$DSK_{i,j}$和部分密文$CT_{CSP}$作为输入，以部分解密密文$CT_{ES}$作为输出。

$DUDecrypt(SP,USK,CT_{ES}) \rightarrow M$。该算法以系统参数SP、用户解密密钥USK和部分解密密文CT_{ES}作为输入，以明文数据M作为输出。

2.3 安全模型

2.3.1 IND-CPA安全模型

本文将使用文献[37]中的安全模型来证明本文提出的多授权机构CP-ABE方案的安全性，模型具体过程如下。

初始化阶段。攻击者$\mathcal{A}$向挑战者$\mathcal{B}$提交挑战访问结构W^*。

参数设置阶段。挑战者$\mathcal{B}$生成系统参数SP和属性授权机构$AA_i(i \in [1,n])$的公钥$AAPK_i$，并发送给攻击者$\mathcal{A}$。攻击者$\mathcal{A}$向挑战者$\mathcal{B}$提交已攻破的属性授权机构的下标集合$I \subset [1,n]$，挑战者$\mathcal{B}$将属性授权机构$AA_i(i \in I)$的主密钥$AASK_i$发送给攻击者$\mathcal{A}$。

密钥查询阶段1。攻击者$\mathcal{A}$向挑战者$\mathcal{B}$提交用户身份标识UID和用户属性集合S进行密钥查询，其中$S \cup (\bigcup_{i \in I} U_i)$不满足$W^*$。

挑战阶段。攻击者$\mathcal{A}$提交长度相等的2个明文数据M_0和M_1给挑战者$\mathcal{B}$。挑战者$\mathcal{B}$选择随机数$b \in \{0,1\}$，根据W^*对M_b进行加密，并将密文发送给攻击者$\mathcal{A}$。

密钥查询阶段2。如密钥查询阶段1，攻击者$\mathcal{A}$继续向挑战者$\mathcal{B}$提交用户身份标识UID和用户属性集合S进行密钥查询，同样$S \cup (\bigcup_{i \in I} U_i)$不满足$W^*$。

猜测阶段。攻击者$\mathcal{A}$输出对b的猜测$b' \in \{0,1\}$，如果$b' = b$，那么称攻击者$\mathcal{A}$赢得了该游戏。攻击者$\mathcal{A}$在该游戏过程中的优势被定义为$|\Pr[b' = b] - \frac{1}{2}|$。

定义4 如果没有多项式时间的攻击者能够以不可忽略的优势在该游戏中取得胜利，则证明本文提出的多授权机构CP-ABE方案满足IND-CPA安全。

2.3.2 访问策略隐藏抵抗AVGA的安全模型

本文将使用文献[29]中用于证明隐藏的访问策略能够抵抗AVGA的安全模型来证明本文方案隐藏的访问策略的安全性，模型的具体过程如下。

初始化阶段。攻击者$\mathcal{A}$向挑战者$\mathcal{B}$提交2个包含相同属性名但属性值仅有一个相同的挑战访问结构W_0和W_1，将W_0和W_1中唯一相同的属性值定义为w^*。

参数设置阶段。挑战者$\mathcal{B}$生成系统参数SP和属性授权机构$AA_i(i \in [1,n])$的公钥$AAPK_i$，并发送给攻击者$\mathcal{A}$。

密钥查询阶段1。攻击者$\mathcal{A}$向挑战者$\mathcal{B}$提交用户属性列表S进行密钥查询，其中$w^* \notin S$。

挑战阶段。攻击者$\mathcal{A}$提交数据M给挑战者$\mathcal{B}$。挑战者$\mathcal{B}$选择随机数$b \in \{0,1\}$，根据W_b对M进行加密，并将密文发送给攻击者$\mathcal{A}$。

密钥查询阶段2。如密钥查询阶段1，攻击者$\mathcal{A}$继续向挑战者$\mathcal{B}$提交用户属性列表S进行密钥查询，同样$w^* \notin S$。

猜测阶段。攻击者$\mathcal{A}$输出对b的猜测$b' \in \{0,1\}$，如果$b' = b$，那么称攻击者$\mathcal{A}$赢得了该游戏。攻击者$\mathcal{A}$在该游戏过程中的优势被定义为$|\Pr[b' = b] - \frac{1}{2}|$。

定义5 如果没有多项式时间的攻击者能够以不可忽略的优势在该游戏中取得胜利，则证明本文方案隐藏的访问策略能够抵抗属性值猜测攻击。

2.3.3 外包密钥抵抗AVGA的安全模型

本文使用文献[29]中用于证明外包密钥能够抵抗AVGA的安全模型，来证明本文方案属性授权机构生成的代理解密密钥和属性验证密钥的安全性，模型的具体过程如下。

初始化阶段。攻击者$\mathcal{A}$向挑战者$\mathcal{B}$提交挑战用户身份标识UID^*和该用户拥有的2个不同属性的属性值v_0和v_1。

参数设置阶段。挑战者$\mathcal{B}$生成系统参数SP和属性授权机构$\mathrm{AA}_i(i\in[1,n])$的公钥AAPK_i，并发送给攻击者$\mathcal{A}$。

密钥查询阶段1。攻击者$\mathcal{A}$向挑战者$\mathcal{B}$提交用户身份标识UID和该用户拥有的属性列表S进行密钥查询，其中$\mathrm{UID}\neq\mathrm{UID}^*$。

挑战阶段。挑战者$\mathcal{B}$选择随机数$b\in\{0,1\}$，生成关于属性值v_b的属性验证密钥和代理解密密钥，并发送给攻击者$\mathcal{A}$。

密钥查询阶段2。如密钥查询阶段1，攻击者$\mathcal{A}$继续向挑战者$\mathcal{B}$提交用户身份标识UID和该用户拥有的属性列表S进行密钥查询，同样$\mathrm{UID}\neq\mathrm{UID}^*$。

猜测阶段。攻击者$\mathcal{A}$输出对b的猜测$b'\in\{0,1\}$，如果$b'=b$，那么称攻击者$\mathcal{A}$赢得了该游戏。攻击者$\mathcal{A}$在该游戏过程中的优势被定义为$|\Pr[b'=b]-\frac{1}{2}|$。

定义6 如果没有多项式时间的攻击者能够以不可忽略的优势在该游戏中取得胜利，则证明本文方案的代理解密密钥和属性验证密钥能够抵抗属性值猜测攻击。

3 方案设计

3.1 系统初始化

$\mathrm{CASetup}(\lambda)\rightarrow\mathrm{SP}$。中央授权机构首先选择以素数$p$为阶的2个乘法循环群$G_1$和$G_T$，并从群$G_1$中选择2个随机元素$g$和$h$；然后令$\hat{e}$表示$G_1\times G_1\rightarrow G_T$的双线性映射，并挑选2个安全的哈希函数$H_1:\{0,1\}^*\rightarrow Z_p^*$和$H_2:G_T\rightarrow Z_p^*$；接下来选择随机数$\tau\in Z_p^*$，并计算$g_1=g^\tau$；最后中央授权机构输出系统参数为

$$\mathrm{SP}=\{p,G,G_\mathrm{T},\hat{e},g,h,g_1,H_1,H_2\}$$

$\mathrm{AASetup}(\mathrm{SP},U_i)\rightarrow(\mathrm{AAPK}_i,\mathrm{AASK}_i)$。对于由属性授权机构$\mathrm{AA}_i$管理的属性集合$U_i$中的属性$\mathrm{att}_{i,j}(j\in[1,|U_i|])$的第$k$个属性值$v_{i,j,k}(k\in[1,|V_{i,j}|])$，属性授权机构$\mathrm{AA}_i$从$Z_p^*$中选择随机数$x_{i,j,k}$，并计算$X_{i,j,k}=h^{x_{i,j,k}}$；然后$\mathrm{AA}_i$选择随机数$y_i\in Z_p^*$，并计算$Y_i=\hat{e}(g_1,h)^{y_i}=\hat{e}(g,h)^{\tau y_i}$；最后$\mathrm{AA}_i$输出公钥和主密钥为

$$\mathrm{AAPK}_i=\{\{X_{i,j,k}\}_{k\in[1,|V_{i,j}|],j\in[1,|U_i|]},Y_i\}$$
$$\mathrm{AASK}_i=\{\{x_{i,j,k}\}_{k\in[1,|V_{i,j}|],j\in[1,|U_i|]},y_i\}$$

3.2 密钥生成

$\mathrm{DUKeyGen}(\mathrm{SP})\rightarrow(\mathrm{USK},\mathrm{TSK})$。数据使用者首先从$Z_p^*$中选择随机数$u$作为用户解密密钥USK，并计算转换密钥$\mathrm{TSK}=g_1{}^u=g^{\tau u}$；然后数据使用者将用户身份标识UID、转换密钥TSK和拥有的用户属性集合S发送给中央授权机构，以申请属性验证密钥和代理解密密钥。

中央授权机构收到密钥申请后，首先检查追踪列表T中是否已包含转换密钥TSK，如果追踪列表T中已包含TSK，则密钥生成过程终止，数据使用者需重新选择用户解密密钥USK，否则，中央授权机构将数据元组$(\mathrm{UID},\mathrm{TSK})$添加到追踪列表$T$中；然后中央授权机构根据用户属性集合$S$，将用户身份标识UID、转换密钥TSK和部分用户属性集合S_i发送给相关属性授权机构AA_i，用于计算属性验证密钥和代理解密密钥。

$\mathrm{AAKeyGen}(\mathrm{SP},\mathrm{AASK}_i,\mathrm{TSK},S_i,\mathrm{UID})\rightarrow(\mathrm{VSK}_{i,j},\mathrm{DSK}_{i,j})$。对于用户部分属性集合$S_i$中包含的每一个属性值$v_{i,j,k}$，属性授权机构$\mathrm{AA}_i$首先选择随机数$r_{i,j,k}\in Z_p^*$，并计算属性验证密钥$\mathrm{VSK}_{i,j}=\{\mathrm{K1}_{i,j}=\mathrm{TSK}^{x_{i,j,k}}g^{r_{i,j,k}H_1(\mathrm{UID})},\mathrm{K2}_{i,j}=h^{r_{i,j,k}}\}$；然后，属性授权机构$\mathrm{AA}_i$计算代理解密密钥$\mathrm{DSK}_{i,j}=\mathrm{TSK}^{y_i}g_1{}^{x_{i,j,k}H_1(\mathrm{UID})}=g^{\tau u y_i}g^{\tau x_{i,j,k}H_1(\mathrm{UID})}$；最后$\mathrm{AA}_i$分别将$\{\mathrm{UID},\bar{S}_i,\{\mathrm{VSK}_{i,j}\}\}$和$\{\mathrm{UID},\bar{S}_i,\{\mathrm{DSK}_{i,j}\}\}$发送给云服务提供商和边缘服务器，其中$\bar{S}_i$表示将$S_i$中的属性值$v_{i,j,k}$隐藏起来，只保留对应的属性名称$\mathrm{att}_{i,j}$。

3.3 数据加密

$\mathrm{Encrypt}(\mathrm{SP},\mathrm{AAPK}_i,M,W)\rightarrow\mathrm{CT}$。数据拥有者首先随机选择秘密值$s\in Z_p^*$，并计算

$$C_0=M\left(\prod_{Y_i\in\mathrm{AAPK}_W}Y_i\right)^s=M\hat{e}(g,h)^{s\tau\sum_{Y_i\in\mathrm{AAPK}_W}y_i}$$
$$C_1=g^s$$
$$C_2=h^s$$
$$C_3=\hat{e}\left(g_1,\prod_{X_{i,j,k}\in\mathrm{AAPK}_W}X_{i,j,k}\right)^s=\hat{e}(g,h)^{s\tau\sum_{X_{i,j,k}\in\mathrm{AAPK}_W}x_{i,j,k}}$$

$$C_4 = H_2\left(\left(\prod_{Y_i \in \mathrm{AAPK}_W} Y_i\right)^s\right) = H_2\left(\hat{e}(g,h)^{s\tau \sum_{Y_i \in \mathrm{AAPK}_W} y_i}\right)$$

其中，AAPK_W是管理访问策略W中属性的属性授权机构的集合；然后数据拥有者将访问结构W中包含的属性所对应的属性值$v_{i,j,k}$隐藏起来，只保留对应的属性名称$\mathrm{att}_{i,j}$，将修改后的访问结构定义为$\overline{W}$;最后数据拥有者输出密文为

$$\mathrm{CT} = \{\overline{W}, C_0, C_1, C_2, C_3, C_4\}$$

3.4　数据解密

$\mathrm{CSPVerify}(\mathrm{SP}, \{\mathrm{VSK}_{i,j}\}, \mathrm{CT}) \rightarrow \mathrm{CT}_{\mathrm{CSP}}$。云服务提供商收到用户的密文查询请求后，首先根据用户身份标识UID汇总相关属性授权机构发送的属性验证密钥$\{\mathrm{UID}, \bar{S}, \{\mathrm{VSK}_{i,j}\}\}$，并对比$\overline{W}$包含的属性名和$\bar{S}$包含的属性名，检查$\bar{S}| = \overline{W}$是否成立，如果$\bar{S}| \neq \overline{W}$，算法输出⊥，云服务提供商拒绝用户此次提交的密文查询请求，如果$\bar{S}| = \overline{W}$，则云服务提供商将密文CT中包含的C_3发送给用户，用户利用用户解密密钥USK计算属性验证部分$C_3' = {C_3}^u = \hat{e}(g,h)^{s\tau u \sum_{X_{i,j,k} \in \mathrm{AAPK}_W} x_{i,j,k}}$后再将其发送给云服务提供商；接下来，云服务提供商验证$\hat{e}\left(\prod_{\mathrm{att}_{i,j} \in \bar{W}} \mathrm{K1}_{i,j}, C_2\right) = C_3' \hat{e}\left(\prod_{\mathrm{att}_{i,j} \in \bar{W}} \mathrm{K2}_{i,j}, C_1\right)^{H_1(\mathrm{UID})}$是否成立，如果成立，则表明用户拥有的属性集合满足密文的访问策略，云服务提供商将部分密文$\mathrm{CT}_{\mathrm{CSP}} = \{\overline{W}, C_0, C_2, C_3, C_4\}$发送给边缘服务器，否则，算法输出⊥，云服务提供商拒绝用户此次提交的密文查询请求。

$\mathrm{ESDecrypt}(\mathrm{SP}, \{\mathrm{DSK}_{i,j}\}, \mathrm{CT}_{\mathrm{CSP}}) \rightarrow \mathrm{CT}_{\mathrm{ES}}$。边缘服务器收到云服务提供商发送的密文$\mathrm{CT}_{\mathrm{CSP}}$后，首先根据用户身份标识UID汇总相关属性授权机构发送的代理解密密钥$\{\mathrm{UID}, \bar{S}, \{\mathrm{DSK}_{i,j}\}\}$；然后计算

$$C_0' = \frac{\hat{e}\left(\prod_{\mathrm{att}_{i,j} \in \bar{W}} \mathrm{DSK}_{i,j}, C_2\right)}{{C_3}^{H_1(\mathrm{UID})}} = \frac{\hat{e}(g,h)^{s\tau u \sum_{Y_i \in \mathrm{AAPK}_W} y_i} \hat{e}(g,h)^{s\tau H_1(\mathrm{UID}) \sum_{X_{i,j,k} \in \mathrm{AAPK}_W} x_{i,j,k}}}{\hat{e}(g,h)^{s\tau H_1(\mathrm{UID}) \sum_{X_{i,j,k} \in \mathrm{AAPK}_W} x_{i,j,k}}} = \hat{e}(g,h)^{s\tau u \sum_{Y_i \in \mathrm{AAPK}_W} y_i}$$

最后，边缘服务器生成部分解密密文$\mathrm{CT}_{\mathrm{ES}} = \{C_0, C_0', C_4\}$，并将其发送给用户。

$\mathrm{DUDecrypt}(\mathrm{SP}, \mathrm{USK}, \mathrm{CT}_{\mathrm{ES}}) \rightarrow M$。用户收到边缘服务器发送的部分解密密文$\mathrm{CT}_{\mathrm{ES}}$后，首先利用本地存储的用户解密密钥USK进行计算得到$C^* = (C_0')^{\frac{1}{\mathrm{USK}}} = \hat{e}(g,h)^{s\tau \sum_{Y_i \in \mathrm{AAPK}_W} y_i}$；然后用户对比$H_2(C^*)$和$C_4$是否相等，如果$H_2(C^*) = C_4$，则说明密文在存储和传输过程中没有被恶意篡改，用户可进一步计算得到明文数据$M = \frac{C_0}{C^*} = \frac{M\hat{e}(g,h)^{s\tau \sum_{Y_i \in \mathrm{AAPK}_W} y_i}}{\hat{e}(g,h)^{s\tau \sum_{Y_i \in \mathrm{AAPK}_W} y_i}}$。

3.5　追踪和撤销

1) 恶意用户追踪。由于中央授权机构维护的追踪列表T中包含的转换密钥TSK和用户身份标识UID是一一对应的，因此可以通过恶意用户泄露的用户解密密钥USK计算转换密钥TSK，从而实现对恶意用户抗抵赖的白名单追踪。

2) 用户或属性撤销。由于密文的整个解密过程包含3部分：云服务提供商执行的属性验证、边缘服务器执行的外包代理解密和数据使用者执行的本地解密。因此属性授权机构可以通过更新云服务提供商存储的属性验证密钥$\mathrm{VSK}_{i,j}$或边缘服务器存储的代理解密密钥$\mathrm{DSK}_{i,j}$，实现用户或用户某一个属性的直接撤销。

4　安全性与理论分析

4.1　安全性讨论

4.1.1　密钥免托管

本文方案利用多授权管理机制，将系统属性集合分配给不同的属性授权机构管理，且属性验证密钥$\mathrm{VSK}_{i,j}$和代理解密密钥$\mathrm{DSK}_{i,j}$是根据用户提供的转换密钥TSK计算的，因此不存在某一属性授权机构具有解密任何密文的能力，避免了密钥托管问题。

4.2.2　抗共谋攻击

属性验证密钥$\mathrm{VSK}_{i,j}$和代理解密密钥$\mathrm{DSK}_{i,j}$是与用户身份标识UID和转换密钥TSK绑定的，因此云服务提供商和边缘服务器无法联合其他用户的属性验证密钥和代理解密密钥为某一用户提供属性验证和外包解密服务。

4.1.3　前向安全性

在本文方案的系统模型介绍中，将云服务提供商和边缘服务器设定为诚实但好奇的，使得本文方案可以通过更新云服务提供商存储的属性验证密钥$\mathrm{VSK}_{i,j}$或边缘服务器存储的代理解密密钥$\mathrm{DSK}_{i,j}$，实现基于代理的属性直接撤销机制，使被撤销的用

户无法继续解密密文，保证方案的前向安全性。

4.1.4　外包解密安全

在本文方案设计中，完整的解密密钥可分为2个部分：用户解密密钥USK是由用户独立生成的；代理解密密钥$\mathrm{DSK}_{i,j}$是由属性授权机构根据用户提供的转换密钥TSK生成的。因此即使攻击者获得用户的全部代理解密密钥，并运行ESDecrypt解密算法得到$C_0' = \hat{e}(g,h)^{s\tau u \sum_{Y_i \in \mathrm{AAPK}_w} y_i}$，但由于不知道具体的用户解密密钥，使其无法通过计算得到$C^* = (C_0')^{\frac{1}{\mathrm{USK}}} = \hat{e}(g,h)^{s\tau \sum_{Y_i \in \mathrm{AAPK}_w} y_i}$，从而无法获得具体的明文数据。

4.2　安全性分析

4.2.1　IND-CPA安全证明

定理1　如果判定性q-BDHE假设成立，则不存在多项式时间的攻击者能够以不可忽略的优势攻破本文提出的多授权CP-ABE方案。

证明　假设存在一个多项式时间的攻击者$\mathcal{A}$可以在本文所定义的IND-CPA安全模型下，以不可忽略的优势ε攻破本文提出的多授权CP-ABE方案，那么挑战者$\mathcal{B}$则可以以$\frac{\varepsilon}{2}$的优势攻破判定性q-BDHE假设。挑战者$\mathcal{B}$输入判定性q-BDHE挑战元组(g,y,T)，其中，$y = (g^s,g^a,g^{a^2},\cdots,g^{a^q},g^{a^{q+2}},\cdots,g^{a^{2q}}) \in {G_1}^{2q}$，$T$为$G_T$中的随机元素或者$T = \hat{e}(g,g)^{sa^{q+1}}$。不失一般性，本文设置$\beta \in \{0,1\}$，如果$\beta = 0$，那么$T = \hat{e}(g,g)^{sa^{q+1}}$；否则，$T$为$G_T$中的随机元素。挑战者$\mathcal{B}$和攻击者$\mathcal{A}$按如下步骤模拟交互游戏过程。

初始化阶段。攻击者$\mathcal{A}$向挑战者$\mathcal{B}$发送挑战访问结构$W^* = \{w_1,w_2,\cdots,w_m\} = \Lambda_{l \in L_{W^*}} w_l$，其中$L_{W^*} = \{1,2,\cdots,m\}$为下标索引集合。不失一般性，本文假设只有属性授权机构AA_1未被攻击者$\mathcal{A}$攻破，AA_1管理的属性集合U_1的下标索引集合记为L_{AA_1}，且$L^* = L_{\mathrm{AA}_1} \cap L_{W^*} \neq \varnothing$。挑战者$\mathcal{B}$初始化列表$\mathcal{L}$来记录与攻击者$\mathcal{A}$的交互结果。

参数设置阶段。挑战者$\mathcal{B}$首先选择系统参数$\{p,G_1,G_T,\hat{e},g,H_1,H_2\}$，并选择随机数$\delta,\tau \in Z_p^*$计算$h = g^{\delta}$和$g_1 = g^{\tau}$；然后挑战者$\mathcal{B}$从$L^*$中随机选择下标索引$l^* \in L^*$，且将下标索引$l^*$在$W^*$中所对应的属性记为$w^* \in W^*$，并为系统中的每一个属性授权机构$\mathrm{AA}_i$选择随机数$y_i \in Z_p^*$，为$\mathrm{AA}_i$管理的属性集合$U_i$中的每一个属性值$v_{i,j,k}$选择随机数$x_{i,j,k} \in Z_p^*$；接下来，挑战者$\mathcal{B}$利用以下方式计算属性授权机构$\mathrm{AA}_i$的公钥。

① 如果$w^* \in U_i$，则$Y_i = \hat{e}(g,g)^{\delta\tau y_i}\hat{e}(g,g)^{a^{q+1}}$，否则，$Y_i = \hat{e}(g,g)^{\delta\tau y_i}$。

②如果$v_{i,j,k} = w^*$，则$X_{i,j,k} = g^{\delta x_{i,j,k}} \prod_{t \in L^* - \{l^*\}} g^{a^{q+1-t}}$。

③ 如果$v_{i,j,k} \neq w^* \wedge v_{i,j,k} \in W^* \wedge l \in L^*$，其中$l$为$v_{i,j,k}$在$W^*$中的下标索引，则$X_{i,j,k} = g^{\delta x_{i,j,k}} g^{-a^{q+1-l}}$。

④ 如果$v_{i,j,k} \neq w^* \wedge v_{i,j,k} \in W^* \wedge l \notin L^*$或者$v_{i,j,k} \notin W^*$，则$X_{i,j,k} = g^{\delta x_{i,j,k}}$。

最后，挑战者$\mathcal{B}$将$\mathrm{SP} = \{p,G_1,G_T,\hat{e},g,h,g_1,H_1,H_2\}$、$\mathrm{AAPK}_i = \{\{X_{i,j,k}\},Y_i\}_{i \in [1,n]}$和$\mathrm{AASK}_i = \{\{x_{i,j,k}\},y_i\}_{i \in [2,n]}$发送给攻击者$\mathcal{A}$。

密钥查询阶段1。攻击者$\mathcal{A}$提交(UID,S)向挑战者$\mathcal{B}$进行密钥查询，其中$S \cup (\bigcup_{i \in [2,n]} U_i)$不满足$W^*$。挑战者$\mathcal{B}$首先检查UID是否已存在列表$\mathcal{L}$中，如果$\mathcal{L}$中不存在该用户标识UID，那么挑战者$\mathcal{B}$选择随机数$u \in Z_p^*$，令$\mathrm{USK} = u$并将$(\mathrm{UID},u)$保存到列表$\mathcal{L}$中；然后，挑战者$\mathcal{B}$为$S$中的每一个属性值$v_{i,j,k}$选择随机数$r_{i,j,k} \in Z_p^*$，计算$\mathrm{VSK}_{i,j} = \{\mathrm{K1}_{i,j} = g^{\tau u x_{i,j,k}} g^{r_{i,j,k}H_1(\mathrm{UID})}, \mathrm{K2}_{i,j} = g^{\delta r_{i,j,k}}\}$，并利用以下方式计算$\mathrm{DSK}_{i,j}$。

用户属性集合S的下标索引集合记为L_S，由于$S \cup (\bigcup_{i \in [2,n]} U_i)$不满足$W^*$，因此$L^* \not\subset L_S$，必然存在一个属性值$v'_{i,j,k}$满足$v'_{i,j,k} \notin S \wedge v'_{i,j,k} \in W^*$，其下标索引$l'$满足$l' \notin L_S \wedge l' \in L^*$。

① 如果$v_{i,j,k} = w^*$，则$\mathrm{DSK}_{i,j} = g^{\tau u y_i} g^{\tau x_{i,j,k} H_1(\mathrm{UID})} \prod_{t \in L^* - \{l^*,l'\}} g^{-a^{q+1-t+l'}}$。

② 如果$v_{i,j,k} \neq w^* \wedge v_{i,j,k} \in W^* \wedge l \in L^*$，其中$l$为$v_{i,j,k}$在$W^*$中的下标索引，则$\mathrm{DSK}_{i,j} = g^{\tau u y_i} g^{\tau x_{i,j,k} H_1(\mathrm{UID})} g^{a^{q+1-l+l'}}$。

③ 如果$v_{i,j,k} \neq w^* \wedge v_{i,j,k} \in W^* \wedge l \notin L^*$或者$v_{i,j,k} \notin W^*$，则$\mathrm{DSK}_{i,j} = g^{\tau u y_i} g^{\tau x_{i,j,k} H_1(\mathrm{UID})}$。

最后，挑战者$\mathcal{B}$将$\{\{\mathrm{VSK}_{i,j}\},\{\mathrm{DSK}_{i,j}\},u\}$发送给攻击者$\mathcal{A}$。

挑战阶段。攻击者$\mathcal{A}$提交长度相等的2个明文数据M_0和M_1给挑战者$\mathcal{B}$。挑战者$\mathcal{B}$选择随机数$b \in \{0,1\}$,根据W^*对数据M_b进行加密，并将密文CT返回给攻击者。挑战者$\mathcal{B}$选择随机数$s \in Z_p^*$，并

按如下方式计算密文CT = $\{\bar{W}^*, C_0, C_1, C_2, C_3, C_4\}$

$$C_0 = M_b\left(\prod_{Y_i \in \mathrm{AAPK}_{W^*}} Y_i\right)^s = M_b T\hat{e}(g,g)^{s\delta\tau \sum_{Y_i \in \mathrm{AAPK}_{W^*}} y_i}$$

$$C_1 = g^s$$

$$C_2 = g^{\delta s}$$

$$C_3 = \hat{e}\left(g_1, \prod_{X_{i,j,k} \in \mathrm{AAPK}_{W^*}} X_{i,j,k}\right)^s = \hat{e}(g,g)^{s\tau\delta \sum_{X_{i,j,k} \in \mathrm{AAPK}_{W^*}} x_{i,j,k}}$$

$$C_4 = H_2\left(\left(\prod_{Y_i \in \mathrm{AAPK}_{W^*}} Y_i\right)^s\right) = H_2\left(\hat{e}(g,g)^{s\delta\tau \sum_{Y_i \in \mathrm{AAPK}_{W^*}} y_i}\right)$$

其中，$\bar{W}^*$表示将W^*中的属性值$v_{i,j,k}$隐藏起来，只保留对应的属性名称$\mathrm{att}_{i,j}$。

密钥查询阶段2。同密钥查询阶段1一样，攻击者$\mathcal{A}$向挑战者$\mathcal{B}$提交查询与用户属性列表S相关的密钥，但$S \cup (\bigcup_{i \in [2,n]} U_i)$不满足$W^*$。

猜测阶段。攻击者$\mathcal{A}$输出b的猜测结果b'。如果$b' = b$，则挑战者$\mathcal{B}$输出0，表示猜测$T = \hat{e}(g,g)^{a^{q+1}s}$；否则挑战者$\mathcal{B}$输出1，表示猜测$T$为$G_T$中的随机元素。

①如果$T = \hat{e}(g,g)^{a^{q+1}s}$，则表明CT是根据$W^*$对数据$M_b$进行加密的结果。由于攻击者$\mathcal{A}$的优势为$\varepsilon$，因此在该情况下攻击者$\mathcal{A}$正确猜测出$b$的概率为$\Pr(\mathcal{A}(b' = b)) = \frac{1}{2} + \varepsilon$。

②如果T为G_T中的随机元素，在该情况下攻击者$\mathcal{A}$正确猜测出b的概率为$\Pr(\mathcal{A}(b' = b)) = \frac{1}{2}$。

综上所述，挑战者$\mathcal{B}$解决判定性q-BDHE问题的优势为

$$\frac{1}{2}(\Pr[\mathcal{B}(g,y,\hat{e}(g,g)^{sa^{q+1}}) = 0]) + \frac{1}{2}(\Pr[\mathcal{B}(g,y,T) = 0]) - \frac{1}{2} = \frac{\varepsilon}{2}$$

由于不存在多项式时间的攻击者能够以不可忽略的优势解决判定性q-BDHE问题，因此本文提出的多授权CP-ABE方案满足IND-CPA安全。证毕。

4.2.2 访问策略隐藏抵抗AVGA的安全证明

定理2 如果DBDH假设成立，则不存在多项式时间的攻击者能够以不可忽略的优势利用属性值猜测攻击获取本文方案访问策略隐藏的属性值。

证明 假设存在一个多项式时间的攻击者$\mathcal{A}$可以在本文所定义的访问策略隐藏抵抗AVGA的安全模型下，以不可忽略的优势ε获取本文方案访问策略隐藏的属性值，那么挑战者$\mathcal{B}$则可以以$\frac{\varepsilon}{2}$的优势攻破DBDH假设。挑战者$\mathcal{B}$输入DBDH挑战元组(g, g^a, g^b, g^c, T)，其中T为G_T中的随机元素或者$T = \hat{e}(g,g)^{abc}$。不失一般性，本文设置$\beta \in \{0,1\}$，如果$\beta = 0$，那么$T = \hat{e}(g,g)^{abc}$；否则，T为G_T中的随机元素。挑战者$\mathcal{B}$和攻击者$\mathcal{A}$按如下步骤模拟交互游戏过程。

初始化阶段。攻击者$\mathcal{A}$向挑战者$\mathcal{B}$提交2个包含相同属性名但属性值仅有一个相同的挑战访问结构W_0和W_1。挑战者$\mathcal{B}$首先选择随机数$b \in \{0,1\}$，设置$W^* = W_b$，然后将W_0和W_1中唯一相同的属性值定义为w^*，最后初始化列表$\mathcal{L}$来记录与攻击者$\mathcal{A}$的交互结果。

参数设置阶段。挑战者$\mathcal{B}$首先选择系统参数$\{p, G_1, G_T, \hat{e}, g, H_1, H_2\}$和随机数$\delta \in Z_p^*$，令$g_1 = g^a$并计算$h = g^\delta$；然后挑战者$\mathcal{B}$为系统中的每一个属性授权机构$\mathrm{AA}_i$选择随机数$y_i \in Z_p^*$计算$Y_i = \hat{e}(g^a, g^\delta)^{y_i} = \hat{e}(g,g)^{a\delta y_i}$，并为$\mathrm{AA}_i$管理的属性集合$U_i$中的每一个属性值$v_{i,j,k}$按如下方式计算$X_{i,j,k}$。

①如果$v_{i,j,k} \neq w^*$，挑战者$\mathcal{B}$选择随机数$x_{i,j,k} \in Z_p^*$，计算$X_{i,j,k} = g^{\delta x_{i,j,k}}$。

②如果$v_{i,j,k} = w^*$，挑战者$\mathcal{B}$计算$X_{i,j,k} = \dfrac{g^{\delta b}}{\prod_{v_{i,j,k} \in W^* - \{w^*\}} g^{\delta x_{i,j,k}}}$。

最后，挑战者$\mathcal{B}$将$\mathrm{SP} = \{p, G_1, G_T, \hat{e}, g, h, g_1, H_1, H_2\}$、$\mathrm{AAPK}_i = \{\{X_{i,j,k}\}, Y_i\}$发送给攻击者$\mathcal{A}$。

密钥查询阶段1。攻击者$\mathcal{A}$提交(UID, S)向挑战者$\mathcal{B}$进行密钥查询，其中$w^* \notin S$。挑战者$\mathcal{B}$首先检查UID是否已存在列表$\mathcal{L}$中，如果$\mathcal{L}$中不存在该用户标识UID，那么挑战者$\mathcal{B}$选择随机数$u \in Z_p^*$，令$\mathrm{USK} = u$并将(UID, u)保存到列表$\mathcal{L}$中；然后，挑战者$\mathcal{B}$为S中的每一个属性值$v_{i,j,k}$选择随机数$r_{i,j,k} \in Z_p^*$，计算

$$\mathrm{VSK}_{i,j} = \{\mathrm{K1}_{i,j} = g^{aux_{i,j,k}} g^{r_{i,j,k} H_1(\mathrm{UID})}, \mathrm{K2}_{i,j} = g^{\delta r_{i,j,k}}\}$$

$$\mathrm{DSK}_{i,j} = g^{auy_i} g^{ax_{i,j,k} H_1(\mathrm{UID})}$$

最后，挑战者$\mathcal{B}$将$\{\{\mathrm{VSK}_{i,j}\}, \{\mathrm{DSK}_{i,j}\}, u\}$发送给攻击者$\mathcal{A}$。

挑战阶段。攻击者$\mathcal{A}$提交明文数据M给挑战者$\mathcal{B}$。挑战者$\mathcal{B}$根据W^*对数据M进行加密，并将密文CT返回给攻击者。密文$\mathrm{CT} = \{\bar{W}^*, C_0, C_1, C_2, C_3, C_4\}$的计算方式为

$$C_0 = M\hat{e}(g^c,g^a)^{\delta \sum_{Y_i \in \mathrm{AAPK}_{w^*}} y_i}$$
$$C_1 = g^c$$
$$C_2 = g^{\delta c}$$
$$C_3 = \hat{e}(g_1, \prod_{X_{i,j,k} \in \mathrm{AAPK}_{W^*}} X_{i,j,k})^s = \hat{e}(g,g)^{abc\delta} = T^{\delta}$$
$$C_4 = H_2\left(\hat{e}(g,g)^{ac\delta \sum_{Y_i \in \mathrm{AAPK}_{w^*}} y_i}\right)$$

密钥查询阶段2。同密钥查询阶段1一样，攻击者$\mathcal{A}$向挑战者$\mathcal{B}$提交查询与用户属性列表S相关的密钥，但$w^* \notin S$。

猜测阶段。攻击者$\mathcal{A}$输出b的猜测结果b'。如果$b'=b$，则挑战者$\mathcal{B}$输出0表示猜测$T=\hat{e}(g,g)^{abc}$；否则挑战者$\mathcal{B}$输出1表示猜测T为G_T中的随机元素。

① 如果$T=\hat{e}(g,g)^{abc}$，则表明CT是根据W^*对数据M进行加密的结果。由于攻击者$\mathcal{A}$的优势为ε，因此在该情况下攻击者$\mathcal{A}$正确猜测出b的概率为$\Pr(\mathcal{A}(b'=b))=\frac{1}{2}+\varepsilon$。

②如果T为G_T中的随机元素，在该情况下攻击者$\mathcal{A}$正确猜测出b的概率为$\Pr(\mathcal{A}(b'=b))=\frac{1}{2}$。

综上所述，挑战者$\mathcal{B}$解决DBDH问题的优势为

$$\frac{1}{2}(\Pr[\mathcal{B}(g,g^a,g^b,g^c,\hat{e}(g,g)^{abc})=0])+$$
$$\frac{1}{2}(\Pr[\mathcal{B}(g,g^a,g^b,g^c,T)=0])-\frac{1}{2}=\frac{\varepsilon}{2}$$

由于不存在多项式时间的攻击者能够以不可忽略的优势解决DBDH问题，因此攻击者无法利用属性值猜测攻击获取本文方案访问策略隐藏的属性值。证毕。

4.2.3　外包密钥抵抗AVGA的安全证明

定理3　如果DL假设成立，则不存在多项式时间的攻击者能够以不可忽略的优势利用属性值猜测攻击从本文方案的属性验证密钥和代理解密密钥中获取用户拥有的属性值。

证明　假设存在一个多项式时间的攻击者$\mathcal{A}$可以在本文所定义的外包密钥抵抗AVGA的安全模型下，从本文方案的属性验证密钥或代理解密密钥中获取用户拥有的属性值，则挑战者$\mathcal{B}$可以攻破DL假设。挑战者$\mathcal{B}$输入DL假设挑战数据$A=g^a$。挑战者$\mathcal{B}$和攻击者$\mathcal{A}$按如下步骤模拟交互游戏过程。

初始化阶段。攻击者$\mathcal{A}$向挑战者$\mathcal{B}$提交挑战用户身份标识UID^*和该用户拥有的2个不同属性的属性值v_0和v_1。挑战者$\mathcal{B}$初始化列表$\mathcal{L}$来记录与攻击者$\mathcal{A}$的交互结果。

参数设置阶段。挑战者$\mathcal{B}$运行本文方案中的CASetup和AASetup算法，并将系统参数$\mathrm{SP}=\{p,G_1,G_T,\hat{e},g,h,g_1,H_1,H_2\}$和属性授权机构$\mathrm{AA}_i$的公钥$\mathrm{AAPK}_i=\{\{X_{i,j,k}\},Y_i\}$发送给攻击者$\mathcal{A}$。

密钥查询阶段1。攻击者$\mathcal{A}$提交(UID,S)向挑战者$\mathcal{B}$进行密钥查询，其中$\mathrm{UID}\neq\mathrm{UID}^*$。挑战者$\mathcal{B}$首先检查UID是否已存在列表$\mathcal{L}$中，如果$\mathcal{L}$中不存在该用户标识UID，那么挑战者$\mathcal{B}$选择随机数$u\in Z_p^*$，令$\mathrm{USK}=u$，并将$(\mathrm{UID},u)$保存到列表$\mathcal{L}$中；然后，挑战者$\mathcal{B}$为$S$中的每一个属性值$v_{i,j,k}$选择随机数$r_{i,j,k}\in Z_p^*$，计算

$$\mathrm{VSK}_{i,j}=\{\mathrm{K1}_{i,j}=g^{\tau u x_{i,j,k}}g^{r_{i,j,k}H_1(\mathrm{UID})},\mathrm{K2}_{i,j}=h^{r_{i,j,k}}\}$$
$$\mathrm{DSK}_{i,j}=g^{\tau u y_i}g^{\tau x_{i,j,k}H_1(\mathrm{UID})}$$

最后，挑战者$\mathcal{B}$将$\{\{\mathrm{VSK}_{i,j}\},\{\mathrm{DSK}_{i,j}\},u\}$发送给攻击者$\mathcal{A}$。

挑战阶段。挑战者$\mathcal{B}$选择随机数$b\in\{0,1\}$和$r_{i,j,k}\in Z_p^*$，计算属性值v_b的属性验证密钥为$\mathrm{VSK}_{v_b}=\{\mathrm{K1}_{v_b}=A^{\tau x_{v_b}}g^{r_{i,j,k}H_1(\mathrm{UID})},\mathrm{K2}_{v_b}=h^{r_{i,j,k}}\}$和代理解密密钥$\mathrm{DSK}_{v_b}=A^{\tau y_i}g^{\tau x_{v_b}H_1(\mathrm{UID})}$，并将属性验证密钥和代理解密密钥发送给攻击者$\mathcal{A}$。

密钥查询阶段2。同密钥查询阶段1一样，攻击者$\mathcal{A}$向挑战者$\mathcal{B}$提交(UID,S)进行密钥查询，但同样$\mathrm{UID}\neq\mathrm{UID}^*$。

猜测阶段。攻击者$\mathcal{A}$输出b的猜测结果b'。如果$b'=b$，则挑战者$\mathcal{B}$利用攻击者$\mathcal{A}$选择的$\alpha\in Z_p^*$来攻破DL假设。

由于不存在多项式时间的攻击者能够以不可忽略的优势解决DL假设，使得攻击者$\mathcal{A}$不能有效选择$\alpha\in Z_p^*$，满足$\frac{\hat{e}(\mathrm{K1}_{v_b},h)}{\hat{e}(\mathrm{K2},g)^{H_1(\mathrm{UID})}}=\hat{e}(g_1^{\alpha},X_{v_b})$和$\frac{\hat{e}(\mathrm{DSK}_{v_b},h)}{\hat{e}(g_1,X_{v_b})^{H_1(\mathrm{UID})}}=\hat{e}(g,h)^{\alpha\tau y_i}$，因此攻击者无法从本文方案的属性验证密钥和代理解密密钥中获取用户拥有的属性值。证毕。

4.3　理论分析

本节将对本文提出的密文长度固定的策略部分隐藏多授权CP-ABE方案进行理论分析，使用的符号含义如表1所示。本文方案与现有CP-ABE方案的功能对比如表2所示。

表1 符号含义

符号	含义
n	与密钥生成过程有关的属性授权机构的个数
m	与数据加密过程有关的属性授权机构的个数
v	系统包含的属性总数
k	用户属性集合S中包含的属性个数
t	访问结构W中包含的属性个数
r	用户撤销列表中包含的用户的个数
l	密文中包含的授权用户的个数
$\|G_1\|$	G_1中元素的长度
$\|G_2\|$	G_2中元素的长度
$\|G_T\|$	G_T中元素的长度
$\|Z_p\|$	Z_p中元素的长度
E_{G_1}	G_1中指数操作的计算开销
E_{G_2}	G_2中指数操作的计算开销
E_{G_T}	G_T中指数操作的计算开销
M_{G_1}	G_1中乘法操作的计算开销
M_{G_2}	G_2中乘法操作的计算开销
M_{G_T}	G_T中乘法操作的计算开销
T_p	双线性配对操作的计算开销

从表2中可以看出，文献[23-24,34-35]方案与本文方案通过部署多授权机构，可避免密钥托管问题；文献[21,26,34-35]方案和本文方案可实现用户撤销，但文献[21,34]方案在撤销过程中需更新密文，存在系统消耗大、操作复杂的问题，且文献[21,26]方案无法实现细粒度的属性级撤销，而文献[35]方案和本文方案可以实现用户或用户某一个属性的直接撤销；文献[21]方案和本文方案可实现基于白名单的恶意用户追踪，但文献[21]方案需维护与用户信息相关联的二叉树以实现用户追踪，而本文方案仅需要保证追踪列表T中包含的转换密钥TSK和用户身份标识UID是一一对应的，具有方便维护、存储开销小和检索速度快等优点，适合部署在终端海量化的物联网场景中；文献[23,26,28,32,34-35]方案和本文方案通过利用外包代理解密技术，减少了用户的解密计算开销；除文献[32,34-35]方案，其余对比方案和本文方案实现了访问策略隐藏，但文献[25-26,28-29]方案和本文方案隐藏的访问控制策略可以抵抗属性值猜测攻击，攻击者无法利用属性值猜测攻击获取访问控制策略中隐藏的属性值，减少了用户隐私数据泄露的风险；文献[32,34]方案和本文方案可以实现密文长度固定，有效减少了方案总体的计算、存储和通信开销。

本文方案与现有CP-ABE方案的密钥和密文长度对比如表3所示。从表3中可以看出，相比于现有基于策略隐藏的CP-ABE方案，本文方案通过改变密钥生成过程，用户解密密钥由用户独立生成，代理解密密钥和属性验证密钥由属性授权机构根据用户发送的转换密钥生成，使得本文方案中的用户仅需要存储长度为$|Z_p|$的用户解密密钥即可，也有效地减少了用户密钥更新时需要的通信开销。另外，相比于现有基于策略隐藏的CP-ABE方案，本文方案的密文长度与访问结构W中包含的属性数量无关，这有效地减少了用户上传密文时需要的通信开销。相比于现有文献[32,34]方案支持密文长度固定的CP-ABE方案，本文方案在没有增加用户存储和通信开销的前提下，实现了访问策略的部分隐藏，减少了用户隐私数据泄露的风险，提高了方案的安全性。

表2 功能对比

方案	多授权机构	用户/属性撤销	用户追踪	外包解密	策略隐藏	抗属性值猜测攻击	密文长度固定
文献[19]	否	否	否	否	是	否	否
文献[21]	否	是	是	否	是	否	否
文献[23]	是	否	否	是	是	否	否
文献[24]	是	否	否	否	是	否	否
文献[25]	否	否	否	否	是	是	否
文献[26]	否	是	否	是	是	是	否
文献[28]	否	否	否	是	是	是	否
文献[29]	否	否	否	否	是	是	否
文献[32]	否	否	否	是	否	—	是
文献[34]	是	是	否	是	否	—	是
文献[35]	是	是	否	是	否	—	否
本文	是	是	是	是	是	是	是

表3　密钥和密文长度对比

方案	用户存储的密钥长度	代理解密密钥长度	属性验证密钥长度	密文长度
文献[19]	$(3k+2)\|G_1\|$	—	$(k+1)\|G_1\|$	$(t+2v+2)\|G_1\|+\|G_T\|$
文献[21]	$(k+4)\|G_1\|$	—	—	$(3t+r+2)\|G_1\|+\|G_T\|$
文献[23]	$(3n+k)\|G_1\|$	$(n+k)\|G_1\|$	$2n\|G_1\|$	$(3t+1)\|G_1\|+2t\|Z_p\|+\|G_T\|$
文献[24]	$2k\|G_1\|$	—	—	$3t\|G_1\|+(t+1)\|G_T\|$
文献[25]	$(k+4)\|G_1\|$	—	—	$(v+3)\|G_1\|+\|G_T\|$
文献[26]	$(5k+2)\|G_1\|$	$(5k+2)\|G_1\|$	—	$(6t+3)\|G_1\|+\|G_T\|$
文献[28]	$(4k+2)\|G_1\|$	$(3k+1)\|G_1\|$	$k\|G_1\|$	$(5t+2)\|G_1\|+2\|G_T\|$
文献[29]	$(2k+4)\|G_1\|$	—	$(k+2)\|G_1\|$	$(3t+4)\|G_1\|+\|G_T\|$
文献[32]	$2\|G_1\|$	$2\|G_1\|$	—	$\|G_1\|+2\|G_2\|+\|G_T\|$
文献[34]	$\|Z_p\|$	$k\|G_1\|$	—	$2\|G_1\|+\|G_T\|+\|Z_p\|$
文献[35]	$\|Z_p\|$	$2n\|G_1\|+k\|G_2\|$	—	$m\|G_1\|+2m\|G_2\|+\|G_T\|$
本文	$\|Z_p\|$	$k\|G_1\|$	$2k\|G_1\|$	$2\|G_1\|+2\|G_T\|+\|Z_p\|$

本文方案与现有CP-ABE方案的计算开销对比如表4所示。由于E_{G_1}、E_{G_2}和T_p操作的计算开销远大于E_{G_T}、M_{G_1}、M_{G_2}和M_{G_T}操作的计算开销，因此可以用方案中计算E_{G_1}、E_{G_2}和T_p操作的次数来对比方案的计算开销。从表4中可以看出，数据加密阶段和外包代理解密阶段，文献[34]方案和本文方案需要计算E_{G_1}、E_{G_2}或T_p操作的次数均为常数，其他方案需要计算E_{G_1}、E_{G_2}或T_p操作的次数都与属性数量有关；在属性验证阶段，相比于其他方案，文献[19]和本文方案只需要计算2次T_p操作，且不需要进行E_{G_1}操作的计算；在用户本地解密阶段，文献[32,34-35]方案和本文方案不需要进行E_{G_1}、E_{G_2}或T_p操作的计算。对比可以发现本文方案相比于现有方案的总体计算开销更小，适合部署在资源受限的轻量级终端设备中。

5　实验验证与分析

本节将通过仿真实验对比本文方案与文献[19,23,28-29,32,34-35]方案在密钥生成、数据加密、属性验证、代理解密和用户解密等方面的计算开销，

表4　计算开销对比

方案	数据加密	属性验证	代理解密	用户解密
文献[19]	$(3t+2)E_{G_1}+E_{G_T}$	$2tM_{G_1}+2T_p+M_{G_T}$	—	$(2t+1)T_p+3M_{G_T}$
文献[21]	$(4t+r+2)E_{G_1}+E_{G_T}$	—	—	$(3t+1)T_p+2E_{G_1}+2M_{G_1}+E_{G_T}+3M_{G_T}$
文献[23]	$(2m+2)tE_{G_1}+mtM_{G_1}+mE_{G_T}$	$mt(M_{G_1}+E_{G_1})+2mtT_p$	$(2t+1)mT_p+mt(E_{G_1}+E_{G_T})$	$2E_{G_T}+M_{G_T}$
文献[24]	$2(t+1)E_{G_T}+4tE_{G_1}+2M_{G_T}$	—	—	$3tT_p+tE_{G_T}+(3t+1)M_{G_T}$
文献[25]	$(3t+4)E_{G_1}+E_{G_T}$	—	—	$5tT_p+2M_{G_T}$
文献[26]	$(8t+4)E_{G_1}+(l+2)M_{G_1}+E_{G_T}$	—	$(6t+2)T_p+tE_{G_T}+(l-1)M_{G_1}$	$E_{G_T}+M_{G_T}+2E_{G_1}+M_{G_1}$
文献[28]	$(8t+3)E_{G_1}+(3t+1)M_{G_1}+2E_{G_T}$	$tT_p+tE_{G_T}$	$4tT_p+tE_{G_T}$	$T_p+2M_{G_T}+E_{G_T}+2E_{G_1}+M_{G_1}$
文献[29]	$(t+1)5E_{G_1}+2M_{G_1}+E_{G_T}$	$2tE_{G_1}+2T_p$	—	$(2t+1)T_p+tE_{G_T}+M_{G_T}+2E_{G_1}+M_{G_1}$
文献[32]	$E_{G_1}+2(v-t+1)E_{G_2}+E_{G_T}+2(v-t)M_{G_2}$	—	$3T_P+(v-t)(M_{G_2}+E_{G_2})$	$M_{G_T}+3E_{G_T}$
文献[34]	$(m+1)M_{G_T}+tM_{G_1}+E_{G_T}+E_{G_1}$	—	$tM_{G_1}+2T_p+M_{G_T}$	$M_{G_T}+E_{G_T}$
文献[35]	$mE_{G_1}+2(v-t+1)E_{G_2}+E_{G_T}+2(v-t)M_{G_2}$	—	$3mT_p+(v-t)(M_{G_2}+E_{G_2})+m(2M_{G_T}+E_{G_T})$	E_{G_T}
本文	$(m+1)M_{G_T}+tM_{G_1}+T_p+2E_{G_1}$	$2tM_{G_1}+2T_p+M_{G_T}$	$tM_{G_1}+T_p+M_{G_T}+E_{G_T}$	$M_{G_T}+E_{G_T}$

以及方案在用户解密密钥、代理解密密钥、属性验证密钥和密文等方面的存储和通信开销。

本文实验使用的处理器是2.6 GHz Intel Core i7，操作系统为Ubuntu Linux 16.04.7，实验代码是基于charm-crypto v 0.50库编写的，选择的是charm-crypto库中SS512椭圆曲线。实验结果为30轮实验的平均值。在本文的实验环境下，计算一次T_p、E_{G_1}、E_{G_2}、E_{G_T}、M_{G_1}、M_{G_2}和M_{G_T}操作的时间分别为0.7 ms、1.25 ms、1.32 ms、0.2 ms、0.002 ms、0.003 ms和0.0009 ms，群G_1、G_2、G_T和Z_p中的元素在序列化后不压缩情况下的字节长度分别为174 B、174 B、174 B和30 B。为了实验对比的公平性，本文在实验过程中将文献[23,34-35]方案和本文方案系统中包含的属性授权机构的数量设置为5个，其中每个属性授权机构包含12种不同类型的属性，将文献[19,28-29,32]方案系统包含的属性种类总数设置为60种。

图2是8种方案在密钥生成时间上的对比。为了方便对比，本文在实验过程中将用户解密密钥生成、属性验证密钥生成和代理解密密钥生成一并归为密钥生成。从图2中可以看出，文献[32,35]方案的密钥生成时间是固定的，与用户属性集合中包含的属性数量无关，文献[19,23,28-29,34]方案和本文方案的密钥生成时间与用户拥有的属性数量是成正比的；本文方案的密钥生成时间要短于文献[28-29]方案的密钥生成时间，但要长于文献[19,23,32,34]方案；与文献[35]方案的密钥生成时间相比，本文方案在用户属性集合包含的属性数量较少的情况下占优，随着属性数量的增加，本文方案的密钥生成时间要逐渐高于文献[35]方案。

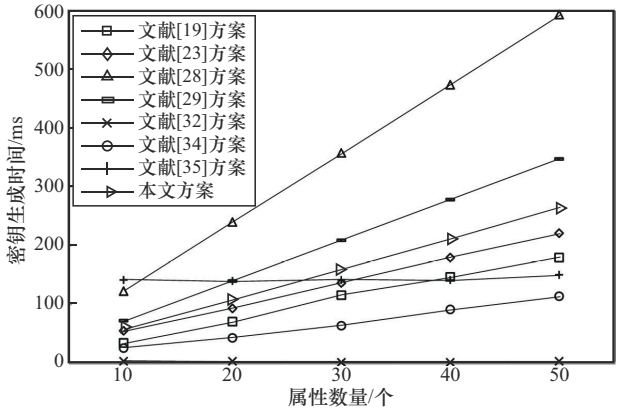

图2 密钥生成时间对比

相比于文献[32,34-35]方案，由于本文方案实现了访问控制策略的属性值隐藏，且为了减少在数据解密阶段给未授权用户带来的大量不必要的计算开销，因此需要额外生成属性验证密钥，增加了密钥生成时间。在本文方案密钥生成过程中，用户在本地生成用户解密密钥和转化密钥的过程中仅需要计算一次E_{G_1}操作，属性验证密钥和代理解密密钥由属性授权机构根据用户发送的转换密钥计算后发送给云服务提供商和边缘服务器，而文献[19,23,32]方案的属性验证密钥或代理解密密钥是由用户根据属性授权机构发送的用户解密密钥计算生成后再发送给边缘服务器或云服务提供商，使得本文方案的总体密钥生成时间虽然高于文献[19,23,32]方案，但在密钥生成过程中的终端用户的计算和通信开销要远远低于这3种方案。

图3是8种方案在数据加密时间上的对比。从图3中可以看出，文献[19,23,28-29]方案的数据加密时间随着访问结构中包含的属性数量增加而增大；文献[32,35]方案的数据加密时间与属性数量成反比，这是由于这2种方案在数据加密过程中计算E_{G_2}操作的次数与访问结构中未包含的属性数量有关；文献[34]方案和本文方案的数据加密时间几乎恒定，与访问结构中包含的属性数量无关，且要低于其他6种方案的数据加密时间。在文献[34]方案和本文方案的数据加密过程中需要计算E_{G_1}、E_{G_2}或T_p操作的次数均为常数，而其余对比文献中的方案在数据加密过程中需要计算E_{G_1}、E_{G_2}或T_p操作的次数均与属性数量有关，这使得文献[34]方案和本文方案在数据加密过程中有效减少了终端用户的计算资源的消耗。相比于文献[34]方案，本文方案在没有增加数据加密过程中用户计算资源的情况下实现了访问策略的属性值隐藏，减少了攻击者通过窃听访问策略获取用户隐私数据的风险，有效地提高了方案的总体安全性。

图4是文献[19,23,28-29]方案和本文方案在属性验证时间上的对比。从图4中可以看出，文献[23,28-29]方案的属性验证时间随着属性数量的增加而增多，且文献[23,29]方案中属性验证时间的增长速率要快于文献[28]方案；文献[19]方案和本文方案中的属性验证时间与属性数量几乎无关，且要低于文献[23,28-29]方案。相比于文献[19,23]方案，本文方案在属性验证的过程中可以抵抗属性值猜测攻击，

云服务提供商既无法利用属性值猜测攻击获取访问策略隐藏的属性值，也无法利用属性值猜测攻击从属性验证密钥中获取用户拥有的属性值，减少了用户隐私数据泄露的风险，保障了方案的安全性。

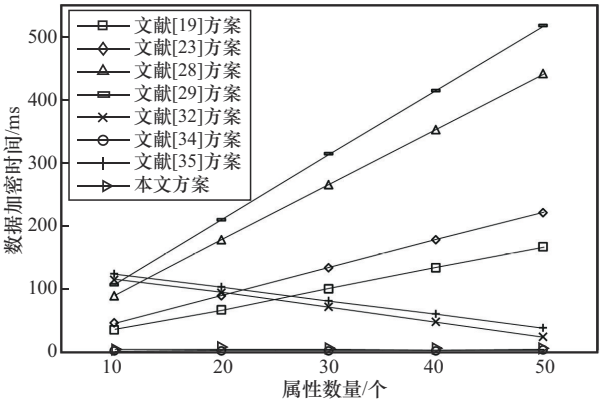

图3　数据加密时间对比

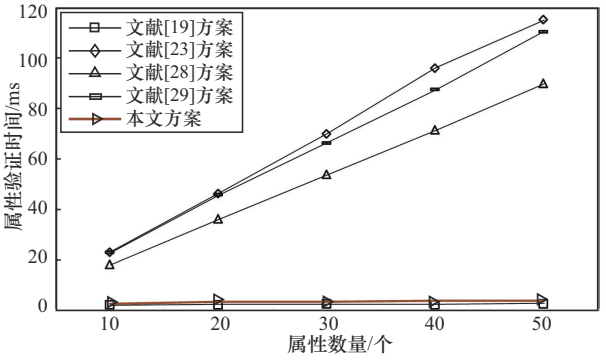

图4　属性验证时间对比

图5是文献[23,28,32,34-35]方案和本文方案在代理解密过程中的时间对比。从图5中可以看出，文献[23,28]方案的代理解密时间与访问结构中包含的属性数量成正比，随着属性数量的增加而增加；文献[32,34-35]方案和本文方案的代理解密时间几乎与属性数量无关；相比于其他5种方案，本文方案代理解密过程中所需要的时间要更短。

相比于文献[32,34-35]方案，文献[23,28]方案和本文方案实现了访问策略的属性值隐藏，边缘服务器无法在代理解密过程中直接获取密文中包含的访问策略。相比于[23,28]方案，本文方案在代理解密过程中还可以抵抗属性值猜测攻击，边缘服务器无法利用属性值猜测攻击从代理解密密钥中获取用户拥有的属性集合，也不能从访问策略中获取隐藏的属性值。因此，本文方案可以为用户实现速度更快、安全性更高的外包代理解密服务。

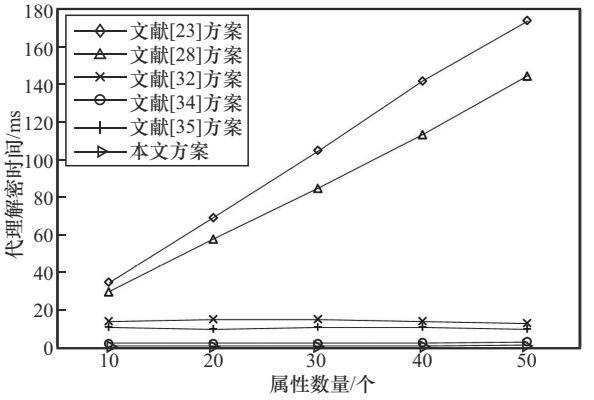

图5　代理解密时间对比

图6是8种方案在用户解密过程中的时间对比。从图6中可以看出，文献[19,29]方案在用户解密过程中的计算时间与用户拥有的属性数量成正比，且文献[29]方案在该过程中的时间增长速率要高于文献[19]方案；相比于文献[19,29]方案，其他5种方案和本文方案由于使用了计算外包技术，将与属性相关的解密计算操作外包给边缘服务器，极大地降低了终端用户在用户解密过程中的计算资源消耗，使得用户解密计算时间与用户拥有的属性数量无关，且边缘服务器由于在进行代理解密计算后，只需将部分密文发送给终端用户，也有效地降低了终端用户在接收密文过程中的通信资源消耗。

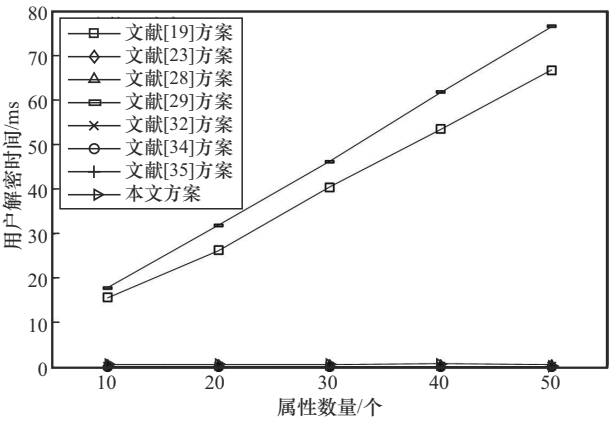

图6　用户解密时间对比

图7是8种方案中用户存储的密钥长度对比。从图7中可以看出，文献[19,23,28-29]方案的用户存储的密钥长度与用户拥有的属性数量成正比，这会极大地限制方案在物联网轻量级终端设备中的使用；相比于文献[19,23,28-29]中方案，文献[32,34-35]方案和本文方案终端用户需要存储的密钥的长度固定且更短，与用户拥有的属性数量无关，更加适合部

署在资源受限的轻量级物联网设备中。相比于文献[32,35]方案，本文方案的用户解密密钥是由用户独立生成并存储的，可以有效解决密钥托管问题和密钥分发过程中的密钥泄露问题，提高了用户解密密钥生成和存储的安全性。

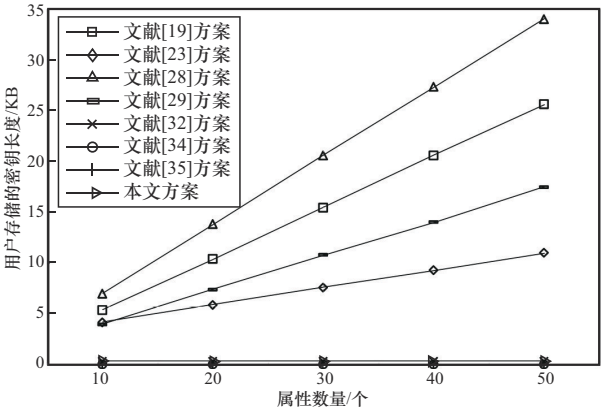

图7　用户存储的密钥长度对比

图8是文献[19,23,28-29]方案和本文方案生成的属性验证密钥的长度对比。从图8中可以看出，所有对比方案生成的属性验证密钥的长度与用户拥有的属性数量成正比，但本文方案生成的属性验证密钥长度要大于其他方案生成的属性验证密钥的长度。

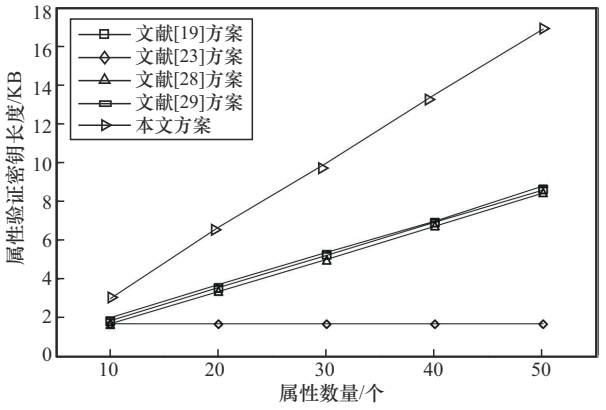

图8　属性验证密钥长度对比

虽然本文方案生成的属性验证密钥的长度要大于文献[19,23,28-29]方案生成的属性验证密钥的长度，但属性验证密钥是由云服务提供商保存的，而云服务提供商拥有巨大的存储和通信资源，因此属性验证密钥的长度并不会成为系统出现性能瓶颈的主要因素。

文献[19,23,28-29]方案的属性验证密钥是由终端用户根据属性授权机构发送的用户解密密钥计算生成的，再由终端用户将其发送给边缘服务器，而本文方案的属性验证密钥是由属性授权机构根据用户发送的转换密钥生成，再由属性授权机构发送给边缘服务器。因此，相比于文献[19,23,28-29]方案，由于本文方案在属性验证密钥生成过程中并不需要终端用户参与计算，使得本文方案在该过程中可以有效减少终端用户的计算和通信资源的消耗。相比于云服务提供商拥有的存储和通信资源，物联网终端设备在属性验证密钥生成过程中的资源消耗更易成为系统出现性能瓶颈的主要原因。另外，相比于文献[19,23]方案，本文方案生成的属性验证密钥能够抵抗属性值猜测攻击，使得攻击者无法从属性验证密钥中获取用户拥有的具体属性值，有效提高了方案的安全性。

图9是文献[23,28,32,34-35]方案和本文方案生成的代理解密密钥的长度对比。从图9中可以看出，文献[32]方案生成的代理解密的密钥长度与用户拥有的属性数量无关；文献[23,28,34-35]方案和本文方案生成的代理解密密钥的长度与用户拥有的属性数量成正比，且文献[34]和本文方案生成的代理解密密钥的长度要小于文献[23,28,35]方案。

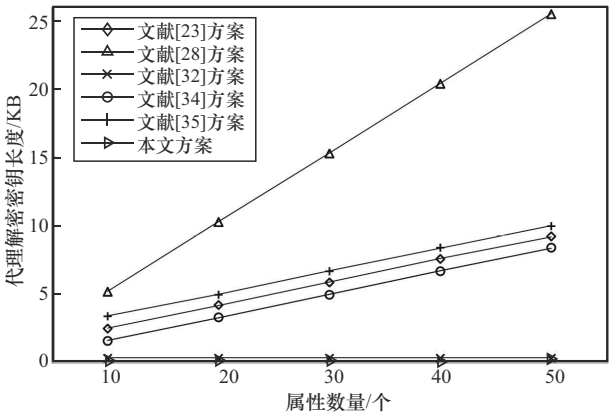

图9　代理解密密钥长度对比

本文方案的代理解密密钥与属性验证密钥生成过程一样，因此虽然本文方案生成的代理解密密钥的长度要大于文献[32]方案，但相比于文献[23,28,32]方案，本文方案在生成代理解密密钥的过程中不需要终端用户参与计算，减少了终端用户在该过程中的计算和通信资源的消耗。

另外，相比于文献[34]方案采用的属性间接撤销机制，即通过更新密文或未撤销用户的密钥实现属性的撤销，本文方案由于在属性验证密钥和代理

解密密钥的生成过程中不需要终端用户参与计算，因此可以更新用户的属性验证密钥或代理解密密钥，在不更改密文和未撤销用户密钥的前提下实现属性的直接撤销，有效减少了因使用属性间接撤销机制而产生的撤销操作复杂和系统消耗大的问题。

图10是8种方案生成密文的长度对比。从图10中可以看出，文献[19,23,28-29]方案生成的密文长度与访问策略中包含的属性数量成正比；文献[32,34-35]方案和本文方案生成的密文长度固定，且要小于其他4种方案。相比于文献[19,23,28-29]方案，本文方案在实现访问策略属性值隐藏的基础上，通过固定密文长度，有效减少了用户的计算、存储和通信开销。相比于文献[32,34-35]方案，本文方案在不增加密文长度的前提下，实现了访问策略属性值的隐藏，有效提高了方案的安全性。

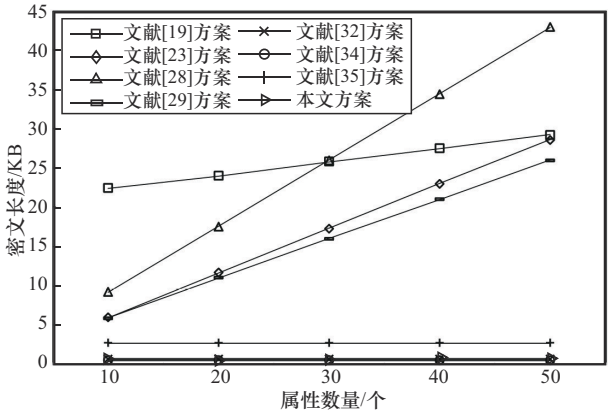

图10　密文长度对比

6　结束语

本文提出了一种密文长度固定的策略部分隐藏多授权机构CP-ABE方案，该方案通过部署多授权机构、隐藏数据访问结构中的属性值和固定密文长度，避免了密钥托管问题，降低了用户隐私数据泄露的风险，减少了用户的资源开销。通过安全性分析可证明，本文提出的多授权机构CP-ABE方案可实现IND-CPA的安全，且攻击者无法从访问策略和外包密钥中利用属性值猜测攻击获取访问策略隐藏的属性值和用户拥有的属性值。通过理论分析和仿真实验验证可知，本文方案可以有效地减少用户的计算、存储和通信开销，适合部署在资源受限的物联网设备中。

本文方案满足IND-CPA安全，但为了将本文方案应用到更多实际场景中，还需进一步提升方案的安全性。目前，有一些通用方法可将满足IND-CPA安全的方案转变成满足选择密文攻击下不可区分性安全，在未来工作中，笔者将从该研究方向出发，对本文方案做出进一步的改进。

参考文献：

[1] SANDHU A K. Big data with cloud computing: discussions and challenges[J]. Big Data Mining and Analytics, 2022, 5(1): 32-40.

[2] CAO K Y, LIU Y F, MENG G J, et al. An overview on edge computing research[J]. IEEE Access, 2020, 8: 85714-85728.

[3] 邓桦, 宋甫元, 付玲, 等. 云计算环境下数据安全与隐私保护研究综述[J]. 湖南大学学报(自然科学版), 2022, 49(4): 1-10.
DENG H, SONG F Y, FU L, et al. A review of data security and privacy preserving in cloud computing environment[J]. Journal of Hunan University (Natural Sciences), 2022, 49(4): 1-10.

[4] SHI W S, CAO J, ZHANG Q, et al. Edge computing: vision and challenges[J]. IEEE Internet of Things Journal, 2016, 3(5): 637-646.

[5] 张晓东, 张朝昆, 赵继军. 边缘智能研究进展[J]. 计算机研究与发展, 2023, 60(12): 2749-2769.
ZHANG X D, ZHANG C K, ZHAO J J. State-of-the-art survey on edge intelligence[J]. Journal of Computer Research and Development, 2023, 60(12): 2749-2769.

[6] SAMIE F, BAUER L, HENKEL J. Edge computing for smart grid: an overview on architectures and solutions[C]//IoT for Smart Grids. Berlin: Springer, 2019: 21-42.

[7] ARTHURS P, GILLAM L, KRAUSE P, et al. A taxonomy and survey of edge cloud computing for intelligent transportation systems and connected vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(7): 6206-6221.

[8] HARTMANN M, HASHMI U S, IMRAN A. Edge computing in smart health care systems: review, challenges, and research directions[J]. Transactions on Emerging Telecommunications Technologies, 2022, 33 (3): e3710.

[9] FERRAIOLO D F, CUGINI J, KUHN D R. Role-based access control (RBAC): Features and motivations[C]//Proceedings of 11th Annual Computer Security Application Conference. New Orleans: NIST, 1995: 241-248.

[10] SAXENA N, TSUDIK G, YI J H. Identity-based access control for ad hoc groups[C]//Information Security and Cryptology – ICISC 2004. Berlin: Springer, 2005: 362-379.

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

[12] 刘帅南, 刘彬, 郭真, 等. 一种支持分级用户访问的文件分层CP-ABE方案[J]. 软件学报, 2023, 34(7): 3329-3342.
LIU S N, LIU B, GUO Z, et al. File hierarchy CP-ABE scheme supporting graded user access[J]. Journal of Software, 2023, 34(7): 3329-3342.

[13] 赵开强, 康萍, 刘彬, 等. 支持云代理重加密的CP-ABE方案[J]. 电子学报, 2023, 51(3): 728-735.
ZHAO K Q, KANG P, LIU B, et al. A CP-ABE scheme with cloud proxy re-encryption[J]. Acta Electronica Sinica, 2023, 51(3): 728-735.

[14] SUN J F, XIONG H, LIU X M, et al. Lightweight and privacy-aware fine-grained access control for IoT-oriented smart health[J]. IEEE In-

ternet of Things Journal, 2020, 7(7): 6566-6575.
[15] CHEN Y, LI W M, GAO F, et al. Efficient attribute-based data sharing scheme with hidden access structures[J]. The Computer Journal, 2019, 62(12): 1748-1760.
[16] 张学旺, 姚亚宁, 付佳丽, 等. 策略隐藏的高效多授权机构CP-ABE物联网数据共享方案[J]. 计算机研究与发展, 2023, 60(10): 2193-2202.
ZHANG X W, YAO Y N, FU J L, et al. Efficient multi-authority CP-ABE IoT data sharing scheme with hidden policies[J]. Journal of Computer Research and Development, 2023, 60(10): 2193-2202.
[17] NISHIDE T, YONEYAMA K, OHTA K. Attribute-based encryption with partially hidden encryptor-specified access structures[C]//Proceedings of the 6th Applied Cryptography and Network Security International Conference.New York: ACM Pressr, 2008: 111-129.
[18] 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 Press, 2013: 511-516.
[19] LI J, WANG H, ZHANG Y, et al. Ciphertext-policy attribute-based encryption with hidden access policy and testing[J]. KSII Transactions on Internet and Information Systems, 2016, 10(7): 3339-3352.
[20] QIU S, LIU J Q, SHI Y F, et al. Hidden policy ciphertext-policy attribute-based encryption with keyword search against keyword guessing attack[J]. Science China Information Sciences, 2016, 60(5): 052105.
[21] 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.
[22] KIM I, SUSILO W, BAEK J, et al. Harnessing policy authenticity for hidden ciphertext policy attribute-based encryption[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(3): 1856-1870.
[23] TIAN H, LI X, QUAN H Y, et al. A lightweight attribute-based access control scheme for intelligent transportation system with full privacy protection[J]. IEEE Sensors Journal, 2021, 21(14): 15793-15806.
[24] XUE L L, LI J N, ZHANG K J, et al. Decentralized multi-authority ciphertext-policy attribute-based encryption with hidden policy for cloud data sharing[C]//Proceedings of the 2023 4th International Conference on Computer Engineering and Intelligent Control. Piscataway: IEEE Press, 2023: 180-185.
[25] ZHANG L, CUI Y, MU Y. Improving privacy-preserving CP-ABE with hidden access policy[C]//Proceedings of the 4th International Conference Cloud Computing and Security. Berlin: Springer, 2018: 596-605..
[26] XIONG H, ZHAO Y N, PENG L, et al. Partially policy-hidden attribute-based broadcast encryption with secure delegation in edge computing[J]. Future Generation Computer Systems, 2019, 97: 453-461.
[27] 张嘉伟, 马建峰, 马卓, 等. 云计算中基于时间和隐私保护的可撤销可追踪的数据共享方案[J]. 通信学报, 2021, 42(10): 81-94.
ZHANG J W, MA J F, MA Z, et al. Time-based and privacy protection revocable and traceable data sharing scheme in cloud computing[J]. Journal on Communications, 2021, 42(10): 81-94.
[28] HU G C, ZHANG L Y, MU Y, et al. An expressive “test-decrypt-verify” attribute-based encryption scheme with hidden policy for smart medical cloud[J]. IEEE Systems Journal, 2021, 15(1): 365-376.
[29] ZHANG Z S, ZHANG W, QIN Z G. A partially hidden policy CP-ABE scheme against attribute values guessing attacks with online privacy-protective decryption testing in IoT assisted cloud computing [J]. Future Generation Computer Systems, 2021, 123: 181-195.
[30] YANG W T, WANG R M, GUAN Z T, et al. A lightweight attribute based encryption scheme with constant size ciphertext for Internet of things[C]//Proceedings of the ICC 2020 IEEE International Conference on Communications . Piscataway: IEEE Press, 2020: 1-6.
[31] 丁晟, 曹进, 李晖. 基于OBDD访问结构的无配对CP-ABE方案[J]. 通信学报, 2019, 40(12): 1-8.
DING S, CAO J, LI H. Efficient pairing-free CP-ABE based on ordered binary decision diagram[J]. Journal on Communications, 2019, 40(12): 1-8.
[32] ZHANG Z S, ZHANG W, QIN Z G. Fully constant-size CP-ABE with privacy-preserving outsourced decryption for lightweight devices in cloud-assisted IoT[J]. Security and Communication Networks, 2021, 2021: 6676862.
[33] DOSHI N. An enhanced constant length traceable CP-ABE in IoT paradigm[J]. International Journal of Electronic Security and Digital Forensics, 2023, 15(3): 315.
[34] LI X, LIU T, CHEN C Y, et al. A lightweight and verifiable access control scheme with constant size ciphertext in edge-computing-assisted IoT[J]. IEEE Internet of Things Journal, 2022, 9(19): 19227-19237.
[35] CHAUDHARY C K, SARMA R, BARBHUIYA F A. RMA-CPABE: a multi-authority CPABE scheme with reduced ciphertext size for IoT devices[J]. Future Generation Computer Systems, 2023, 138: 226-242.
[36] ZHANG Y C, LI J G, YAN H. Constant size ciphertext distributed CP-ABE scheme with privacy protection and fully hiding access structure [J]. IEEE Access, 2019, 7: 47982-47990.
[37] CHASE M. Multi-authority attribute based encryption[C]//Proceedings of the 4th Theory of Cryptography Conference. Berlin: Springer, 2007: 515-534.

[作者简介]

刘怡龙（1997– ），男，山东济宁人，北京邮电大学博士生，主要研究方向为数据安全、访问控制、属性加密等。

许盛伟（1976– ），男，江西吉安人，博士，北京电子科技学院教授、博士生导师，主要研究方向为大数据安全、人工智能与密码应用等。

岳梓岩（1998– ），男，新疆哈密人，北京邮电大学博士生，主要研究方向为车联网密码应用、属性加密等。