基于属性隐藏的高效去中心化的移动群智数据共享方案

蒋沥泉，秦志光*

(电子科技大学信息与软件工程学院 成都 611731)

【摘要】移动群智技术是一种能够突破时间与地点的限制，实现随时随地大规模的实时群智数据感知、传输和共享的技术。然而，现有的移动群智场景在数据共享过程中面临诸多安全、隐私和效率问题，如非授权数据访问、访问控制隐私泄漏、单权威密钥托管、访问开销过高等。为了同时解决以上问题，提出了一个面向移动群智场景的高效去中心化属性隐藏的数据共享方案。该方案不仅允许群智用户指定基于属性的访问控制用于加密群智数据，使得只有满足访问控制的用户才能访问该群智数据，还允许多个权威机构为群智用户共同生成私钥，使得单独的权威机构无法伪装成合法的用户来非法访问目标群智数据。此外，该方案在不泄漏访问控制的属性隐私的情况下，群智用户能够以最低的能耗快速解密和访问目标群智数据。通过安全性和性能分析，证明该方案能够实现安全高效的移动群智数据共享。

关 键 词 访问控制； 属性隐私； 去中心化； 快速解密； 移动群智

中图分类号 TP371 **文献标志码** A doi:10.12178/1001-0548.2022225

Attribute-Hiding Based Efficient and Decentralized Scheme for Mobile Crowdsensing Data Sharing

JIANG Liquan and QIN Zhiguang*

(School of Information and Software Engineering, University of Electronic Science and Technology of China Chengdu 611731)

Abstract Mobile crowdsensing technology is a technique that can break through the limitations of time and place, and realize large-scale real-time crowdsensing data perception, transmission and sharing anytime, anywhere. However, the existing mobile crowdsensing applications confront with some security, privacy and efficiency problems in the crowdsensing data sharing, such as unauthorized data access, privacy leakage of access control, key escrow of single-authority, and high access overhead. In order to tackle the above problems simultaneously, this paper proposes an attribute-hiding based efficient and decentralized scheme for mobile crowdsensing data sharing, which not only allows mobile users to specify attribute-based access control for encrypting crowdsensing data, such that only users who meet the access control can access the data, but also allows multiple authorities to jointly generate private keys for swarm crowdsensing users, so that any a single authority cannot illegally access the target crowdsensing data by pretending to be a legitimate user. In addition, it enables fast decryption and accessing target data with the lowest energy consumption without leaking attribute privacy of access control. This paper also gives strict security analysis and performance analysis to prove that our scheme is secure, efficient and feasible for the mobile crowdsensing data sharing.

Key words access control; attribute hiding; decentralized; fast decryption; mobile crowdsensing

随着传感技术、大数据技术以及移动物联网的快速发展，移动群智技术作为一种新型大规模感知技术，能够利用用户随身携带的移动设备突破时间与地点的限制，随时随地地借助云服务平台进行大规模的实时数据感知、传输和共享[1-3]。随着便携式移动设备传感器集成的精细化以及功能的多样化，其应用也越来越广泛，如交通导航、环境监测、医疗服务等[4-5]。尽管移动群智应用能够极大地提升人类生活质量，然而由于在应用过程中涉及大量的数据传输、交换和共享，这使得群智感知的应用也面临着一系列数据隐私和安全问题。如攻击者可以通过非法获取用户上传的群智医疗等敏感信息来推导

收稿日期：2022－07－21；修回日期：2022－12－10

作者简介：蒋沥泉 (1977－)，女，博士生，主要从事密码学等方面的研究.

*通信作者：秦志光，E-mail：qinzg@uestc.edu.cn

其健康状况，进而进行一系列恶意造谣和攻击。社交用户传输给应用服务器的群智数据通常带有时空信息（含有收集数据时的位置），攻击者可以非法获取这些数据并可能利用这些数据推导出用户的生活习惯、行为、家庭住址等敏感信息，从而获取用户的隐私并可能对用户发起恶意攻击。因此，在保证数据隐私性的前提下，如何实现对群智数据的授权访问是移动群智应用首要解决的问题[6-8]。

基于属性加密的访问控制技术是一种有效的解决方法[9-10]。在该技术中，用户的私钥和一组属性集（或一个访问控制）绑定在一起，加密的数据和访问控制（或一组属性集）绑定在一起。当用户私钥中的属性集（访问控制）和密文中的访问控制（属性集）相匹配时，该用户才有权访问数据。然而，在现有的大多数基于属性加密的访问控制中，用户的密钥通常是由一个中央权威去生成和分配，这就需要该权威机构是完全可信的。而在现实的应用场景中，中央权威机构由于托管着用户所有的密钥，可能伪装成合法用户去访问用户的数据，使得用户数据隐私性遭到破坏。因此，如何实现去中心化和分布式的访问控制减少中央权威的信任成为亟待解决的挑战。此外，现有的大多数基于属性的访问控制方案中都过于专注用户数据机密性的保护，很少考虑用户属性的隐私性。如在移动群智的医疗服务场景中，群智用户选择一个访问控制，如“人民医院”“精神科医生”“生理医生”“心理医生”，对自己的群智医疗数据进行加密，使得只有人民医院的精神科医生、生理医生或心理医生才能访问其医疗数据。然而，由于密文中的访问控制是以明文的形式附加在密文数据上的，这就使得任何非法用户即使不能解密其密文数据，也能通过访问控制大致推测该用户可能患有生理或心理疾病，这无疑在一定程度上损害了用户的隐私。因此，如何防止访问控制的隐私性泄漏也成为另一个待解决的挑战之一。除了实现去中心化和分布式的访问控制以及保证访问控制的隐私性之外，考虑到大多数的基于属性加密的方案其密文长度过长、解密效率过低，这对于资源受限的移动群智用户难以快速地解密并访问数据，因此，如何保证资源有限的群智用户能以最少的耗能快速实现对目标数据的访问也是一个现实的挑战。

目前来说，大多数基于属性的加密方案都只能部分解决以上挑战。如具有去中心化功能的基于属性的加密方案[11-18]仅能够实现中心化和分布式的访问控制，无法实现对访问控制的隐私保护和高效的数据访问。具有策略隐藏功能的基于属性的加密方案[19-25]仅能够实现对访问控制的隐私保护，无法实现去中心化和高效的数据访问；具有外包功能的基于属性的加密方案[26-33]仅能够实现高效的数据访问，而没有考虑去中心化和访问控制的隐私保护；此外，还有一些具有隐私保护的去中心化功能的基于属性的加密方案或基于外包的具有隐私保护的属性基加密方案要么没有考虑用户解密效率，要么未考虑去中心化问题[14, 25, 34-35]。

为了实现移动群智应用场景下的属性隐藏、去中心化以及高效的数据访问，本文提出了一个基于属性隐藏的高效去中心化的移动群智数据共享方案。本文的主要贡献如下。

1）细粒度访问控制：本方案允许群智用户指定基于属性的访问控制用于加密群智数据，使得只有满足访问控制的用户才能访问该群智数据。与之前的细粒度访问控制相比，本方案的访问控制更高效。

2）权威去中心化：本方案允许多个权威机构为群智用户共同生成私钥，使得单独的权威机构无法伪装成合法的用户非法访问目标数据。相较于之前中心化的属性权威的问题，本方案能够防止抗权威密钥泄漏。

3）属性隐藏： 本方案支持对访问控制的隐私保护，本质上来说访问控制是一组属性的描述，实现对访问控制的隐私保护等同于实现对用户属性的隐藏。与之前的访问控制方案相比，本方案考虑了访问控制的属性隐私。

4）外包解密： 本方案允许群智用户能够以最低的能耗去快速解密和访问目标数据。

1 理论知识

1.1 困难性问题

n-线性假设：给定一个群(p, G_1, G_2, G_T, e)，不存在一个多项式区分者可以以不可忽略的优势区分$\mathcal{T}_0=\left(g_1, g_2, g_1^{\boldsymbol{R}}, g_1^{\boldsymbol{R}\boldsymbol{\gamma}}\right)$和$\mathcal{T}_1=\left(g_1, g_2, g_1^{\boldsymbol{R}}, g_1^{\boldsymbol{Z}}\right)$，这里，$\boldsymbol{\gamma}$是从$Z_p$选取长度为$n$的随机矩阵，$\boldsymbol{Z}$是从$Z_p$选取$n+1$行1列的随机矩阵，$\boldsymbol{R}$为从$Z_p$选取$n+1$行$n$列的随机整数矩阵。

1.2 系统模型

在图 1 所示的本系统模型中，涉及 4 种不同类型的实体: 权威机构、云服务器、数据拥有者、数据发送者。具体来说，首先权威机构生成系统公开参数，并向系统中的所有实体公开。此外，所有的

权威机构为用户生成私钥，并将生产的私钥发送给用户。数据拥有者通过加密算法将其群智数据加密生成密文，并将生成的密文发送到云服务器上存储和共享。当数据使用者想访问存储在云服务器上的密文数据，他首先盲化其私钥生成盲化密钥和转换密钥，然后将盲化密钥发送给云服务器。云服务器在接收到盲化密钥时，执行外包解密操作，并将转换后的外包密文发送给该数据使用者。数据使用者在接收到转换的外包密文后，使用转换密钥恢复明文信息。

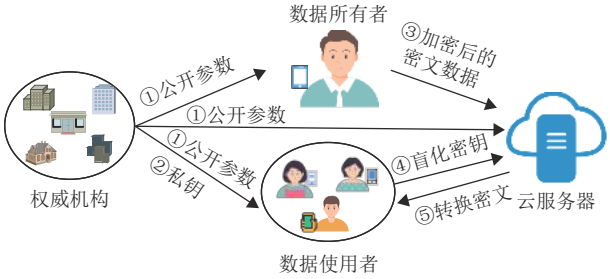

图 1　系统模型图

和其他类似方案的安全模型定义相同[14-15, 18]，本方案中所有的权威机构都是半可信的第三方，即诚实好奇的第三方，它们能忠实地执行公钥生成和发布，为用户生成其各自的私钥，但可能伪装成合法用户非法访问数据。云服务器是半可信的，即为用户提供无限的存储资源以及为用户忠实地执行其指示的操作，但也很好奇地试图去了解其存储的数据或执行的解密内容。数据拥有者是诚实的数据发送方，主要负责上传数据，以分享给其他用户实现非交互式的数据访问。数据访问者是不可信的数据访问方，即非授权用户试图通过发起包含合谋攻击等手段以获取合法权限，从而达到其非法访问非授权用户数据的目的。

1.3　形式化定义

本方案由如下若干个算法组成。

SETUP(λ): 输入安全参数λ，输出公共参数pp，该算法由所有权威机构执行。

AuthSetup(pp, i): 输入公共参数pp、权威机构索引i，生成其公私钥PK_i和SK_i，该算法由权威机构执行。

Encrypt(pp, PK_i, $\boldsymbol{x}$, m): 输入公共参数pp、公钥PK_i、访问控制向量$\boldsymbol{x}$、加密消息m，该加密算法输出密文CT，该算法由数据所有者执行。

KeyGen(pp, SK_i, PK_i, GID, $\boldsymbol{z}$): 输入公共参数pp，所有权威机构私钥SK_i、所有权威机构的公钥PK_i、用户的全局身份GID、属性向量$\boldsymbol{z}$，该密钥生成算法为用户生成私钥UK_i，该算法由各权威机构执行。

$\mathrm{KeyGen}_{\mathrm{out}}$(pp, UK_i): 输入公共参数pp、用户私钥UK_i，该密钥盲化算法为用户生成盲化私钥(z', UK'_i)和转换密钥tk，该算法由数据使用者执行。

$\mathrm{Decrypt}_{\mathrm{out}}$(pp, CT, (z', UK'_i)): 输入公共参数pp、密文CT、盲化私钥(z', UK'_i)，该外包解密算法生成外包密文CT′，该算法由云服务器执行。

Decrypt(pp, CT′, tk): 输入公共参数pp、外包解密密文CT′、转换私钥tk，该解密算法输出明文消息m，该算法由数据使用者执行。

1.4　安全游戏

定义 1　对所有攻击者$\mathcal{A}$来说，若能以可忽略的优势赢得与挑战者C之间的游戏，那么本方案能够实现语义安全性，即明文的机密性。

参数建立阶段(Setup)：挑战者C执行Setup(λ)和AuthSetup(pp, i)算法生成公共参数pp和权威机构的公共参数PK_i，并将其发给攻击者$\mathcal{A}$。

密钥询问阶段 (Key Query)：攻击者$\mathcal{A}$发送对于属性向量$\boldsymbol{z}$的密钥请求，挑战者C执行KeyGen(pp, SK_i, PK_i, GID, z)为攻击者生成如下密钥$\mathrm{UK}_{i,\,\mathrm{GID},\,z}$。注意在此阶段，允许攻击者获取部分$\mathrm{UK}_{i,\,\mathrm{GID},\,z}$，且在获得密钥后允许执行$\mathrm{KeyGen}_{\mathrm{out}}$(pp, UK_i)进行密钥盲化。

密文生成阶段 (Ciphertext)：攻击者$\mathcal{A}$选择两个等长的消息m_c, $c \in \{0, 1\}$以及发送访问向量$\boldsymbol{x}_0$、$\boldsymbol{x}_1$，挑战者C执行Encrypt(pp, PK_i, $\boldsymbol{x}$, m)生成CT_c。

猜测阶段Guess：攻击者$\mathcal{A}$输出一个对消息m_c的猜测比特c'，若$c = c'$，则攻击者$\mathcal{A}$赢得该游戏。

2　基本构造方案

SETUP(λ)：该算法由共同权威机构执行。输入安全参数λ，该算法首先选取一个双线性群$\mathrm{BG} = (p, G_1, G_2, G_T, e)$，其中，$g_1$，$g_2$分别表示群$G_1$和$G_2$的一个生成元。随后，该算法随机从$Z_p$选取一个$n+1$行$n$列的矩阵$\boldsymbol{R} \in Z_p^{(n+1)\times n}$，一个$n+1$行$n+1$列的矩阵$\boldsymbol{V} \in Z_p^{(n+1)\times(n+1)}$。其次，选取$n+2$个哈希函数$H, H_1, \cdots, H_{n+1} : \{0,1\}^* \to Z_p$。最后，该算法生成公共参数$\mathrm{pp} = (g_1, g_2, H, H_1, \cdots, H_{n+1}, g_1^{\boldsymbol{R}}, g_1^{\boldsymbol{V}^{\mathrm{T}}\boldsymbol{R}})$。

AuthSetup(pp, i)：该算法由每个权威机构生成各自的公私钥。输入公共参数pp、权威机构索引i，该算法首先从Z_p选取一个$n+1$行$n+1$列的矩阵$\boldsymbol{S}_i \in Z_p^{(n+1)\times(n+1)}$、一个$n+1$维向量$\boldsymbol{\alpha}_i \in Z_p$、一个数$\beta_i$，生成和存储其私钥$\mathrm{SK}_i = (\boldsymbol{S}_i, \boldsymbol{\alpha}_i, \beta_i)$，并公开其

公钥$\mathrm{PK}_i=(g_1^{\boldsymbol{S}_i^{\mathrm{T}}\boldsymbol{R}}, e(g_1, g_2)^{\boldsymbol{\alpha}_i^{\mathrm{T}}\boldsymbol{R}}, y_i=g_2^{\beta_i})$。

Encrypt(pp, PK_i, x, m): 输入公共参数pp、公钥PK_i、访问控制向量x、加密消息m，该算法首先选取n维的一个随机向量$\boldsymbol{\gamma}$，计算生成密文$\mathrm{CT}=(C_0, C_i, C')$: $C_0=g_1^{\boldsymbol{R}\gamma}$, $Ci=g_1^{(x_i\boldsymbol{V}^{\mathrm{T}}+\boldsymbol{S}_i^{\mathrm{T}})\boldsymbol{R}\gamma}$, $C'=m\prod_{i=2}^{n}e(g_1, g_2)^{\boldsymbol{\alpha}_i^{\mathrm{T}}\boldsymbol{R}\gamma}$。

$\mathrm{KeyGen}_{\mathrm{out}}$(pp, SK_i, PK_i, GID, z)：该算法由各权威机构执行。输入公共参数pp、所有权威机构私钥SK_i、所有权威机构的公钥PK_i、用户的全局身份GID、属性向量$\boldsymbol{z}$，该算法首先计算$\mu_i=\sum_{j=1}^{i-1}H(y_j^{\beta_i},\mathrm{GID},z)-\sum_{j=i+1}^{n}H(y_j^{\beta_i},\mathrm{GID},z)$，注意$\sum_{i=1}^{n}\mu_i=0$。其次，该算法使用$H_1(\mathrm{GID}, z), \cdots, H_{n+1}(\mathrm{GID}, z)$生成$g_2^h$，这里$h=H(\mathrm{GID}, z)=(H_1(\mathrm{GID},z),\cdots,H_{n+1}(\mathrm{GID}, z))^{\mathrm{T}}$。最后，该算法生成用户私钥$\mathrm{UK}_i=g_2^{\boldsymbol{\alpha}_i-z_i\boldsymbol{S}_ih+\mu_i}$。请注意本文中私钥的分配是通过安全信道分配和发送的。

$\mathrm{KeyGen}_{\mathrm{out}}$(pp, UK_i)：该算法由数据使用者执行。输入公共参数pp、用户私钥UK_i、该算法首先从Z_p中随机选取一个随机数$\hat{t}$，该算法生成用户盲化私钥$\mathrm{UK}_i'=\mathrm{UK}_i^{1/\hat{t}}=g_2^{(\alpha_i-z_iS_ih+\mu_i)/\hat{t}}$，$z'=(z_1/t,\cdots,z_n/\hat{t})$，$g_2^h=H(\mathrm{GID}, z)$，并保存转换密钥$\mathrm{tk}=\hat{t}$。

$\mathrm{Decrypt}_{\mathrm{out}}$(pp, CT, (z', UK'_i))：该算法由云服务器执行。输入公共参数pp、密文CT，盲化私钥$(z', \mathrm{UK}_i', g_2^h)$，该算法首先计算并生成外包密文CT′为$e(g_1, g_2)^{\boldsymbol{\alpha}^{\mathrm{T}}R_\gamma/t}$。

Decrypt(pp, CT′, tk)：该算法由数据使用者执行。输入公共参数pp，外包解密密文CT′，转换私钥tk，该算法可以恢复明文消息$m=C'/(\mathrm{CT}')^{\hat{t}}$。

3 正确性和安全性分析

3.1 正确性分析

$$A=e\left(C_0,\prod_{i=1}^{n}\mathrm{UK}'_i\right)e\left(\prod_{i=1}^{n}C_i^{Z_i'},g_2^{\boldsymbol{h}}\right)=$$

$$e\left(g_1^{\boldsymbol{R}\gamma},\prod_{i=1}^{n}g_2^{(\alpha_i-z_i\boldsymbol{S}_i\boldsymbol{h}+\mu_i)/\hat{t}}\right)e\left(g_1^{\sum_{i=1}^{n}z'_i\left(x_i\boldsymbol{V}^{\mathrm{T}}+\boldsymbol{S}_i^{\mathrm{T}}\right)\boldsymbol{R}\gamma}\right)=$$

$$e\left(g_1^{\boldsymbol{R}\gamma},\prod_{i=1}^{n}g_2^{(\alpha_i-z_i\boldsymbol{S}_i\boldsymbol{h}+\mu_i)/\hat{t}}\right)e\left(g_1^{\sum_{i=1}^{n}z'_i\left(x_i\boldsymbol{V}^{\mathrm{T}}+\boldsymbol{S}_i^{\mathrm{T}}\right)\boldsymbol{R}\gamma},g_2^{\boldsymbol{h}}\right)=$$

$$e(g_1,g_2)^{\boldsymbol{\alpha}^{\mathrm{T}}\boldsymbol{R}_\gamma-\sum_{i=1}^{n}z_i\boldsymbol{h}^{\mathrm{T}}\boldsymbol{S}_i^{\mathrm{T}}\boldsymbol{R}_\gamma}\times e(g_1,g_2)^{\langle x,z'\rangle\boldsymbol{h}^{\mathrm{T}}\boldsymbol{V}^{\mathrm{T}}\boldsymbol{R}_\gamma+\sum_{i=1}^{n}z_i\boldsymbol{h}^{\mathrm{T}}\boldsymbol{S}_i^{\mathrm{T}}\boldsymbol{R}_\gamma}=$$

$$e(g_1,g_2)^{\boldsymbol{\alpha}^{\mathrm{T}}\boldsymbol{R}_\gamma/\hat{t}}e(g_1,g_2)^{\langle x,z'\rangle\boldsymbol{h}^{\mathrm{T}}\boldsymbol{V}^{\mathrm{T}}\boldsymbol{R}}$$

当用户的属性向量和访问向量正相交时，即$\langle x,z\rangle=0$表示用户的属性集合满足密文中的访问控制，则以上等式$A=e(g_1,g_2)^{\boldsymbol{\alpha}^{\mathrm{T}}R_\gamma/\hat{t}}$，其中，$\boldsymbol{\alpha}=\sum_{i=1}^{n}\boldsymbol{\alpha}_i$。随后，用户可以正确恢复消息$m=C'/A^{\hat{t}}$。

3.2 安全性分析

为了能够证明本方案的语义安全性，定义了一系列的游戏Game如下。

Game_0：该游戏与定义 1 中一样，模拟的是方案真实的安全游戏。

Game_1：该游戏除了随机预言机回答的询问不一样外，其他均与游戏Game_0和一样。具体来说随机预言机模拟的过程如下：挑战者C从Z_p中随机选取一个长度为n的向量$\boldsymbol{r}$，计算$\boldsymbol{h}=\boldsymbol{Br}$，然后存储$\boldsymbol{h}$的值去回答攻击者的随机预言机询问。

$\mathrm{Game}_{2,j,1}$：该游戏几乎与游戏Game_1一样，除了挑战者C选择$\boldsymbol{R},\boldsymbol{a}^{\perp},\boldsymbol{B},\boldsymbol{b}^{\perp},\hat{t}$，使得$\boldsymbol{R}^{\mathrm{T}}\boldsymbol{a}^{\perp}=0$以及$\boldsymbol{B}^{\mathrm{T}}\boldsymbol{b}^{\perp}=0$，具体密钥询问如下。

1）前$j-1$密钥询问的回答如下：$\mathrm{UK}=g_2^{\boldsymbol{\alpha}+\boldsymbol{\alpha}^{\perp}\hat{t}-\sum_{i=1}^{n}z_i\boldsymbol{S}_i\boldsymbol{h}}$，这里$h$和游戏$\mathrm{Game}_1$中的一样，即挑战者$C$从$Z_p$中随机选取一个长度为$n$的向量$\boldsymbol{r}$，计算$h=\boldsymbol{Br}$。

2）第j个密钥询问的回答如下：$\mathrm{UK}=g_2^{\boldsymbol{\alpha}-\sum_{i=1}^{n}z_i\boldsymbol{S}_i\boldsymbol{h}}$，这里$h$和游戏$\mathrm{Game}_1$中的一样，即挑战者$C$从$Z_p$中随机选取一个长度为$n$的向量$\boldsymbol{r}$以及一个随机数$\hat{r}$，使得$h=\boldsymbol{Br}+\boldsymbol{a}^{\perp}\hat{r}$。

3）最后q—j个密钥询问回答如下: $\mathrm{UK}=g_2^{\boldsymbol{\alpha}-\sum_{i=1}^{n}z_i\boldsymbol{S}_i\boldsymbol{h}}$，这里$\boldsymbol{h}=\boldsymbol{Br}$，$\boldsymbol{r}$是从$Z_p$中随机选取一个长度为$n$的向量。

$\mathrm{Game}_{2,j,2}$：该游戏几乎与游戏$\mathrm{Game}_{2,j,1}$一样，除了第j个密钥询问时回答不同，具体来说，$\mathrm{UK}=g_2^{\boldsymbol{\alpha}+\boldsymbol{\alpha}^{\perp}\hat{t}-\sum_{i=1}^{n}z_i\boldsymbol{S}_i\boldsymbol{h}}$，这里挑战者$C$从$Z_p$中随机选取一个长度为$n$的向量$\boldsymbol{r}$以及一个随机数$\hat{r}$，使得$\boldsymbol{h}=\boldsymbol{Br}+\boldsymbol{a}^{\perp}\hat{r}$。

$\mathrm{Game}_{2,j,3}$：该游戏几乎与游戏$\mathrm{Game}_{2,j,2}$一样，除了前j个密钥询问时回答不同，具体来说，$\mathrm{UK}=g_2^{\boldsymbol{\alpha}+\boldsymbol{\alpha}^{\perp}\hat{t}-\sum_{i=1}^{n}z_i\boldsymbol{S}_i\boldsymbol{h}}$，这里挑战者$C$从$Z_p$中随机选取一个长度为$n$的向量$\boldsymbol{r}$，使得$\boldsymbol{h}=\boldsymbol{Br}$。

Game_3：该游戏几乎与游戏Game_2一样，除了生成的挑战密文与其不同。具体来说，挑战者C从Z_p中选取一个长度为$n+1$的向量$\boldsymbol{a}$，并生成如下密文：$C_0=g_1^{\boldsymbol{a}}$，$C_i=g_1^{\left(\boldsymbol{x}_{b,i}\boldsymbol{V}^{\mathrm{T}}+\boldsymbol{S}_i^{\mathrm{T}}\right)\boldsymbol{a}}$，$C'=m_ce(g_1,g_2)^{\boldsymbol{\alpha}^{\mathrm{T}}\boldsymbol{a}}$。

Game_4：该游戏几乎与游戏Game_3一样，除了加密消息时随机选取的群中的元素。

Game_5：该游戏几乎与游戏Game_4一样，除了

选取的访问向量$\boldsymbol{x}$被一个随机向量$\boldsymbol{x}^*$取代。注意该游戏从攻击者$\mathcal{A}$的角度无法区分加密的消息，因此无法以一定的优势赢得该游戏。

引理 1　游戏Game_0和游戏Game_1的不可区分性

如果存在一个攻击者$\mathcal{A}$能够区分游戏Game_0和游戏Game_1，那么就存在一个挑战者C能够以不可忽略的优势解决线性判定性问题（decisional linear problem）。

证明：挑战者C接收一个判定性线性问题的实例$\left(g_2^B, g_2^h\right)$，目标是区分$h=Br$或$h$是$Z_p$中一个随机数，其中$r$是$Z_p$中随机选取的。可以很容易观察到公共参数、权威机构的公钥和挑战密文如实际方案被构建出来。针对用户私钥询问，可以通过如下计算得出$\text{UK}=g_2^{\alpha}\prod_{i=1}^{n}\left(g_2^{\boldsymbol{h}}\right)^{-z_i\boldsymbol{S}_i}=g_2^{\alpha-\sum_{i=1}^{n}z_i\boldsymbol{S}_i\boldsymbol{h}}$。

当$h\in\text{Span}(B)h\in\text{Span}(B)$时，密钥和随机预言机响应的分布与游戏$\text{Game}_1$完全相同，而在另一种情况下，其分布与游戏$\text{Game}_0$完全相同。通过$k$-判定性线性问题，可以得知攻击者$\mathcal{A}$只能够以可忽略的优势区分这两个游戏。

引理 2　游戏$\text{Game}_{2,j-1,3}$和游戏$\text{Game}_{2,j,1}$的不可区分性

如果存在一个攻击者$\mathcal{A}$能够区分游戏$\text{Game}_{2,j-1,3}$和游戏$\text{Game}_{2,j,1}$，那么就存在一个挑战者C能够以不可忽略的优势解决线性判定性问题。

证明：挑战者C接收一个判定性线性问题的实例$\left(g_2^{\boldsymbol{B}}, g_2^{\boldsymbol{h}}\right)$，目标是区分$\boldsymbol{h}=\boldsymbol{Br}$或$\boldsymbol{h}$是$Z_p$中的一个随机数，其中$\boldsymbol{t}$是$Z_p$中随机选取长度为$n$的向量。

参数建立阶段(Setup)：挑战者C如实际方案中一样随机选择一个长度为$n+1$的向量$\boldsymbol{\alpha}_i\in Z_p$、一个随机数$\hat{t}\in Z_p$、随机矩阵$\boldsymbol{R}$，$\boldsymbol{a}^{\perp}$，$\boldsymbol{S}_i$，$\boldsymbol{V}$，生成公开参数$g_1^{\boldsymbol{R}}$，$g_1^{\boldsymbol{V}^{\mathrm{T}}\boldsymbol{R}}$以及权威机构的公钥$g_1^{\boldsymbol{S}_i^{\mathrm{T}}\boldsymbol{R}}$，$e(g_1,g_2)^{\boldsymbol{\alpha}_i^{\mathrm{T}}\boldsymbol{R}}$。

密钥询问阶段(Key,Query)：输入第m个密钥询问，挑战者C为攻击者生成如下密钥：

$$\text{UK}=\begin{cases}g_2^{\boldsymbol{\alpha}+\boldsymbol{\alpha}^{\perp}\boldsymbol{t}-\sum_{i=1}^{n}z_i\boldsymbol{S}_i\boldsymbol{Br}} & m<j\\ g_2^{\boldsymbol{\alpha}-\sum_{i=1}^{n}z_i\boldsymbol{S}_i\boldsymbol{h}} & m=j\\ g_2^{\boldsymbol{\alpha}-\sum_{i=1}^{n}z_i\boldsymbol{S}_i\boldsymbol{Br}} & m>j\end{cases}$$

式中，$\boldsymbol{r}$表示从Z_p中选取的随机值组成的一个长度为n的向量。注意攻击者在拿到密钥后可以进行密钥盲化，模拟外包的过程。

密文生成阶段 (Ciphertext)：攻击者$\mathcal{A}$选择两个等长的消息$m_b, b\in\{0,1\}$，挑战者C随机选择一个$\boldsymbol{\gamma}$，计算如下：$C_0=g_1^{\boldsymbol{R}\boldsymbol{\gamma}}$，$C_i=g_1^{\left(\boldsymbol{x}_{b,i}\boldsymbol{V}^{\mathrm{T}}+\boldsymbol{S}_i^{\mathrm{T}}\right)\boldsymbol{R}\boldsymbol{\gamma}}$，$C'=m_b e(g_1,g_2)^{\boldsymbol{\alpha}^{\mathrm{T}}\boldsymbol{R}\boldsymbol{\gamma}}$。

当$h\in\text{Span}(B)$时，密钥和随机预言机响应的分布与游戏$\text{Game}_{2,j-1,3}$完全相同，而在另一种情况下，其分布与游戏$\text{Game}_{2,j,1}$完全相同。通过k-判定性线性问题，可以得知攻击者$\mathcal{A}$只能够以可忽略的优势区分这两个游戏。

引理 3　游戏$\text{Game}_{2,j,1}$和游戏$\text{Game}_{2,j,2}$不可区分性

如果存在一个攻击者$\mathcal{A}$能够区分游戏$\text{Game}_{2,j,1}$和游戏$\text{Game}_{2,j,2}$，那么就存在一个挑战者C能够以不可忽略的优势解决线性判定性问题。

证明：两种游戏的不同之处在于在后面的游戏中需要用$g_2^{\boldsymbol{a}^{\perp}\hat{t}}$乘以第$j$个密钥，其中$\hat{t}$是由挑战者$C$从$Z_p$中随机采样的。在第$j$个密钥询问中，攻击者$\mathcal{A}$向挑战者$C$发送有关密钥的属性向量$\boldsymbol{z}$，挑战者$C$执行如下操作：

$$\boldsymbol{S}_i'=\begin{cases}\boldsymbol{S}_i+\left(z_i\boldsymbol{a}^{\perp\mathrm{T}}\boldsymbol{b}^{\perp}\right)^{-1}\boldsymbol{a}^{\perp}\boldsymbol{b}^{\perp\mathrm{T}} & z_i\neq 0\\ \boldsymbol{S}_i & z_i=0\end{cases}$$

从以上可以看出$\boldsymbol{S}_i$和$\boldsymbol{S}_i'$的分布显然是相同的。此外，还可以得知若密文和权威机构的公钥是使用$\boldsymbol{S}_i'$而不是$\boldsymbol{S}_i$生成的，则二者没有区别。具体来说，对于公钥的生成如下：

$$g_1^{\boldsymbol{S}_i'^{\mathrm{T}}\boldsymbol{R}}=g_1^{\boldsymbol{S}_i^{\mathrm{T}}\boldsymbol{R}+\left(z_i\boldsymbol{a}^{\perp\mathrm{T}}\boldsymbol{b}^{\perp}\right)^{-1}\left(\boldsymbol{a}^{\perp}\boldsymbol{b}^{\perp\mathrm{T}}\right)^{\mathrm{T}}\boldsymbol{R}}=g_1^{\boldsymbol{S}_i^{\mathrm{T}}\boldsymbol{R}}$$

对于密文生成如下：

$$C_{1,i}=g_1^{\left(x_i\boldsymbol{V}^{\mathrm{T}}+\boldsymbol{S}'^{\mathrm{T}}_i\right)\boldsymbol{R}_\gamma}=$$

$$g_1^{\left(\boldsymbol{x}_i\boldsymbol{V}^{\mathrm{T}}+\boldsymbol{S}_i^{\mathrm{T}}\right)\boldsymbol{R}_\gamma+\left(z_i\boldsymbol{a}^{\perp\mathrm{T}}\boldsymbol{b}^{\perp}\right)^{-1}\left(\boldsymbol{a}^{\perp}\boldsymbol{b}^{\perp\mathrm{T}}\right)^{\mathrm{T}}\boldsymbol{R}}=g_1^{\left(x_i\boldsymbol{V}^{\mathrm{T}}+\boldsymbol{S}_i^{\mathrm{T}}\right)\boldsymbol{R}_\gamma}$$

挑战者C使用S_i'可以针对攻击者$\mathcal{A}$针对第j个密钥询问做如下操作:

$$\text{UK}=g_2^{\alpha-\sum_{i=1}^{n}z_i\boldsymbol{S}_i'h}$$

式中，$\boldsymbol{h}=\boldsymbol{Br}+(\boldsymbol{t}/n)\boldsymbol{a}^{\perp}$；$\boldsymbol{r}\in Z_p^n$；$\boldsymbol{t}\in Z_p$。可以得到

$$\boldsymbol{S}'_i\boldsymbol{h}=\boldsymbol{S}_i\boldsymbol{h}+\left(z_i\boldsymbol{a}^{\perp\mathrm{T}}\boldsymbol{b}^{\perp}\right)^{-1}\boldsymbol{a}^{\perp}\boldsymbol{b}^{\perp\mathrm{T}}(\boldsymbol{Br}+(\boldsymbol{t}/n)\boldsymbol{a}^{\perp})=$$

$$\boldsymbol{S}_i\boldsymbol{h}+(z_i)^{-1}\left(\boldsymbol{a}^{\perp\mathrm{T}}\boldsymbol{b}^{\perp}\right)^{-1}\left(\boldsymbol{a}^{\perp}\boldsymbol{b}^{\perp\mathrm{T}}\right)\boldsymbol{a}^{\perp}(\boldsymbol{t}/n)=$$

$$\boldsymbol{S}_i\boldsymbol{h}+(z_i)^{-1}\left(\boldsymbol{a}^{\perp\mathrm{T}}\boldsymbol{b}^{\perp}\right)^{-1}\boldsymbol{a}^{\perp}\left(\boldsymbol{a}^{\perp}\boldsymbol{b}^{\perp\mathrm{T}}\right)(\boldsymbol{t}/n)=$$

$$\boldsymbol{S}_i\boldsymbol{h}+(z_i)^{-1}\boldsymbol{a}^{\perp}(\boldsymbol{t}/n)$$

因此，用户私钥可以得到:

$$\mathrm{UK}=g_2^{\alpha-\sum_{i=1}^{n}z_iS_i'h}=g_2^{\alpha+a^{\perp}t-\sum_{i=1}^{n}z_iS_ih}$$

这样可以轻易得知游戏$\mathrm{Game}_{2,j,2}$的精确分布。

引理 4 游戏$\mathrm{Game}_{2,j,2}$和游戏$\mathrm{Game}_{2,j,3}$的不可区分性

如果存在一个攻击者$\mathcal{A}$能够区分游戏$\mathrm{Game}_{2,j,2}$和游戏$\mathrm{Game}_{2,j,3}$，那么就存在一个挑战者C能够以不可忽略的优势解决k-线性判定性问题（decisional linear problem）。

证明：挑战者C接收一个判定性线性问题的实例$\left(g_2^{\boldsymbol{B}},g_2^{\boldsymbol{h}}\right)$，目标是区分$\boldsymbol{h}=\boldsymbol{Br}$或$\boldsymbol{h}$是$Z_p$中的一个随机数，其中$\boldsymbol{t}$是$Z_p$中随机选取长度为$n$的向量。

参数建立阶段 (Setup)：挑战者C如实际方案中一样随机选择一个长度为$n+1$的向量$\boldsymbol{\alpha}_i\in Z_p$，一个随机数$\boldsymbol{t}\in Z_p$，随机矩阵$\boldsymbol{R}$，$\boldsymbol{a}^{\perp}$，$\boldsymbol{S}_i$，$\boldsymbol{V}$，生成公开参数$g_1^{\boldsymbol{R}}$，$g_1^{\boldsymbol{V}^{\mathrm{T}}\boldsymbol{R}}$以及权威机构的公钥$g_1^{\boldsymbol{S}_i^{\mathrm{T}}\boldsymbol{R}}$，$e(g_1,g_2)^{\alpha_i^{\mathrm{T}}\boldsymbol{R}}$。

密钥询问阶段 (Key,Query)：输入第 m个密钥询问，挑战者C为攻击者生成如下密钥：

$$\mathrm{UK}=\begin{cases}g_2^{\alpha+\boldsymbol{a}^{\perp}t-\sum_{i=1}^{n}z_i\boldsymbol{S}_i\boldsymbol{h}} & m\leqslant j\\ g_2^{\alpha-\sum_{i=1}^{n}z_i\boldsymbol{S}_iBr} & m>j\end{cases}$$

式中，$\boldsymbol{r}$表示从Z_p中选取的随机值组成的一个长度为 n 的向量。注意攻击者在拿到密钥后可以进行密钥盲化，模拟外包的过程。

密文生成阶段 (Ciphertext)：攻击者$\mathcal{A}$选择两个等长的消息$m_b,b\in\{0,1\}$，挑战者C随机选择一个$\boldsymbol{\gamma}$，计算如下：$C_0=g_1^{\boldsymbol{R}\boldsymbol{\gamma}}$，$C_i=g_1^{\left(\boldsymbol{x}_{b,i}\boldsymbol{V}^{\mathrm{T}}+\boldsymbol{S}_i^{\mathrm{T}}\right)\boldsymbol{R}\boldsymbol{\gamma}}$，$C'=m_b\times e(g_1,g_2)^{\boldsymbol{\alpha}^{\mathrm{T}}\boldsymbol{R}\boldsymbol{\gamma}}$

当$\boldsymbol{h}\in\mathrm{Span}(\boldsymbol{B})$时，密钥和随机预言机响应的分布与游戏$\mathrm{Game}_{2,j-1,3}$完全相同，而在另一种情况下，其分布与游戏$\mathrm{Game}_{2,j,2}$完全相同。通过$k$-判定性线性问题，可以得知攻击者$\mathcal{A}$只能够以可忽略的优势区分这两个游戏。

引理 5 游戏$\mathrm{Game}_{2,q,3}$和游戏Game_3的不可区分性

如果存在一个攻击者$\mathcal{A}$能够区分游戏$\mathrm{Game}_{2,q,3}$和游戏Game_3，那么就存在一个挑战者C能够以不可忽略的优势解决线性判定性问题。

证明：给定一个判定性线性问题的实例$\left(g_1^{\boldsymbol{R}},g_1^{\boldsymbol{a}}\right)$，目标是判断$\boldsymbol{a}=\boldsymbol{R}_{\gamma}$或$\boldsymbol{a}$是一个从$Z_p$中随机采样长度为$n+1$的随机分布。挑战者$C$如实际方案中一样随机选取矩阵样本$\boldsymbol{V}$，$\boldsymbol{S}_i$以及一个向量$\boldsymbol{\alpha}_i$，并输出公开参数$g_1^{\boldsymbol{R}}$，$g_1^{\boldsymbol{V}^{\mathrm{T}}\boldsymbol{R}}$以及权威机构的公钥$g_1^{\boldsymbol{S}_i^{\mathrm{T}}\boldsymbol{R}}$，$e\left(g_1^{\boldsymbol{R}},g_2^{\alpha_i}\right)=e(g_1,g_2)^{\alpha_i^{\mathrm{T}}\boldsymbol{R}}$。

生成挑战密文如下：$C_0=g_1^{\boldsymbol{a}}$，$C_i=g_1^{\left(\boldsymbol{x}_{b,i}V^{\mathrm{T}}+\boldsymbol{S}_i^{\mathrm{T}}\right)\boldsymbol{a}}$，$C'=m_ce(g_1,g_2)^{\alpha^{\mathrm{T}}\boldsymbol{a}}$。

当$a\in\mathrm{Span}(\boldsymbol{R})$时，密钥和随机预言机响应的分布与游戏 Game_3 完全相同，而在另一种情况下，其分布与游戏$\mathrm{Game}_{2,q,3}$完全相同。通过k-判定性线性问题，可以得知攻击者$\mathcal{A}$只能够以可忽略的优势区分这两个游戏。

引理 6 游戏Game_3和游戏Game_4的不可区分性

如果存在一个攻击者$\mathcal{A}$能够区分游戏Game_3和游戏Game_4，那么就存在一个挑战者C能够以不可忽略的优势解决线性判定性问题。

证明：挑战者C随机化选取一个矩阵$\boldsymbol{R}$，$\boldsymbol{a}^{\perp}$，使得$\boldsymbol{R}^T\boldsymbol{a}^{\perp}=0$，一个从$Z_p$中选取的随机值组成的一个长度为$n+1$随机向量$\boldsymbol{\alpha}$，一个从$Z_p$中选取的随机数$\hat{s}$。随后，挑战者$C$计算$\hat{\boldsymbol{\alpha}}=\boldsymbol{\alpha}-\boldsymbol{a}^{\perp}\hat{s}$。

参数建立阶段(Setup)：挑战者C如实际方案中一样生成公开参数$g_1^{\boldsymbol{R}}$，$g_1^{\boldsymbol{V}^{\mathrm{T}}\boldsymbol{R}}$以及权威机构的公钥$g_1^{\boldsymbol{S}_i^{\mathrm{T}}\boldsymbol{R}}$，$e\left(g_1^{\boldsymbol{R}},g_2^{\alpha_i}\right)=e(g_1,g_2)^{\alpha_i^{\mathrm{T}}\boldsymbol{R}}$。

密钥询问阶段(Key,Query): 挑战者C为攻击者生成如下密钥:

$$\mathrm{UK}=g_2^{\hat{\alpha}-\sum_{i=1}^{n}z_i\boldsymbol{S}_ih}$$

注意在此阶段，攻击者在拿到密钥后可以进行密钥盲化，模拟外包的过程。

密文生成阶段(Ciphertext)：攻击者$\mathcal{A}$选择两个等长的消息$m_c,c\in\{0,1\}$，挑战者C随机选择一个向量$\boldsymbol{\gamma}$，一个随机数$\hat{\gamma}$，令$a=\boldsymbol{R}_{\boldsymbol{\gamma}}+\boldsymbol{b}^{\mathrm{T}}\hat{\gamma}$。随后计算$m'=m_ce(g_1,g_2)^{(\boldsymbol{a}^{\perp}\hat{s})^{\mathrm{T}}\boldsymbol{a}}=m_ce(g_1,g_2)^{\hat{\gamma}\hat{s}(\boldsymbol{a}^{\perp})^{\mathrm{T}}\boldsymbol{b}^{\mathrm{T}}}$，由以上公式可以得知元素$m'$很大概率是群中的一个随机值。那么，密文可以被计算如下：

$$C_0=g_1^{\boldsymbol{a}},\ C_{1,i}=g_1^{\left(\boldsymbol{x}_{b,i}\boldsymbol{V}^{\mathrm{T}}+\boldsymbol{S}_i^{\mathrm{T}}\right)\boldsymbol{a}}$$

$$C'=m'e(g_1,g_2)^{\hat{\alpha}^{\mathrm{T}}\boldsymbol{a}}=$$

$$m_ce(g_1,g_2)^{\hat{\gamma}\hat{s}(\boldsymbol{a}^{\perp})^{\mathrm{T}}\boldsymbol{b}^{\mathrm{T}}}e(g_1,g_2)^{\boldsymbol{\alpha}^{\mathrm{T}}\boldsymbol{a}}=m_ce(g_1,g_2)^{\boldsymbol{\alpha}^{\mathrm{T}}\boldsymbol{a}}$$

很容易可以得知游戏Game_3被准确模拟出来，攻击者$\mathcal{A}$只能够以可忽略的优势区分这两个游戏。

引理 7 游戏Game_4和游戏Game_5的不可区分性

如果存在一个攻击者$\mathcal{A}$能够区分游戏Game_4和

游戏Game$_5$，那么就存在一个挑战者C能够以不可忽略的优势解决线性判定性问题。

证明：挑战者C可以生成如下密文：

$$C_{1,i}=g_1^{(x_{b,i}V^{\mathrm{T}}+S_i^{\mathrm{T}})(R\gamma+b^{\mathrm{T}}\hat{y})}=g_1^{x_{b,i}V^{\mathrm{T}}(R\gamma+b^{\mathrm{T}}\hat{y})}g_1^{S_i^{\mathrm{T}}(R\gamma+b^{\mathrm{T}}\hat{y})}$$

式中，$R,\gamma\in Z_p^n$，$b^{\perp}\in Z_p^n$，使得$B^{\mathrm{T}}b^{\perp}=0$。此外，当$\hat{y}\in Z_p$，给定$g_1^{R}$，$g_1^{R\gamma+b^{\mathrm{T}}\hat{y}}$，$g_1^{S_i^{\mathrm{T}}R}$以及$g_2^{B}$，那么可以得到$g_1^{S_i^{\mathrm{T}}(R\gamma+b^{\mathrm{T}}\hat{y})}$在群$G_1$中均匀分布的。也就是说$C_{1,i}$在群$G_1$中均匀分布的。因此，攻击者$\mathcal{A}$只能够以可忽略的优势区分这两个游戏。

属性隐私：攻击者很容易从密文中获取访问控制属性的隐私，这是因为对于基于属性相关的密码体制来说，访问控制通常以明文的形式附贴在密文上。在本方案中，将属性和访问控制转化成属性和访问向量，这两种向量分别用于私钥和密文的生成。在密文生成过程中，访问向量不必以明文的形式附贴在密文上，而是隐藏在密文中，从而避免了攻击者从密文中获取访问控制属性的隐私的可能。

4　性能分析

4.1　功能分析

从表 1 可以得知，文献 [11] 仅支持细粒度访问控制，而不支持权威去中心化、访问控制的属性隐私保护和高效的数据访问；文献 [12-13, 16-17, 19] 支持细粒度访问控制和权威去中心化，而不支持访问控制的属性隐私保护和高效的数据访问；文献 [14, 15, 35] 支持细粒度访问控制、权威去中心化、访问控制的属性隐私保护，但不支持高效的数据访问；文献 [18] 支持细粒度访问控制、权威去中心化、高效的数据访问，但不支持访问控制的属性隐私保护；本方案支持细粒度访问控制、权威去中心化、访问控制的属性隐私保护和高效的数据访问。

表 1　基于多权威的属性基的方案对比

方案	功能			
	细粒度访问控制	权威去中心化	属性隐私保护	高效数据访问
文献[11]	√	×	×	×
文献[12-13, 16-17, 19]	√	√	×	×
文献[14-15, 35]	√	√	√	×
文献[18]	√	√	×	√
本方案	√	√	√	√

4.2　计算和存储开销理论分析

由于文献 [14, 15, 35] 与本方案大部分的功能实现相类似，因此本部分仅将文献 [14, 15, 35] 与本方案进行理论开销对比分析。表 2 展示了多权威去中心化属性隐藏的属性基方案的各算法计算开销对比。m，n分别代表权威机构的个数和用户属性的个数；e_0，e_1分别表示在群G_1，G_T中一个指数运算的执行时间，p指的是一个对运算的执行时间。$|G_1|$和$|G_T|$分别代表G_1和G_T中元素的长度。

从表 2 可以得知，在以上所有多权威去中心化属性隐藏的属性基方案中，每一个权威机构参数建立算（AuthSetup）的计算开销都与系统中用户的属性个数相关；用户私钥生成算法（KeyGen）的计算开销与用户属性的个数和权威机构的个数有关；加密算法（Encryption）的计算开销与权威机构个数和属性个数都相关；在解密算法（Decryption）的计算开销方面，只有本方案能够实现高效的解密，即其开销与用户的属性个数和权威机构的个数无关。此外，可以很明显观察到在密钥生成和解密方面，本方案相较于其他方案计算开销最低。

表 2　相关方案各算法计算开销对比

算法方案	AuthSetup	KeyGen	Encryption	Decryption
文献[14]	$2ne_0$	$4mne_0$	$(mn+n+1)e_0+n(p+e_1)$	$(mn+n+1)p+mne_0$
文献[15]	$2ne_0+n(p+e_1)$	$8mne_0$	$(mn+n)p+(2n+mn+1)e_0$	$(3n+2mn)p$
文献[18]	$2ne_0$	$4mne_0$	$m(4n+2)e_0+2mp$	$p+e_0$
文献[35]	$(2n+5)e_0+n(p+e_1)$	$5mne_0$	$(m+1)p+(3m+3mn+1)e_0$	$(2mn+2m+1)p+mne_0$
本方案	$n(n+2)e_0+n(n+1)(p+e_1)$	mne_0	$2n(n+1)e_0+n(n+1)(p+e_1)$	e_0

从表 3 中可以得知，在以上方案中，存储权威机构生成的公开参数开销与属性个数和权威机构的个数呈正相关；存储用户私钥的开销同样与属性个数和权威机构的个数相关；文献 [14-15, 35] 存储密文的开销与属性个数和权威机构的个数相关，而本方案的密文存储开销仅与属性个数相关。此外，很容易从表 3 观察到本方案用户私钥和密文的存储开销相较于其他方案的存储较低。

表 3 相关方案参数存储开销对比

算法方案	|PK|	|UK|	|CT|
[14]	$m(n+1)\|G_1\|+m\|G_T\|$	$2mn\|G_1\|$	$m(n+2)\|G_1\|+\|G_T\|$
[15]	$2m\|G_1\|+nm\|G_T\|$	$m(3n+2)G_1\|$	$nm\|G_1\|+(mn+2)\|G_T\|$
[18]	$(n+2)m\|G_1\|$	$2mn\|G_1\|$	$(4mn+2m)\|G_1\|+\|G_T\|$
[35]	$(2m+5)\|G_1\|+m\|G_T\|$	$(3m+mn)\|G_1\|$	$(2mn+2m+1)\|G_1\|+\|G_T\|$
本方案	$2nm(n+1)\|G_1\|+nm(n+1)\|G_T\|$	$mn\|G_1\|$	$n(n+1)\|G_1\|+\|G_T\|$

综上所述，本方案在密钥生成和解密的计算开销相较于其他两个方案明显较低。在存储用户私钥和密文的开销方面，本方案相较于其他方案同样明显较低。

4.3 实验分析

由于本方案使用基于属性向量和访问向量来实现策略隐藏，而文献 [14-15] 方案都是基于线性秘密共享矩阵或访问树的访问结构实现访问策略隐藏。通过以上理论分析可以发现，本方案在计算效率和存储效率存在一定的优势。因此，本部分主要对属性个数和权威机构个数对本方案的各算法计算性能进行评估。本方案在 64 bit 的 Ubuntu 118.04.6 LTS 版本中安装 python 3.5 的运行环境，使用的是 Charm-Crypto 0.43 的 PBC 安装包[35]，本实验是基于 512 位基本字段的对称曲线 SS512。电脑硬件的配置如下: Intel Core i9-9900K CPU@3.60GHz*16，Graphics: GetForce RTX 2 070 Super/PCIe/SSE2，32 GB 内存。

图 2 表示的是当权威机构的个数固定为 5 时，本方案中相应算法运算时间随着属性向量的长度的变化。图 3 表示的是属性向量的长度固定为 5 时，本方案中相应算法运算时间随着权威机构的个数的变化。从图 2 中可以看出，当权威机构的个数固定时，本方案的 AuthSetup，Encryption 和 KeyGen 算法的计算时间随着属性向量的长度呈线性关系，而 Decryption 算法的计算时间与属性向量的长度无关。

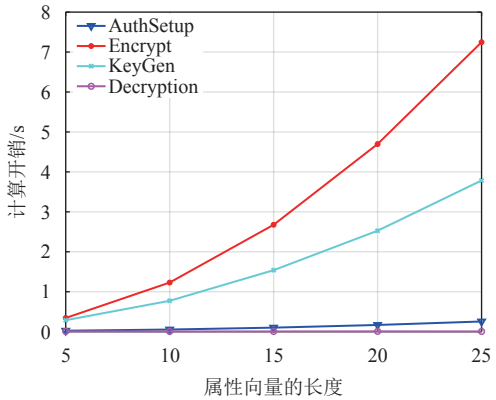

图 2 各算法随属性向量长度变化的计算开销

从图 3 中可以看出，当属性向量的长度固定时，本方案的 Encryption 和 KeyGen 算法的计算时间随着权威机构的个数呈线性关系，而 AuthSetup 和 Decryption 算法的计算时间与属性向量的长度无关。

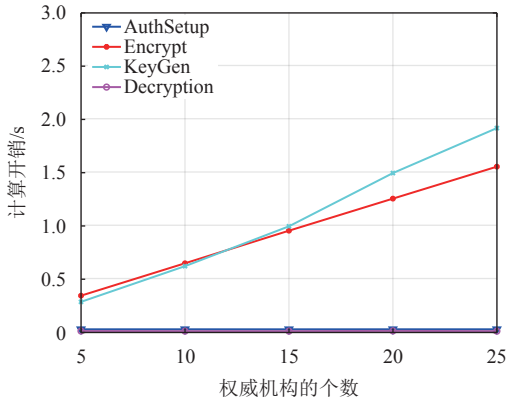

图 3 各算法随权威机构个数变化的计算开销

综上所知，本方案的解密计算开销基本保持恒定，表明本方案能够使移动用户在资源受限的条件下依然可以高效访问密文数据。

5 结 束 语

本文针对移动群智场景中数据共享过程存在安全、隐私和效率的问题，提出了一个基于属性隐藏的高效去中心化的移动群智数据共享方案。本方案能够实现细粒度的授权访问、访问控制的隐私保护、权威去中心化以及高效数据访问。并通过严格的安全性分析和性能分析，证明了本方案在应用到移动群智数据共享场景中的安全性、高效性和可行性。本方案访问控制的表达性较弱，即仅支持与门的访问控制的向量转化。未来工作将基于本方案进行扩展，设计出支持可搜索、可撤销的方案。

参 考 文 献

[1] 熊金波, 毕仁万, 田有亮, 等. 移动群智感知安全与隐私: 模型、进展与趋势[J]. 计算机学报, 2021, 44(9): 1949-1966.
XIONG J B, BI R W, TIAN Y L, et al. Security and privacy

in mobile crowdsening: Models, progress and trends[J]. Chinese Journal of Computers, 2021, 44(9): 1949-1966.

[2] 黄大欣, 甘庆晴, 王晓明, 等. 群智感知网络环境下的一种高效安全数据聚合方案[J]. 密码学报, 2021, 8(5): 868-880.
HUANG D X, GAN Q Q, WANG X M, et al. An efficient secure data aggregation in mobile crowdsening networks[J]. Journal of Cryptologic Research, 2021, 8(5): 868-880.

[3] WANG L, ZHANG D, WANG Y, et al. Sparse mobile crowdsensing: Challenges and opportunities[J]. IEEE Communications Magazine, 2016, 54(7): 161-167.

[4] 王涛春, 金鑫, 吕成梅, 等. 移动群智感知中融合数据的隐私保护方法[J]. 计算机研究与发展, 2020, 57(11): 2337-2347.
WANG T C, JIN X, LYU C M, et al. Privacy-preseving data aggregation method in mobile crowdsensing[J]. Journal of Computer Research and Development, 2020, 57(11): 2337-2347.

[5] 唐裕彪. 物联网时代移动群智感知技术中的安全问题浅析[J]. 数字通信世界, 2021(11): 41-42.
TANG Y B. Analysis of security issues in mobile crowdsensing technology in the internet of things era[J]. Digital Communication World, 2021(11): 41-42.

[6] NGUYEN T N, ZEADALLY S. Mobile crowd-sensing applications: Data redundancies, challenges, and solutions[J]. ACM Transactions on Internet Technology (TOIT), 2021, 22(2): 1-15.

[7] DING X, LVY R, PANG X, et al. Privacy-preserving task allocation for edge computing-based mobile crowdsensing[J]. Computers & Electrical Engineering, 2021, 97(22): 107528.

[8] CAPPONI A, FIANDRINO C, KANTARCI B, et al. A survey on mobile crowdsensing systems: Challenges, solutions, and opportunities[J]. IEEE Communications Surveys & Tutorials, 2019, 21(3): 2419-2465.

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

[10] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//Proceedings of the 13th ACM Conference on Computer and Communications Security. [S.l.]: ACM, 2006: 89-98.

[11] CHASE M. Multi-authority attribute-based encryption [C]//Theory of Cryptography Conference. Berlin, Heidelberg: Springer, 2007: 515-534.

[12] LIN H, CAO Z, LIANG X, et al. Secure threshold multi authority attribute-based encryption without a central authority[C]//International Conference on Cryptology in India. [S. l.]: Springer, 2008: 426-436.

[13] LEWKO A, WATERS B. Decentralizing attribute-based encryption[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer, 2011: 568-588.

[14] HAN J, SUSILO W, MU Y, et al. Privacy-preserving decentralized key-policy attribute-based encryption[J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(11): 2150-2162.

[15] QIAN H, LI J, ZHANG Y. Privacy-preserving decentralized ciphertext-policy attribute-based encryption with fully hidden access structure[C]//International Conference on Information and Communications Security. Cham: Springer, 2013: 363-372.

[16] RUJ S, STOJMENOVIC M, NAYAK A. Decentralized access control with anonymous authentication of data stored in clouds[J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 25(2): 384-394.

[17] ZHANG L, GAO X, KANG L, et al. Distributed ciphertext-policy attribute-based encryption with enhanced collusion resilience and privacy preservation[J]. IEEE Systems Journal, 2021, DOI: 10.1109/JSYST.2021.3072793.

[18] YE Y, ZHANG L, YOU W, et al. Secure decentralized access control policy for data sharing in smart grid[C]//IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). [S.l.]: IEEE, 2021: 1-6.

[19] CHASE M, CHOW S S M. Improving privacy and security in multi-authority attribute-based encryption [C]//Proceedings of the 16th ACM Conference on Computer and Communications Security. [S. l.]: ACM, 2009: 121-130.

[20] NISHIDE T, YONEYAMA K, OHTA K. ABE with partially hidden encryptor-specified access structure [C]//International Conference on Applied Cryptography and Network Security. Berlin, Heidelberg: Springer, 2008: 21-29.

[21] RAO Y S, DUTTA R. Recipient anonymous ciphertext-policy attribute-based encryption[C]//International Conference on Information Systems Security. Berlin, Heidelberg: Springer, 2013: 329-344.

[22] LAI J, DENG R H, LI Y. Fully secure cipertext-policy hiding CP-ABE[C]//International Conference on Information Security Practice and Experience. Berlin, Heidelberg: Springer, 2011: 24-39.

[23] ZHANG Y, CHEN X, 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. [S. l.]: ACM, 2013: 511-516.

[24] HUR J. Attribute-based secure data sharing with hidden policies in smart grid[J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 24(11): 2171-2180.

[25] ZHOU Z, HUANG D, WANG Z. Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption[J]. IEEE Transactions on Computers, 2013, 64(1): 126-138.

[26] ZHANG Y, ZHENG D, DENG R H. Security and privacy in smart health: Efficient policy-hiding attribute-based access control[J]. IEEE Internet of Things Journal, 2018, 5(3): 2130-2145.

[27] GREEN M, HOHENBERGER S, WATERS B. Outsourcing the decryption of ABE ciphertexts[C]// USENIX Security Symposium. San Francisco: USENIX Association, 2011: 1-16.

[28] ZHOU Z, HUANG D. Efficient and secure data storage operations for mobile cloud computing[C]//8th International Conference on Network and Service Management (CNSM) and 2012 Workshop on Systems Virtualiztion Management (SVM). [S.l.]: IEEE, 2012: 37-45.

[29] LI J, JIA C, LI J, et al. Outsourcing encryption of attribute-based encryption with mapreduce[C]// International Conference on Information and Communications Security. [S.l.]: Springer, 2012: 191-201.

[30] LAI J, DENG R H, GUAN C, et al. Attribute-based encryption with verifiable outsourced decryption[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(8): 1343-1354.

[31] QIN B, DENG R H, LIU S, et al. Attribute-based encryption with efficient verifiable outsourced decryption[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(7): 1384-1393.

[32] LIN S, ZHANG R, MA H, et al. Revisiting attribute-based encryption with verifiable outsourced decryption[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(10): 2119-2130.

[33] MAO X, LAI J, MEI Q, et al. Generic and efficient constructions of attribute-based encryption with verifiable outsourced decryption[J]. IEEE Transactions on Dependable and Secure Computing, 2015, 13(5): 533-546.

[34] WANG H, HE D, SHEN J, et al. Verifiable outsourced ciphertext-policy attribute-based encryption in cloud computing[J]. Soft Computing, 2017, 21(24): 7325-7335.

[35] ZHANG L, GAO X, KANG L, et al. Distributed ciphertext-policy attribute-based encryption with enhanced collusion resilience and privacy preservation[J]. IEEE Systems Journal, 2021, 16(1): 735-746.

编 辑 叶 芳