基于云边计算的车联网数据双边访问控制方案

张嘉伟[1]，赵一帆[1]，杨颜博[2]，姜奇[1]，李腾[1]，李兴华[1]，马建峰[1]
（1.西安电子科技大学网络与信息安全学院，陕西 西安 710071；2.内蒙古科技大学信息工程学院，内蒙古 包头 014040）

摘　要：针对车联网中共享数据面临的机密性与完整性破坏等安全威胁问题，提出了面向车路云数据共享场景的免密钥托管且支持动态完整性验证的分布式可信数据双边访问控制方案。该方案设计了一种分布式多机构密钥生成机制，以实现车路云环境中分布式车载单元的密钥生成，同时避免了密钥托管问题。进一步地，基于路侧单元实现分布式可信密钥策略属性基加密，对分布式数据使用者进行细粒度访问控制，同时结合匹配加密确保数据来源的匹配性和真实性。此外，利用双线性映射累加器技术实现动态车联网共享数据的完整性验证。严格的形式化安全分析表明，该方案可以满足威胁模型的安全要求，大量的仿真实验证明了方案的高效性和实用性。

关键词：车路云；车联网；属性基加密；匹配加密；动态数据完整性验证
中图分类号：TP309
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025183

Cloud-edge computing based dual access control scheme for IoV data

ZHANG Jiawei[1], ZHAO Yifan[1], YANG Yanbo[2], JIANG Qi[1], LI Teng[1], LI Xinghua[1], MA Jianfeng[1]
1. School of Cyber Engineering, Xidian University, Xi'an 710071, China
2. School of Information Engineering, Inner Mongolia University of Science & Technology, Baotou 014040, China

Abstract: To address the security threats to confidentiality and integrity of shared data in the Internet of vehicles (IoV), a distributed dual access control scheme with key escrow-free and dynamic data integrity verification for vehicle-road-cloud data sharing scenarios was proposed. This scheme designed a distributed multi-organization key generation mechanism to enable key generation for distributed on-board units in the vehicle-road-cloud environment while avoiding key escrow issues. Furthermore, distributed trusted key policy attribute-based encryption was implemented based on roadside units, providing fine-grained access control for distributed data users. Matching encryption was also used to ensure data source matching and authenticity. Furthermore, a bilinear map accumulator technique was used to verify the integrity of dynamic IoV shared data. A rigorous formal security analysis demonstrates that the scheme meets the security requirements of the threat model, and extensive simulation experiments demonstrate its efficiency and practicality.

Keywords: vehicle-road-cloud, Internet of vehicles, attribute-based encryption, matchmaking encryption, dynamic data integrity verification

收稿日期：2025–06–06；**修回日期：**2025–10–09
通信作者：赵一帆，25151111369@stu.xidian.edu.cn
基金项目：国家自然科学基金资助项目（No.U24A20243）；陕西省自然科学基础研究计划资助项目（No.2024JC-YBMS-544）；中央高校基本科研业务费专项资金资助项目（No.ZYTS25066）；国家重点研发计划基金资助项目（No.2023YFB3106902）
Foundation Items: The National Natural Science Foundation of China (No.U24A20243), The Natural Science Basic Research Program of Shaanxi (No.2024JC-YBMS-544), The Fundamental Research Funds for the Central Universities (No.ZYTS25066), The National Key Research and Development Program of China (No.2023YFB3106902)

0 引言

人工智能和自动驾驶技术使得智能网联车的发展迎来了新的机遇，5G网络和物联网（IoT, Internet of things）的普及促进了车车互联技术、汽车与基础设施互联技术和云边协同技术不断增强[1]。车联网（IoV, Internet of vehicles）应用领域日益扩大，进一步推动了车路云一体化系统（VRCIS, vehicle-road-cloud integration system）建设，云平台对资源受限的车载单元（OBU, on-board unit）和路侧单元（RSU, roadside unit）实时收集的海量异构数据进行存储和整合分析，通过分布式的RSU以及无处不在的开放式移动通信网络向车辆终端提供实时服务[2-4]。但是云端共享数据很容易被来自开放网络的恶意用户进行非法访问[5-7]，从而破坏车辆和交通数据的机密性和完整性，甚至造成用户隐私信息泄露、交通管控服务不可用等严重后果[8-9]。因此，有效的访问控制技术成为VRCIS中数据共享安全的基石。

目前，学术界和工业界已经提出大量解决方案来实现对共享数据的访问控制。强制访问控制和基于角色的访问控制等方案能够确保只有授权实体才能访问机密数据，但是无法适用于分布式场景中的细粒度访问控制。Sahai等[10]提出了属性基加密（ABE, attribute-based encryption）以实现面向大规模用户的数据细粒度访问控制，文献[10-11]使用ABE技术保护了分布式应用场景中的数据机密性。但在分布式的VRCIS中，RSU节点容易受到来自攻击者的渗透或腐化，导致存储在其中的敏感数据被窃取以及访问控制元数据被破坏，存在隐私泄露、访问控制不可信等问题。此外，考虑到车辆的快速移动导致所属区域变化，其进行交互的RSU也会随之改变，而分布式的RSU节点间可能由于操作顺序不同或更新不及时，导致状态一致性难以保证。因此，实现分布式RSU的可信环境对车辆数据的完整性和可用性至关重要。

为了实现分布式环境下的可信访问控制，区块链技术被广泛应用于IoV领域。文献[12]分析了在IoV区块链应用中因本地数据受篡改而带来的安全威胁，并提出了一种基于混合RSU分层架构的攻击检测和恢复方法。文献[13]将区块链与车载边缘计算网络相结合，提出了一种创新共识机制，优化了交通数据的可信分布式存储与传输。但这些方案依赖于完全可信的中央机构（CA, central authority），存在CA负担过大、响应时间慢、单点失效等问题。为了解决这些问题，文献[14-15]分别利用代理机构（PA, proxy authority）和分布式RSU分担CA管理用户访问权限的负担。然而，上述方案无法在实现分布式可信访问控制的同时避免密钥生成与管理中密钥托管等问题。因此，如何在开放式VRCIS中提供可信细粒度访问控制的同时实现免密钥托管的分布式密钥生成机制成为一个挑战性的问题。

此外，云端外包存储和共享的数据来自网络不同区域中的不同终端，其真实性、正确性和可靠性会对数据使用者的服务质量带来重大影响。因此，对于云端共享数据的真实性和匹配性鉴别是保障服务质量的一个必要手段。为了对数据拥有者提供的云端共享数据的来源进行认证并鉴别其与数据使用者的数据请求是否相符，文献[16]通过结合密钥策略的属性基加密（KP-ABE, key-policy attribute-based encryption）与匹配加密[17]技术，在边缘计算环境中同时实现了对数据拥有者和数据使用者的双边访问控制。进一步，云控平台也可能出于故障或利益等原因擅自删除或更改存储的共享数据，因此对云端数据的完整性验证成为保障共享数据质量的另一个必要手段。考虑到在实际场景中，RSU和OBU动态地将数据上传至云控平台进行存储，而相关方案[18-19]并不能实现动态的分布式共享场景下的数据完整性验证。因此，如何在VRCIS中对数据拥有者的云端共享数据进行真实性和正确性匹配鉴别的同时实现动态数据的完整性验证，是另一个挑战性问题。

为了应对上述挑战，本文提出了面向车路云数据共享场景的免密钥托管且支持动态完整性验证的分布式可信数据双边访问控制方案（KEF-DVDA, distributed dual access control scheme with key escrow-free and dynamic data integrity verification）。本文方案在多机构密钥策略属性基加密（MA-KP-ABE, multi-authority key-policy attribute-based encryption）和匹配加密的基础上，创新性地结合了区块链和智能合约技术，实现了可信的分布式双边访问控制。具体而言，在VRCIS中，本文方案分别对数据使用者和数据拥有者的云端共享数据实现细粒度的分布式可信访问控制和匹配性鉴别。同时，本文方案还支持动态数据的完整性验证，并通过去中心化的密钥生成与管理机制，有效解决了传统方案中存在的密钥托管和单点失效问题。这一设

计提升了车路云架构开放网络环境的安全性和可靠性，并为分布式环境下的数据共享与访问控制提供了高效的解决方案。本文的主要贡献如下。

1) 可信分布式双边访问控制。针对RSU节点的分布式和易受攻击等特性，创新性地引入区块链和智能合约技术，设计了分布式可信数据匹配和策略匹配机制。该机制通过RSU构建区块链，分布式账本和智能合约的自动化执行确保了数据访问过程的透明性与可信性，同时确保数据拥有者云端共享数据的来源真实性，从而实现了高效且安全的分布式数据可信访问控制。利用MA-KP-ABE技术，对数据使用者实现灵活高效的细粒度访问控制，同时结合匹配加密技术，对云端数据来源进行真实性和匹配性鉴别。

2) 动态数据完整性验证。利用双线性映射累加器技术，结合智能合约，确保云服务器按照数据拥有者的需求对外包存储的共享数据进行正确的修改操作，实现动态数据完整性。

3) 分布式密钥管理机制。为了避免集中式密钥生成机制的单点失效问题，结合去中心化技术，引入各区域的PA，用户密钥由用户、用户所属区域PA和CA共同参与计算生成。利用致盲因子解决密钥托管问题，在分布式的VRCIS环境中实现了高效的免密钥托管的密钥生成机制。

4) 安全性和实用性。严格的形式化安全分析证明了本文方案可以抵抗威胁模型中各种攻击，大量的实验仿真和性能分析证明了本文方案的高效性和实用性。

1　预备知识

表1给出了本文中常用的符号。

表1　常用符号

参数	含义
Ω_{snd}	该区域内数据拥有者（DO, data owner）的属性全集
Ω_{rcv}	该区域内数据使用者（DU, data user）的属性全集
S	DO的属性集合
R	DO指定的能够对密文进行解密的用户的属性集合
$\mathbb{S}$	DU指定的想要接收的数据来源的属性策略
$\mathbb{R}$	DO的属性策略
acc_{B}	原始数据经过加密和哈希等操作后进行累加得到的累加值
$\text{aux}_1,\text{aux}_2$	DO发送给RSU的辅助验证值，发送给CSP的辅助验证值

令$\mathbb{G}$和$\mathbb{G}_T$为2个素数p阶循环乘法群，$\mathbb{Z}_p$为以p为模的有限域，g为$\mathbb{G}$的一个生成元。

1.1　双线性映射和困难性假设

定义1　双线性映射。如果$e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$是一个具有以下特性的映射，则称$e$为一个双线性映射。

1) 双线性：对于任意$a,b\in\mathbb{Z}_p$，有$e\left(g^a,g^b\right)=e\left(g,g\right)^{ab}$。

2) 非退化性：$e\left(g,g\right)\neq 1$。

3) 可计算：对于任意$g_1,g_2\in\mathbb{G}$，能够高效计算$e\left(g_1,g_2\right)$。

定义2　判定性双线性Diffie-Hellman假设（DBDH, decisional bilinear Diffie-Hellman assumption）。令$a,b,c,z\in\mathbb{Z}_p$，没有概率多项式时间算法$\mathcal{A}$可以大于可忽略不计的优势区分元组$\left(A=g^a,B=g^b,C=g^c,D=e\left(g,g\right)^{abc}\right)$和元组$\left(A=g^a,B=g^b,C=g^c,Z=e\left(g,g\right)^{z}\right)$。

定义3　计算双线性Diffie-Hellman假设（CBDH, computational bilinear Diffie-Hellman assumption）。令$a,b,c,z\in\mathbb{Z}_p$，没有概率多项式时间算法$\mathcal{A}$可以从元组$\left(A=g^a,B=g^b,C=g^c\right)$中以大于可忽略不计的优势计算出$e\left(g,g\right)^{abc}$。

定义4　q阶强Diffie-Hellman假设（q-SDH, q-strong Diffie-Hellman assumption）。令$a,\tau\in\mathbb{Z}_p$，对于任意概率多项式时间的算法$\mathcal{A}$，有

$$\Pr\left[\mathcal{A}\left(g,g^a,g^{a^2},\cdots,g^{a^q}\right)=\left(\tau,g^{\frac{1}{(a+\tau)}}\right)\right]\leqslant\varepsilon$$

其中，概率仅取决于g和a的随机选取，ε可忽略不计。

1.2　线性秘密共享方案

定义5　线性秘密共享方案（LSSS，linear secret sharing scheme）。一个在一组群体$\mathcal{P}$中进行的秘密共享方案π如果满足以下性质，则称其在$\mathbb{Z}_p$中是线性的。

1) 每一个群体的共享值构成了$\mathbb{Z}_p$上的一个向量。

2) 存在一个被称作π的生成矩阵的m行d列的矩阵$\boldsymbol{M}$。对于$i=1,\cdots,m$，$\boldsymbol{M}$的第i行被标记为群

体$\boldsymbol{\rho}(\boldsymbol{i})$，其中$\boldsymbol{\rho}$是从$\{1,2,\cdots,m\}$到$\mathcal{P}$的一个映射。给出一个列向量$\boldsymbol{v}=\left(s,r_2,\cdots,r_d\right)^{\mathrm{T}}$，其中$s\in\mathbb{Z}_p$是被共享的秘密值，$r_2,\cdots,r_d\in\mathbb{Z}_p$是被随机选择的值。$\boldsymbol{M}\cdot\boldsymbol{v}$是根据$\pi$生成的秘密值$s$的$m$个分享。群体$\boldsymbol{\rho}(\boldsymbol{i})$拥有的共享值为$\boldsymbol{\lambda}_i=(\boldsymbol{Mv})_i$，即$\boldsymbol{M}$的第$i$行$\boldsymbol{M}_i$与向量$\boldsymbol{v}$的内积。

1.3　双线性映射累加器技术

加密累加器是一种动态累加器方案，将有限集$X=\{x_1,\cdots,x_n\}$中的所有元素累加至合约值acc_X，对于X中的任意元素x_i，能够高效地计算出x_i在acc_X中的成员证明wit_{x_i}，验证方通过将x_i的成员证明wit_{x_i}作双线性映射变换从而验证有限集X的完整性。双线性映射累加器技术的安全性基于q-SDH假设，方案流程如下。

令s为$\mathbb{Z}_p^*$中一个随机选取的元素，集合X的累加值为

$$\mathrm{acc}_X=g^{\prod_{x\in X}(x+s)}$$

其中，$\prod_{x\in X}(x+s)$为X的特征多项式。元素x_i的成员证明值可以构造为

$$\mathrm{wit}_{x_i}=\mathrm{acc}_X^{(x_i+s)^{-1}}$$

若等式

$$e\left(\mathrm{acc}_X,g\right)=e\left(\mathrm{wit}_{x_i},g^{x_i}g^s\right)$$

成立，则证明元素x_i确为集合X中的元素。

1.4　标签索引表

标签索引表（TIT, tag index table）是在映射表的基础上通过特定简化修改得到的。数据拥有者为每块数据生成特定的抗碰撞的标签τ_i，将标签值存储在验证方，后续通过标签值对数据实现动态操作。TIT由2个部分组成：用于快速定位数据块的索引值和每个区块的标签值。对数据完整性进行验证时，验证方通过查找TIT能够快速定位用于挑战的数据块，从而高效地对云服务器的响应进行验证。此外，数据拥有者通过TIT能够快速地对数据进行插入、删除和更新操作。

2　系统定义

2.1　系统架构

KEF-DVDA系统架构如图1所示，包括以下几个实体：CA、PA、云服务器（CSP, cloud service provider）、RSU、DO和DU。

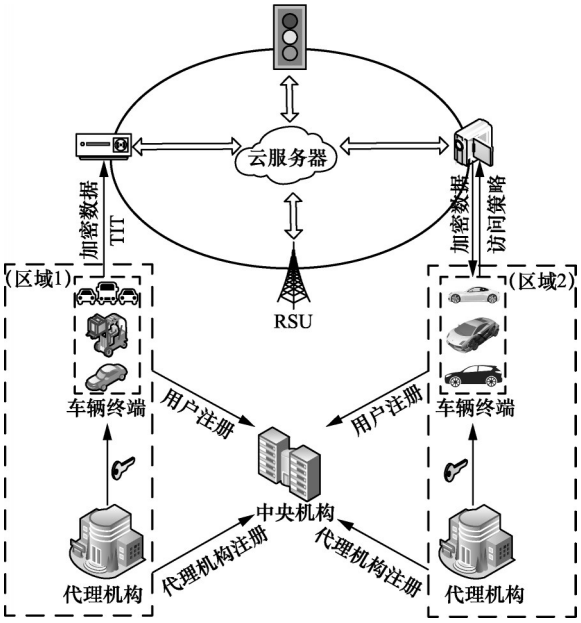


图1　KEF-DVDA系统架构

CA。管理着系统中所有OBU的注册和代理机构的注册信息。

PA。每个区域部署一个PA，向该区域中注册的OBU用户终端分发部分加密密钥和部分解密密钥。

CSP。CSP是拥有大量存储空间的远程服务器，存储RSU发送的长期数据。收到数据拥有者OBU对数据的修改请求后，对相应外包数据进行修改，并接受RSU发送的数据完整性验证请求，向RSU回应相关证明。

RSU。接收数据拥有者OBU上传的数据和相应的TIT，将短期数据进行本地缓存，将长期数据转发至CSP，将TIT本地存储。接收数据使用者OBU发送的请求密文数据的搜索令牌和访问策略，根据部署的智能合约对以密文形式存储的车联网数据进行查找、数据源鉴别和完整性验证，将符合要求且完整的车联网数据发送给数据使用者OBU。在验证数据完整性时，向CSP发送挑战，根据部署的智能合约对CSP返回的证明值进行正确与否的判断。

DO。车联网终端用户，向RSU发送数据和相应的TIT，若想对存储在CSP中的数据进行修改，向CSP发送相应请求，本地更新TIT并发送给RSU。

DU。车联网终端用户，向RSU发送请求的密文数据的搜索令牌和指定的访问策略，得到返回的

密文数据后，若该DU的属性策略与密文中指定的属性相符合，则可以用解密密钥对密文进行解密。

2.2　威胁模型

本文方案中，CA是完全可信的实体，管理系统中所有用户和PA的注册信息，并生成系统参数，作为整个系统的维护者，不会与PA共谋。PA是半可信的，可能会尝试为非授权的用户生成密钥或者自行生成密钥对密文进行解密。CSP和RSU是诚实且好奇的，可能会在执行自身功能时对数据产生好奇，从而对数据进行窃听等。DO和DU是完全不可信的，前者可能假冒成任何非授权的其他用户发送消息，后者可能尝试对任何非授权的信息进行解密，同时用户之间可能共同合作发动共谋攻击。

3　方案构造

3.1　工作流程

算法的流程如图2和图3所示。图2描述了系统初始化阶段CA生成系统公共参数，PA和用户通过CA进行注册，以及CA和PA共同参与计算为用户生成加密密钥与解密密钥。

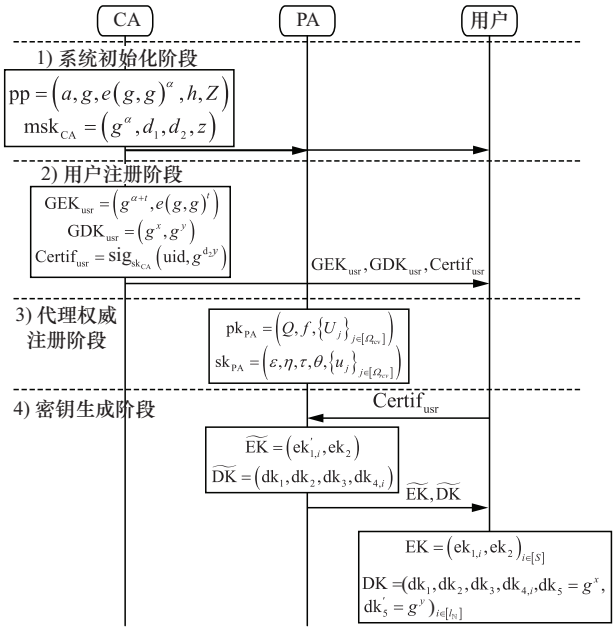


图2　系统初始化至密钥生成流程

图3描述了DO指定DU的属性并加密明文数据，向RSU上传加密后的数据，DU向RSU请求指定访问策略的密文，RSU对密文进行匹配验证和完整性验证，以及DO向CSP发送数据修改操作。

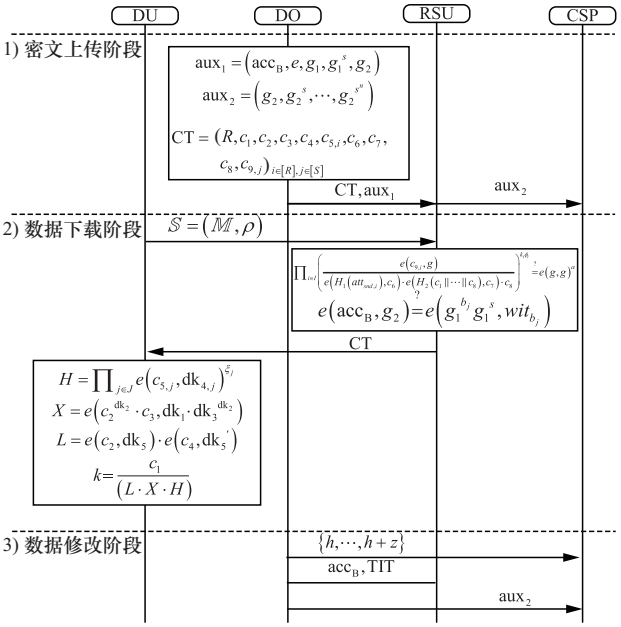


图3　密文上传至数据修改流程

3.2　具体构造

1) 系统初始化阶段

$\mathrm{Setup_{CA}}(1^{\lambda})$：CA运行该算法，运行群生成器$\mathcal{G}$生成双线性群$(p,g,\mathbb{G},\mathbb{G}_T,e)$，随机挑选$a,\alpha,d_1,d_2,z\in\mathbb{Z}_p^*$和2个哈希函数$H_1:\Omega_{\mathrm{snd}}\to\mathbb{G}$,$H_2:\{0,1\}^*\to\mathbb{G}$，计算$h=g^{d_1}$,$Z=e(g,g)^z$。系统公共参数为$\mathrm{pp}=\left(a,g,e(g,g)^{\alpha},h,Z\right)$。

CA将pp发送给系统中其余所有实体。在后面的每一步算法中，都需要输入pp。简化起见，后面每一步算法的输入将不写明pp。CA的私钥为$\mathrm{msk_{CA}}=\left(g^{\alpha},d_1,d_2,z\right)$。

CA挑选用于数字签名的公私钥对$\mathrm{pk_{CA}}$,$\mathrm{sk_{CA}}$，并本地保存。

2) 用户注册阶段

$\mathrm{Reg_{usr}}(\mathrm{uid},\mathrm{msk_{CA}})$：用户向CA提交身份信息uid用于注册，CA为该用户随机挑选$t,x\in\mathbb{Z}_p^*$并计算满足等式(1)的y值。

$$x+\left(d_1+d_2\right)y=z\left(\mathrm{mod}\,p\right)\tag{1}$$

CA计算该用户加密密钥和解密密钥的部件

$$\mathrm{GDK_{usr}}=\left(g^{x},g^{y}\right)$$

$$\mathrm{GEK_{usr}}=\left(g^{\alpha+t},e\left(g,g\right)^{t}\right)$$

CA使用$\mathrm{sk_{CA}}$生成该用户的证书

$$\mathrm{Certif}_{\mathrm{usr}}=\mathrm{Sig}_{\mathrm{sk}_{\mathrm{CA}}}\left(\mathrm{uid},g^{d_2y}\right)$$

CA通过安全信道将$\mathrm{GEK}_{\mathrm{usr}},\mathrm{GDK}_{\mathrm{usr}},\mathrm{Certif}_{\mathrm{usr}}$发送给该用户，并在本地记录元组$\left(\mathrm{uid},\mathrm{GDK}_{\mathrm{usr}}\right)$。

$\mathrm{Setup}_{\mathrm{usr}}(1^{\lambda})$：用户生成用于验证外包数据完整性的元组$\left(p,g_1,g_2,\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T',e\right)$，并随机挑选$s\in\mathbb{Z}_p^*$。

3) 代理机构注册阶段

$\mathrm{Reg}_{\mathrm{PA}}(\mathrm{pid})$：PA向CA提交身份信息pid用于注册，CA通过安全信道将$\mathrm{pk}_{\mathrm{CA}}$发送给PA。

$\mathrm{Setup}_{\mathrm{PA}}(\Omega_{\mathrm{snd}},\Omega_{\mathrm{rcv}})$：PA管理着该区域中的$\Omega_{\mathrm{snd}}$和$\Omega_{\mathrm{rcv}}$。PA随机挑选$\varepsilon,\eta,\tau,\theta\in\mathbb{Z}_p$，计算

$$Q=e\left(g,g\right)^{\varepsilon+\eta},f=g^{\tau}$$

其中，在不同的区域中，ε、η、τ、θ是不同的。对于Ω_{rcv}中每一个元素$\mathrm{att}_{\mathrm{rcv},j}$，$j\in\left[\Omega_{\mathrm{rcv}}\right]$，PA随机挑选$u_j\in\mathbb{Z}_p$并计算$U_j=g^{u_j}$。PA的公私钥为

$$\mathrm{pk}_{\mathrm{PA}}=\left(Q,f,\left\{U_j\right\}_{j\in\left[\Omega_{\mathrm{rcv}}\right]}\right)$$

$$\mathrm{sk}_{\mathrm{PA}}=\left(\varepsilon,\eta,\tau,\theta,\left\{u_j\right\}_{j\in\left[\Omega_{\mathrm{rcv}}\right]}\right)$$

4) 密钥生成阶段

$\mathrm{EKGen}(\mathrm{pk}_{\mathrm{CA}},\mathrm{Certif}_{\mathrm{usr}},S)$：加密密钥的生成分为两步。第一步，用户向所属区域的PA提交$\mathrm{Certif}_{\mathrm{usr}}$申请加密密钥，PA使用$\mathrm{pk}_{\mathrm{CA}}$对该用户的$\mathrm{Certif}_{\mathrm{usr}}$进行验证，并随机挑选$r\in\mathbb{Z}_p$。对于该用户的属性集合$S$中的每一个元素$\mathrm{att}_{\mathrm{snd},i}$，$i\in[S]$，PA计算

$$\mathrm{ek}_{1,i}'=H_1\left(\mathrm{attsnd},i\right)^{r},\mathrm{ek}_2=g^{r}$$

PA将用户的部分加密密钥$\widetilde{\mathrm{EK}}=\left(\mathrm{ek}_{1,\mathrm{i}}',\mathrm{ek}_2\right)$发送给该用户。第二步，用户接收到$\widetilde{\mathrm{EK}}$后，根据从$\mathrm{GEK}_{\mathrm{usr}}$中得到的$g^{\alpha+t}$计算$\mathrm{ek}_{1,i}=g^{\alpha+t}\cdot\mathrm{ek}_{1,i}'$，最终得到完整的加密密钥

$$\mathrm{EK}=\left(\mathrm{ek}_{1,i},\mathrm{ek}_2\right),i\in[S]$$

$\mathrm{DKGen}(\mathrm{pk}_{\mathrm{CA}},\mathrm{sk}_{\mathrm{PA}},\mathrm{Certif}_{\mathrm{usr}},\mathbb{R})$：解密密钥的生成分为2步。第一步，用户向所属区域的PA提交$\mathrm{Certif}_{\mathrm{usr}}$申请解密密钥，PA使用$\mathrm{pk}_{\mathrm{CA}}$验证该用户的$\mathrm{Certif}_{\mathrm{usr}}$并得到$g^{d_2y}$。$\mathbb{R}=(\mathbb{N},\pi)$，其中$\mathbb{N}$是一个$l_{\mathbb{N}}\times n_{\mathbb{N}}$的矩阵，$\pi:\left[l_{\mathbb{N}}\right]\to\Omega_{\mathrm{rcv}}$是一个映射。PA为该用户随机挑选$\sigma,\varpi,v_2,\cdots,v_{n_{\mathbb{N}}}\in\mathbb{Z}_p^*$，构造向量

$$\boldsymbol{v}=\left(\eta-\theta\varpi,v_2,\cdots,v_{n_{\mathbb{N}}}\right)^{\mathrm{T}}\in\mathbb{Z}_p^{n_{\mathbb{N}}}$$

并计算$\varsigma=\mathbb{N}\cdot\boldsymbol{v}$。对于$\mathbb{N}$的每一行$\mathbb{N}_i,i\in\left[l_{\mathbb{N}}\right]$，对应的秘密分享值为$\varsigma_i=\mathbb{N}_i\cdot\boldsymbol{v}$。PA计算部分解密密钥组件

$$\mathrm{dk}_1=g^{\frac{\varepsilon}{\tau+\sigma}}\cdot\left(g^{d_2y}\right)^{\frac{1}{\tau+\sigma}}\cdot\left(g^{\theta-\sigma}\right)^{\frac{\varpi}{\tau+\sigma}}$$

$$\mathrm{dk}_2=\sigma,\mathrm{dk}_3=g^{\frac{\varpi}{\tau+\sigma}}$$

对于$i\in\left[l_{\mathbb{N}}\right],j\in\left[\Omega_{\mathrm{rcv}}\right]$，找到满足$\mathrm{att}_{\mathrm{rcv},i}=\mathrm{att}_{\mathrm{rcv},j}$的$j$，计算

$$\mathrm{dk}_{4,i}=g^{\frac{\varsigma_i}{u_j}}$$

将用户的部分解密密钥$\widetilde{\mathrm{DK}}=(\mathrm{dk}_1,\mathrm{dk}_2,\mathrm{dk}_3,\mathrm{dk}_{4,i})$发送给该用户。第二步，用户接收到$\widetilde{\mathrm{DK}}$后，根据从$\mathrm{GDK}_{\mathrm{usr}}$中得到的$g^x,g^y$，得到完整解密密钥

$$\mathrm{DK}=\left(\mathrm{dk}_1,\mathrm{dk}_2,\mathrm{dk}_3,\mathrm{dk}_{4,i},\mathrm{dk}_5=g^x,\mathrm{dk}_5'=g^y\right)_{i\in\left[l_{\mathbb{N}}\right]}$$

5) 密文上传阶段

$\mathrm{Enc}(M,S,R,\mathrm{pk}_{\mathrm{PA}},\mathrm{EK},\mathrm{GEK}_{\mathrm{usr}})$：DO首先将原始明文数据$M$分为$n$段，每段长$l_1$比特，即$M=\left\{m_1,\cdots,m_n\right\}$。DO随机挑选一个密钥$k\in\mathbb{G}_T$，将每段明文$m_i$，$i\in[n]$对称加密得到$c_i'=E\left(m_i\right)$，计算$o_i=H\left(c_i'\right)$生成对应的标签并在TIT中记录相应的$o_i^s$。DO生成元组$B=\left\{b_1,\cdots,b_n\right\}$，其中$b_i=c_i'\|o_i$。对$B$进行累加得到

$$\mathrm{acc}_{\mathrm{B}}=g_1^{\prod_{i=1}^{n}\left(b_i+s\right)}$$

从而得到元组式(2)用于辅助验证完整性

$$\begin{aligned}\mathrm{aux}_1&=\left(\mathrm{acc}_{\mathrm{B}},e,g_1,g_1^s,g_2\right)\\\mathrm{aux}_2&=\left(g_2,g_2^s,\cdots,g_2^{s^n}\right)\end{aligned}\tag{2}$$

DO的属性集合为S，指定能够对密文解密的用户的属性集合R，随机挑选$\omega\in\mathbb{Z}_p$，计算

$$c_1=k\cdot Z^{\omega}\cdot Q^{\omega},c_2=g^{\omega},c_3=f^{\omega},c_4=h^{\omega}$$

对于$i\in[R],j\in\left[\Omega_{\mathrm{rcv}}\right]$，找到满足$\mathrm{att}_{\mathrm{rcv},i}=\mathrm{att}_{\mathrm{rcv},j}$的$j$，计算$c_{5,i}=U_j^{\omega}$。DO随机挑选$r',\psi\in\mathbb{Z}_p$，计算$c_6=\mathrm{ek}_2\cdot g^{r'},c_7=g^{\psi}$。DO通过解析$\mathrm{GEK}_{\mathrm{usr}}$得到$c_8=e(g,g)^t$，计算

$$c_{9,j}=\mathrm{ek}_{1,j}\cdot H_1\left(\mathrm{att}_{\mathrm{snd},j}\right)^{r'}\cdot H_2\left(c_1\|\cdots\|c_8\right)^{\psi}{}_{j\in[S]}$$

最终DO生成的密文数据为

$$\mathrm{CT}=\left(R,c_1,c_2,c_3,c_4,c_{5,i},c_6,c_7,c_8,c_{9,j}\right)_{i\in[R],j\in[S]}$$

DO将CT、TIT、aux_1发送给RSU，将B、aux_2上传至CSP。

6) 数据下载阶段

VeriDO($\mathbb{S}$,CT)：DU向RSU发送请求的数数据来源的访问策略$\mathbb{S}=(\mathbb{M},\rho)$，其中$\mathbb{M}$是一个$l_{\mathbb{M}}\times n_{\mathbb{M}}$的矩阵，$\rho:\left[l_{\mathbb{M}}\right]\to\Omega_{\mathrm{snd}}$为一个映射。RSU随机挑选$x_2,\cdots,x_{n_{\mathbb{M}}}\in\mathbb{Z}_p^*$，构造向量

$$\boldsymbol{x}=\left(1,x_2,\cdots,x_{n_{\mathbb{M}}}\right)^{\mathrm{T}}\in\mathbb{Z}_p^n$$

并计算$\boldsymbol{k}=\mathbb{M}\cdot\boldsymbol{x}$。对于$\mathbb{M}$的每一行$\mathbb{M}_i,i\in\left[l_{\mathbb{M}}\right]$，对应的秘密分享值为$\boldsymbol{k}_i=\mathbb{M}_i\cdot\boldsymbol{x}$。令$I$为$S$中符合$\mathbb{S}$的属性构成的集合。如果$S$符合$\mathbb{S}$，那么可以找到满足$\sum_{i\in I}\phi_i\mathbb{M}_i=(1,0,\cdots,0)$的$\phi_i$，判断等式(3)是否成立，若成立，则RSU继续对密文进行完整性验证。

$$\prod\nolimits_{i\in I}\left(\frac{e\left(c_{9,i},g\right)}{e\left(H_1\left(\mathrm{att}_{\mathrm{snd},i}\right),c_6\right)\cdot e\left(H_2\left(c_1\|\cdots\|c_8\right),c_7\right)\cdot c_8}\right)^{k_i\phi_i}=e(g,g)^{\alpha}\tag{3}$$

VeriDT(TIT,aux_1)：该算法由RSU运行。RSU向CSP发送挑战的数据块的索引j，CSP不知道s的值，无法直接计算$\prod_{b\in B\setminus\{bj\}}(b+s)$，只能将其表示为$s$的多项式$\sum_{i=0}^{n-1}a_i\cdot s^i$，其中$\{a_0,\cdots,a_{n-1}\}$为$s$的系数。CSP根据$\mathrm{aux}_2$计算

$$\mathrm{wit}_{b_j}=\prod_{i=0}^{n-1}\left(g_2^{s^i}\right)^{a_i}$$

CSP将$\left(\mathrm{wit}_{b_j},b_j\right)$作为证明值返回给RSU。RSU根据TIT验证元素$b_j$的正确性。验证通过，判断等式(4)是否成立，若成立，RSU将密文发送给DU。

$$e\left(\mathrm{acc}_{\mathrm{B}},g_2\right)=e\left(g_1^{b_j}g_1^{s},\mathrm{wit}_{b_j}\right)\tag{4}$$

Dec(CT,DK)：DU接收到RSU发送的密文CT，并尝试用DK对其解密。令J为R中符合$\mathbb{R}$的元素的集合，如果其属性策略$\mathbb{R}$与密文中嵌入的属性集合R相符，那么可以找到满足$\sum_{j\in J}\xi_j\mathbb{N}_j=(1,0,\cdots,0)$的$\xi_j$。DU计算

$$H=\prod\nolimits_{j\in J}e\left(c_{5,j},\mathrm{dk}_{4,j}\right)^{\xi_j}$$

$$X=e\left(c_2^{\mathrm{dk}_2}\cdot c_3,\mathrm{dk}_1\cdot\mathrm{dk}_3^{\mathrm{dk}_2}\right)$$

$$L=e\left(c_2,\mathrm{dk}_5\right)\cdot e\left(c_4,\mathrm{dk}_5'\right)$$

可得对称密钥$k=\dfrac{c_1}{L\cdot X\cdot H}$。

7) 数据修改阶段

Insert：DO欲插入数据$\{m_h,\cdots,m_{h+z}\}$，首先进行加密并生成标签$\{o_h,\cdots,o_{h+z}\}$以及对应的$\{b_h,\cdots,b_{h+z}\}$。DO向CSP发送数据插入请求

$$\left\{\left(b_h,h\right),\cdots,\left(b_{h+z},h+z\right)\right\}$$

DO更新TIT和$\mathrm{acc}_{\mathrm{B}}$发送给RSU，更新$\mathrm{aux}_2$发送给CSP。

Delete：DO向CSP发送数据删除请求

$$\{h,\cdots,h+z\}$$

CSP在B中进行定位并删除$\{b_h,\cdots,b_{h+z}\}$。DO更新TIT和$\mathrm{acc}_{\mathrm{B}}=\mathrm{acc}_{\mathrm{B}}^{\left(\prod_{i=h}^{h+z}(b_i+s)\right)^{-1}}$发送给RSU，更新$\mathrm{aux}_2$发送给CSP。

Update：DO向CSP发送数据更新请求

$$\left\{\left(b_h',h\right),\cdots,\left(b_{h+z}',h+z\right)\right\}$$

DO更新$\mathrm{acc}_{\mathrm{B}}=\mathrm{acc}_{\mathrm{B}}^{\left(\prod_{i=h}^{h+z}(b_i+s)\right)^{-1}\cdot\prod_{i=h}^{h+z}(b_i'+s)}$并发送给RSU。

3.3　正确性分析

如果S符合$\mathbb{S}$，根据式(5)，密文CT可以通过数据源鉴别

$$\prod\nolimits_{i\in I}\left(\frac{e\left(c_{9,i},g\right)}{e\left(H_1\left(\mathrm{att}_{\mathrm{snd},i}\right),c_6\right)\cdot e\left(H_2\left(c_1\|\cdots\|c_8\right),c_7\right)\cdot c_8}0\right)^{k_i\phi_i}=\prod\nolimits_{i\in I}\left(\frac{e\left(g^{\alpha+t},g\right)}{e\left(g,g\right)^{t}}\right)^{k_i\phi_i}=e\left(g,g\right)^{\alpha}\tag{5}$$

如果R符合$\mathbb{R}$，根据式(6)~式(9)，DO可以成功对密文CT进行解密。

$$H=\prod\nolimits_{j\in J}e\left(c_{5,j},\mathrm{dk}_{4,j}\right)^{\xi_j}=\prod\nolimits_{j\in J}e\left(g^{u_j\omega},g^{\frac{\varsigma_j}{u_j}}\right)^{\xi_j}=e\left(g,g\right)^{\omega\sum_{j\in J}\varsigma_j\xi_j}=e\left(g,g\right)^{\omega(\eta-\theta\varpi)}\tag{6}$$

$$X = e\left(c_2^{\mathrm{dk}_2} \cdot c_3, \mathrm{dk}_1 \cdot \mathrm{dk}_3^{\mathrm{dk}_2}\right) =$$

$$e\left(g^{\omega\sigma} \cdot g^{\tau\omega}, g^{\frac{\varepsilon}{\tau+\sigma}} \cdot \left(g^{d_2 y}\right)^{\frac{1}{\tau+\sigma}} \cdot \left(g^{\theta-\sigma}\right)^{\frac{\varpi}{\tau+\sigma}} \cdot g^{\frac{\varpi\sigma}{\tau+\sigma}}\right) =$$

$$e\left(g^{\omega\sigma+\varpi}, g^{\frac{\varepsilon+d_2 y+\theta\varpi}{\tau+\sigma}}\right) \tag{7}$$

$$L = e\left(c_2, \mathrm{dk}_5\right) \cdot e\left(c_4, \mathrm{dk}_5'\right) = e\left(g,g\right)^{\omega\left(x+d_1 y\right)} \tag{8}$$

$$\frac{c_1}{L \cdot X \cdot H} = \frac{k \cdot e\left(g,g\right)^{z\omega} \cdot e\left(g,g\right)^{\omega(\varepsilon+\eta)}}{e\left(g,g\right)^{\omega\left(\eta+\varepsilon+x+\left(d_1+d_2\right)y\right)}} = k \tag{9}$$

4　安全分析

4.1　安全模型

定义6　选择明文攻击下的不可区分性（IND-CPA, indistinguishability under chosen-plaintext attack）。如果对于任何概率多项式时间的敌手$\mathcal{A}$，优势

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{IND\text{-}CPA}}\left(1^{\lambda}\right) = \left| \Pr\left[\mathrm{Exp}_{\mathcal{A}}^{\mathrm{IND\text{-}CPA}}\left(1^{\lambda}\right)=1\right] - \frac{1}{2} \right|$$

都是可忽略的，那么称方案是IND-CPA安全的。其中，$\mathrm{Exp}_{\mathcal{A}}^{\mathrm{IND\text{-}CPA}}\left(1^{\lambda}\right)$的具体描述为

$\mathrm{Exp}_{\mathcal{A}}^{\mathrm{IND\text{-}CPA}}(1^{\lambda})$
$R^* \leftarrow \mathcal{A}(1^{\lambda})$
$(\mathrm{pp}, \mathrm{msk}_{\mathrm{CA}}) \leftarrow \mathrm{Setup}_{\mathrm{CA}}(1^{\lambda})$
$(\mathrm{pk}_{\mathrm{PA}}, \mathrm{sk}_{\mathrm{PA}}) \leftarrow \mathrm{Setup}_{\mathrm{PA}}(\Omega_{\mathrm{snd}}, \Omega_{\mathrm{rev}})$
$b \in \{0,1\}$
$(m_0, m_1, S_0, S_1,) \leftarrow \mathcal{A}(\mathrm{pp})$
$\mathrm{ek} \leftarrow \mathrm{EKGen}(\mathrm{pk}_{\mathrm{CA}}, S_b)$
$c \leftarrow \mathrm{Enc}(m_b, S, R^*, \mathrm{ek})$
$b' \leftarrow \mathcal{A}(c)$
return 1 if $b = b'$ and $R^* \neq \mathbb{R}$

IND-CPA安全模型考虑以下攻击。

1) 共谋攻击：$\mathcal{A}$能够请求得到任意加密密钥，从而可以作为一个加密者群体发动共谋攻击，如将多个加密者的属性组合成一个具有未授权属性集合的加密者发送密文；$\mathcal{A}$能够请求得到除可解密c外的任意解密密钥，从而发动一个除属性策略为$\mathbb{R}$在内的解密者外的解密者群体的共谋攻击。

2) 窃听攻击：$\mathcal{A}$输出两则消息m_0和m_1。在挑战环节，根据b的值选择加密m_0或m_1。在猜测阶段，$\mathcal{A}$输出b'，表示被加密的消息为$m_{b'}$。若$b' = b$，则$\mathcal{A}$赢得游戏。如果$\mathcal{A}$能够成功发动窃听攻击，则$\mathcal{A}$赢得游戏的概率应大于$\frac{1}{2}$（随机猜测的概率）。

定义7　选择明文攻击下的存在性不可伪造（EU-CMA, existential unforgeability against chosen-message attack）。如果对于任何概率多项式时间的敌手$\mathcal{A}$，优势

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{EU\text{-}CMA}}\left(1^{\lambda}\right) = \Pr\left[\mathrm{Exp}_{\mathcal{A}}^{\mathrm{EU\text{-}CMA}}\left(1^{\lambda}\right)=1\right]$$

都是可忽略的，那么称方案是EU-CMA安全的。其中，$\mathrm{Exp}_{\mathcal{A}}^{\mathrm{EU\text{-}CMA}}\left(1^{\lambda}\right)$的具体描述为

$\mathrm{Exp}_{\mathcal{A}}^{\mathrm{IND\text{-}CPA}}(1^{\lambda})$
$\mathbb{S}^* \leftarrow \mathcal{A}(1^{\lambda})$
$(\mathrm{pp}, \mathrm{msk}_{\mathrm{CA}}) \leftarrow \mathrm{Setup}_{\mathrm{CA}}(1^{\lambda})$
$(\mathrm{pk}_{\mathrm{PA}}, \mathrm{sk}_{\mathrm{PA}}) \leftarrow \mathrm{Setup}_{\mathrm{PA}}(\Omega_{\mathrm{snd}}, \Omega_{\mathrm{rev}})$
$\mathrm{ek} \leftarrow \mathrm{EKGen}(\mathrm{pk}_{\mathrm{CA}}, S)$
$c^* \leftarrow \mathcal{A}(\mathrm{pp})$
return 1 if $\mathrm{VeriDO}(\mathbb{S}^*, c) = 1$ and
$S \neq \mathbb{S}^*$ and $c^* \neq c$

EU-CMA安全模型考虑以下攻击。

1) 假冒攻击：$\mathcal{A}$可以通过请求加密密钥获得除了属性符合$\mathbb{S}^*$的加密者的信息。$\mathcal{A}$能够通过请求获得密文。若$\mathcal{A}$能够对密文进行修改，当对修改后的密文c进行关于来源是否符合$\mathbb{S}^*$的检验通过时，$\mathcal{A}$赢得游戏。若$\mathcal{A}$能够成功发动假冒攻击，$\mathcal{A}$赢得游戏的概率应不可被忽略。

2) 共谋攻击：$\mathcal{A}$能够请求得到任何解密密钥，可作为解密者群体发动共谋攻击；$\mathcal{A}$能够请求除了生成密文c的任意加密密钥，从而可作为除了属性符合$\mathbb{S}^*$的加密者在内的加密者群体发动共谋攻击。

4.2　安全性分析

1) 分布式密钥分发的安全性

PA无法独自对密文进行解密。PA能够根据CT得到g^{ω}，但是根据离散对数问题可知，PA无法计算ω，从而无法计算致盲因子Q^{ω}。此外，由于

$$Z^{\omega} = e\left(g,g\right)^{z\omega} = e\left(g,g\right)^{(x+(d_1+d_2)y)\omega} =$$

$$e\left(g,g\right)^{x\omega} \cdot e\left(g,g\right)^{d_1 y\omega} \cdot e\left(g,g\right)^{d_2 y\omega}$$

若PA想要计算出Z^{ω}，首先需要获得g^x和g^y。然而，上述值由CA生成并通过安全信道发送给用户，而在威胁模型中已经说明CA不会参与PA的共谋。因此，PA无法获得该致盲因子。类似地，PA无法独自生成完整的解密密钥。

2) 双边访问控制的安全性

定理 1　如果 DBDH 成立，那么所有概率多项式时间的敌手打破本文方案的 IND-CPA 安全性的概率都是可忽略不计的。

定理 2　如果 CBDH 成立，那么所有概率多项式时间的敌手打破本文方案的 EU-CMA 安全性的概率都是可忽略不计的。

定理 3　如果本文方案同时是 IND-CPA 安全的以及 EU-CMA 安全的，那么本文方案可以抵抗下述攻击。

窃听攻击：CSP、RSU 和 PA 因为没有任何解密密钥，所以无法对获得到的密文进行分析。拥有合法解密密钥但是属性策略与密文中指定的属性不相符的解密者群体会尝试将各自拥有的解密密钥组合起来，以尝试得到能够对密文进行正确解密的解密密钥。但是每位用户的解密密钥在生成时都引入了一个独特的共享秘密值，因此将不同用户的密钥进行组合得到的至少具有 2 种秘密值，生成的是无效的解密密钥，无法正确对密文解密（同理可知，本文方案同时能够抵抗解密者群体发动的共谋攻击）。

假冒攻击：CSP、RSU 和 PA 因为没有任何加密密钥，所以无法生成并发送合法且有效的密文数据。拥有加密密钥的加密者群体会组合起来假冒成一位未授权的用户发送消息。但是每位用户的加密密钥在生成时都引入了一个独特的共享秘密值，因此将不同用户的密钥进行组合得到的至少具有 2 种秘密值，生成的是无效的加密密钥，无法生成有效的密文（同理，本文方案抵抗加密者群体的共谋攻击）。此外，本文方案中抗碰撞的哈希函数的使用使得对密文的篡改几乎不可能实现。因此，密文被修改后，将不会通过 RSU 的检验环节。

5　性能分析

表 2 将本文方案与文献[16]提出的匹配属性基加密方案（MABE, matchmaking attribute-based encryption）、文献[20]提出的隐藏密文和属性的可信访问控制方案（TrustAccess, trustworthy secure ciphertext-policy and attribute hiding access control scheme）、文献[21]提出的用于车内终端设备端到端安全保护的实用且安全的车载通信协议（PS-E2EID, practical and secure vehicular communication protocol for E2E security to in-vehicle end-devices）、文献[22]出的高效可验证的恒定密文大小细粒度双向访问控制方案（EVBAC, efficient and verifiable fine-grained bilateral access control scheme with constant-size ciphertext）的实现功能进行了比较。其中 $\mathcal{F}_1$、$\mathcal{F}_2$、$\mathcal{F}_3$、$\mathcal{F}_4$ 分别代表了双边访问控制功能、动态数据完整性功能、分布式可信访问控制和分布式密钥生成功能，符号“√”“×”分别代表了方案是否实现了相应功能。文献[16]实现了在云雾数据共享系统中对数据的细粒度双边访问控制，文献[20]利用区块链技术将访问策略嵌入密文数据中，并对存储地址进行加密，文献[21]在车联网环境中基于 ABE 提供策略保护的访问控制其中，结合基于身份的签名实现消息源认证，文献[22]利用门限 ABE 实现云雾计算中的双边访问控制，并使用签名技术对外包数据的机密性和真实性进行了验证。本文方案实现了更综合的功能，在分布式的车路云环境中实现可信的数据细粒度双边访问控制，同时提供高效的动态完整性验证功能。可以看出，本文方案能够创新性地实现分布式环境下的可信双边访问控制，同时实现动态数据完整性验证功能，并且具有较高的安全性。

表 2　　**功能对比**

方案	$\mathcal{F}_1$	$\mathcal{F}_2$	$\mathcal{F}_3$	$\mathcal{F}_4$	安全性
文献[16]	√	×	×	×	IND-CPA
文献[20]	×	×	√	×	CPA
文献[21]	×	√	×	×	IND-CPA
文献[22]	√	×	×	×	CCA
本文方案	√	√	√	√	IND-CPA

5.1　理论分析

表 3 将本文方案与文献[16,20-22]方案就各阶段算法所需计算复杂度和生成的各参数的存储复杂度进行了比较。其中 U 代表了属性全集，表示 Threshold ABE 的门限值。在密钥生成阶段，本文方案需要分别处理数据拥有者属性以及数据使用者属性策略对应的密钥组件，因此计算复杂度分别与上述 2 种属性数量有关。本文方案在加密阶段需要同时生成与数据拥有者属性 S 和指定能够对密文进行解密的属性 R 相关的密文组件，因此计算开销略高于文献[21-22]。文献[16]不需要实现对密文来源

表3 计算复杂度和存储复杂度对比

方案	计算复杂度							存储复杂度			
	Setup	EKGen	DKGen	Enc	Veri_{DO}	Veri_{DT}	Dec	pp	EK	DK	CT
文献[16]	$\mathcal{O}(1)$	$\mathcal{O}(S)$	$\mathcal{O}(\mathbb{R})$	$\mathcal{O}(R+S)$	$\mathcal{O}(\mathbb{S})$	—	$\mathcal{O}(\mathbb{R})$	$\mathcal{O}(1)$	$\mathcal{O}(S)$	$\mathcal{O}(\mathbb{R})$	$\mathcal{O}(R+S)$
文献[20]	$\mathcal{O}(1)$	—	$\mathcal{O}(\mathbb{R})$	$\mathcal{O}(\mathbb{R})$	—	—	$\mathcal{O}(\mathbb{R})$	$\mathcal{O}(1)$	—	$\mathcal{O}(\mathbb{R})$	$\mathcal{O}(1)$
文献[21]	$\mathcal{O}(1)$	—	$\mathcal{O}(R)$	$\mathcal{O}(\Omega_{\text{snd}})$	—	$\mathcal{O}(1)$	$\mathcal{O}(\Omega_{\text{rcv}})$	$\mathcal{O}(U)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(U)$
文献[22]	$\mathcal{O}(U)$	$\mathcal{O}(U)$	$\mathcal{O}(U)$	$\mathcal{O}(S)$	$\mathcal{O}(t^2+S)$	—	$\mathcal{O}(R)$	$\mathcal{O}(U)$	$\mathcal{O}(S)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$
本文方案	$\mathcal{O}(1)$	$\mathcal{O}(S)$	$\mathcal{O}(\mathbb{R})$	$\mathcal{O}(R+S)$	$\mathcal{O}(\mathbb{S})$	$\mathcal{O}(n)$	$\mathcal{O}(\mathbb{R})$	$\mathcal{O}(1)$	$\mathcal{O}(S)$	$\mathcal{O}(\mathbb{R})$	$\mathcal{O}(R+S)$

真实性的鉴别，只需要计算与DU属性策略相关的密文组件。在数据完整性验证阶段，本文方案中CSP在产生证明时需计算除挑战数据块之外的数据块的累加值，因此该算法的计算复杂度应与相应数据规模有关。而文献[21]利用了数字签名技术来实现数据完整性验证，其计算复杂度与属性数量或消息规模无关。但是使用数字签名的方案需要为用户实时生成并分发用于签名的公私密钥，这将会带来额外的存储开销。在计算密文时，本文方案和文献[16]需要计算DO拥有的属性和DO指定的属性有关的密文部件，以实现双边访问控制功能。而文献[20]则将DU属性策略有关的密文部件全部进行计算，因此生成的密文存储开销与方案中属性参数大小无关。

5.2 实验环境与参数配置

本文方案的实验使用Java语言实现了加密和解密功能，使用jPBC的开发包[23]实现双线性群的各种操作。仿真实验使用一台装有Windows10操作系统且内存为16 GB处理器为4核Intel i5-1035G1的主机作为云服务器，以及2台内存为4 GB的4核Ubuntu20.04虚拟机作为边缘节点。同时，基于geth1.10.8在2个边缘节点之间搭建了多级多节点的以太坊私有链[24]。在仿真实验中，把本文方案与文献[17,20-22]进行了原型实现，并将其在算法运行时间、参数规模等方面进行比较分析，取算法运行100次的平均值作为实验结果。

5.3 实验结果及对比分析

图4描述了本文方案和文献[16,20-22]在不同属性全集大小下的系统公共参数规模对比。可以看到，方案中的公共参数规模与属性全集的变化无关。本文方案为了避免分布式密钥生成带来的密钥托管问题，CA需生成一个致盲因子d_1并在公共参数中计算$h=g^{d_1}$。此外，DO将指定的能对密文解密的属性嵌入密文中实现对共享数据的访问控制，RSU通过密文中嵌入的DO的属性集合进行数据源的匹配鉴别并利用元数据对数据完整性进行验证。因此，本文方案需额外产生用于数据源鉴别和用于动态数据完整性验证的参数。此外，RSU对元数据acc_{B}和TIT变更的记录也会带来额外一定的存储开销。综上所述，本文方案的公共参数规模相较于文献[16,20]略高，但是仍在合理范围内。为了提高加密阶段的计算效率，文献[21-22]对系统中的每个属性预计算生成对应的属性密钥部件，其公共参数规模与属性全集的变化呈正相关。

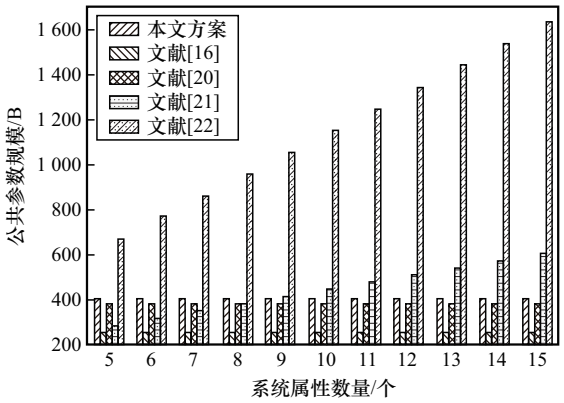


图4 公共参数规模对比

对于本文方案和文献[16,20-22]中密文所需的存储开销，图5进行了具体的描述。当DO的属性集合增大时，本文方案和文献[16,21]的密文规模增大；而当DO的属性集合大小相同时，本文方案密文规模略大于文献[16,21]。相较于文献[16]，本文方案的加密密钥中包含为解决密钥托管问题而产生的致盲因子$h=g^{d_1}$和$f=g^{r}$，计算密文时将生成对应的密文组件，这会带来额外的密文存储开销。但理论和实验证明，该存储开销非常微小。此外，文

献[21]只需要对每个属性计算对应群元素并且访问策略被隐藏在这些元素中，因此最终密文开销略低于本文方案。而文献[22]利用多项式插值和双线性群指数聚合技术将访问策略压缩为单一的密文元素，使该方案具有恒定且较小的密文存储开销。但这无法实现精确的属性与策略匹配，并且需要较高的公共参数开销以支持后续的聚计算。

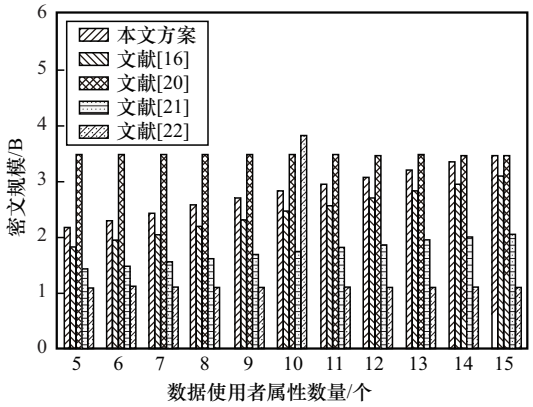


图5　密文规模对比

图6和图7分别描述了本文方案与文献[16,21-22]的加密密钥和解密密钥的规模。本文方案加密密钥规模与DO属性规模呈正相关。文献[21]在生成加密密钥时引入了求和操作，将加密密钥的存储开销压缩至恒定值，以此解决传统ABE访问控制方案中存在的密钥与属性绑定所带来的性能瓶颈。但是这将产生额外的计算开销。本文方案解密密钥规模与DU属性规模呈正相关。与文献[16]相比，R中每增加一个元素，本文方案解密密钥只需计算一个$g^{\frac{\zeta_i}{u_i}}$组件，解密密钥存储开销增加相对缓慢。

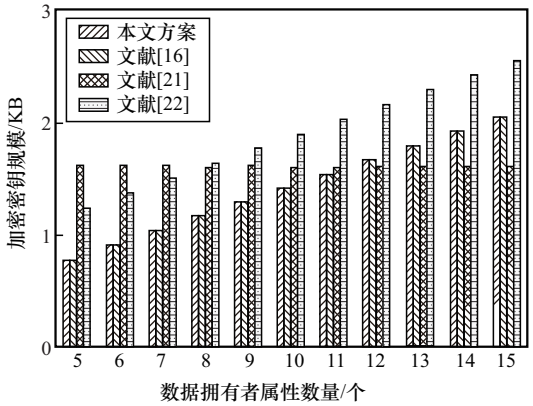


图6　加密密钥规模对比

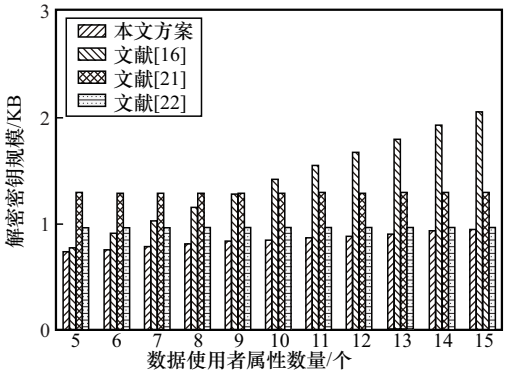


图7　解密密钥规模对比

方案加密所用时间和解密所用时间皆随着DO属性策略增大而增加，如图8和图9所示。其中，文献[20]在加密时只需考虑$\mathbb{R}$的规模，而本文方案和文献[16]在处理$\mathbb{R}$相关密文部件时还需考虑S中属性的相关密文部件，以实现后续对密文数据源的鉴别。随着属性数量的增大，文中方案的解密时间代价为38~105 ms，文献[16]的解密时间代价为88~443 ms。文献[20]需要根据埃尔伽莫加密算法的同乘性核实DU发送的属性集合从而实现细粒度的访问控制。文献[21]通过将部分解密计算外包至安全代理（SA, security agent）执行，一定程度上降低了加解密阶段的时延。但是这完全依赖SA的安全性，若SA返回错误的计算结果将导致密文无效。若在此基础上引入用于验证外包计算结果的机制，将增加系统复杂性。在DO的属性集合S大小相同的情况下，本文方案对密文CT进行数据源鉴别所用的时间几乎与文献[16]所用的时间相同。当S属性数量在25个以内时，该算法运行时间维持在460 ms以内，如图10所示。文献[22]在初始化阶段为每个属性生成了对应的验证部件，在数据源鉴别阶段利用相应部件计算，时间开销较低。

本文方案在密钥存储开销和计算效率方面均表现出显著优势。与文献[16,20-22]相比，本文方案通过引入致盲因子有效解决了密钥托管问题，同时实现了数据源鉴别和完整性验证功能。实验结果表明，本文方案的公共参数规模不受属性全集大小影响，在属性数量低于一定值时密文存储开销优于文献[20]，且解密效率较文献[16,21]提升较多。特别地，本文方案在系统用户属性25个以内的运行时间始终控制在460 ms以下，在保证安全性的同时兼顾了系统性能，为动态环境下的车联网中分布式数据安全共享提供了高效解决方案。

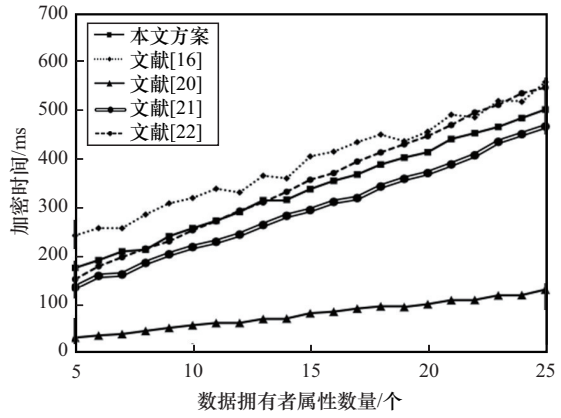


图8　加密时间对比

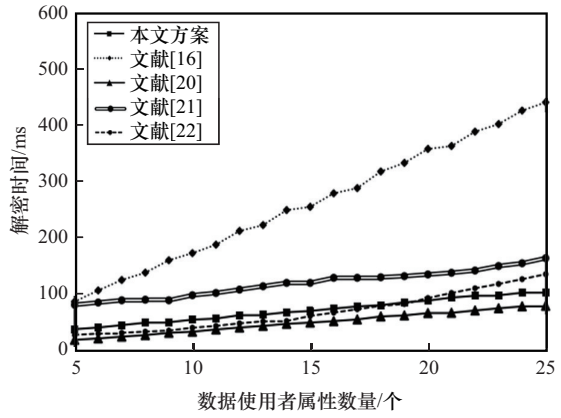


图9　解密时间对比

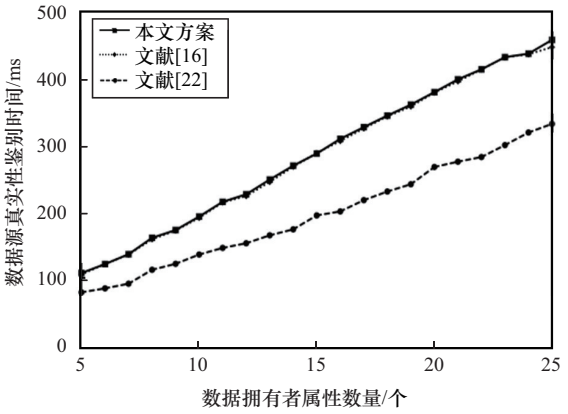


图10　数据源真实性鉴别时间

6　场景部署

为了验证本文方案的实用性，根据实际应用时的常用配置，设定DO的属性集合大小$|S|=10$，DO指定的能够对密文进行解密的DU的属性集合大小$|R|=10$，DU指定的想要接收的数据来源的属性策略复杂度为15，DO的属性策略复杂度为15。在测试平台上，分别运行文献[16,20-22]方案和本文方案中的数据加密、数据源真实性鉴别和数据解密算法100次取其算术平均值，得到表4中的实际性能测试结果。

表4　实际性能测试结果对比

方案	Enc/ms	Dec/ms	Veri_{DO}/ms
文献[16]	407.66	319.51	343.3
文献[20]	81.39	61.12	—
文献[21]	296.96	131.21	—
文献[22]	359.65	80.11	230.80
本文方案	339.55	81.20	344.45

7　结束语

本文针对车路云环境中的数据共享安全问题提出了一种面向车路云数据共享场景的免密钥托管且支持动态完整性验证的分布式可信数据双边访问控制方案，该方案使用属性基加密对数据使用者进行细粒度访问控制，同时基于匹配加密对数据源的真实性进行鉴别。在此基础上，引入双线性映射累加器技术实现动态数据的完整性验证，基于区块链的不可篡改性实现安全的分布式存取，同时构建可信中央机构与代理机构的密钥生成中心以实现免密钥托管的密钥分发。本文方案通过将数据源真实性鉴别和动态数据完整性验证功能外包至边缘节点，减轻了用户本地计算负担。但是车联网环境中用户的属性和访问策略需要频繁更新，而当前方案并未着重考虑对动态策略的实现。在后续工作中我们将进一步考虑跨域、动态操作等工作，以应对车联网复杂动态环境下的安全挑战。

参考文献：

[1] CLANCY J, MULLINS D, DEEGAN B, et al. Wireless access for V2X communications: research, challenges and opportunities[J]. IEEE Communications Surveys & Tutorials, 2024, 26(3): 2082-2119.

[2] GAO B L, LIU J X, ZOU H D, et al. Vehicle-road-cloud collaborative perception framework and key technologies: a review[J]. IEEE Transactions on Intelligent Transportation Systems, 2024, 25(12): 19295-19318.

[3] CHEN X H, YANG A J, TONG Y, et al. A multisignature-based secure and OBU-friendly emergency reporting scheme in VANET[J]. IEEE Internet of Things Journal, 2022, 9(22): 23130-23141.

[4] 周浩, 马建峰, 刘志全, 等. 车联网中区块链辅助的紧急消息信任评估方案[J]. 西安电子科技大学学报, 2023, 50(4): 148-156.
ZHOU H, MA J F, LIU Z Q, et al. Blockchain-assisted solution for emergency message trust evaluation in the VANET[J]. Journal of Xidian

University, 2023, 50(4): 148-156.

[5] 范其纲, 蒋忠元, 李兴华, 马建峰. 基于序参量的云边端分布式体系协同安全评估[J]. 网络与信息安全学报, 2024, 10(3):38-51.
FAN Q G, JIANG Z Y, LI X H, MA J F. Collaborative security assessment of cloud-edge-device distributed systems based on order parameters[J]. Chinese Journal of Network and Information Security, 2024, 10(3):38-51.

[6] GU H X, ZHAO L Q, HAN Z, et al. AI-enhanced cloud-edge-terminal collaborative network: survey, applications, and future directions[J]. IEEE Communications Surveys & Tutorials, 2024, 26(2): 1322-1385.

[7] KAR B, YAHYA W, LIN Y D, et al. Offloading using traditional optimization and machine learning in federated cloud – edge – fog systems: a survey[J]. IEEE Communications Surveys & Tutorials, 2023, 25(2): 1199-1226.

[8] 杨颜博, 张嘉伟, 马建峰. 一种使用区块链保护车联网数据隐私的方法[J]. 西安电子科技大学学报(自然科学版), 2021, 48(3): 21-30.
YANG Y B, ZHANG J W, MA J F. Blockchain-based privacy preserving distributed data sharing in Internet of Vehicles[J]. Journal of Xidian University, 2021, 48(3): 21-30.

[9] LIU H, HAN D Z, LI D. Fabric-iot: a blockchain-based access control system in IoT[J]. IEEE Access, 2020, 8: 18207-18218.

[10] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//Advances in Cryptology – EUROCRYPT 2005. Berlin, Heidelberg: Springer, 2005: 457-473.

[11] LUO F C, WANG H Y, YAN X F, 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.

[12] SHRUTI, RANI S, SRIVASTAVA G. Secure hierarchical fog computing-based architecture for industry 5.0 using an attribute-based encryption scheme[J]. Expert Systems with Applications, 2024, 235: 121180.

[13] GAO Z, ZHANG D B, ZHANG J Z, et al. World state attack to blockchain based IoV and efficient protection with hybrid RSUs architecture[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(9): 9952-9965.

[14] HE X, LI L X, PENG H P. A key escrow-free KP-ABE scheme and its application in standalone authentication in IoT[J]. IEEE Internet of Things Journal, 2024, 11(7): 11381-11394.

[15] YANG Q, ZHU X Q, WANG X L, et al. A novel authentication and key agreement scheme for Internet of Vehicles[J]. Future Generation Computer Systems, 2023, 145: 415-428.

[16] XU S M, NING J T, LI Y J, et al. Match in my way: fine-grained bilateral access control for secure cloud-fog computing[J]. IEEE Transactions on Dependable and Secure Computing, 2020: 1.

[17] ATENIESE G, FRANCATI D, NUÑEZ D, et al. Match me if you can: matchmaking encryption and its applications[J]. Journal of Cryptology, 2021, 34(3): 16.

[18] YAZID M, FAHMI F, SUTANTO E, et al. Simple authentication method for vehicle monitoring IoT device with verifiable data integrity[J]. IEEE Internet of Things Journal, 2023, 10(8): 7027-7037.

[19] TONG W, CHEN W J, JIANG B B, et al. Privacy-preserving data integrity verification for secure mobile edge storage[J]. IEEE Transactions on Mobile Computing, 2023, 22(9): 5463-5478.

[20] GAO S, PIAO G R, ZHU J M, et al. TrustAccess: a trustworthy secure ciphertext-policy and attribute hiding access control scheme based on blockchain[J]. IEEE Transactions on Vehicular Technology, 2020, 69(6): 5784-5798.

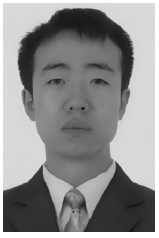
[21] YU D, LEE S, HSU R H, et al. Ensuring end-to-end security with fine-grained access control for connected and autonomous vehicles[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 6962-6977.

[22] YAO M T, HUANG J J, WENG J, et al. Efficient and verifiable bilateral fine-grained access control for cloud-edge IoT healthcare[J]. IEEE Internet of Things Journal, 2025, 12(20): 43181-43194.

[23] ANGELO D C, VINCENZO I. jPBC: Java pairing cryptography[C]// Proceeding of the 2011 IEEE Symposium on Computers and Communications. Piscataway: IEEE Press, 2011: 850-855.

[24] BUTERIN VITALIK. A next-generation smart contract and decentralized application platform[R]. 2014.

[作者简介]



张嘉伟（1985– ），男，山西太原人，博士，西安电子科技大学讲师、硕士生导师，主要研究方向为数据安全、网络安全、云计算安全和区块链等。

赵一帆（2002– ），女，山东青岛人，西安电子科技大学博士生，主要研究方向为应用密码学。

杨颜博（1983– ），男，内蒙古包头人，博士，内蒙古科技大学讲师、硕士生导师，主要研究方向为大数据、人工智能算法的理论与应用、网络编码理论与应用。

姜奇（1983– ），男，安徽全椒人，博士，西安电子科技大学教授，主要研究方向为安全协议分析、无线网络安全。

李腾（1991– ），男，陕西西安人，博士，西安电子科技大学教授，主要研究方向为网络安全、系统日志分析、攻击检测、数据安全和隐私保护。

李兴华（1978– ），男，河南南阳人，博士，西安电子科技大学教授，主要研究方向为隐私保护、网络与信息安全。

马建峰（1963– ），男，陕西西安人，博士，西安电子科技大学教授，主要研究方向为网络安全、系统安全、数据安全和无人机安全等。