区块链架构下高效的车联网跨域数据安全共享研究

刘雪娇[1]，曹天聪[1]，夏莹杰[2,3]

（1. 杭州师范大学信息科学与技术学院，浙江 杭州 311121；2. 浙江大学计算机科学与技术学院，浙江 杭州 310027；
3. 浙江大学台州研究院，浙江 台州 318000）

摘 要：为了解决车联网环境下跨信任域数据共享中跨域数据泄露严重、跨域共享不可控、跨域访问效率低的问题，提出了一种区块链架构下高效的车联网跨域数据安全共享方案。不同信任域的可信机构构成区块链，采用改进的密文策略属性基加密算法加密数据，结合区块链和星际文件系统进行存储，构建了基于区块链的跨域数据细粒度、安全共享方案；设计了基于混淆布隆过滤器的跨域访问验证方法，智能合约基于链上访问策略进行快速的解密测试，提高大量跨域密文的访问效率；设计了基于外包解密的跨域数据获取方法，可信机构为跨域访问请求进行密文转换，并执行包含复杂双线性配对运算的外包解密，减少了车辆在解密过程的时间开销。实验结果表明，所提方案有效提高了跨域密文转换和车辆解密的效率，与现有方案相比，跨域数据访问效率平均提升了 60%。

关键词：车联网；跨域；数据共享；属性基加密；区块链

中图分类号：TN92

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2023031

Research on efficient and secure cross-domain data sharing of IoV under blockchain architecture

LIU Xuejiao[1], CAO Tiancong[1], XIA Yingjie[2,3]

1. School of Information Science and Technology, Hangzhou Normal University, Hangzhou 311121, China
2. College of Computer Science and Technology, Zhejiang University, Hangzhou 310027, China
3. Research Institute of Zhejiang University-Taizhou, Taizhou 318000, China

Abstract: To solve the problems of data disclosure, uncontrolled data access, and inefficiency of cross-domain data sharing in the Internet of vehicles (IoV), an efficient and secure cross-domain data sharing scheme of IoV under blockchain architecture was proposed. A blockchain was maintained by trusted authorities of different trust domains. A modified ciphertext-policy attribute-based encryption scheme was adopted to encrypt data, and encrypted data was stored in interplanetary file system (IPFS) with relevant information recorded on the blockchain, constructing a fine-grained and secure cross-domain data sharing scheme based on blockchain. A verification algorithm for cross-domain access based on the garbled Bloom filter was designed, and a smart contract executed fast decryption tests based on access policies on the blockchain, improving the access efficiency of a mass of ciphertext. A cross-domain data access method based on outsourcing decryption was designed, and the trusted authorities transformed ciphertexts while performing outsourcing decryption with complex bilinear pairing calculations, reducing the time overhead of vehicle decryption. Experiment results show that the proposed scheme is superior to other schemes in the process of cross-domain ciphertext transformation and vehicle decryption, and the cross-domain data access efficiency is increased by 60% on average.

Keywords: IoV, cross-domain, data sharing, attribute-based encryption, blockchain

收稿日期：2022−07−22；**修回日期：**2022−11−14

通信作者：夏莹杰，xiayingjie@zju.edu.cn

基金项目：浙江省自然科学基金资助项目（No.LZ22F030004）；浙江省大学生科技创新活动计划（新苗人才计划）基金资助项目（No.2022R426B067）；杭州师范大学研究生科研创新基金资助项目（No.1115B20500416）

Foundation Items: The Natural Science Foundation of Zhejiang Province (No.LZ22F030004), Zhejiang Students' Technology and Innovation Program (No.2022R426B067), The Postgraduate Research Innovation Promotion of Hangzhou Normal University (No.1115B20500416)

0　引言

车联网（IoV, Internet of vehicles）是一种典型的具有分布式自治域的自组织网络架构[1]，不同区域按照地理位置划分，并由各域可信机构（TA, trusted authority）进行管理，从而形成相互独立的信任域。由于快速移动的车辆频繁跨越不同信任域，车载服务的优化、驾驶体验的改善依赖于不同信任域间的海量数据共享[2-4]，如跨域交通事件、跨域道路状况等。然而，跨信任域的数据共享必然会打破数据管理的安全边界[5]，大量的跨信任域信息交互使高效的跨域数据共享难以实现[6-7]。

车联网环境下，不同信任域之间缺少协同管理，使数据在跨域共享时存在被窃取、篡改和重放等风险[8-9]，同时脱离数据所有者所在域，使数据所有者难以控制其他信任域实体对数据的访问。另一方面，车联网中网络拓扑高度动态、道路交通状况变化频繁，这对车联网跨域数据共享过程的时效性提出了较高的要求。因此，面对车联网大量的跨域数据共享需求，如何进行跨域数据的安全共享，并实现高效的数据获取，是车联网数据共享中具有挑战性的研究工作。

针对以上问题，本文提出了一种区块链架构下高效的车联网跨域数据安全共享方案。为了实现不同信任域数据安全共享，由不同信任域的 TA 构成区块链，采用改进的密文策略属性基加密（CP-ABE, ciphertext-policy attribute-based encryption）算法和对称加密算法，保证跨域数据共享的机密性，结合区块链和星际文件系统（IPFS, interplanetary file system）存储密文数据，基于隐藏的链上访问策略实现细粒度的跨域数据访问控制。为了实现高效的跨域数据访问，设计了基于混淆布隆过滤器（GBF, garbled bloom filter）的跨域访问验证方法，智能合约基于链上访问策略对数据访问请求进行快速解密测试，验证访问者的属性是否满足访问策略，提高大量跨域访问请求下的密文访问效率；设计了基于外包解密的跨域数据获取方法，TA 为跨域访问请求进行密文转换，并执行包含复杂双线性配对的解密运算，减少车辆在解密过程的时间开销。

本文的主要贡献总结如下。

1) 提出了基于区块链的车联网跨域数据安全共享方案，不同信任域的 TA 构成区块链，基于改进的 CP-ABE 算法，将共享数据的访问策略隐藏，存储在区块链上，实现了不同信任域数据安全共享。

2) 设计了基于混淆布隆过滤器的跨域访问验证方法，智能合约基于链上访问策略进行快速解密测试，不需要解密即可安全地验证访问者属性是否满足访问策略，提高了大量跨域密文的访问效率。

3) 设计了基于外包解密的跨域数据获取方法，各域可信机构为跨域访问请求进行密文转换，并执行包含复杂双线性配对的解密运算，减少了车辆在解密过程的时间开销。

1　相关工作

1.1　物联网中的跨域数据共享研究

车联网是物联网（IoT, Internet of things）在汽车行业的应用，车联网中信任域的概念也存在于物联网中，物联网爆发式增长的跨域数据共享需求使跨域数据安全共享成为一个研究重点[10]。物联网中跨域数据安全共享技术可以被概括为基于会话密钥协商和基于代理重加密两类。

在基于会话密钥协商的方法上，文献[11]提出了一种安全无线传感器网络跨域访问机制，利用多层证书授权机构实现不同域间的信任传递，基于 Diffie-Hellman 协议进行密钥协商实现跨域数据安全共享。文献[12]提出了一种基于区块链的工业物联网传感器数据共享机制，基于签名验证实体访问权限后，产生会话密钥对数据资源进行加密，将统一资源定位器（URL, uniform resource locator）上传至区块链实现跨域数据共享。文献[13]提出了一种基于区块链的物联网跨域数据安全共享方案，区块链存储访问策略并做出访问控制决策，使用基于身份的前缀加密为不同访问请求生成会话密钥。基于会话密钥协商的方法能够保证跨域数据的安全性，但协商密钥需要车辆之间进行多次交互，且会话密钥在使用的过程中需要频繁更换，因此难以适用于车联网大量跨域数据共享的场景。

代理重加密技术允许代理机构在不透露数据相关信息的前提下对密文进行转换，因此能够避免共享数据在跨域存储和访问的过程中被泄露或恶意篡改，成为跨信任域的数据安全共享研究重点。文献[14]提出了一种基于区块链的物联网跨域数据共享的方法，使用门限代理重加密的方法对密文进行处理，避免恶意的代理机构与访问者合谋，保证数据在跨域存储、共享过程的安全。文献[15]提出了一种基于区块链和代理重加密的工业物联网数

据共享方案，使用 CP-ABE 算法实现细粒度访问控制，将访问策略存储在区块链上；数据用户请求跨域数据时，云服务器验证用户属性是否满足访问策略，并生成解密参数发送给用户。但代理重加密方法在重加密阶段需要的时间开销较大，难以满足车联网大量数据跨域共享的高效性需求。

1.2 车联网中的跨域数据共享研究

车联网作为物联网的一个分支，存在车辆移动速度快、网络拓扑变化快、消息时效性强等特点。基于会话密钥协商的方法需要在数据拥有者和数据访问者之间建立通信关系，在车联网中，车辆的高速移动性使车辆之间难以维持长期稳定的网络通信。因此在车联网场景下，跨域数据共享研究的重点在于对跨域密文数据的处理方式，即跨域密文转换方法[16]。

文献[2]提出了一个基于区块链的车载社交网络数据共享系统，区块链记录数据哈希值，保证共享数据的不可篡改；通过密钥聚合技术为一组来自不同区域的车辆生成共享密钥。该方案能够实现一对多的数据安全共享，但需要提前确定共享车辆身份，难以实现大范围、细粒度的数据共享。文献[17]提出了一种基于边缘计算的车联网数据共享方案，车辆间通过边缘车辆和云服务器进行交互式认证后，数据共享车辆通过 CP-ABE 对数据进行加密，发送给数据接收车辆，实现数据安全共享；但该方案将车辆作为跨域数据共享的边缘节点，车辆的数据存储能力有限，难以满足大量跨域数据共享的需求。文献[18]提出了一种基于区块链和 CP-ABE 的智能交通数据安全共享方案，TA 构成区块链，并对跨域密文进行代理重加密，实现了跨 TA 域的密文共享。文献[19]提出了一种基于区块链和 CP-ABE 的车联网公告信息共享方案，将密文公告信息存储在区块链上实现跨域传递，区域 TA 对密文数据解密，使用目标域的公开参数对数据进行重新加密，实现跨域数据共享。文献[18-19]分别采用代理重加密、解密后再次加密的跨域密文转换方法，在密文转换阶段均产生了较大的时间开销，难以支持大量跨域数据的高效共享。

上述研究中，文献[17-19]均基于 CP-ABE 保证数据的机密性，实现细粒度的访问控制。然而，CP-ABE 方案的访问策略以明文形式附在数据密文后进行传输，攻击者可以通过访问策略分析数据访问者拥有的属性[20-22]。其次，数据访问者在尝试解密的过程中需要大量的时间开销，随着车联网跨域数据共享需求不断增加，跨域共享的时间开销成为车联网跨域数据共享的瓶颈之一。

2 预备知识

2.1 双线性映射

双线性映射又称双线性配对。令 G 和 G_T 是素数 p 阶乘法循环群，Z_p 是整数模 p 加法群。双线性映射 $e:G\times G\to G_T$ 满足以下性质。

1) 双线性：对于任意的 $a,b\in Z_p$ 和 $g_1,g_2\in G$，都有 $e(g_1^{\,a},g_2^{\,b})=e(g_1,g_2)^{ab}=e(g_1^{\,b},g_2^{\,a})$。

2) 非退化性：存在 $g_1,g_2\in G$，且 $e(g_1,g_2)\neq 1$。

3) 可计算性：对于任意的 $g_1,g_2\in G$，都存在有效的多项式时间算法可以计算 $e(g_1,g_2)\in G_T$。

2.2 线性秘密共享方案

令 $P=\{P_1,P_2,\cdots,P_l\}$ 为一系列参与者的集合，当且仅当满足如下 2 个条件时，P 上的一个秘密共享方案 Π 是线性的。

1) 每个参与者关于秘密值 s 的份额构成 Z_p 上的一个向量。

2) 秘密共享方案 Π 存在一个 l 行 n 列的分享生成矩阵 $\boldsymbol{M}$，$\boldsymbol{\rho}$ 是从 $\{1,2,\cdots,l\}$ 到 P 的映射，$\boldsymbol{M}$ 中的第 i 行 $\boldsymbol{M}_i$ 对应参与者 $\rho(i)$，$i\in[1,l]$。给定一个列向量 $\boldsymbol{v}=(s,y_2,\cdots,y_n)^{\mathrm{T}}\in Z_p^n$，其中 $s\in Z_p$ 为要共享的秘密值，$y_2,\cdots,y_n$ 为 Z_p 上随机选取的值。则向量 $\boldsymbol{Mv}$ 是 Π 的 l 个份额，其中第 i 个份额 $\lambda_i=(\boldsymbol{Mv})_i$ 属于参与者 $\rho(i)$。

线性秘密共享方案（LSSS, linear secret sharing scheme）具有线性重构的特性。假设一个线性秘密共享方案 Π 代表一个访问结构，令 S 为一个授权的属性集合，定义 $I=\{i,\rho(i)\in S\}$，其中 $I\subset\{1,2,\cdots,l\}$，则存在一组常数 $\{w_i\in Z_p\}_{i\in I}$，使 $s=\sum_{i\in I}w_i\lambda_i$，且这些常数能在多项式时间内找到。对于任何非授权的集合，找不到满足条件的一组常数。因此，通过检验等式 $\sum_{i\in I}\boldsymbol{M}_i w_i=(1,0,\cdots,0)$ 是否成立即可验证属性集合是否满足访问策略。若等式成立，说明属性满足访问策略。

2.3 密文策略的属性基加密

文献[23]首次提出密文策略的属性基加密方案，将访问策略嵌入密文，用户属性嵌入密钥，只

有用户属性满足访问策略时，才能正确解密。其主要流程如下。

1) 系统初始化：可信机构输入系统安全参数 λ 和系统属性集合 U，输出系统公钥 PK 和主私钥 MK。

2) 密钥生成：可信机构输入主私钥 MK 和用户属性集合，输出用户私钥 SK。

3) 加密：加密者输入明文 message、系统公钥 PK 和访问策略 $(\boldsymbol{M},\boldsymbol{\rho})$，输出密文 CT。

4) 解密：解密者输入密文 CT 和私钥 SK，输出明文 message。

2.4　布隆过滤器

布隆过滤器于 1970 年由 Bloom 提出，它是由一系列哈希函数和一个二进制向量构成的数据结构，可以用来检查一个元素是否存在于集合中，但存在一定的误识别率。

混淆布隆过滤器由文献[24]提出，它使用 L bit 字符串向量代替布隆过滤器的二进制向量。GBF 算法能有效降低误识别率，因为其不仅取决于哈希函数的碰撞概率，还取决于 L bit 字符串的异或计算结果。

在此基础上，文献[20]提出了一种特殊的布隆过滤器——属性布隆过滤器（ABF, attribute bloom filter）来解决 CP-ABE 方案中访问策略泄露用户属性的问题。ABF 针对基于 LSSS 的访问策略 $(\boldsymbol{M},\boldsymbol{\rho})$ 设计，其中 $\boldsymbol{\rho}$ 将 $\boldsymbol{M}$ 中的每一行映射到每个属性。

ABF 引入一个特定的字符串作为 GBF 的元素，从而在访问控制矩阵中定位到相应行号的属性。ABF 中的元素字符串构造如图 1 所示，L bit 的元素由 2 个固定长度的字符串组成：低位字符串为属性名称，高位字符串为属性对应的矩阵行号。

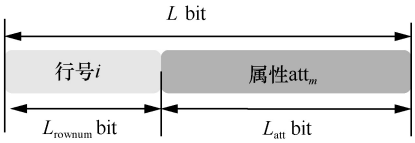

图 1　ABF 中的元素字符串构造

3　本文方案

本节介绍了本文方案的系统模型及其各实体，并给出了本文方案的主要流程。

3.1　系统模型

车联网中不同信任域的车辆密钥和共享数据由其域内 TA 分别管理。为了实现安全的跨域数据共享，本文方案基于 TA 构建区块链，记录各信任域中共享数据的信息，IPFS 分布式地存储密文数据，结合智能合约实现细粒度的跨域访问控制。设计了具有策略隐藏和外包解密的密文策略属性基加密（OD-CP-ABE-HP, outsourcing decryption ciphertext-policy attribute-based encryption hidden policy）方案，数据共享车辆制定访问策略并加密数据，隐藏访问策略中的属性以保护隐私；TA 执行高效的跨域访问验证和跨域密文转换后，数据访问车辆解密并根据区块链上的信息验证数据完整性。

基于区块链的车联网跨域数据共享系统模型如图 2 所示，系统实体包括 TA、区块链、IPFS、路侧单元（RSU, road side unit）和车辆。

1) TA。每个域的 TA 生成和存储系统公共参数，并为其信任域范围内的车辆生成密钥，对数据请求

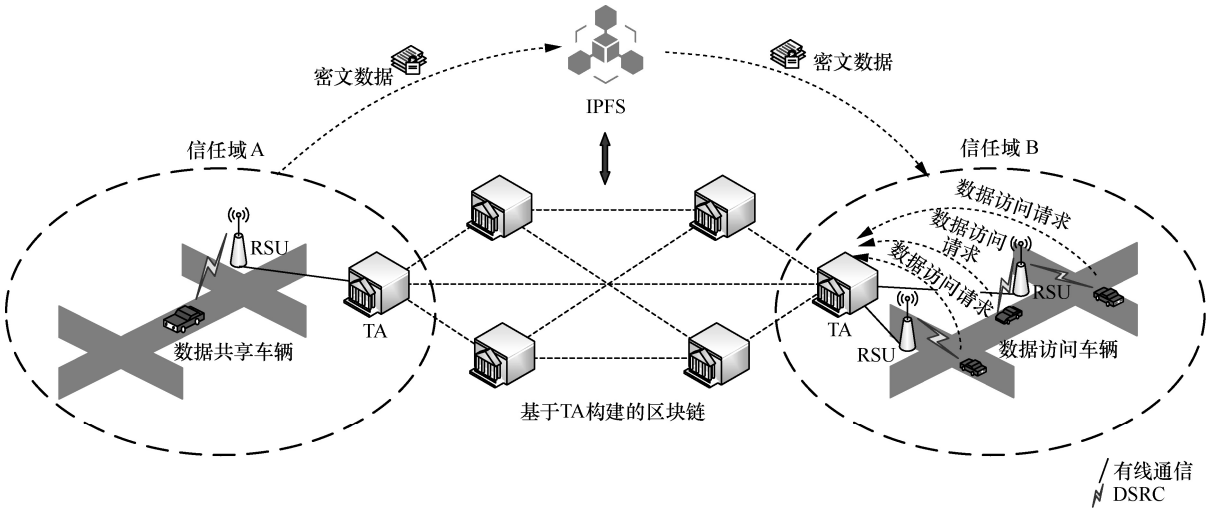

图 2　基于区块链的车联网跨域数据共享系统模型

进行跨域密文转换。

2) 区块链。区块链由所有 TA 共同维护，记录共享数据的相关信息。部署在区块链上的智能合约进行数据查询和跨域访问验证。

3) IPFS。IPFS 分布式地存储加密车联网数据，并将数据的哈希值记录到区块链上作为数据索引。

4) RSU。同一个信任域内的 RSU 由该域的 TA 管理。RSU 使用安全传输协议与 TA 通信；使用专用短程通信（DSRC, dedicated short range communication）协议与车辆通信。RSU 通信范围为 500～1 000 m[25-27]。

5) 车辆。车辆密钥安全存储在车载单元（OBU, on board unit）的防篡改设备（TPD, tamper proof device）中。

3.2 方案流程

基于区块链的车联网跨域数据安全共享流程如图 3 所示，共分为系统初始化、数据加密与访问策略隐藏、跨域访问验证和跨域数据获取 4 个部分。

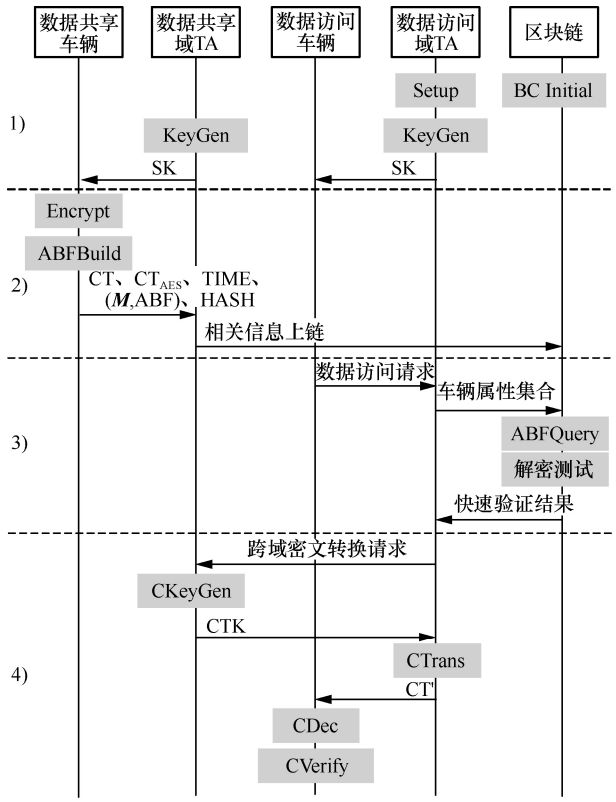

图 3 基于区块链的车联网跨域数据安全共享流程

1) 系统初始化。TA 进行区块链初始化，并执行 Setup 算法进行系统参数初始化。当车辆进入 TA 域范围时，TA 验证车辆 OBU 模块、确定它是有效合法的设备后，获取车辆属性的信息（车辆位置、行驶方向、速度、注册时间等），执行 KeyGen 算法为车辆生成有效私钥，并通过安全信道发送给车辆。

2) 数据加密与访问策略隐藏。数据共享车辆对共享数据进行混合加密和访问策略隐藏，这一步骤中使用的系统参数均为车辆加密数据时所在 TA 域的系统参数。然后，车辆通过附近 RSU 将数据相关信息上传至 TA，若车辆即将驶出 RSU 通信范围而数据传输未完成时，通过断点续传的方式，与下一个 RSU 继续传输数据。TA 采用拜占庭容错共识（PBFT）算法，将数据相关信息记录到区块链上。

3) 跨域访问验证。数据访问车辆通过附近 RSU 向域 TA 请求其他区域的数据时，TA 调用数据查询合约查询链上数据；若数据查询成功，TA 调用跨域访问验证合约进行解密测试，验证用户属性是否满足密文访问策略。

4) 跨域数据获取。若解密测试通过，TA 将车辆属性集发送给数据共享域 TA_i，由数据共享域 TA_i 使用该域主私钥生成转换密钥后，并将转换密钥发送给数据访问域 TA。数据访问域 TA 进行密文转换，生成转换密文，通过 RSU 发送给数据请求车辆，车辆进行解密，并根据区块链上信息验证数据完整性。

4 区块链架构下高效的车联网跨域数据访问方案

车联网中车辆移动速度快、道路交通状况变化频繁，使跨域交通信息共享等需求增加，车辆对跨域数据的访问更加频繁，因此高效的跨域数据访问成为影响车联网跨域数据共享的关键。本节结合基于区块链的跨域数据安全共享流程，介绍 TA 进行系统初始化、数据共享车辆进行数据加密与访问策略隐藏、TA 结合区块链智能合约进行跨域访问验证、TA 辅助车辆进行跨域数据获取 4 个过程的相关算法细节。

4.1 系统初始化

各域 TA 进行区块链初始化，并进行 OD-CP-ABE-HP 方案的系统参数初始化，以及为域内车辆生成有效私钥。

首先，各域的 TA 进行区块链初始化。具体来说，由区块链管理员为各域 TA 生成区块链交易的公私钥，并配置数据查询、跨域访问验证智能合约（见 4.3 节）；区块链管理员生成创世区块，将各 TA

的区块链地址、采用的共识算法、区块大小等写入其中，同步到每一个 TA。完成上述配置后，管理员本身不再参与后续区块的生成、查询等操作。

然后，各域 TA 使用 Setup 算法初始化各自的系统公钥和主私钥，并使用 KeyGen 算法为域内车辆生成有效私钥。

Setup：输入系统安全参数 λ 和系统属性集合 U，输出系统公钥 PK 和主私钥 MK。

1) 选择具有素数阶 p 的群 G 及其生成元 g，随机选择群元素 $h_1,\cdots,h_U\in G$，其中 $h_1,\cdots,h_U$ 是与 U 中属性相关联的群元素。选择哈希函数 $H{:}\{0,1\}^*\to Z_p$、$H'{:}\{0,1\}^*\to\{0,1\}^{\text{key}}$。

2) 选择哈希函数 $H_1,\cdots,H_k$ 用于将字符串映射到 ABF 中。设 L_{att} 表示系统中属性 att_m 的最大长度，L_{rownum} 表示访问控制矩阵中行号 i 的最大长度，L 表示 ABF 数组中每个位置上字符串的长度，$L=L_{\text{att}}+L_{\text{rownum}}$。这一步骤选择的参数用于访问策略隐藏的实现。

3) 随机选择 $\alpha,a\in Z_p$，生成系统公私钥

$$\begin{aligned}&\text{PK}:(g,e(g,g)^{\alpha},g^{a},h_1,\cdots,h_U,L_{\text{att}},\\&L_{\text{rownum}},L,H,H',H_1,\cdots,H_k)\\&\text{MK}:g^{\alpha}\end{aligned}$$

KeyGen：输入主私钥 MK 和车辆属性集合 S，输出车辆私钥，包括转换密钥 TK 和用户私钥 SK。

1) 选择随机数 $t'\in Z_p$，生成

$$\text{SK}':\left(K'=g^{\alpha}g^{at'},L'=g^{t'},\forall x\in S:K_x'=h_x^{t'}\right)$$

2) 随机选择 $z\in Z_p$，令 $t=\dfrac{t'}{z}$，生成车辆私钥

$$\begin{aligned}&\text{TK}:\left(K=K'^{\frac{1}{z}}=g^{\frac{\alpha}{z}}g^{a\left(\frac{t'}{z}\right)}=g^{\frac{\alpha}{z}}g^{at},L=L'^{\frac{1}{z}}=\right.\\&\left.g^{\frac{t'}{z}}=g^{t},\forall x\in S:K_x=K_x'^{\frac{1}{z}}=h_x^{\frac{t'}{z}}\right)\\&\text{SK}:(z,\text{TK})\end{aligned}$$

4.2　区块链架构下支持策略隐藏的数据加密共享

为了实现安全的车联网跨信任域数据共享，本文设计了基于区块链的数据加密共享方案，在加密数据的同时隐藏访问策略，防止隐私泄露，并利用区块链实现跨域数据的安全、可信传递。具体来说，数据共享车辆基于 OD-CP-ABE-HP 算法和对称加密算法对数据进行加密，对访问策略进行隐藏，并将相关信息上传至区块链。

4.2.1　数据加密

数据共享车辆首先使用对称密钥 key 对数据 message 进行 AES 对称加密，得到密文 CT_{AES}。然后制定访问策略，使用算法 Encrypt 对密钥 key 进行加密。

Encrypt：输入 AES 的对称密钥 key、系统公钥 PK 和访问策略 $(\boldsymbol{M},\boldsymbol{\rho})$，输出密文 CT。

1) 该算法使用 LSSS 定义访问策略 $(\boldsymbol{M},\boldsymbol{\rho})$，随机选择 $r_i\in Z_p$，$R\in G_T$，计算 $s=H(R,\text{key})$ 作为 LSSS 中的共享秘密值，计算 $r=H'(R)$。

2) 计算密文 $\text{CT}=(C,C',C'',C_i,D_i)$

$$\begin{cases}C=Re(g,g)^{\alpha s}\\C'=g^{s}\\C''=(\text{key})\oplus r\\C_i=g^{a\lambda_i}h_{\rho(\text{i})}^{-r_i}\\D_i=g^{r_i}\end{cases}$$

4.2.2　访问策略隐藏

数据共享车辆执行 ABFBuild 算法对访问策略中的映射 ρ 进行隐藏。

ABFBuild：输入访问策略 $(\boldsymbol{M},\boldsymbol{\rho})$，输出 ABF。

1) 将访问策略中的属性与 $\boldsymbol{M}$ 中相应的行号绑定，得到一组元素 $S_m=\{i\,\|\,\text{att}_m\}_{i\in[i,l]}$，表示矩阵的第 i 行映射到属性 $\text{att}_m=\rho(i)$。

2) 将集合 S_m 中的元素 m 添加到 ABF 中。将元素 m 通过 $(k,\,k)$ 异或秘密共享方案进行隐藏，即随机生成 $k-1$ 个 L bit 字符串 $r_{1,m},r_{2,m},\cdots,r_{k-1,m}$，并令

$$r_{k,m}=r_{1,m}\oplus r_{2,m}\cdots\oplus r_{k-1,m}\oplus m$$

3) 用 k 个哈希函数对与元素 m 关联的属性 att_m 进行哈希计算，得到

$$H_1(\text{att}_m),H_2(\text{att}_m),\cdots,H_k(\text{att}_m)$$

其中，$H_i(\text{att}_m)(i\in[1,k])$ 表示分量 $r_{i,m}$ 在 ABF 中存储的位置，将第 i 个随机分量 $r_{i,m}$ 存储在 ABF 中 $H_i(\text{att}_m)$ 对应的位置。当添加元素出现冲突时，使用这个位置上已有的元素分量代替随机分量。

4.2.3　数据上传与相关信息上链

数据共享车辆将 CT_{AES}、CT、$(\boldsymbol{M},\text{ABF})$、TIME 和数据哈希值 HASH 发送至附近 RSU。RSU 首先将数据密文 CT_{AES} 上传到 IPFS，返回存储地址 address；再将数据相关信息 Info 上传至 TA。TA 采用 PBFT 共识算法，将数据相关信息 Info 记录到区块链上。

$\text{Info}=\left(\text{TA}_{\text{ID}},\text{address},\text{TIME},\text{CT},(\boldsymbol{M},\text{ABF}),\text{HASH}\right)$

4.3 区块链架构下高效的跨域访问验证方法

为了实现高效的跨域数据访问，设计了基于混淆布隆过滤器的跨域访问验证方法，并在区块链上部署相应的智能合约，实现大量访问请求的快速解密测试。TA 对链上数据查询后，调用跨域访问验证合约，基于链上访问策略进行快速密文解密测试，验证数据请求车辆属性是否满足访问策略。

4.3.1 链上数据查询

TA 调用数据查询合约（合约 1）查询链上数据，若数据查询成功，进行下一步骤，否则返回 $\perp$。

合约 1 数据查询合约

输入 请求 TA 域编号 QTA_{ID}，请求数据的时间 $\text{TIME}_{\text{MIN}},\text{TIME}_{\text{MAX}}$

输出 查询成功则返回数据相关信息，否则返回 0

1) for $i=0,\cdots,\text{length}$:
2) if 数据时间戳 $\geqslant \text{TIME}_{\text{MIN}}$ 且数据时间戳 $\leqslant \text{TIME}_{\text{MAX}}$ 且 $\text{QTA}_{\text{ID}}=$ 数据 TA_{ID}:
3) return 链上数据;
4) else
5) return 0

4.3.2 跨域访问验证

由于数据加密过程中，访问策略中的映射 $\boldsymbol{\rho}$ 被隐藏，因此需要首先对其进行重构，原理如下。

ABFQuery：输入加密数据对应的 ABF 和数据访问车辆属性集合 S，输出重构向量 $\boldsymbol{\rho}'$。

1) 对于每个 $\text{att}\in S$，使用 k 个哈希函数计算其位置索引

$$H_1(\text{att}),H_2(\text{att}),\cdots,H_k(\text{att})$$

2) 从 ABF 中 $H_i(\text{att})(\ i\in[1,k])$ 的位置上获取相应的字符串 $r_{1,m},r_{2,m},\cdots,r_{k,m}$，通过下式得到重构元素 m

$$m=r_{1,m}\oplus r_{2,m}\cdots\oplus r_{k-1,m}\oplus r_{k,m}=$$
$$r_{1,m}\oplus r_{2,m}\cdots\oplus r_{k-1,m}\oplus r_{1,m}\oplus r_{2,m}\cdots\oplus r_{k-1,m}\oplus m$$

3) 重构元素 m 由行号 i 和属性 att_m 组成。取后 L_{att} bit 字符串得到属性 att_m。若 att_m 与属性 S 中的 att_m 相同，则该属性在访问结构中，取重构元素 m 的前 L_{rownum} bit，得到该属性的行号 i，重构向量 $\boldsymbol{\rho}'=\{i\,\|\,\text{att}'\}_{\text{att}\in S}$。

TA 调用跨域访问验证合约（合约 2）执行 ABFQuery 算法并验证用户属性是否满足密文访问策略。若验证通过，执行接下来的步骤，否则返回 $\perp$。

合约 2 跨域访问验证合约

输入 数据访问策略 $(\boldsymbol{M},\text{ABF})$ 和车辆属性集合 S

输出 车辆属性满足访问策略输出 1，否则输出 0

//首先重构 $\boldsymbol{\rho}'$

1) for each $\text{att}\in S$:
2) 取ReStr为λ bit的全0字符串;
3) for $i=0,\cdots,k-1$:
4) 计算 $\text{Pos}=H_{i+1}(\text{att})$;
5) 计算ReStr = ReStr ⊕ ABF[Pos];
6) 取att_mStr为ReStr的后att bit;
7) 取att_m为移除左侧0的att_mStr;
8) if $\text{att}_m=\text{att}$:
9) 取rownumStr为ReStr的前rownum bit;
10) 取rownum为移除左侧0的rownumStr;
11) 将 att 添加到第 rownum 行，得到 $\boldsymbol{\rho}'$

//根据 $(\boldsymbol{M},\boldsymbol{\rho}')$ 判断车辆属性是否满足访问策略

12) if $\sum_{i\in I}\boldsymbol{M}_i w_i=(1,0,\cdots,0)$:
13) return 1;
14) else
15) return 0

4.4 区块链架构下高效的跨域数据获取方法

为了实现高效的跨域数据获取，设计了基于外包解密的密文转换算法，相比代理重加密等方法，所需要的双线性配对运算大大减少。对通过跨域访问验证的访问请求，TA 为其生成转换密钥和转换密文，执行外包解密运算，减少车辆计算负担。

4.4.1 转换密钥生成

TA 将车辆属性集合 S 和私钥 TK、SK 发送给数据共享域 TA_i，由数据共享域 TA_i 执行 CKeyGen 算法为车辆生成转换密钥 CTK，并将转换密钥发送给数据访问域 TA。

CKeyGen：输入 TA_i 的系统主私钥，输出转换密钥 CTK

$$\text{CTK}:\left(CK=g^{\frac{\alpha}{z}}g^{at},CL=g^{t},\forall x\in S:CK_x=h_x^{\frac{t'}{z}}\right)$$

4.4.2 转换密文生成

数据访问域 TA 执行 CTrans 算法，将原始密文 CT 转换为 CT′，发送给数据访问车辆。

CTrans：输入数据访问车辆的 CTK 和密文 CT，输出转换密文 CT′。

计算 $\mathrm{CT}'=\left(C,C'',T\right)$，其中

$$T=\frac{e\left(\mathrm{C}',CK\right)}{e\left(\prod_{i\in I}C_i^{w_i},CL\right)\prod_{i\in I}e\left(D_i^{w_i},CK_{\rho(i)}\right)}=$$

$$\frac{e\left(g,g\right)^{\frac{s\alpha}{z}}e\left(g,g\right)^{ast}}{\prod_{i\in I}e\left(g,g\right)^{ta\lambda_i w_i}}=e\left(g,g\right)^{\frac{s\alpha}{z}}$$

4.4.3　车辆解密

车辆执行 CDec 算法进行解密得到 AES 的对称密钥 key，使用 key 解密得到明文信息 message′，并通过 CVerify 算法验证数据完整性。

CDec：输入转换后的密文 CT'、车辆的私钥 SK，输出 AES 对称密钥 $\mathrm{CT}_{\mathrm{AES}}$ 或⊥。

$$R=\frac{C}{T^z}$$

$$\mathrm{key}=C''\oplus H'(R)$$

$$s=H(R,\mathrm{key})$$

验证 $C=Re(g,g)^{\alpha s}$ 是否成立，若成立，则输出 key；否则输出⊥。

CVerify：计算 message′的哈希值，并验证这个值是否与区块链上 HASH 一致。若一致，说明明文 message′未被篡改；否则说明数据损坏或被篡改。

5　安全性分析

本节对本文方案的安全性进行分析，如表 1 所示，将本文方案与目前同类方案进行对比，包括核心加密算法、加密方案安全性、密文数据存储、访问策略存储和访问策略构造 5 个方面。

1) 加密方案安全性。表 1 中各方案均采用混合加密方法保护共享数据安全，数据本身由 AES 对称加密，只有能获取到对称密钥的实体才能够解密；基于 CP-ABE 算法对 AES 密钥进行加密，只有属性满足访问策略的车辆才能够解密密文。本文具有外包解密（OD, outsourcing decryption）和策略隐藏（HP, hidden policy）的 OD-CP-ABE-HP 方案是基于文献[20]和文献[28]构建的，可以证明 ABF 不会增加安全游戏中敌手的优势，因此基于判定性 q-BDHE（decisional q-bilinear Diffie Hellman exponent）困难问题可证明其具有 RCCA（replayable chosen-ciphertext attack）安全性[29]，该安全性高于其他同类方案达到的 CPA 安全，同时支持在密文上安全地进行外包计算。

2) 密文数据存储。本文方案基于区块链和 IPFS 存储跨域共享数据，分布式地保存数据副本，能够避免中心化单点故障或数据被某个恶意节点删改，保证数据的可用性[30]。构成区块链的 TA 节点间采用 PBFT 共识机制，当网络中的恶意节点数量少于总节点数的 $\frac{1}{3}$ 时，区块链中的数据无法被篡改[31]。相比文献[17]将大量数据存储在边缘车辆和云服务器上，本文方案能够避免车辆丢失或恶意篡改数据；相比文献[18]直接将数据存储在区块链中，本文方案能够避免区块链中大量数据导致的区块链性能降低。

3) 访问策略的隐私保护。本文方案使用区块链公开记录访问策略，将访问策略中的属性利用异或秘密共享技术存储在 ABF 中，实现对访问策略属性的保护。攻击者无法分析数据访问者所获取数据的访问策略，推断数据访问者拥有的属性。相比其他跨域数据共享方案中，通过访问树或 LSSS 构造的访问策略能够被各实体获取，本文基于 LSSS 和 ABF 构造访问策略，能够保护访问策略中的属性信息。

6　性能分析

本文方案在车联网跨域数据共享过程中的高效性体现在跨域数据访问过程的高效性。本节通过实验评估了本文跨域数据访问中 3 个主要部分的性能，即跨域访问验证、跨域密文转换和车辆侧解密，并对比了大量数据请求下各方案跨域数据访问全流程所需要的时间。

6.1　实验设置

跨域数据安全共享仿真实验中设置 2 个 TA，

表 1　　**安全性对比**

方案	核心加密算法	加密方案安全性	密文数据存储	访问策略存储	访问策略构造
文献[17]	CP-ABE	CPA	边缘车辆+云	—	LSSS
文献[18]	CP-ABE	CPA	区块链	区块链	访问树
文献[19]	OD-CP-ABE	CPA	区块链+IPFS	RSU+策略管理中心	LSSS
本文方案	OD-CP-ABE-HP	RCCA	区块链+IPFS	区块链	LSSS+ABF

每个 TA 中设置 10 个 RSU，共 10 000 辆车随机分布、随机移动，不断地进行数据上传和数据请求。仿真实验环境参数如下：处理器 Intel(R) Core(TM) i7-9750H CPU @ 2.60 GHz，内存 8 GB，磁盘 150 GB。

1) 跨域访问验证。仿真实验对比了大量跨域数据访问请求下，不同方案跨域密文转换的性能。本文方案在进行跨域密文转换前，对跨域访问请求进行访问验证，若验证不通过，则不执行跨域密文转换。因此记访问请求总数为 N_{all}，其中能够被解密的访问请求数量为 N_{succ}，跨域访问验证通过概率为 $P_f=\dfrac{N_{\text{succ}}}{N_{\text{all}}}$，取 10%～100%进行实验；设置访问策略中属性数量为 25 个，密文数量为 200 个。在 Hyperledger Fabric 平台上部署区块链，基于 Java 语言编写跨域访问验证合约进行测试。

2) 跨域密文转换。仿真实验采用 Java 中基于配对的密码学（JPBC）库实现了本文方案和对比方案的跨域密文转换过程，其中对比方案的跨域密文转换方法如下。

① 文献[17]进行跨域身份验证后，为数据共享对象进行 CP-ABE 加密。

② 文献[18]使用代理重加密的方法进行密文转换。

③ 文献[19]将密文数据解密后，使用数据共享域的公开参数进行加密，最后执行外包解密。

此外，评估了 2 种因素对跨域密文转换时间开销的影响。2 种因素介绍如下。

① 密文访问策略中属性数量。由于本文方案与对比方案均基于 CP-ABE 算法进行跨域数据共享，密文访问策略中属性数量是影响跨域密文转换时间开销的关键因素。将密文访问策略中属性数量记为 N_{att}，取 10～50 个进行实验。

② 跨域访问请求数量。由于车联网场景中，短时间内存在大量跨域密文数据访问请求，需要进行跨域密文转换，因此将同一时刻跨域请求数量记为 N_{c}，取 10～200 个进行实验。

3) 车辆侧解密。仿真实验评估了访问策略中属性数量、车辆同时解密时的密文数量对车辆侧解密时间开销的影响，取车辆侧同一时刻需要解密的密文数量为 1～10 个进行实验。

4) 跨域数据访问。仿真实验对各方案跨域数据访问的时间开销进行对比。同一时刻跨域访问验证数量和密文转换数量为 100 个，跨域访问验证通过概率为 100%，车辆侧解密密文数量为 10 个。

6.2 跨域访问验证

为评估本文方案的跨域访问验证通过概率对大量跨域密文访问请求下密文转换时间开销的影响，将本文方案与文献[17-19]方案进行对比，如图 4 所示。

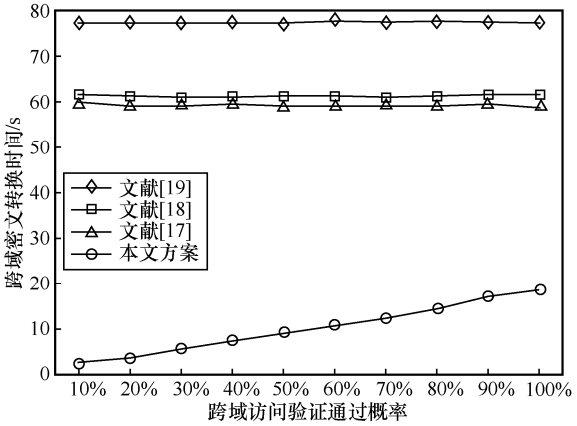

图 4 跨域访问验证通过概率对大量密文转换时间开销的影响

由图 4 可知，随着跨域访问验证通过概率的增加，本文方案的跨域密文转换时间开销呈线性增长，而对比方案的转换时间开销恒定，这是由于在本文方案中，TA 仅需为通过跨域访问验证的访问请求进行密文转换。并且，本文方案转换时间开销始终小于对比方案，当跨域访问验证通过概率达到 100%，即本文方案中所需转换时间开销最大时，相比文献[17-19]方案，本文方案的跨域密文转换效率依然分别提高了 62%、63%和 69%。

6.3 跨域密文转换

为评估跨域密文转换过程的效率，对比了不同方案在 2 种因素影响下的跨域密文转换时间开销，分别如图 5 和图 6 所示。

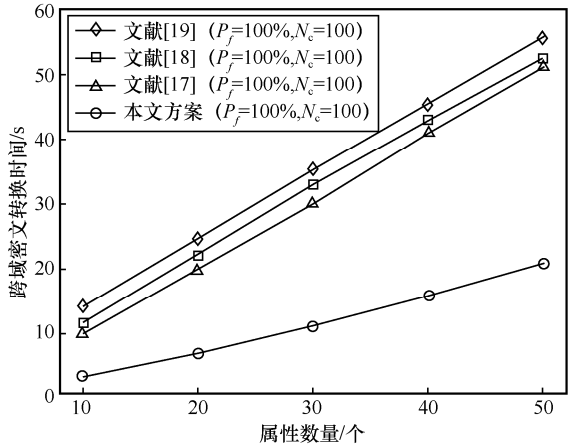

图 5 属性数量对密文转换时间开销的影响

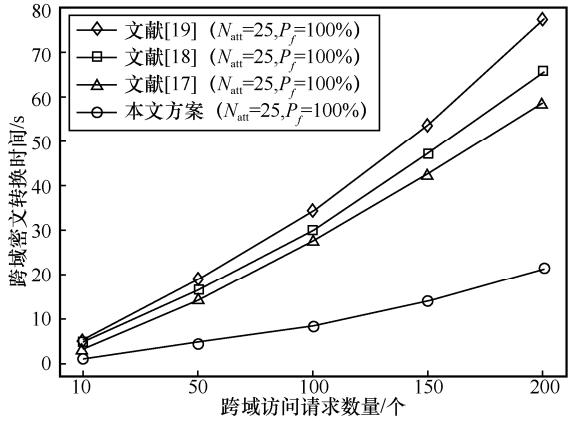

图 6　跨域访问请求数量对密文转换时间开销的影响

由图 5 可知，随着密文访问策略中属性数量的增加，各方案的跨域密文转换时间开销均线性增长，而本文所需的跨域密文转换时间开销最小，在访问策略中当属性数量达到 50 时，相比文献[17-19]方案，本文方案的跨域密文转换效率分别提高了 59%、60%和 62%。这是由于本文设计的基于外包解密的跨域密文转换方法，在访问策略中属性数量相同时需要更少的双线性配对运算。

由图 6 可知，随着跨域访问请求数量的增加，各方案的跨域密文转换时间开销呈指数增长，其中本文方案转换时间开销增长速度较慢。当跨域访问请求数量为 10 个时，各方案的跨域密文转换时间开销接近，随着跨域请求数量的增长，文献[17-19]方案与本文方案之间的差距逐渐增大；当跨域访问请求数量达到 200 个时，相比文献[17-19]方案，本文方案的跨域密文转换效率分别提高了 63%、67%和 72%。

6.4　车辆侧解密

为验证本文方案车辆侧解密时间开销较小，对比了不同方案中密文访问策略中属性数量、密文数量对车辆侧解密时间开销的影响，分别如图 7 和图 8 所示。

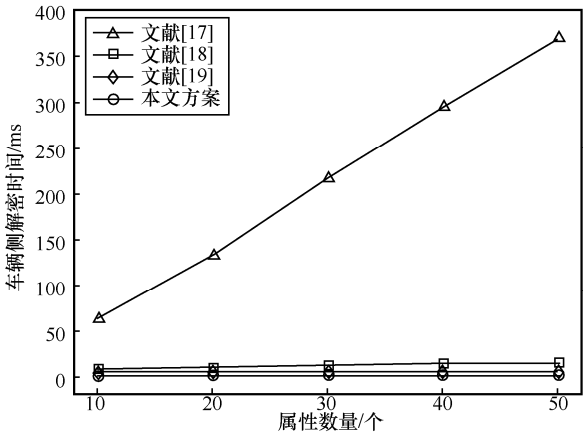

图 7　属性数量对车辆侧解密时间开销的影响

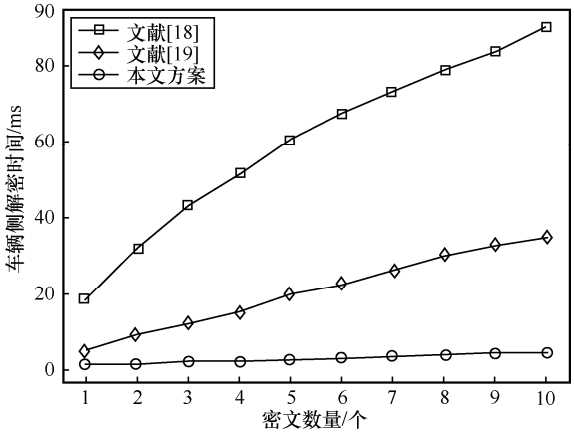

图 8　密文数量对车辆侧解密时间开销的影响

由图 7 可知，随着访问策略中属性数量的增加，文献[17]方案的解密时间开销呈线性增长，文献[18]方案的解密时间开销缓慢增加，本文方案和文献[19]方案的解密时间开销恒定，且本文方案的解密时间开销较小。这是由于本文方案对密文进行外包解密，且车辆侧仅需要一个恒定的指数运算即可完成解密。

由图 8 可知，随着车辆在同一时刻解密密文数量的增加，各方案的解密时间开销均增长，其中本文方案的增长趋势较平缓，车辆侧仅需 4.8 ms 即可解密 10 个密文数据。

6.5　跨域数据访问

为评估跨域数据访问的时间开销，对各方案中大量跨域数据访问时间开销进行对比分析，如图 9 所示。

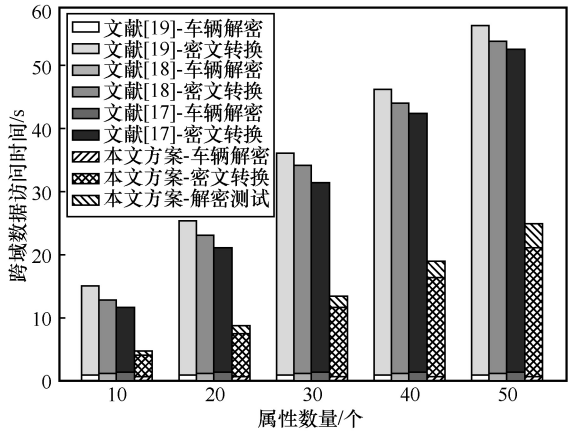

图 9　跨域数据访问时间开销对比

由图 9 可知，虽然本文方案在跨域访问验证上存在时间开销，但跨域数据访问效率更高，相比于文献[17-19]方案，本文方案的跨域数据访问效率平均提升了 57%、60%和 63%。这是由于本文方案设计了跨域访问验证方法，提高了大量数据的访问效

率；设计了基于外包解密的跨域密文转换方法，提高了跨域密文转换和车辆侧解密的效率。

7 结束语

针对车联网跨信任域数据共享场景下跨域数据泄露、跨域数据共享不可控的问题，本文提出了基于区块链的车联网跨域数据安全共享方案，由不同信任域的 TA 构成区块链，结合 IPFS 分布式地存储跨域共享数据，采用改进的 CP-ABE 算法和对称加密算法保证数据机密性，实现细粒度的跨域数据安全共享。针对跨域密文数据访问效率低的问题，设计了基于混淆布隆过滤器的跨域访问验证方法，智能合约基于链上访问策略对跨域数据请求进行快速解密测试，不需要解密即可安全地验证访问者属性是否满足访问策略；设计了基于外包解密的跨域数据获取方法，TA 为跨域访问请求生成转换密文，执行复杂的双线性配对解密运算，减少了数据跨域数据访问过程的时间开销。对方案的分析表明，本文的跨信任域数据共享方案具有 RCCA 安全，并且支持访问策略的隐藏；实验结果表明，本文方案在跨域密文转换和车辆解密过程的性能均优于现有方案，跨域数据访问效率平均提升了 60%。

未来，本文将在保证数据安全的前提下，探索基于区块链的具有条件隐私保护的车联网跨域数据安全共享方法。

参考文献：

[1] TAN H W, CHUNG I. RSU-aided remote V2V message dissemination employing secure group association for UAV-assisted VANETs[J]. Electronics, 2021, 10(5): 548-570.

[2] SUN J F, XIONG H, ZHANG S F, et al. A secure flexible and tampering-resistant data sharing system for vehicular social networks[J]. IEEE Transactions on Vehicular Technology, 2020, 69(11): 12938-12950.

[3] TSUKAMOTO K, TAMURA H, TAENAKA Y, et al. Geolocation-centric information platform for resilient spatio-temporal content management[J]. IEICE Transactions on Communications, 2021, 104(3): 199-209.

[4] LU Z J, QU G, LIU Z L. A survey on recent advances in vehicular network security, trust, and privacy[J]. IEEE Transactions on Intelligent Transportation Systems, 2019, 20(2): 760-776.

[5] ZHANG X H, CHEN X F. Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network[J]. IEEE Access, 2019, 7: 58241-58254.

[6] JIANG D D, WANG Z H, HUO L W, et al. A performance measurement and analysis method for software-defined networking of IoV[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(6): 3707-3719.

[7] KANG J W, YU R, HUANG X M, et al. Blockchain for secure and efficient data sharing in vehicular edge computing and networks[J]. IEEE Internet of Things Journal, 2019, 6(3): 4660-4670.

[8] GROVER J. Security of vehicular ad hoc networks using blockchain: a comprehensive review[J]. Vehicular Communications, 2022, 34: 100458-100477.

[9] ZHONG H, WEN J Y, CUI J, et al. Efficient conditional privacy-preserving and authentication scheme for secure service provision in VANET[J]. Tsinghua Science and Technology, 2016, 21(6): 620-629.

[10] MA Z F, WANG L Y, ZHAO W Z. Blockchain-driven trusted data sharing with privacy protection in IoT sensor network[J]. IEEE Sensors Journal, 2021, 21(22): 25472-25479.

[11] WU J, DONG M X, OTA K, et al. A fine-grained cross-domain access control mechanism for social Internet of things[C]//Proceedings of 2014 IEEE 11th International Conference on Ubiquitous Intelligence and Computing and 2014 IEEE 11th International Conference on Autonomic and Trusted Computing and 2014 IEEE 14th International Conference on Scalable Computing and Communications and Its Associated Workshops. Piscataway: IEEE Press, 2015: 666-671.

[12] MENG Y F, LI J Z. Data sharing mechanism of sensors and actuators of industrial IoT based on blockchain-assisted identity-based cryptography[J]. Sensors, 2021, 21(18): 6084-6103.

[13] TRUONG H T T, ALMEIDA M, KARAME G, et al. Towards secure and decentralized sharing of IoT data[C]//Proceedings of 2019 IEEE International Conference on Blockchain (Blockchain). Piscataway: IEEE Press, 2019: 176-183.

[14] CHEN Y W, HU B W, YU H J, et al. A threshold proxy re-encryption scheme for secure IoT data sharing based on blockchain[J]. Electronics, 2021, 10(19): 2359-2377.

[15] YU K P, TAN L, ALOQAILY M, et al. Blockchain-enhanced data sharing with traceable and direct revocation in IIoT[J]. IEEE Transactions on Industrial Informatics, 2021, 17(11): 7669-7678.

[16] SUN J F, XU G W, ZHANG T W, et al. Secure data sharing with flexible cross-domain authorization in autonomous vehicle systems[J]. IEEE Transactions on Intelligent Transportation Systems, 2022: doi.org/10.1109/TITS. 2022.3157309.

[17] PAN J W, CUI J, WEI L, et al. Secure data sharing scheme for VANETs based on edge computing[J]. EURASIP Journal on Wireless Communications and Networking, 2019(1): 1-11.

[18] WANG D, ZHANG X H. Secure data sharing and customized services for intelligent transportation based on a consortium blockchain[J]. IEEE Access, 2020, 8: 56045-56059.

[19] MA J F, LI T, CUI J, et al. Attribute-based secure announcement sharing among vehicles using blockchain[J]. IEEE Internet of Things Journal, 2021, 8(13): 10873-10883.

[20] YANG K, HAN Q, LI H, et al. An efficient and fine-grained big data access control scheme with privacy-preserving policy[J]. IEEE Internet of Things Journal, 2017, 4(2): 563-571.

[21] RAMU G. A secure cloud framework to share EHRs using modified CP-ABE and the attribute bloom filter[J]. Education and Information Technologies, 2018, 23(5): 2213-2233.

[22] HAN Q, ZHANG Y H, LI H. Efficient and robust attribute-based encryption supporting access policy hiding in Internet of things[J].

Future Generation Computer Systems, 2018, 83: 269-277.

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

[24] DONG C Y, CHEN L Q, WEN Z K. When private set intersection meets big data: an efficient and scalable protocol[C]//Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. New York: ACM Press, 2013: 789-800.

[25] ZHOU H B, LIU B, LUAN T H, et al. ChainCluster: engineering a cooperative content distribution framework for highway vehicular communications[J]. IEEE Transactions on Intelligent Transportation Systems, 2014, 15(6): 2644-2657.

[26] MA X T, ZHAO J H, GONG Y, et al. Carrier sense multiple access with collision avoidance-aware connectivity quality of downlink broadcast in vehicular relay networks[J]. IET Microwaves, Antennas & Propagation, 2019, 13(8): 1096-1103.

[27] NGUYEN B L, NGO D T, TRAN N H, et al. Dynamic V2I/V2V cooperative scheme for connectivity and throughput enhancement[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(2): 1236-1246.

[28] GREEN M, HOHENBERGER S, WATERS B. Outsourcing the decryption of ABE ciphertexts[C]//Proceedings of the 20th USENIX Conference on Security. New York: ACM Press, 2011: 34-50.

[29] CANETTI R, KRAWCZYK H, NIELSEN J B. Relaxing chosen-ciphertext security[C]//Annual International Cryptology Conference. Berlin: Springer, 2003: 565-582.

[30] DANIEL E, TSCHORSCH F. IPFS and friends: a qualitative comparison of next generation peer-to-peer data networks[J]. IEEE Communications Surveys & Tutorials, 2022, 24(1): 31-52.

[31] CASTRO M, LISKOV B. Practical Byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems, 2002, 20(4): 398-461.

[作者简介]

刘雪娇（1984− ），女，河南安阳人，博士，杭州师范大学副教授，主要研究方向为网络安全、云安全、车联网安全等。

曹天聪（1999− ），女，河北唐山人，杭州师范大学硕士生，主要研究方向为网络安全、区块链和车联网。

夏莹杰（1982− ），男，浙江宁波人，博士，浙江大学研究员，主要研究方向为智能交通、信息安全等。