车内网中基于属性加密的可撤销访问控制机制研究

张静，张佳轩，沈韵*，崔杰，魏璐
（安徽大学计算机科学与技术学院，合肥 230601）

摘要：随着车内网（in-vehicle network，IVN）对数据安全性和灵活访问控制的需求日益提升，传统车载以太网及其应用层协议因缺乏内置身份验证与细粒度权限管控机制，已难以满足 IVN 的精细化安全访问控制需求。同时，IVN 环境下车载设备计算资源受限的特性，进一步提升了细粒度访问控制方案的落地实现难度。针对 IVN 环境资源受限、通信实时性要求高，细粒度访问控制难以高效实现的难题，本文面向高级驾驶辅助系统（advanced driver assistance systems，ADAS）场景，开展动态数据访问控制机制研究。该方案引入轻量级椭圆曲线密码学，有效降低计算开销、提升系统执行效率；设计动态属性撤销机制，可在不影响其他网络实体的基础上，实现单一属性的精准撤销。实验结果表明，该方案在保障系统安全性的基础上，可为资源受限的车内网络提供高效、可扩展的访问控制解决方案，能够有效适配 ADAS 场景的车载通信安全与性能需求。

关键词：车内网络；访问控制；密文策略属性基加密；椭圆曲线密码学；属性撤销
中图分类号：TP399；TP393.08 **文献标志码：**A
DOI: 10.20172/j.issn.2097-3136.260526

Research on revocable attribute-based encryption access control mechanism for in-vehicle networks

Zhang Jing, Zhang Jiaxuan, Shen Yun*, Cui Jie, Wei Lu
（Department of Computer Science and Technology, Anhui University, Hefei 230601, China）

Abstract: With the growing demand for data security and flexible access control in in-vehicle network (IVN), traditional automotive Ethernet and its application-layer protocols lack built-in authentication and fine-grained permission control mechanisms, which cannot meet the refined security access control requirements of IVN. Furthermore, the limited computing resources of in-vehicle devices in IVN further increase the difficulty of implementing fine-grained access control. Aiming at the difficulties in implementing fine-grained access control under the conditions of limited resources and high real-time communication requirements in IVN, this paper investigates a dynamic data access control strategy applicable to advanced driver assistance systems (ADAS). The proposed scheme adopts lightweight elliptic curve cryptography to reduce computational overhead and improve system execution efficiency, and designs a dynamic attribute revocation mechanism to realize the precise revocation of a single attribute without interfering with other network entities. Experimental results show that the proposed scheme can ensure system security while providing an efficient and scalable access control solution for resource-constrained IVN. It can well balance the performance and security requirements of in-vehicle communication systems and adapt to the data access security needs of ADAS scenarios.

Keywords: in-vehicle networks; access control; ciphertext-policy attribute-based encryption; elliptic curve cryptography; attribute revocation

* **通信作者：**E-mail: zs_shenyun@163.com

基金项目：国家自然科学基金（62272002；62472003；62202008）；国家自然科学基金联合基金重点项目（U23A20308）

引用格式：张静，张佳轩，沈韵，等. 车内网中基于属性加密的可撤销访问控制机制研究 [J]. 网络空间安全科学学报，2026，4（3）：105 - 116.

Citation Format: Zhang J，Zhang J X，Shen Y，et al. Research on revocable attribute-based encryption access control mechanism for in-vehicle networks[J]. Journal of Cybersecurity，2026，4（3）：105 - 116.

0 引言

随着智能网联汽车（intelligent connected vehicles，ICV）与高级驾驶辅助系统（advanced driver assistance systems，ADAS）的持续发展，车载通信网络已成为支撑车内信息交互的重要支柱。然而，传统控制器局域网络（controller area network，CAN）、本地互联网络（local interconnect network，LIN）在设计之初并未充分考虑网络安全问题，普遍缺乏内置身份验证与访问控制机制。这使得车载系统易遭受中间人攻击、重放攻击，还会出现非法访问问题，进而威胁车辆运行安全与通信数据机密性。因此，在车载通信系统中构建高效、动态、安全的数据访问控制机制，是当前研究的关键挑战之一。

随着车载通信需求的持续增长和电子电气架构的演进，车载以太网在车内的应用日益广泛[1]。在车载以太网通信体系中，为满足车内异构电子控制单元（electronic control units，ECU）的高效通信需求，数据分发服务（data distribution service，DDS）[2-5]作为发布 / 订阅式中间件协议，常部署于车载以太网架构，支撑 ICV 内部信息交互。然而，车载以太网缺乏认证机制，无法识别数据源是否合法，数据在网络上传输易被篡改或伪造。此外，数据接收方的访问权限会随车辆运行的上下文状态动态变化，设计灵活的动态访问控制方案成为一大难题。

为保障车内网（in-vehicle network，IVN）环境下数据的机密性与完整性、提升系统动态访问控制能力，学术界与工业界已提出多种基于加密和认证机制的解决方案[6-8]。但现有方案仍存在两大短板。其一，车载设备资源受限，现有加密方案采用的双线性配对运算开销较大，难以部署在 ECU 等终端设备中。其二，IVN 的访问策略与属性具有强动态性，传统密文策略属性基加密（ciphertext-policy attribute-based encrytion，CP-ABE）处理属性撤销、策略更新时，效率低、开销大，无法兼顾车内信息交互的实时性与安全需求。

针对车内网场景下的安全需求与性能瓶颈，本文聚焦 3 个核心问题展开研究。

1）车内网不同功能模块的数据访问权限要求具备细粒度、动态可撤销特征，传统基于身份的访问控制无法实现属性级权限管理，难以适配车载系统多等级、多场景的安全管控要求。

2）车载设备计算与存储资源受限，传统基于双线性配对的属性加密方案运算开销极高，难以在资源受限端实现实时解密，限制了安全机制在车内网的部署。

3）现有车载安全方案普遍存在属性撤销机制复杂、时延过高的问题，无法满足自动驾驶的实时性要求。

因此，本文提出一种面向车内网络的细粒度访问控制方案。该方案采用 CP-ABE 技术，实现通信数据的细粒度访问控制。CP-ABE 允许数据发布者根据预定义的访问策略对数据进行加密，只有满足特定属性集合的订阅者才能够解密数据。为进一步提升系统灵活性与安全性，本文设计动态属性撤销机制，可在不影响其他合法用户的前提下，撤销指定用户的访问权限。该机制提升了系统可管理性，同时规避了传统方案因用户属性变更、重新分配密钥产生的计算开销。本文主要贡献如下。

1）基于 DDS 构建主题驱动型访问控制模型，依托其发布 / 订阅机制完成车载数据的主题管理与权限管控；采用椭圆曲线标量乘法替代高开销的双线性配对运算，使方案适配资源受限的 IVN 环境，同时保证仅符合指定属性集合的用户可完成数据解密。

2）设计细粒度属性撤销机制与密钥更新流程，可在用户属性失效、权限变更时动态撤销对应属性，防范非法访问与数据泄露，弥补传统静态密钥管理难以适配动态业务需求的不足。

3）针对车内 ECU 计算资源受限的问题，引入椭圆曲线密码学降低加解密运算开销。理论分析与实验结果表明，本文方案在计算与通信层面均具备较高效率。

1 相关工作

本节从车载以太网、DDS 数据通信安全方案两方面梳理现有研究，分析各类方法在身份认证、数据保护及访问控制层面的不足。

1.1 车载以太网的安全方案

随着智能网联汽车电子电气架构向“中央计算平台+区域控制器”转型，车内网络已成为连接多域 ECU、传感设备与各功能模块的核心枢纽，其安全防护包括节点身份验证、数据传输保密等[9-10]。

Hazem 等[11]提出轻量级消息源认证协议。该方案解决了传统控制器局域网络（controller area network, CAN）总线缺乏身份认证的问题，将认证开销控制在 2 字节 MAC 字段，该协议需在 CAN 协议 29 位标识符空间中预留 8 位标识认证状态，且未提供信息机密性保护。

Groza 等[12] 采用密钥分割与消息认证码混合技术，设计了适用于 CAN 总线的轻量级认证方案。该方案解决了传统认证协议开销过大、与 CAN 总线兼容性差的问题，但仅支持消息完整性验证，无法抵御窃听等被动攻击，且存在密钥泄露的风险。Xiao 等[13] 利用 CAN 信号的时域和频域特征构建隐蔽信道，提出零协议修改和零流量开销的发送端指纹认证方案。该方案解决了传统认证协议占用总线带宽的问题，无需修改硬件或协议即可部署，但环境变化可能导致特征漂移，需要定期校准以保证性能，增加了维护成本。Ueda 等[14] 提出了基于集中式 ECU 的总线消息认证方案。该方案解决了分布式架构下认证协同困难的问题，能够有效拦截伪装攻击，但存在单点故障风险，一旦集中式 ECU 出现故障或遭受拒绝服务攻击，整个认证系统就会崩溃。Hu 等[15] 提出基于网关的广播认证协议，实现车内以太网源认证与拒绝服务攻击（denial of service, DoS）防护，通过网关对广播消息进行集中验证和过滤，防止恶意消息传播。该方案解决了车内以太网缺乏针对性安全防护的问题，但缺乏密钥管理机制，导致方案难以在实际场景中应用。Fassak[16] 提出完整的 CAN 总线身份认证和密钥建立协议。该方案解决了 CAN 总线缺乏完整身份认证与密钥协商机制的问题，首次实现了端到端的安全通信，但协议执行流程复杂，计算开销较大，不适用于资源受限的 ECU，且实时性难以满足高频通信场景。Lodge[17] 设计了基于通用哈希函数的轻量级认证密钥交换协议，适用于车内 CAN/CAN-FD 网络。该方案解决了传统密钥交换协议开销过大的问题，通过简化运算流程降低了计算开销，但该方案采用预共享密钥机制，存在密钥泄露、前向安全性不足等问题，且难以适配动态应用场景。Feng 等[18] 提出可扩展的 CAN 总线加密协议套件，基于中国剩余定理分发初始会话密钥，针对子网内 ECU 间传输、跨子网 ECU 间传输以及基于无证书签名方案的外部设备访问等场景，设计扩展数据帧传输协议。该方案解决了传统加密协议适配性差的问题，支持多场景通信安全，但加密流程复杂、计算开销与通信开销偏大，难以满足 ADAS 等核心系统的毫秒级响应要求。Iorio 等[19] 提出基于 SOME/IP 协议的车内网络身份认证与安全通信方案。该方案解决了域控制器间跨协议通信的安全问题，实现了 SOME/IP 的安全增强，但依赖网关 ECU 进行协同，存在一定的单点故障风险，且密钥更新机制不够灵活。

综上所述，现有车内网络安全方案虽在单一维度实现突破，但仍面临三大核心问题：一是系统安全与实时性难以平衡，复杂的加密认证机制导致计算开销过大，无法适配 ADAS 毫秒级响应需求；二是多域协同适配不足，传统方案针对分布式架构设计，难以应对域间数据交互频繁的新型架构；三是动态场景适应性差，缺乏对驾驶状态切换、ECU 属性变更等动态场景的自适应调整能力。

1.2　车载以太网的访问控制方案

访问控制作为权限精准管理的核心技术，旨在实现按需授权，防止越权访问与数据滥用，其技术发展从传统的节点级粗粒度管控逐步向属性级细粒度协同管控演进。

Ghosal 等[20] 将密文策略属性基加密技术应用于不可信云环境下的车载软件包分发，通过非交互式流程和预解密机制，显著降低通信负载的增长速率，使得车辆可离线接收软件更新包，减少对云端实时交互的依赖，提升了分发效率。但该方案未设计车辆权限撤销机制，在复杂攻击模型中系统鲁棒性不足，难以抵御各类安全攻击。Lamanna 等[21] 完成了属性基加密（attribute-based encryption，ABE）技术在车载场景的适用性验证问题，为后续方案的设计提供了实验支撑，但未涉及权限动态调整与跨域协同等核心问题。Saidi 等[22] 在智能电网场景下提出多属性权威数据共享方案。该方案解决了单权威 ABE 方案中单点故障的问题，其分布式架构为车载跨域场景提供了参考，但未针对车内多域协同的属性异构问题进行优化，且策略隐藏机制在车载高实时性场景下计算开销过大。Yu 等[23] 提出基于优化椭圆曲线密码学（elliptic curve cryptography，ECC）的轻量级加密方案，通过改进密钥生成算法降低密钥生成阶段的计算开销，适配车载资源受限特性。该方案解决了传统加密算法计算开销过大的问题，提升了方案在车载场景中的适配性，但该方案未设置属性权限管理机制，无法实现按需授权，管控粒度较粗，也不支持动态权限调整。Chen 等[24] 提出基于集中式 ECU 的跨域认证方案，该方案由核心 ECU 统一管理多域权限，协调域间数据访问请求，所有跨域通信均需经过核心 ECU 的权限验证。该方案解决了跨域访问场景下权限混乱的问题，实现了权限的集中管理，但存在单点故障风险，且难以适配多域属性异构的场景。

综上所述，现有访问控制技术仍面临三大突出问题：一是细粒度与轻量级难以兼顾，ABE 方案支持细粒度属性管理但计算开销过大，轻量级加密方案

简化了算法却以牺牲管控细粒度为代价；二是跨域协同能力不足，集中式架构存在单点故障风险，分布式架构难以平衡实时性与隐私保护；三是权限动态调整低效，传统属性撤销机制大多依赖全量重加密或全局密钥更新，会干扰合法实体间的通信[25-28]。

近年来，车载细粒度访问控制、轻量化无配对属性加密以及高效属性撤销机制已成为研究热点。为适配资源受限车载场景，大量基于 ECC 的无配对 ABE 方案被提出[29]，在保障安全性的同时大幅降低计算开销；支持动态撤销的访问控制模型，也进一步适配了车内网的高动态运行需求。

2 问题陈述

本节依次介绍本文方案的系统模型、威胁模型及相关基础知识。

2.1 系统模型

图 1 为本文方案的系统模型，模型主要包含 3 类实体：传感单元（sensor）、中央计算单元（central computing unit，CCU）、域控制器（domain controller，DC），各实体功能描述如下。

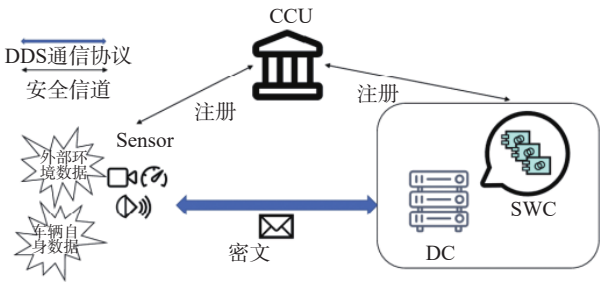

图 1 系统模型

Fig. 1 System model

（1）传感单元

传感单元作为数据发布节点部署于车辆关键位置，涵盖激光雷达、毫米波雷达、车载摄像头、车速传感器等，负责实时采集车辆环境数据与车身状态数据。该单元内置轻量级加密模块，对采集数据完成预处理后，依据预设访问策略对数据加密，并通过 DDS 中间件发布至对应数据主体。

（2）中央计算单元

中央计算单元为系统内的完全可信实体，主要负责初始化系统参数、生成属性公钥与系统主密钥；管理软件组件（software component, SWC）的身份注册与属性列表维护，为合法 SWC 分配全局唯一标识符（global identifier, GID），抵御实体合谋攻击；在属性撤销阶段完成属性密钥与密文参数的同步更新。

（3）域控制器

域控制器为部署 DDS 中间件的功能平台，负责协调 SWC 与 DDS 中间件之间的数据传输。域控制器可转发 SWC 的注册请求与密钥生成请求，并通过中间件主题匹配机制实现密文数据的精准分发。

2.2 威胁模型

车载网络 ADAS 域具备开放性与动态性特征，因此本文方案需同时抵御主动、被动两类网络安全威胁。本文对攻击者能力做如下假设：攻击者可通过物理接入或无线漏洞入侵车载网络，截获、篡改、伪造传输数据；可假冒合法实体发起访问请求，窃取未授权数据；可与其他非授权实体开展合谋攻击。攻击者无法破解椭圆曲线离散对数问题（elliptic curve discrete logarithm problem, ECDLP）等密码学困难性问题[30]，也无法篡改可信实体的存储数据与运算结果。具体威胁类型如下。

1）窃听攻击：攻击者监听 DDS 中间件与各网络实体间的通信链路，窃取加密数据、属性密钥或身份凭证，并通过暴力破解、流量分析等方式推断车辆敏感信息。

2）假冒攻击：攻击者伪造传感单元身份发布虚假感知数据，或伪装合法 SWC 提交密钥生成请求，非法获取未授权的数据访问权限。

3）重放攻击：攻击者截获系统合法密文或密钥请求消息，在后续通信过程中重复发送，欺骗系统执行无效业务操作，引发数据冗余、权限滥用等安全问题。

4）合谋攻击：多个非授权 SWC 相互共享自身属性密钥与访问权限，联合破解超出各自权限范围的密文数据，实现越权访问。

2.3 基础知识

2.3.1 椭圆曲线密码学

在有限域F_p上，椭圆曲线的一般方程为：$E: y^2 = x^3 + ax + b \bmod p$。其中，$p$为素数，定义有限域$F_p$的大小；$a, b \in F_p$且满足$4a^3 + 27b^2 \neq 0$，保证该椭圆曲线为非奇异曲线。椭圆曲线密码体制的安全性依托 ECDLP，其定义如下。

在椭圆曲线密码体系中，求解椭圆曲线离散对数属于计算困难问题。具体地说，设E是有限域 GF(q)上的一条椭圆曲线，G是一个阶为r的生成元，计算$P = kG$，其中，$k \in \mathbb{Z}_r$。这是一个易于执行的点乘运算。然而，给定P和G，在多项式时间内求解整数k几乎是不可行的。与传统的 RSA 相比，ECC 在提供相同安全级别的情况下，使用较短的密钥长度，

从而提高计算效率并降低存储开销。

2.3.2　线性秘密共享方案

线性秘密共享方案（linear secret sharing scheme, LSSS）是一种密码学原语[31]，用于将秘密分配给 n 个参与方，每个参与方都拥有该秘密的份额。除非所有参与方的份额被合并，否则原始秘密不能被泄露。因此，只有授权的参与方集合才能够生成原始秘密。当原始秘密通过线性映射从份额重构时，在 $\mathbb{Z}_p$ 上基于 n 个参与方 $\{F_1,F_2,\cdots,F_n\}$ 的 LSSS 应该满足以下性质。

1）每个 F_i 的秘密份额可以形成 $\mathbb{Z}_p$ 上的向量。

2）$\boldsymbol{A}$ 是一个大小为 $(l\times m)$ 的共享矩阵，其中，每行 $x\in[1,2,\cdots,l]$ 表示集合 F 中的一个实体。函数 $\rho(x)$ 表示 A_x 中的属性（矩阵 $\boldsymbol{A}$ 的第 x 行）。设 $s\in\mathbb{Z}_p$ 是需要共享的秘密消息，为实现该秘密共享，随机选取列向量 $\boldsymbol{v}=(s,v_2,\cdots,v_m)$，其中，$v_2,\cdots,v_m$ 从 $\mathbb{Z}_p$ 中随机选取。然后，$(\boldsymbol{A}\cdot\boldsymbol{v})$ 成为 s 的 l 个份额的向量。向量 $(\boldsymbol{A}_x\cdot\boldsymbol{v})\rightarrow\Lambda_x$ 根据 LSSS 将 s 划分为 l 个份额，其中，$x\in[1,2,\cdots,l]$。$(A_x\cdot v)$ 被称为属于函数 $\rho(x)$ 的共享份额。

3）对于任何授权的属性集 $\alpha\in\boldsymbol{A}'$，可以在多项式时间内生成一个常数集 $c_x\in\mathbb{Z}_p$。通过计算 $\sum_{x\in[1,\cdots,l]}c_x\cdot\Lambda_x=s$，从这个 c_x 中重构秘密 s。

2.3.3　属性基加密

属性基加密可实现数据细粒度访问控制，其核心原理是将用户身份与多维属性绑定，将自定义访问控制策略直接嵌入加密与密钥生成阶段，构建“一次加密、多用户按需解密”的高效数据共享机制[32-33]。ABE 支持数据所有者定义访问策略，只有属性集合满足访问策略的用户才能解密密文，无需为每个接收者单独生成密钥。

3　方案设计

3.1　系统初始化阶段

在这个阶段，CCU 生成系统参数和系统属性公钥并广播。

给定大素数 q 作为安全参数，中央计算单元在有限域 $\mathrm{GF}(q)$ 上生成一个椭圆曲线 E。从椭圆曲线 E 中选取大素数阶 r 的基点 G，该基点生成阶为 r 的循环子群。中央计算单元随机选择 $n\in\mathbb{Z}_r$ 作为主密钥 d_{CCU}，计算公钥为 $\mathrm{PK}_{\mathrm{CCU}}=nG$，并定义哈希函数 H_p。中央计算单元将生成的全局系统参数发布为 $\mathrm{GP}=(E,G,q,r,H_p,\mathrm{PK}_{\mathrm{CCU}})$。对于每个系统属性 i，中央计算单元随机选择 $y_i,k_i\in\mathbb{Z}_r$，计算出属性对应的公钥对 $\{Y_i=y_iG,K_i=k_iG\}$ 并广播至整个系统。

3.2　注册阶段

在这个阶段，为 SWC 分配 GID 与属性密钥，实现设备合法性验证与身份绑定，如图 2 所示。

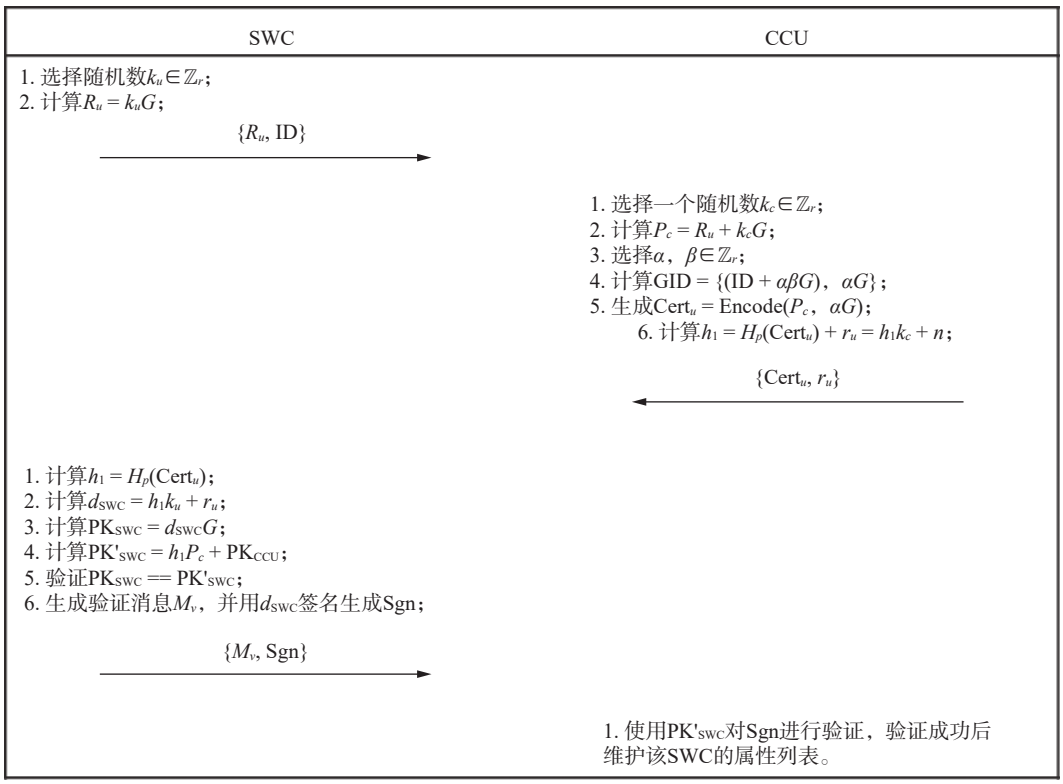

图 2　注册阶段

Fig. 2　Registration phase

1）SWC 随机选择 $k_u \in \mathbb{Z}_r$，并计算认证公钥 $R_u = k_u G$，向 CCU 发送{R_u,ID}进行注册。

2）CCU 接收到注册请求后，随机选择 $k_c \in \mathbb{Z}_r$，并计算 $P_c = R_u + k_c G$。然后随机选择 $\alpha,\beta \in \mathbb{Z}_r$，计算群元素 $\alpha\beta G$，并将其与设备身份 ID 绑定，生成设备的全局唯一标识，GID = $\{H(\mathrm{ID}\|\alpha\beta G), \alpha G\}$。其中 $H(\cdot)$为抗碰撞哈希函数，‖表示字符串拼接操作。GID 的第一部分通过哈希将身份与随机群元素绑定，确保全局唯一性与不可伪造性；第二部分 αG为后续密钥分发的公告参数。对 P_c和GID编码得到 CCU 的证书Cert_u，对 Cert_u进行哈希得到 h_1。CCU 计算 $r_u = h_1 k_c + n$，并把{Cert_u, r_u}发给请求注册的 SWC。

3）收到消息后，SWC 对Cert_u哈希得到h_1。SWC 计算私钥 $d_{\mathrm{SWC}} = h_1 k_u + r_u$，公钥 $\mathrm{PK}_{\mathrm{SWC}} = d_{\mathrm{SWC}} G$。SWC 对 Cert_u解码后得到 P_c和 GID，计算 $\mathrm{PK}'_{\mathrm{SWC}} = h_1 P_c + \mathrm{PK}_{\mathrm{CCU}}$，并判断$\mathrm{PK}_{\mathrm{SWC}} = \mathrm{PK}'_{\mathrm{SWC}}$是否成立。如果成立，SWC 将 GID作为其在系统中的全局标识符。然后，生成验证消息 M_v，并用私钥 d_{SWC}签名生成Sgn，将应答 ack = {M_v,Sgn}发送给 CCU。

4）接收到 ack后，CCU 用 SWC 的公钥$\mathrm{PK}_{\mathrm{SWC}}$进行验证，如果验证成功，CCU 在属性列表中记录该 SWC 的GID以及其属性，否则重新执行此过程。

3.3 密钥请求阶段

在这个阶段，SWC 向 CCU 发起生成属性密钥的请求，如图 3 所示。

1）SWC 将证书{Cert_u}发送给 CCU。

2）CCU 解码得到P_c和GID，计算$\mathrm{PK}'_{\mathrm{CCU}} = \mathrm{PK}_{\mathrm{SWC}} - H_p(\mathrm{Cert}_u)P_c$。根据$\mathrm{PK}'_{\mathrm{CCU}} = \mathrm{PK}_{\mathrm{CCU}}$是否成立，判断GID是否正确。如果GID有效，CCU 用β提取 SWC 的ID。根据属性列表为 SWC 生成其拥有的属性 $i \in S$ 的密钥 $\mathrm{SK}_{i,\mathrm{GID}} = y_i + H(\mathrm{GID})k_i$。同样将证书{$\mathrm{Cert}_u$}发送给 SWC。

（3）SWC 收到证书Cert_u后，计算$\mathrm{PK}''_{\mathrm{CCU}} = \mathrm{PK}_{\mathrm{SWC}} - H_p(\mathrm{Cert}_u)P_c$，并判断$\mathrm{PK}''_{\mathrm{CCU}} = \mathrm{PK}_{\mathrm{CCU}}$是否成立，以决定是否接收密钥$\mathrm{SK}_{i,\mathrm{GID}}$。

3.4 数据加密与发布阶段

在这个阶段，传感单元设置访问策略对数据进行加密并发布，如图 4 所示。

1）传感单元随机选择对称密钥k_0，使用对称加密算法对原始数据 PT加密生成密文$\mathrm{CT} = \mathrm{Enc}(\mathrm{PT})_{k_0}$。传感单元对CT哈希后使用其私钥$\mathrm{SK}_s$进行签名，生成签名$\sigma = \mathrm{Sign}_{\mathrm{SK}_s}(H_p(\mathrm{CT}))$。

2）传感单元根据系统属性集合S设置访问控制策略(A,ρ)。将访问策略转化为$a \times b$阶 LSSS 矩阵$(\boldsymbol{B},\rho)$。映射函数ρ将属性映射到矩阵的行，如$\rho_1,\rho_2,\cdots,\rho_a$。

3）传感单元随机选择 $s \in \mathbb{Z}_r$，向量 $\boldsymbol{v} = (s, v_1, v_2, \cdots, v_b)$，计算$\lambda_x = B_x \boldsymbol{v}$。随机选择$\boldsymbol{u} = (0, u_1, u_2, \cdots, u_b)$，计算$\omega_x = B_x \boldsymbol{u}$。

4）为安全封装对称密钥k_0，计算 $C_0 = sG, C_1 = k_0 \oplus H_p(sG)$。密文组件为：$C_{1,x} = \lambda_x G + Y_i, C_{2,x} = \omega_x G + K_i$。其中，$Y_i = y_i G, K_i = k_i G$为属性公钥。传感单元将密文$\mathrm{CT}_s = \{C_0, C_1, C_{1,x}, C_{2,x}, CT, \sigma\}$发布到 DDS 中间件的主题中。

5）CT_s发布前，CCU 对密文CT哈希得到$H_p(\mathrm{CT})$，用传感单元的公钥PK_s对签名σ进行验证后，确认合法性后写入中间件，否则丢弃。

3.5 数据解密阶段

在这个阶段，SWC 通过属性密钥解密密文，如图 5 所示。

1）SWC 订阅感兴趣的主题，从 DDS 中间件获取密文$\mathrm{CT}_s = \{C_0, C_1, C_{1,x}, C_{2,x}, CT, \sigma\}$。

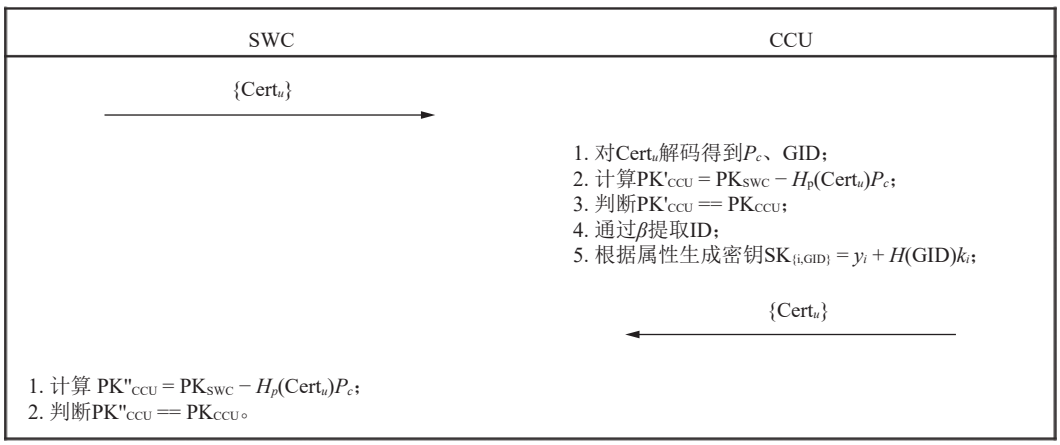

图 3 密钥请求阶段

Fig. 3 Key request phase

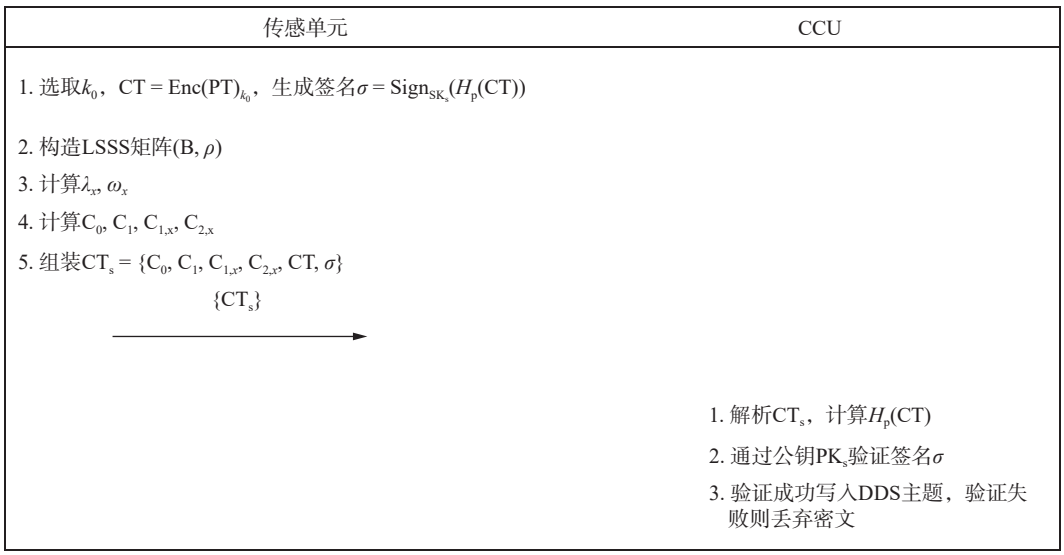

图 4　数据加密与发布阶段流程

Fig. 4　Data encryption and publishing phase process

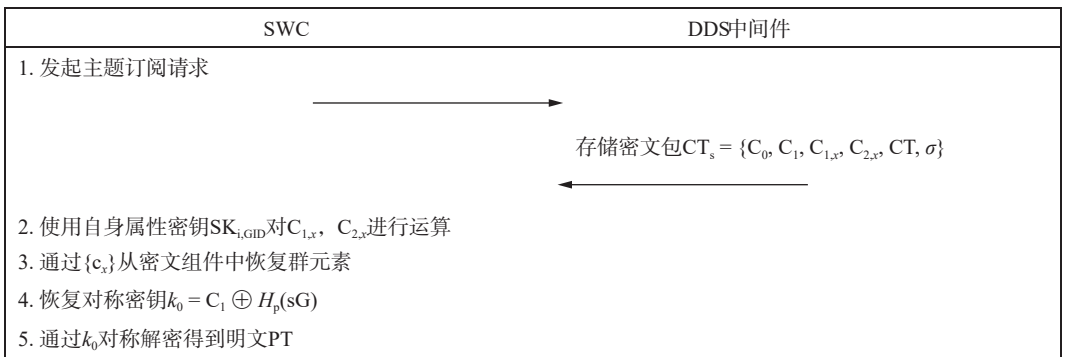

图 5　数据解密阶段流程

Fig. 5　Data decryption phase process

（2）SWC 利用自身的属性密钥 $SK_{i,GID}$ 对 $C_{1,x}$，$C_{2,x}$ 执行以下运算：$C_{1,x} - SK_{i,GID} \cdot G + C_{2,x} \cdot H(GID) = \lambda_x G + \omega_x G \cdot H(GID)$。

3）SWC 通过常数 $\{c_x\}$ 计算 $\sum_x c_x(\lambda_x G + \omega_x G \cdot H(GID)) = sG$，即从密文组件中恢复出 sG。

4）利用 sG 恢复对称密钥：$k_0 = C_1 \oplus H_p(sG)$。

5）获得 k_0 后，SWC 用其解密密文 CT，还原出原始数据：$PT = Dec(CT)_{k_0}$。

3.6　属性撤销阶段

当系统检测到 SWC 的权限发生变更或传感单元存在安全风险时，CCU 将触发属性撤销机制，如图 6 所示。

1）CCU 为被撤销属性 i 重新生成属性密钥参数。随机选择新的 $y_i', k_i' \in \mathbb{Z}_r$，计算新的属性公钥 $Y_i' = y_i' G$，$K_i' = k_i' G$ 并广播至系统。

2）CCU 根据 SWC 的 GID，为未被撤销的合法 SWC 更新属性密钥：$SK_{i,GID}' = y_i' + H(GID) \cdot k_i'$。同时更新系统属性列表，移除被撤销实体的相关权限。

3）传感单元无需对原始数据 PT 重新加密，仅需根据新属性公钥更新与撤销属性相关的密文组件：$NC_{1,x} = \lambda_x G + Y'_{\rho(x)}$，$NC_{2,x} = \omega_x G + K'_{\rho(x)}$。其中，$\rho(x)$ 为 LSSS 矩阵行对应的属性。

4）构造新密文结构：$CT_{s_{new}} = \{C_0, C_1, NC_{1,x}, NC_{2,x}, CT, \sigma\}$。

5）传感单元将 $CT_{s_{new}}$ 发布至 DDS 主题，合法 SWC 使用更新后的属性密钥即可正常解密，被撤销属性的 SWC 因密钥不匹配无法恢复 sG，进而无法获取对称密钥 k_0 与原始数据。

4　分析与性能评估

4.1　安全性分析

本文采用选择集模型分析所提方案的安全性。

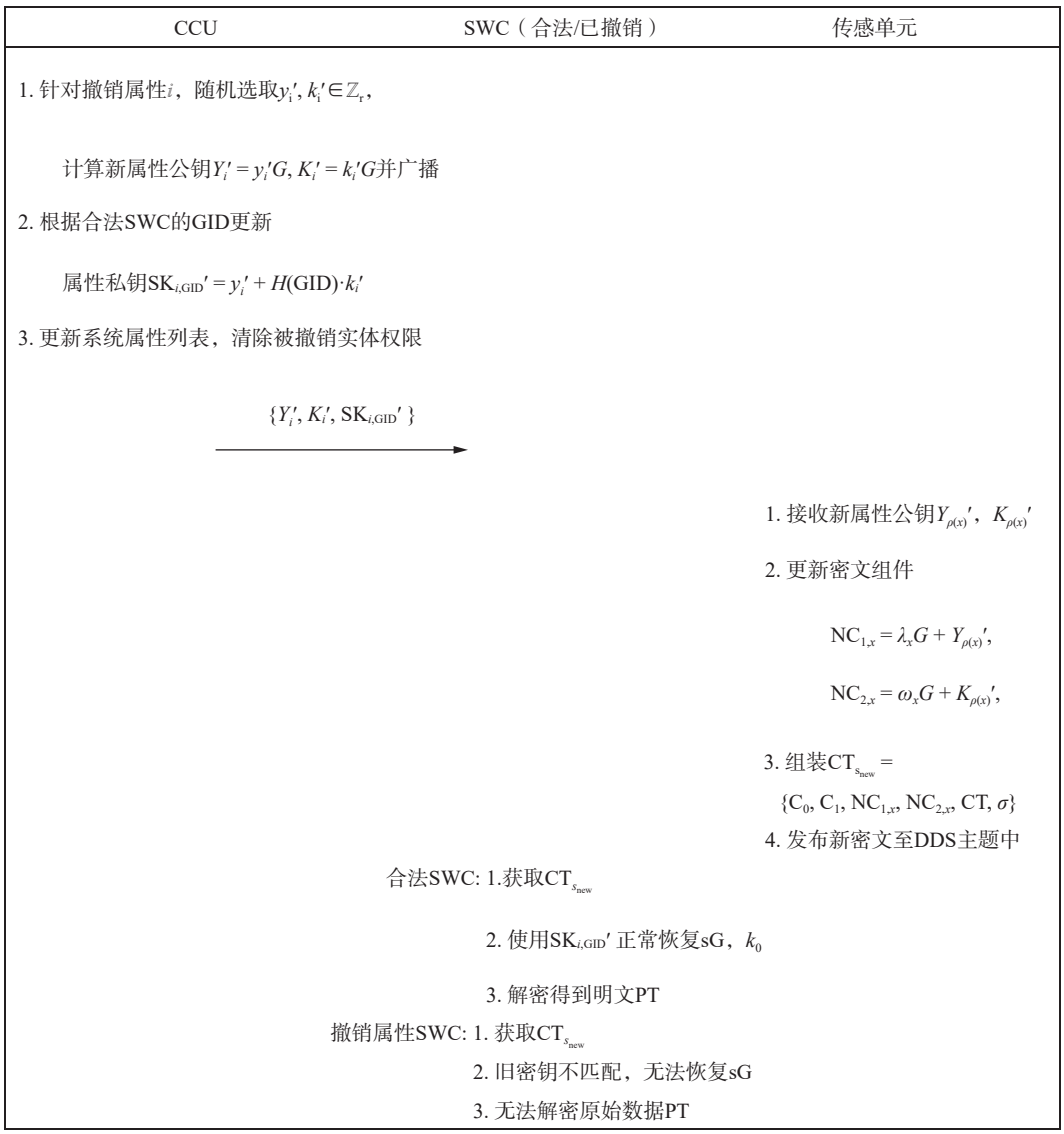

图 6 属性撤销阶段流程

Fig. 6 Attribute revocation phase process

攻击者在游戏开始时选择一个目标属性集，目的是区分两个被加密消息。本文方案的安全性基于 CDH 问题，即攻击者无法区分给定三元组(A,B,Z)是否满足$Z=abG$或是随机值，从而保证本文方案在选择明文攻击下的不可区分性。

定理 1 若存在一个多项式时间的攻击者$\mathcal{A}$，能够在选择集模型下以不可忽略的优势ε破解本文方案，则存在一个模拟器$\mathcal{B}$能够以优势$\varepsilon/2$解出椭圆曲线判定 Diffie-Hellman（elliptic curve decisional diffie-hellman，ECDDH）的问题。

初始化：挑战者在有限域F_p上定义椭圆曲线，选定生成元G，建立q阶循环群G_E。然后随机选择$a,b,z \in \mathbb{Z}_q^*$，并抛掷硬币$\mu \in \{0,1\}$。若$\mu=0$，设三元组$(A,B,Z)=(aG,bG,abG)$，为合法的 ECDDH 实例；若$\mu=1$，设$Z=zG$，则三元组为$(A,B,Z)=(aG,bG,zG)$，为随机实例。

设置阶段：模拟器$\mathcal{B}$根据敌手$\mathcal{A}$预先选定的目标属性集合$\theta \in U$构造系统公钥。首先设系统主公钥$Y=A=aG$。然后对于每个属性$i \in U$。若$i \in \theta$，则随机选择$r_i \in \mathbb{Z}_q^*$，设置$Y_i = r_iG$；若$i \notin \theta$，则随机选择$\beta_i \in \mathbb{Z}_q^*$，设置$Y_i = \beta_i \cdot B = \beta_i bG$。最后，模拟器$\mathcal{B}$将系统公钥参数$\{Y, Y_i | i \in U\}$返回给敌手$\mathcal{A}$。

阶段 1：敌手$\mathcal{A}$可以请求任意不满足目标属性集θ的访问结构γ，即$\gamma(\theta)=0$。模拟器$\mathcal{B}$为访问树中每个节点u分配秘密多项式$Q_u(x)$，并为每个叶节点x构造私钥份额：

$$D_x = \begin{cases} Q_x(0)/r_i, & \text{attr}(x) \in \theta \\ Q_x(0)/(\beta_i b), & \text{attr}(x) \in \theta \end{cases}, \quad i = \text{attr}(x)。$$

挑战：敌手$\mathcal{A}$提交两个等长明文M_0，M_1。模拟器$\mathcal{B}$随机掷硬币$v\in\{0,1\}$，并用目标属性集θ加密消息M_v。模拟器$\mathcal{B}$随机选择$k\in\mathbb{Z}_q^*$，计算$C'=k\cdot Y=k\cdot A=kaG$；对于每个$i\in\theta$，计算$C_i=r_i\cdot B=r_ibG$；设K_x为消息M的加密密钥，K_y为消息M的完整性密钥。构造密文$C=\mathrm{ENC}(M_v,K_x)$，并计算完整性标签$\mathrm{MAC}_{M_v}=\mathrm{HMAC}(M_v,K_y)$。向敌手$\mathcal{A}$发送密文$(C',C,\mathrm{MAC}_{M_v},\{C_i\})$作为挑战。若$\mu=0$，即$Z=abG$，则$C'=Z$，密文为合法加密；若$\mu=1$，则$C'=zG$，对应随机密文，敌手$\mathcal{A}$无法区分。

阶段 2：敌手$\mathcal{A}$继续请求不满足目标属性集θ的私钥，模拟器$\mathcal{B}$重复阶段 1 进行模拟。

猜测：敌手$\mathcal{A}$输出猜测值$v'\in\{0,1\}$判断挑战密文对应的明文。模拟器$\mathcal{B}$判断：若$v'=v$，认为三元组(A,B,Z)为合法 ECDDH 实例，输出$\mu'=0$；否则认为Z是随机元素，输出$\mu'=1$。

根据博弈，模拟器$\mathcal{B}$成功识别μ的概率如下：当$\mu=1$时，敌手$\mathcal{A}$无法获得任何信息，故$\Pr[v\neq v'\mid\mu=1]=\Pr[v=v'\mid\mu=1]=1/2$，有$\Pr[\mu'=\mu\mid\mu=1]=1/2$；当$\mu=0$时，敌手$\mathcal{A}$的优势记为$\varepsilon$，则$\Pr[v=v'\mid\mu=0]=1/2+\varepsilon$，有$\Pr[\mu'=\mu\mid\mu=0]=1/2+\varepsilon$。因此，根据 ABE 的选择集模型，模拟器$\mathcal{B}$在 ECDDH 博弈中的整体成功概率为$\Pr[\mu'=\mu]=\frac{1}{2}\left(\frac{1}{2}+\varepsilon\right)+\frac{1}{2}\times\frac{1}{2}=\frac{1}{2}+\frac{\varepsilon}{2}$。即模拟器$\mathcal{B}$以不可忽略的$\frac{\varepsilon}{2}$成功区分 ECDDH 三元组，从而违反了 ECDDH 假设

本文方案的安全性基于以下统一安全假设：①椭圆曲线离散对数问题与椭圆曲线判定性 Diffie-Hellman 问题在多项式时间内难以求解；②中央计算单元为完全可信实体；③DDS 通信链路存在被动窃听、重放等攻击行为，本文方案侧重实现数据机密性、完整性与访问控制安全，不针对链路层进行防护。

1）抗假冒攻击：注册阶段通过双向签名验证与公钥一致性校验，确保只有合法实体能够完成注册并获取属性密钥。中央计算单元、软件组件与传感器间的通信，均通过签名和哈希验证完成身份校验。

2）抗窃听攻击：传感器采用对称加密与 CP-ABE 相结合的双重加密机制，仅属性匹配访问策略的软件组件可恢复对称密钥。攻击者仅通过窃听无法获取明文，保证车内数据的机密性。

3）抗重放攻击：协议交互引入随机数、证书时效性校验与数字签名机制，保证消息唯一性。攻击者截获的消息无法重复使用，重放消息会在验证阶段被直接拒绝。

4）抗合谋攻击：属性密钥与软件组件的 GID 相互绑定，即使多个软件组件合谋，也无法拼接出未授权属性对应的密钥，进而不能访问超出自身权限的数据。

4.2　性能分析

本文性能分析在统一安全强度与安全目标下开展。本文方案采用 secp256r1 椭圆曲线（经典安全强度 128 位）与 AES-256 算法（后量子安全强度等效为 128 位）。所有性能优化均以满足机密性、完整性、抗假冒、抗重放、抗合谋等安全要求为前提，未降低安全强度，保障实验对比的公平性。

4.2.1　计算开销

实验采用树莓派 5 模拟中央计算单元，采用 S32K344 MQFP172 开发板模拟域控制器（DC）。树莓派搭载 64 位 ARM 架构处理器，主频为 2.4 GHz。S32K344 MQFP172 开发板基于 ARM Cortex-M7 内核，主频为 160 MHz。基于大整数与有理数运算密码库（multiprecision integer and rational arithmetic cryptographic library，MIRACL）[34]，本文采用 C 语言实现各类加密算法，对算法运算耗时重复测试 100 次，表 1 为各密码操作的平均执行时间。

表 1　各密码操作的平均执行时间

Table 1　Average execution time of each cryptographic operations

描述	符号	开发板执行时间/ms	树莓派执行时间/ms
AES-256	T_a	0.437	0.012
RSA-512加密	T_{renc}	2.855	0.049
RSA-512解密	T_{rdec}	37.129	0.926
SHA256	T_{hash}	0.069	0.008
HMAC(SHA256)	T_{hmac}	0.194	0.011
椭圆曲线点加	T_{add}	0.182	0.004
椭圆曲线标量乘	T_{sm}	26.274	0.476
算术乘法	T_{m}	0.004	0.001
模逆运算	T_{mi}	5.935	0.006
RSA-512签名	T_{sign}	38.214	0.946
RSA-512验签	T_{cert}	2.553	0.063

实验所用密码学参数设置如下：对称加密算法选用 AES-256，密钥长度 256 bit；哈希函数选用 SHA-256，输出长度 256 bit；消息认证码选用 HMAC-SHA256，输出长度 256 bit；椭圆曲线密码基于 secp-

表 2 各方案计算开销对比

Table 2 Comparison of computation overhead for each scheme

方案	CCU计算开销/ms	安全代理计算开销/ms	数据发布者计算开销/ms	数据接收者计算开销/ms	总计算开销/ms
文献[6]	$3.358t_A+0.182n_st_R$	$0.313+0.694t_L+0.500t_R$	$1.122+0.583t_L$	$0.113+0.331t_R$	$1.548+3.358t_A+1.277t_L+(0.831+0.182n_s)t_R$
文献[7]	$6.785+3.176t_A+3.609t_R$	$0.444+0.642t_A+0.020t_R$	$3.282+1.306t_A+0.020t_R$	$1.695+0.166t_R$	$12.206+5.124t_A+3.815t_R$
文献[8]	$0.442n_s$	-	$0.065n_s+1.115$	0.218	$0.507n_s+1.333$
本文	$0.004+0.008t_A+3.346n_s+2.622n_p+0.008t_c+0.255t_L$	-	$3.358+1.912t_c+0.476t_L$	$2.875+0.956t_R$	$6.237+0.008t_A+3.346n_s+2.622n_p+1.920t_c+0.731t_L+0.956t_R$

表 3 控制信令阶段通信开销对比

Table 3 Communication overhead comparison in control signaling phase

方案	CCU通信开销/byte	SWC通信开销/byte	总通信开销/byte
文献[6]	$2l_{\mathrm{id}}+l_h$	$l_p+l_{\mathrm{id}}+l_{\mathrm{ts}}+l_{\mathrm{hmac}}$	96
文献[7]	$l_{p_{\mathrm{id}}}+l_{\mathrm{cip}}+l_h$	$l_{\mathrm{hmac}}+l_r$	112
文献[8]	$l_{\mathrm{ts}}+l_r+l_{\mathrm{hmac}}$	$l_{\mathrm{cip}}+l_{\mathrm{hmac}}$	96
本文	$l_{\mathrm{hmac}}+l_{p_{\mathrm{id}}}+l_h$	$l_{p_{\mathrm{id}}}+l_{\mathrm{id}}$	84

256r1 曲线实现，椭圆点坐标采用未压缩格式，单个群元素长度 512 bit；RSA 算法模数长度设为 512 bit，用于完成对照组的签名与验证操作。

假设t_A是系统中属性总数，t_L是访问策略树中叶节点个数，t_R是 SWC 的属性个数，t_c是撤销的属性个数，n_s是 SWC 个数，n_p是传感单元个数。在本文方案中，CCU 的计算开销为$0.004+0.008t_A+3.346n_s+2.622n_p+0.008t_c+0.255t_L$。SWC 的计算开销为$2.875+0.956t_R$。传感单元的计算开销为$3.358+1.912t_c+0.476t_L$。表 2 给出各方案的计算开销对比。

本文设置t_A、t_L、t_R从 5，10，15，20，25 递增，固定 SWC 和传感单元个数为 5。图 7 是各方案计算开销对比，可以看出随着属性数量的增加，本文方案与文献 [8]（不是基于属性的访问控制）的增长趋势相近。但对比同为属性加密的文献 [6-7]，本文方案有着较低的时间开销。

4.2.2 通信开销

结合文献 [6-8] 对本文方案的通信开销进行分析。为保证开销计算的一致性，本文统一设置以下参数长度。假名、哈希值、HMAC 值和随机数长度设置为$l_{p_{\mathrm{id}}}=l_h=l_{\mathrm{hmac}}=l_r=160$ bit。身份标识、时间戳长度设置为$l_{id}=l_{ts}=32$ bit。椭圆曲线群元素长度为320 bit。对称密钥长度为256 bit。对称密文长度为$l_{\mathrm{cip}}=256$ bit。

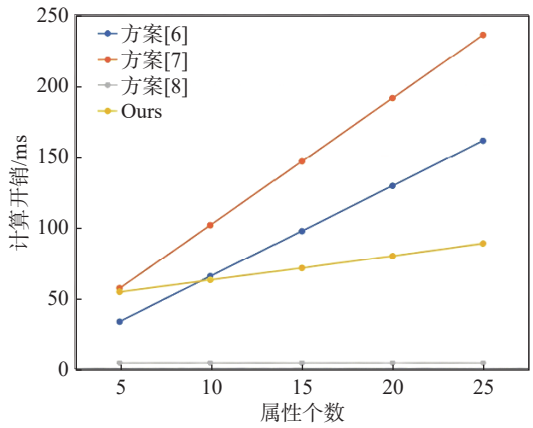

图 7 各方案计算开销对比

Fig. 7 Comparison of computation overhead for each scheme

表 3 统计了本文方案和相关方案在注册、密钥分发等控制信令阶段的通信开销，并与文献 [6-8] 中的方案进行了对比。结果表明，本文方案在控制信令阶段的通信开销显著低于对比方案。

除控制信令外，本文方案的密文由对称密钥封装组件、属性基加密群元素和数据签名 3 部分组成，

其长度随访问策略复杂度线性增长。对称密钥封装组件包含 1 个群元C_0和 1 个对称密钥封装值C_1，共 72 byte；属性基加密群元素中每个属性对应 2 个群元素$(C_{1,x},C_{2,x})$，共 80 byte，随属性数量t_L线性增长；数据签名包含 1 个群元素，共 40 byte。因此，单条数据密文的总长度$l_{\text{cipher}}=112+80\times t_L$(byte)。

5　结束语

本文结合轻量级椭圆曲线密码学与密文策略属性基加密机制，基于 DDS 构建主题驱动的数据访问模型，支持属性级动态撤销与密钥更新，兼顾系统的安全性、执行效率与可扩展性。本文从系统架构、密钥管理、数据加解密流程等方面完整阐述方案设计思路，并通过理论分析与实验评估，验证了方案在计算开销与通信性能上的优势。未来将在真实车载场景中开展端到端时延测试、多场景性能对比及大规模实验验证，进一步完善方案的性能评估体系。

参考文献：

[1] Lobello L，Patti G，Leonardi L. A perspective on ethernet in automotive communications：current status and future trends[J]. Applied Sciences，2023，13（3）：1278.

[2] Rodríguez M J，Bilbao S，Martínez B，et al. An optimized，data distribution service-based solution for reliable data exchange among autonomous underwater vehicles[J]. Sensors，2017，17（8）：1802.

[3] Frank F，Püllen D，Kampmann A，et al. Towards deterministic DDS communication for secure service-oriented software-defined vehicles[M]//Availability，Reliability and Security. Cham Springer Nature Switzerland，2025：186-208.

[4] Püllen D，Frank F，Christl M，et al. A security process for the automotive service-oriented software architecture[J]. IEEE Transactions on Vehicular Technology，2024，73（4）：5036-5053.

[5] 施文征，王成野. 用于资源有限设备的 DDS 通信中间件开发 [J]. 汽车实用技术，2024，49（11）：40-46.
Shi W Z，Wang C Y. Development of DDS communication middleware for resource-limited devices[J]. Automobile Technology，2024，49（11）：40-46.

[6] Yu D，Hsu R H，Lee J，et al. EC-SVC：secure CAN bus in-vehicle communications with fine-grained access control based on edge computing[J]. IEEE Transactions on Information Forensics and Security，2022，17：1388-1403.

[7] 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.

[8] Shang C，Cao J，Liu J J，et al. CEAMP：a cross-domain entity authentication and message protection framework for intra-vehicle network[J]. IEEE Transactions on Intelligent Transportation Systems，2024，25（7）：6780-6795.

[9] Rajkumar R R，Lee I，Sha L，et al. Cyber-physical systems：the next computing revolution[C]//Proceedings of the 47th Design Automation Conference. New York：ACM，2010：731-736.

[10] Bandur V，Selim G，Pantelic V，et al. Making the case for centralized automotive E/E architectures[J]. IEEE Transactions on Vehicular Technology，2021，70（2）：1230-1245.

[11] Hazem A，Fahmy H. LCAP-a lightweight CAN authentication protocol for securing in-vehicle networks[C]//10th Escar Embedded Security in Cars Conference，Berlin，Germany：Vol. 6. 2012：172.

[12] Groza B，Popa L，Murvay P S. Highly efficient authentication for CAN by identifier reallocation with ordered CMACs[J]. IEEE Transactions on Vehicular Technology，2020，69（6）：6129-6140.

[13] Xiao L，Lu X Z，Xu T W，et al. Reinforcement learning-based physical-layer authentication for controller area networks[J]. IEEE Transactions on Information Forensics and Security，2021，16：2535-2547.

[14] Ueda H，Kurachi R，Takada H，et al. Security authentication system for in-vehicle network[J]. SEI Technical Review，2015，81：5-9.

[15] Hu S T，Zhang Q Z，Weimerskirch A，et al. Gatekeeper：a gateway-based broadcast authentication protocol for the in-vehicle Ethernet[C]//Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security. New York：ACM，2022：494-507.

[16] Fassak S，El H Y，Zahid N，et al. A secure protocol for session keys establishment between ECUs in the CAN bus[C]//Proceedings of the 2017 International Conference on Wireless Networks and Mobile Communications（WINCOM）. Piscataway：IEEE Press，2017：1-6.

[17] Lodge N，Tambe N，Saqib F. Addressing vulnerabilities in CAN-FD：an exploration and security enhancement approach[J]. IoT，2024，5（2）：290-310.

[18] Feng Y，Qin G H，Zhang Z Z，et al. In-vehicle CAN bus security communication protocol based on identity encryption[C]//Proceedings of SPIE Conference on International Conference on

Computer Network Security and Software Engineering（CNSSE 2024），2024：150.

[19] Iorio M，Buttiglieri A，Reineri M，et al. Protecting in-vehicle services：security-enabled SOME/IP middleware[J]. IEEE Vehicular Technology Magazine，2020，15（3）：77-85.

[20] Ghosal A, Halder S, Conti M. Secure over-the-air software update for connected vehicles[J/OL]. Computer Networks, 2022. https://doi.org/10.1016/j.comnet.2022.109394.

[21] Lamanna M，Treccozzi L，Perazzo P，et al. Performance evaluation of attribute-based encryption in automotive embedded platform for secure software over-the-air update[J]. Sensors，2021，21（2）：515.

[22] Saidi A，Amira A，Nouali O. A secure multi-authority attribute based encryption approach for robust smart grids[J]. Concurrency and Computation：Practice and Experience，2024，36（7）：e7972.

[23] Yu S X，Cao Q，Wang C Y，et al. Efficient ECC-based conditional privacy-preserving aggregation signature scheme in V_2V[J]. IEEE Transactions on Vehicular Technology，2023，72（11）：15028-15039.

[24] Chen Y X，Zhang J，Wei X Y，et al. Cross-domain authentication scheme for vehicles based on given virtual identities[J]. IEEE Internet of Things Journal，2024，11（9）：15869-15879.

[25] Benyahya M，Lenard T，Collen A，et al. A systematic review of threat analysis and risk assessment methodologies for connected and automated vehicles[C]//Proceedings of the 18th International Conference on Availability，Reliability and Security. New York：ACM，2023：1-10.

[26] Luo F，Wang J J，Zhang X，et al. In-vehicle network intrusion detection systems：a systematic survey of deep learning-based approaches[J]. PeerJ Computer Science，2023，9：e1648.

[27] Devincenzi M, Pesé M, Bodei C, et al. Contextualizing security and privacy of software-defined vehicles: a literature review and industry perspectives[J/OL]. ACM Computing Surveys, 2026, https://doi.org/10.1145/3814955. https://dl.acm.org/doi/10.1145/3814955.

[28] Giraldo J，Sarkar E，Cardenas A A，et al. Security and privacy in cyber-physical systems：a survey of surveys[J]. IEEE Design & Test，2017，34（4）：7-17.

[29] Bhaskar S，Parmar K，Jinwala D C. Comparative evaluation of pairing-free and pairing-based CP-ABE schemes for resource constrained environments[J]. Cluster Computing，2025，28（7）：431.

[30] Boneh D. The decision Diffie-Hellman problem[M]//Algorithmic Number Theory. Berlin，Heidelberg Springer，1998：48-63.

[31] Shamir A. How to share a secret[J]. Communications of the ACM，1979，22（11）：612-613.

[32] Waters B. Ciphertext-policy attribute-based encryption：an expressive，efficient，and provably secure realization[M]//Public Key Cryptography – PKC 2011. Berlin，Heidelberg Springer，2011：53-70.

[33] Bethencourt J，Sahai A，Waters B. Ciphertext-policy attribute-based encryption[C]//Proceedings of the 2007 IEEE Symposium on Security and Privacy（SP '07）. Piscataway：IEEE Press，2007：321-334.

[34] Zhang X Y，Thakur N，Ogundepo O，et al. MIRACL：a multilingual retrieval dataset covering 18 diverse languages[J]. Transactions of the Association for Computational Linguistics，2023，11：1114-1131.