车联网边云协同下可搜索属性签密方法

俞惠芳*①② 王庆归① 王子豪①
①(西安邮电大学网络空间安全学院 西安 710121)
②(浙江大学区块链与数据安全全国重点实验室 杭州 310058)

摘 要：动态开放的网络环境使车联网难免遭受窃听、数据篡改和伪造，传统云计算因高延迟难以满足海量数据的实时性需求，安全性和性能之间固有冲突制约着车联网发展。为了解决上述问题，该文专为车联网设计出边云协同可搜索属性签密方法，可允许授权用户无须解密密文，就能通过云端快速匹配机制高效检索所需信息。利用边缘计算下沉计算能力到网络边缘，协同云服务器、边缘服务器和车载终端设备共同工作。通过属性签密和线性秘密共享机制的融合，实现车联网数据的细粒度访问控制，更好地保障数据的安全性。针对车载设备资源受限问题，将解签密过程中的复杂运算外包给高性能边缘节点处理，减轻了车载终端的运算负担且提升了响应速度，能够很好地适应车联网这种动态的资源受限复杂环境。

关键词：车联网边云协同；属性签密；关键词搜索；细粒度访问控制

中图分类号：TN915.08; TP309 **文献标识码**：A **文章编号**：1009-5896(2026)01-0001-09

DOI: 10.11999/JEIT250750 **CSTR**: 32379.14.JEIT250750

1 引言

车联网(Internet of Vehicles, IoV)在当前已成为智能交通系统的基石[1]。通过实现车与车、车与基础设施之间的数据交互，IoV提升了交通运行效率和道路安全。因高度动态开放的特性和涉及大量敏感通信，IoV在安全性与信任管理方面存在严峻挑战；这些潜在漏洞一旦被利用，可能会导致交通中断、车辆失控乃至威胁乘车人员生命安全[2]。因此，为了实现IoV在资源受限且高度动态环境中的可靠性与安全性，对数据安全保障和细粒度访问控制的需求十分迫切。

面对IoV的海量数据、实时性要求和车载设备资源受限的挑战，传统集中式云计算模式难以满足需求。下沉计算能力到网络边缘[3]成为解决这些问题的关键途径。边缘计算[4]作为一种新兴的分布式计算范式，核心是将传统集中式云数据中心的计算与数据存储能力下沉至网络边缘侧，使其更靠近数据生成的源头物理位置[5]。边云端架构[6]是融合云服务器、边缘服务器和各类终端设备为一体的边缘计算体系结构。IoV复杂生态系统中，边云协同架构在数据实时处理、计算任务分担和整体系统架构优化方面发挥着巨大作用。虽然边云协同架构为IoV提供了高效计算框架，但其在传输和存储过程中的数据安全和隐私保护问题仍未得到全面保障，尤其在实现精细化访问控制方面。在IoV环境中引入属性签密 (Attribute-Based SignCryption, ABSC)[7]，能够保障隐私安全、数据的完整性和更为灵活的数据共享机制。

文献[8]专为电子医疗提出基于属性的可搜索签密方法，实现了去中心化细粒度访问控制，但在大规模部署中的复杂性值得探究。文献[9]提出支持等值测试的轻量级属性广播签密方法，实现了对数据的细粒度访问控制并通过外包计算减轻了用户端计算负担，但未提供对消息的可搜索功能。文献[10]提出基于云计算的属性签密方法，有效保护了数据隐私，通过云服务器辅助解密和验证数据完整性，但密钥生成效率较低，算法设计中的复杂运算导致整体计算效率有所下降。文献[11]提出基于区块链属性签密的安全数据共享方法，解决了传统云存储模式中数据可用性和中心化存储的问题，但未使用外包计算模式，导致本地用户面临巨大计算压力。文献[12]提出基于国密SM9的边云协同属性签密方法，引入边云协同模式减轻本地用户的计算压力，但密钥设计存在冗余问题。文献[13]提出基于区块链的属性可撤销签密方法，实现了密钥的去中心化生成与分发，部分加解密和验证计算外包给雾节点，智能合约部署和互操作性等带来系统复杂性。

综上，现有研究在车联网应用中仍存在局限性：文献[9,10,12,13] 采用外包计算机制减轻终端

收稿日期：2025-08-07；改回日期：2025-10-31；网络出版：2025-12-19
*通信作者： 俞惠芳 yuhuifang@xupt.edu.cn
基金项目：陕西省自然科学基础研究计划(2025JC-YBMS-652, 2025JC-YBMS-676)，浙江大学区块链与数据安全全国重点实验室开放课题(A2510)
Foundation Items: The Natural Science Basis Research Projects of Shannxi Province (2025JC-YBMS-652, 2025 JC-YBMS-676), The Open Project of the State Key Laboratory of Blockchain and Data Security, Zhejiang University (A2510)

负荷，但其在功能和效率上普遍未能实现完备性。文献[9–11]缺乏关键词密文搜索功能，忽略IoV数据高效检索的关键需求。文献[12]在密钥设计、安全性、外包效率上仍有优化空间。目前很少有能同时满足细粒度属性访问控制、关键词密文搜索和高效计算外包这3项IoV应用核心需求的技术方案，也缺乏对资源受限车载终端进行深度优化的体系结构。

本文专为IoV环境打造边云协同可搜索属性签密方法。通过实现上述3项IoV应用需求，本方案不仅保障了数据的安全性，且授权用户在无须解密的情况下可快速检索信息。同时通过边缘节点与云服务器的协作，复杂耗时的计算任务转移到边缘侧处理，降低了车载终端的计算压力。因此，本文方法为IoV实现更强隐私保护和高效访问控制提供了可行技术路径。主要贡献：(1) 属性签密技术减少了证书验证的开销，实现了IoV数据的细粒度访问控制和安全性，可抵御窃听、数据篡改、身份伪造等恶意攻击。(2) 充分利用边缘节点的高并发与高计算性能，将解签密中计算复杂度最高的$O(n)$级双线性对运算外包给边缘节点处理，使得用户在本地只需执行简单运算即可完成最终解签密，加快了IoV环境下各方交互的响应速度，尤其适用于资源受限的轻量级车载设备，实现了优于同类外包方案的本地计算性能，该优势已通过计算外包效率指标量化证明。(3) 引入关键词可搜索功能，允许数据使用者在不解密的情况下，根据关键词请求查询，通过云端匹配机制检索所需密文。为了确保搜索过程的安全性，陷门信息不可伪造性依赖于SM9签名的安全假设[14]。本文通过单向哈希索引，使海量数据下查找操作仅需$O(1)$的时间复杂度，此设计在保持关键词隐私和不可伪造性的前提下，为IoV大规模密文数据的即时检索难题提供了有效解决方案。

2 预备知识

2.1 双线性映射

假设p是大素数，G_1,G_2,G_{T}都是阶为p的循环乘法群，P_1,P_2分别是G_1,G_2的生成元，双线性映射$e\colon G_1\times G_2\to G_{\mathrm{T}}$ 满足下列条件：(1)对于任意的 $a,b\in Z_p$，满足$e(aP_1,bP_2)=e(P_1,P_2)^{ab}$；(2)至少存在一对元素$P_1\in G_1,P_2\in G_2$，满足$e(P_1,P_2)\neq 1$；(3) $e(P_1,P_2)$可通过多项式时间算法高效计算。

本文方法的安全性依赖于下列两个公认的困难性问题。

(1)判定双线性Diffie-Hellman (Decisional Bilinear Diffie-Hellman, DBDH)问题：对于任意的$a,b,c\in Z_p^*,R\in G_{\mathrm{T}}$，给定一个随机元组$(P^a,P^b,P^c,Q^a,Q^b,Q^c,e(P,Q)^{abc},Z\in G_{\mathrm{T}})$，如果没有任何多项式时间算法能够以超过可忽略优势$\varepsilon$判定$Z$是否等同于$e(P,Q)^{abc}$(而非随机元素$R$)，则称DBDH问题是困难的。

(2)q-SDH(q-Strong Diffie-Hellman)问题：对于任意的$a\in Z_p^*$，随机选择$c\in Z_p^*$，提供由$q+2$个元素构成的元组$(P,Q,aQ,a^2Q,\cdots,a^qQ)$，如果没有任何多项式时间算法能够以超过可忽略优势$\varepsilon$计算$(c,(1/(c+a)P)$，则称 q-SDH问题是困难的。

2.2 线性秘密共享方案

线性秘密共享方案(Linear Secret Sharing Scheme, LSSS) 安全分发秘密$s\in z_r$ 给多个参与者，秘密s嵌入到随机向量$\boldsymbol{v}=(s,v_1,v_2,\cdots,v_m)$，与预定义共享矩阵$\boldsymbol{A}$的每行$\boldsymbol{A}_x$线性映射$(\boldsymbol{A}_x\cdot\boldsymbol{v})\to\lambda_x$生成每个参与者持有的股份$\lambda_x$。LSSS的访问结构由$l\times m$共享矩阵$\boldsymbol{A}$和属性映射函数$\rho(x)$精确定义，确保只有满足预设授权属性的参与者集合，才能通过其持有 λ_x和特定常数$c_x\in z_r$线性求和：$s=\sum_{x\in[1,2,\cdots,l]}c_x\cdot\lambda_x$，重构出原始秘密。

访问结构基于有限参与实体集合$P=\{P_1,P_2,\cdots,P_n\}$，精确定义了秘密共享和访问控制中哪些参与者集合被授权访问或重构秘密。访问结构M被定义为P的非空子集所组成的集合，满足单调性：对于任意的$B,C\subseteq P$，如果 $B\in M$且$B\subseteq C$，$C\in M$必然成立。此定义下，属于M的集合被称为授权集；反之，称为非授权集。访问结构的设计精确规定了具备合作恢复秘密权限的参与者群体，可有效实现细粒度的访问控制策略。

3 系统模型

基于本文方法的系统模型如图1所示。核心实体协同完成系统各项安全与功能需求。可信机构(Trusted Authority, TA)负责系统初始化配置和全局密钥的管理；车载单元(On-Board Unit, OBU)用于车载环境中生成数据和加密操作；云服务器(Cloud Server, CS)承担密文集中存储和基于关键词的加密检索任务；边缘服务器(Edge Server, ES)提供部分解密服务，分担云端计算，提升整体响应效率；数据使用者(Data User, DU)完成解密和信息获取。

实体协作过程：(1)TA设定系统参数并初始化公私钥对。(2)OBU与DU向TA注册身份标识，TA生成并分发绑定其身份的公私钥。(3)OBU采集实时数据，根据设定访问策略执行属性签密操作生成密文；同时针对消息内容提取对应关键词且生成关键词密文并计算相应索引标识符。OBU关联绑定消息密文和相应关键词密文且上传到CS。(4)DU选

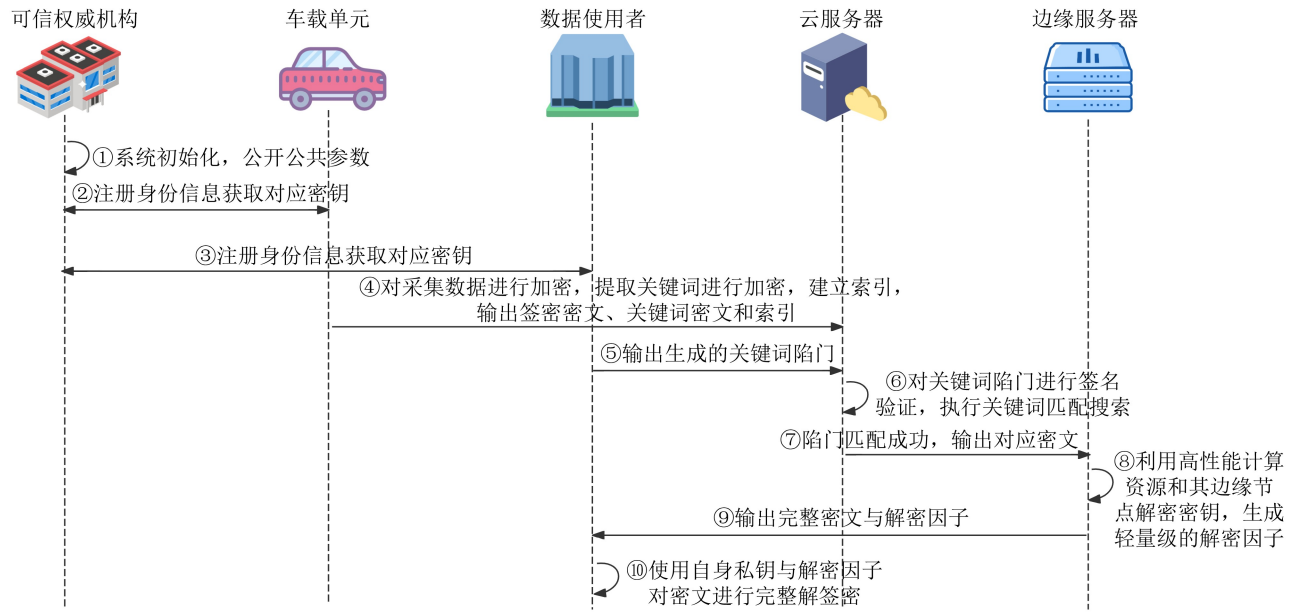

图 1 基于本文方法的系统交互流程

择想要查询消息的关键词，通过SM9签名生成认证陷门且提交给CS请求查询。(5)CS先验证收到的陷门，随后在云端存储的关键词哈希表中检索。如果匹配成功，转发对应的签密密文给ES。(6)ES使用验证密钥，针对签密密文执行部分解密操作，输出解密因子给DU。(7)DU使用自身私钥与解密因子在本地完成最终解密，恢复出明文并验证其完整性与OBU身份合法性。

4　边云协同下可搜索属性签密方法

4.1　系统初始化

TA定义双线性群参数(请见2.1节)，随机选择主私钥$\alpha \in Z_p^*$，计算主公钥$\mathrm{PK}=[\alpha]P_1$。设置固定长度的函数标识符 hid。选取安全哈希函数：$H_1\colon \{0,1\}^* \to Z_p^*$，$H_2\colon \{0,1\}^* \to Z_p^*$，$H_3\colon \{0,1\}^* \to G_2$，$H_4\colon G_{\mathrm{T}} \to \{0,1\}^{\lambda}$，安全参数 λ 的比特串长度是128。TA公布公共参数$\varphi=\{G_1,G_2,G_{\mathrm{T}},e,p,H_1\sim H_4,P_1,P_2,\mathrm{hid},\mathrm{PK}\}$。

4.2　密钥生成阶段

OBU的用户身份标识是ID_i，DU的用户身份标识是$\mathrm{ID}_{\mathrm{DU}}$，用户的属性集合$A=\{A_1,A_2,\cdots,A_l\}$，预设的签名策略是$(\boldsymbol{S},\rho)$。TA随机选择$s\in Z_p^*$ 作为$(\boldsymbol{S},\rho)$的秘密值，选择$s,r_2,\cdots,r_d\in Z_p^n$ 构成列向量$\boldsymbol{v}_s=(s,r_2,\cdots,r_d)$。TA计算每个属性$A_i$对应的秘密值份额$\lambda_i=\boldsymbol{S}_i\times\boldsymbol{v}_s$；选择$\beta\in Z_p^*$作为后续计算的中间参数。

(1)OBU的私钥：$\mathrm{SK}_i=\left[\dfrac{\lambda_i\cdot\alpha}{H_1(\mathrm{ID}_i||\mathrm{hid})+\alpha}\right]P_1$；公钥：$\mathrm{PK}_i=\left[\dfrac{H_1(\mathrm{ID}_i||\mathrm{hid})+\alpha}{s}\right]P_2$。

(2)DU的私钥：$\mathrm{SK}_{\mathrm{DU1}}=\left[\dfrac{\alpha\cdot(\beta+1)}{H_1(\mathrm{ID}_{\mathrm{DU}}||\mathrm{hid})+\alpha}\right]P_2$，$\mathrm{SK}_{\mathrm{DU2}}=\left[\dfrac{\alpha}{H_1(\mathrm{ID}_{\mathrm{DU}}\,\|\,\mathrm{hid})+\alpha}\right]P_1$；公钥：$\mathrm{PK}_{\mathrm{DU}}=[\alpha]P_2$。

(3)边缘节点的私钥：$\mathrm{SK}_1=[\alpha\cdot\beta]P_1$，$\mathrm{SK}_2=[\alpha\cdot\beta\cdot H_2(A_i)]P_1$。

4.3　签密阶段

输入消息$m\in\{0,1\}^*$、加密策略$(\boldsymbol{M},\rho)$、用户属性集合A、公共参数 φ、关键词$m_k\in\{0,1\}^*$。OBU选择随机数$d\in Z_p^*$ 作为访问结构$(\boldsymbol{M},\rho)$的秘密值，$\rho(i)$是属性A_i在G_2的映射。OBU操作如下：

(1)选择$s,r_2,\cdots,r_d\in Z_p^n$构成列向量$\boldsymbol{v}_s=(s,r_2,\cdots,r_d)$，计算每个属性$A_i$对应的秘密值份额$\lambda_i=\boldsymbol{M}_i\times\boldsymbol{\nu}_s$；计算$g=e(\mathrm{PK},P_2)$，$w=e(P_1,P_2)^{\alpha\cdot d}$；选择$\mu_1,\mu_2,\cdots,\mu_l\in Z_p^*$，构造密文分量$C_i=[\lambda_i+\mu_i\cdot H_2(A_i)]P_2$，随机因子$C_i'=[\mu_i]P_2$，计算 $Q=H_1(\mathrm{ID}_{\mathrm{DU}}\,\|\,\mathrm{hid})P_1+\mathrm{PK}$，$C_1=[d]Q$。

(2)通过密钥派生函数(KDF)计算得到对称加密密钥K_1和消息认证密钥K_2：$K_1\,\|\,K_2=\mathrm{KDF}(C_1\,\|\,w\,\|\,\mathrm{ID}_{\mathrm{DU}},\mathrm{ln})$，密钥总长度 $\mathrm{ln}=\mathrm{len1}+\mathrm{len2}$，len1和len2分别是$K_1$和$K_2$的长度；

(3) 计算 $C_2=m\oplus K_1$，$C_3=\mathrm{MAC}(K_2,C_2,\mathrm{ID}_{\mathrm{DU}})$，$h=H_2(m\,\|\,w)$，$l=(d-h)\,\mathrm{mod}p$；计算签名向量 $\boldsymbol{S}_i=[l]\cdot\mathrm{SK}_i$；构造完整的签密密文 $\mathrm{CT}=\{C_1,C_2,C_3,h,\{S_i,C_i,C_i'\}_{i\in\{1,2,\cdots,l\}}\}$。

OBU加密提取的关键词m_k：计算$Q_k=H_3(m_k)$；选择 $r\in Z_p^*$且设置随机因子$T=[r]\cdot P_1$，计算$V=e(P_1,Q_k)$，$C_k=(T,V)$。计算$I_k=H_4(V)$；输出CT、关键词密文C_k和索引标识符I_k给CS。CS以键值形式存储$(I_k,(\mathrm{CT},C_k))$到索引表中。

4.4 陷门生成阶段

DU生成待查询关键词陷门$m_k^{'}$，计算 $Q_k^{'}=H_3(m_k^{'})$；选择$\tau\in Z_p^*$ 且计算$g_{\mathrm{T}}=e(P_1,\mathrm{PK}_{\mathrm{DU}})$，$w_{\mathrm{T}}=g_{\mathrm{T}}^{\tau}$ $h_{\mathrm{T}}=H_2(Q_k^{'}||w_{\mathrm{T}})$ $l_{\mathrm{T}}=(\tau-h_{\mathrm{T}})\mathrm{mod}p$，$S_{\mathrm{T}}=[l_{\mathrm{T}}]\mathrm{SK}_{\mathrm{DU2}}$；输出认证陷门$T_k^{'}=\left(Q_k^{'},\sigma\leftarrow(h_{\mathrm{T}},S_{\mathrm{T}})\right)$给CS以便匹配操作。

4.5 陷门匹配阶段

CS计算 $P=H_1(\mathrm{ID}_{\mathrm{DU}}\parallel\mathrm{hid})P_2+\mathrm{PK}_{\mathrm{DU}}$，$w_{\mathrm{T}}^*=e(S_{\mathrm{T}}^{'},P)\cdot g^{h_{\mathrm{T}}^{'}}$，$h_{\mathrm{T}}^*=H_2(Q_k^{'}\parallel w_{\mathrm{T}}^*)$。如果$h_{\mathrm{T}}^*=h_{\mathrm{T}}^{'}$，陷门签名有效，CS计算$I_q=H_4(e(P_1,Q_k^{'}))$。如果CS的索引表中存在键值对$I_q=I_k$，则匹配成功且转发匹配关键词对应的密文CT给ES执行后续解密操作；如果未匹配成功，输出 $\perp$。正确性分析为

$$\begin{aligned}w_{\mathrm{T}}^*&=e(S_{\mathrm{T}}^{'},P)\cdot g^{h_{\mathrm{T}}^{'}}=e\left((\tau-h_{\mathrm{T}}^{'})\right.\\&\quad\cdot\left[\frac{\alpha}{H_1(\mathrm{ID}_{\mathrm{DU}}\parallel\mathrm{hid})+\alpha}\right]P_1,\\&\quad\left.[H_1(\mathrm{ID}_{\mathrm{DU}}\parallel\mathrm{hid})+\alpha]P_2\right)\cdot e(P_1,P_2)^{\alpha\cdot h_{\mathrm{T}}^{'}}\\&=e(P_1,P_2)^{\alpha\cdot\left(\tau-h_{\mathrm{T}}^{'}\right)+\alpha\cdot h_{\mathrm{T}}^{'}}=e(P_1,P_2)^{\alpha\cdot\tau}\\&=g_{\mathrm{T}}^{\tau}=w_{\mathrm{T}}\end{aligned}$$

4.6 部分解签密阶段

ES在收到解密请求时，利用用户密钥中边缘节点私钥执行部分解签密。用户属性满足预设的访问策略时，存在一组系数$\{\vartheta_{1,i}\in Z_p^*\}_{i\in\{1,2,\cdots,l\}}$ 使得 $\sum_{i=1}^{l}\vartheta_{1,i}\cdot\lambda_i=d$，随后生成解密因子$\mathrm{DF}=\prod_{i=1}^{l}\left(\frac{e(\mathrm{SK}_1,C_i)}{e(\mathrm{SK}_2,C_i^{'})}\right)^{\vartheta_{1,i}}$。最终，输出完整密文$\mathrm{CT}^{'}=\{\mathrm{CT},\mathrm{DF}\}$ 给用户DU。

4.7 完整解签密阶段

DU计算$w^*=\frac{e(C_1,\mathrm{SK}_{\mathrm{DU1}})}{\mathrm{DF}}$，利用$w^*$派生对称解密密钥：$K_1^{'}\parallel K_2^{'}=\mathrm{KDF}(C_1\parallel w^*\parallel\mathrm{ID}_{\mathrm{DU}},\mathrm{ln})$，恢复出明文 $m^{'}=C_2\oplus K_1^{'}$；计算$C_3^{'}=\mathrm{MAC}\left(K_2^{'},C_2,\mathrm{ID}_{\mathrm{DU}}\right)$。如果$C_3^{'}=C_3$，密文有效。DU属性满足访问策略时，存在一组系数$\{\vartheta_{2,i}\in Z_p^*\}_{i\in\{1,2,\cdots,l\}}$使得$\sum_{i=1}^{l}\vartheta_{2,i}\cdot\lambda_i=s$。如果$\prod_{i=1}^{l}(e(S_i,\mathrm{PK}_i))^{\vartheta_{2,i}}=e(P_1,P_2)^{l\cdot\alpha}$，计算$w^{'}=e(P_1,P_2)^{l\cdot\alpha}\cdot e(\mathrm{PK},P_2)^h$，$h^{'}=H_2\left(m^{'}\parallel w^{'}\right)$，如果$h^{'}=h$，签名合法，输出明文 $m^{'}$。正确性分析为

$$\begin{aligned}w^*&=\frac{e(C_1,\mathrm{SK}_{\mathrm{DU1}})}{\mathrm{DF}}=\frac{e\left(d\cdot[H_1(\mathrm{ID}_{\mathrm{DU}}\parallel\mathrm{hid})P_1+\mathrm{PK}],\frac{\alpha\cdot(\beta+1)}{H_1(\mathrm{ID}_{\mathrm{DU}}||\mathrm{hid})+\alpha}\cdot P_2\right)}{e(P_1,P_2)^{\alpha\cdot\beta\cdot d}}\\&=\frac{e(P_1,P_2)^{\alpha\cdot d\cdot(\beta+1)}}{e(P_1,P_2)^{\alpha\cdot\beta\cdot d}}=e(P_1,P_2)^{\alpha\cdot d}=w\end{aligned}$$

$$\prod_{i=1}^{l}(e(S_i,\mathrm{PK}_i))^{\vartheta_{2,i}}=\prod_{i=1}^{l}(e\left(\left[\frac{(d-h)\cdot\lambda_i\cdot\alpha}{H_1(\mathrm{ID}_i||\mathrm{hid})+\alpha}\right]P_1\right),\left[\frac{H_1(\mathrm{ID}_i||\mathrm{hid})+\alpha}{s}\right]P_2)^{\vartheta_{2,i}}=e(P_1,P_2)^{l\cdot\alpha}$$

$$w^{'}=e(P_1,P_2)^{l\cdot\alpha}\cdot e(\mathrm{PK},P_2)^h=e(P_1,P_2)^{(l+h)\cdot\alpha}=e(P_1,P_2)^{(d-h+h)\cdot\alpha}=e(P_1,P_2)^{\alpha\cdot d}=w$$

5 安全性分析

定理1 如果底层的可搜索属性签密方法满足机密性，则本文方法在DBDH假设下同样满足机密性。

证明 如果挑战者Γ收到DBDH问题的随机实例：$(P^a,P^b,P^c,Q^a,Q^b,Q^c,e(P,Q)^{abc},Z)$，$\Gamma$尝试在$G_{\mathrm{T}}$中找到$Z=e(P,Q)^{abc}$，$a,b,c\in Z_p^*$ 对于攻击者和挑战者是未知的。在交互游戏中Γ使用初始为空的列表$(\mathrm{list}_1,\mathrm{list}_2,\mathrm{list}_3,\mathrm{list}_4)$储存不同谕言机询问的结果。$\mathcal{B}$选择访问结构$(\boldsymbol{M}^*,\rho^*)$给$\Gamma$，$\Gamma$随机选取$\alpha^{'}\in Z_p^*$，得到满足$\alpha P_1=abP_1+\alpha^{'}P_1$的$\alpha$，输出调用初始化算法得到的系统参数$\varphi$给$\mathcal{B}$。$\mathcal{B}$在阶段1发出多项式有界次的适应性询问。

H_1询问：$\mathcal{B}$请求身份ID_i的哈希值。如果L_1中有匹配元组，Γ返回h_i。否则，Γ返回随机选择的$h_i\in Z_p^*$且存储(ID_i,h_i)到L_1中。

H_2询问：$\mathcal{B}$请求指定字符串x的哈希值。如果L_2中有匹配元组，Γ返回h_x。否则，Γ返回随机选择的$h_x\in Z_p^*$ 且存储(x,h_x)到L_2中。

H_3询问：$\mathcal{B}$请求指定字符串x_1的群上映射点值。如果L_3中有匹配元组，Γ返回 ξ。否则，Γ返回随机选择的$\xi\in G_2$，存储(x_1,ξ)到L_3中。

H_4询问：$\mathcal{B}$请求群上点x_2映射为固定长度比特字符串。如果L_4中有匹配元组，Γ返回ζ。否则，Γ返回任选的ζ，存储(x_2,ζ)到L_4中。

公钥询问：$\mathcal{B}$ 请求身份ID_i的属性公钥。如果L_3中有用户属性公钥，Γ输出公钥PK_i给$\mathcal{B}$。否则，Γ随机选择$s\in Z_p^*$，设置$\mathrm{PK}_i=\left[\frac{h_i+\alpha}{s}\right]P_2$，添加 $(\mathrm{ID}_i,\mathrm{PK}_i)$ 到L_5中。

私钥询问：$\mathcal{B}$ 请求身份ID_i的私钥且属性集合A不能满足 $(\boldsymbol{M}^*,\rho^*)$。$\Gamma$随选择列向量$\boldsymbol{v}_s=(s,$

$r_2,\cdots,r_d)$，计算每个属性所占秘密值份额 $\lambda_i=\boldsymbol{S}_i\times\boldsymbol{v}_s$，选择 $\beta\in Z_p^*$。如果$\mathrm{ID}_i=\mathrm{ID}_t$($\mathrm{ID}_t$是挑战身份)，$\Gamma$失败。否则，$\Gamma$计算$\mathrm{SK}_i=\left[\dfrac{\lambda_i\cdot\alpha}{h_i+\alpha}\right]P_1$，$\mathrm{SK}_{\mathrm{DU1}}=\left[\dfrac{\alpha\cdot(\beta+1)}{h_i+\alpha}\right]P_2$，$\mathrm{SK}_1=[\alpha\cdot\beta]P_1$，$\mathrm{SK}_2=[\alpha\cdot\beta\cdot H_2(A_i)]P_1$，添加$(\mathrm{ID}_i,\mathrm{SK}_i,\mathrm{SK}_{\mathrm{DU1}},\mathrm{SK}_1,\mathrm{SK}_2)$到$L_6$中。

$\mathcal{B}$选择等长消息m_0,m_1给Γ。Γ选取发送者身份ID_i^*、接收者身份$\mathrm{ID}_{\mathrm{DU}}^*$。在阶段1，$\mathcal{B}$不能询问$\mathrm{ID}_{\mathrm{DU}}^*$的私钥且其公钥不能被替换。如果$\mathrm{ID}_{\mathrm{DU}}^*\neq\mathrm{ID}_t$，$\Gamma$失败。否则，$\Gamma$ 选择$b\in\{0,1\}$和随机数$\mu_1,\mu_2,\cdots,\mu_l\in Z_p^*$，计算$C_1^*=[d]\cdot[h_i\cdot P_1+\mathrm{PK}]$，$K_1^*\parallel K_2^*=\mathrm{KDF}(C_1^*\parallel w\parallel\mathrm{ID}_{\mathrm{DU}}^*,\mathrm{ln})$，$C_i^*=[\lambda_i+\mu_i\cdot H_2(A_i)]P_2$，$C_i^{'*}=[\mu_i]P_2$，$C_2^*=m_b\oplus K_1$，$C_3^*=\mathrm{MAC}(K_2,C_2,\mathrm{ID}_{\mathrm{DU}}^*)$，$w^*=e(P_1,P_2)^{\alpha\cdot d}$，$h^*=H_2(m_b\parallel w)$，$l^*=(d-h)\,\mathrm{mod}p,S_i^*=[l^*]\cdot\left[\dfrac{\lambda_i\cdot\alpha}{h_i+\alpha}\right]P_1$。输出挑战密文$\mathrm{CT}^*=\{C_1^*,C_2^*,C_3^*,h,\{S_i^*,C_2^*,C_i^{'*}\}_{i\in\{1,2,\cdots,l\}}\}$给$\mathcal{B}$。

在阶段2，$\mathcal{B}$ 向Γ提供用户身份ID_i和属性集合A，再次请求像阶段1那样的询问。最后，$\mathcal{B}$输出猜测$b_1\in\{0,1\}$ 给Γ，如果$b_1=b$，$\mathcal{B}$ 在游戏中获胜。$b_1=0$的概率是$\Pr[Z=e(P,Q)^{abc}]=\varepsilon+1/2$。否则，$Z=R$($R$是随机选择的)，$\mathcal{B}$无法获得任何关于$b$的有价值信息；$\mathcal{B}$获取正确猜测的概率是 $\Pr[Z=R]=1/2$。可得：Γ获得DBDH问题实例解的概率为$\varepsilon_{\mathrm{DU}}=\Pr[b_1=b]-\dfrac{1}{2}=\dfrac{1}{2}\left(\Pr\left[Z=e(P,Q)^{abc}\right]+\Pr[Z=R]\right)-\dfrac{1}{2}=\dfrac{1}{2}\left(\dfrac{1}{2}+\dfrac{\varepsilon}{2}+\dfrac{1}{2}\right)-\dfrac{1}{2}=\dfrac{\varepsilon}{2}$。由于在多项式时间内DBDH问题无法以非忽略优势被解决，故攻击者无法以不可忽略优势破解本文方法，这表明攻击者的优势ε是可忽略的，且本文方法在DBDH假设下满足机密性。　　证毕

定理2　如果q-SDH假设成立，则本文方法满足选择消息攻击下的不可伪造性。

证明　$\mathcal{B}$选定访问结构$(\boldsymbol{M}^*,\rho^*)$给挑战者$\Gamma$。如果$\Gamma$收到一个$q$-SDH问题的随机实例：$(P,Q,aQ,a^2Q,\cdots,a^qQ)$，$P=\psi(Q)$，$\Gamma$ 尝试找到一组元素$\left(c,\dfrac{1}{c+a}P\right)$，$c\in Z_p^*$。$\Gamma$设置主私钥$k=\alpha$，$P_2=\sum_{i=0}^{q-1}c_i(\alpha^iQ)=f(\alpha)Q$，$P_1=\psi(P_2)=f(\alpha)P$，$\mathrm{PK}=[\alpha]P_1$，计算$G_{\mathrm{T}}$上元素$g=e(\mathrm{PK}_1,P_2)$，$\mathcal{B}$请求定理1中阶段1的$H_1$询问，定义多项式：$f(x)=\prod_{i=1}^{q-1}(x+h_i)=\sum_{i=0}^{q-1}c_ix^i$，$f_i(x)=f(x)/(x+h_i)$，$c_i\in Z_p^*$。$\mathcal{B}$请求定理1中阶段1的私钥询问获取签名私钥$\mathrm{SK}_i=[\lambda_i\cdot\alpha/(h_i+\alpha)]P_1$。假设$\Gamma$执行 $q-2$ 次签密询问且属性一定满足签名策略。Γ设置$\lambda_i=f(\alpha)+1$，$d=h+1/\alpha$，$w=e(P,Q)^{\alpha h+1}$，$l=d-h$，输出签密密文中的签名结果给$\mathcal{B}$。

最后，$\mathcal{B}$输出伪造签名(m^*,S^*)。如果签名不合法，Γ伪造失败；否则，设置$S^*=\left[\dfrac{f(\alpha)+1}{h_i+\alpha}\right]\psi(Q)$，计算$\gamma(\alpha)=\sum_{i=0}^{q-2}h_i\alpha^i$，$\gamma_{-1}\in Z_p^*$，$f(\alpha)=\gamma(\alpha)(h_i+\alpha)+\gamma_{-1}$，可得$\left[\dfrac{1}{h_i+\alpha}\right]P=\dfrac{1}{1+\gamma_{-1}}(S^*-[\gamma(\alpha)]P)=\frac{1}{1+\gamma_{-1}}(S^*-\sum_{i=0}^{q-2}[h_i\alpha^i]P)$，$\Gamma$通过查询$L_1$得到$h_i$，输出$q$-SDH问题的解$\left(h_i,\left[\dfrac{1}{h_i+\alpha}\right]P\right)$。综上，$q_{H_1}$是访问$H_1$谕言机的次数，$\Gamma$能模拟成功的概率是$1/q_{H_1}$。如果$\mathcal{B}$ 伪造签名的概率是ε，则Γ成功求解q-SDH问题的概率是ε/q_{H_1}。　　证毕

定理3　如果攻击者$\mathcal{B}$不能攻破SM9签名的UF-CMA安全性[14]，则本文方法中生成的关键词陷门是UF-CMA安全的。

证明　Γ与UF-CMA 游戏的挑战者$\mathcal{S}$交互：$\mathcal{S}$运行SM9密钥生成算法得到SM9公钥$\mathrm{PK}_{\mathrm{SM9}}$和签名密钥$\mathrm{SK}_{\mathrm{SM9}}$，提供$\mathrm{PK}_{\mathrm{SM9}}$给$\Gamma$。$\mathcal{S}$持有$\mathrm{SK}_{\mathrm{SM9}}$并提供签名谕言机。$\Gamma$请求对消息$m$签名时，$\mathcal{S}$计算签名并输出之给$\Gamma$。$\mathcal{S}$从$\Gamma$收到伪造的消息签名对$(m^*,\sigma^*)$，检查其有效性以确定$\Gamma$是否赢得UF-CMA游戏。$\Gamma$收到$\mathcal{S}$提供的SM9公钥$\mathrm{PK}_{\mathrm{SM9}}$ 且作为签名验证公钥$\mathrm{PK}_{\mathrm{DU}}$。$\Gamma$输出调用初始化算法得到的系统参数$\varphi$和$\mathrm{PK}_{\mathrm{DU}}$给$\mathcal{B}$。

陷门询问：Γ维护初始为空的列表L_{T} 用于记录询问过的关键词和对应 $Q_k^{'}$值。$\mathcal{B}$发出陷门询问请求，Γ计算$Q_k^{'}=H(m_k)$。如果$H(m_k)$ 尚未在L_2中记录，Γ会按照谕言机的规则生成且记录到L_2中。Γ输出$Q_k^{'}$作为消息m_k给SM9的挑战者$\mathcal{S}$，请求对m_k签名。$\mathcal{S}$ 返回针对m_k的SM9签名σ_k给Γ。Γ输出生成的陷门$T_k^{'}=\left(Q_k^{'},\sigma_k\right)$给$\mathcal{B}$。$\Gamma$添加关键词$m_k$到 L_{T}中。

$\mathcal{B}$输出关键词m_k^*和对应陷门$T_{k^*}^{'}=(Q_{k^*}^{'},\sigma_k^*)$。$\Gamma$计算$Q_{k^*}^{'}=H(m_k^*)$。如果$H(m_k^*)$不在$L_2$中，$\Gamma$会通过随机谕言机生成并记录一个新值。$\Gamma$检查伪造的陷门$T_{k^*}^{'}$是否满UF-CMA 游戏的获胜条件，$\Gamma$使用$\mathrm{PK}_{\mathrm{DU}}$验证$\sigma_k^*$是否是 $Q_{k^*}^{'}$的有效SM9签名且检查关键词m_k^*是否在L_{T}中，如果满足上述条件，则$\mathcal{B}$赢得UF-CMA游戏。如果$\mathcal{B}$能够以不可忽略的

优势ε赢得UF-CMA博弈，Γ就能以相同优势ε成功在UF-CMA 游戏博弈中伪造签名。根据文献[14]，SM9签名具有UF-CMA安全性，任何攻击者攻破UF-CMA安全性的优势可忽略不计，故攻破本文方法的陷门UF-CMA安全性的优势也同样忽略不计。

证毕

6 性能分析

6.1 功能特性

功能特性比较详见表1。文献[9]实现了云边协同属性广播签密，但缺少可搜索功能。文献[10]利用云服务器辅助进行部分解密和数据完整性验证，减轻了数据用户部分负担，但不具备可搜索功能且密钥设计复杂度高。文献[11]解决了云存储可能返回错误结果的问题，不提供可搜索功能且用户计算负担较重，不适于资源受限设备。相较之下，本文方法外包大量计算任务给边缘节点服务器执行且具有可搜索功能，减轻了终端计算负担，提升了用户的计算效率，使之更适于资源受限的轻量级设备。

6.2 开销分析

密码操作平均运行时间如表2所示。依据计算量和通信量分析开销情况(表3)，n表示用户属性数量，$|G_1|,|G_2|,|G_{\rm T}|,|Z_p|$分别表示$G_1,G_2,G_{\rm T},Z_p^*$上的元素大小，设定$|G_1|,|G_2|,|G_{\rm T}|$为64 bit，$|Z_p|$为16 bit。

算法运行时间分析均在本地仿真环境中通过计时方法测得。实验平台搭载64 bit Win 10 OS、Intel(R) Core(TM) i5-8300H处理器和16 GB RAM，采用Java语言配合PBC库[15]实现仿真，同时基于SM9算法和Type-A曲线参数(160位素数阶群)设定安全基准。通过改变属性数量n测试并分析对比方法的性能表现。通过图2可见，对比方法总体时间开销均随属性个数增加而呈现出线性增长的趋势；本文方法的时间开销增长速率最低，曲线最为平缓，这是由于采用计算外包策略，卸载大部分解签密运算到边缘节点执行，最大限度地减少了计算复杂度较高的双线性对运算和指数运算。由图3可见，密文大小随属性个数的变化情况，本文方法的密文大小与文献[10]相近，但在整体性能上略优于文献[10]，这使之在实时性要求极高的车联网复杂环境中能够实现更快速的通信。

6.3 关键词搜索机制效率对比

本节验证本文基于哈希索引的关键词搜索机制在海量密文数据下的即时检索能力。对比分析本文方法的$O(1)$常数时间查找机制与传统$O(N)$线性遍历匹配机制。实验中以密文数量N为变量，测量两种机制的搜索时间开销。实验结果表明两种搜索机制在不同密文数量下的性能差异(详见图4)：本文方法随着密文数量从10增加到5 000条，搜索时间始终稳定在4.85 ms左右，与1次双线性对操作的耗时高度吻合。这证明本文方法通过索引实现了近似$O(1)$的检索效率，即搜索开销几乎不受云端数据量的影响；本文方法在保证关键词隐私性的同时通过引入哈希索引机制，解决了海量IoV数据下实时检索难题。

6.4 计算外包效率分析

针对车载终端资源受限的挑战，本节引入外包效率(Offloading Efficiency, OE)指标定量分析边云协同架构对DU解签密计算负荷的卸载贡献(详见表4)。OE指标反映DU的复杂计算任务成功转移到高性能边缘节点处理的比重，$\mathrm{OE}=(T_{\rm t}-T_{\rm r})/T_{\rm t}\times 100\%$，$T_{\rm t}$代表未外包时DU本地执行完整解签密的总时间开销，$T_{\rm r}$代表外包后DU本地仅执行残余解签密的时间开销。根据属性数量n变化，进行外包效率计算实验。图5表明在属性数量n较少时，外包效率达

表 1 功能特性比较

功能	文献[9]	文献[10]	文献[11]	ECCSABSCM
访问控制策略	线性秘密共享	门限策略	门限策略	线性秘密共享
可搜索	×	×	×	√
外包解密	√	√	×	√

表 2 运算符号说明(ms)

符号及含义	执行一次双线性对操作: $1T_{\rm p}$	执行一次指数操作:$1T_{\rm e}$	执行一次乘法操作:$1T_{\rm m}$	执行一次哈希函数操作:$1T_{\rm h}$
耗时	4.843	7.941	0.043	0.003

表 3 计算开销分析

对比方法	总体时间开销	密文大小
文献[9]	$(4+4n)T_{\rm e}+3T_{\rm m}+T_{\rm h}+T_{\rm p}$	$(2n+7)\,\lvert G_1\rvert$
文献[10]	$(6n+10)T_{\rm e}+T_{\rm m}+2T_{\rm p}+(3n+2)T_{\rm h}$	$4\,\lvert Z_p\rvert+6\,\lvert G_1\rvert+(n+1)\,\lvert G_{\rm T}\rvert$
文献[11]	$(3n+7)\,T_{\rm e}+3T_{\rm h}+(n+5)T_{\rm m}+4T_{\rm p}$	$2\,\lvert Z_p\rvert+(2n+3)\,\lvert G_1\rvert$
ECCSABSCM	$2T_{\rm e}+(4n+9)\,T_{\rm m}+(n+4)T_{\rm p}+(2n+5)T_{\rm h}$	$\lvert Z_p\rvert+(n+2)\,\lvert G_1\rvert+2\,\lvert G_2\rvert$

到84.67%；n增加到90时，外包效率达到96.26%。这表明本文方法能为资源受限车载终端卸载超96% 的复杂计算开销至高性能边缘服务器。未外包总开销T_{t}随n的增加呈线性增长趋势，这反映双线性对运算在本地执行时的巨大耗时。外包后的残余开销T_{r}增长极慢，表明DU实际承担的计算负荷已降级为轻量级运算。

6.5 搜索延迟分析

实时响应是车联网服务的核心要求。本节评估端到端(End-to-End, E2E)搜索延迟T_{E2E}(详见表5)，验证本文方法在实际动态场景中的适用性。T_{E2E}综合了陷门生成、关键词匹配、部分解密和通信开销，是从用户查询到获取解密因子的完整时间路径，$T_{\mathrm{E2E}} = T_{\mathrm{Calc}} + T_{\mathrm{Comm}}$，$T_{\mathrm{Comm}}$是固定的网络通信开销，IoV典型延迟模型设定$T_{\mathrm{Comm}} \approx 80\mathrm{ms}$，$T_{\mathrm{Calc}}$主要受边缘服务器上的$O(n)$级部分解密操作影响。$T_{\mathrm{E2E}}$随属性数量$n$的增加呈线性增长趋势，$n = 90$的最复杂策略下达到约1 019.55 ms，此亚秒级的响应时间仍满足IoV对非安全关键数据传输的实时性要求。固定通信开销(80 ms)在总延迟中占比很小，计算总耗时T_{Calc}占总延迟的主导地位，这表明高性能边缘服务器侧的$O(n)$级部分解密操作是本文方法限制端到端实时性能的主要瓶颈。这为后续研究提供了明确优化方向，在保证安全性前提

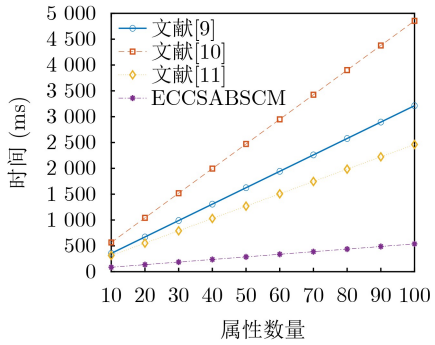

图 2 总体时间开销的比较情况

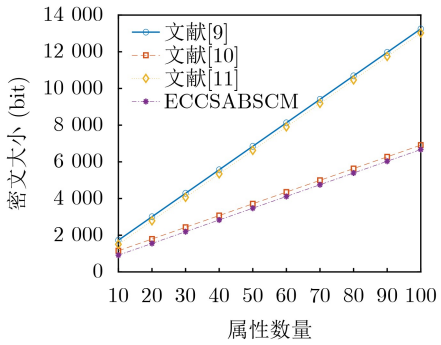

图 3 通信开销的比较情况

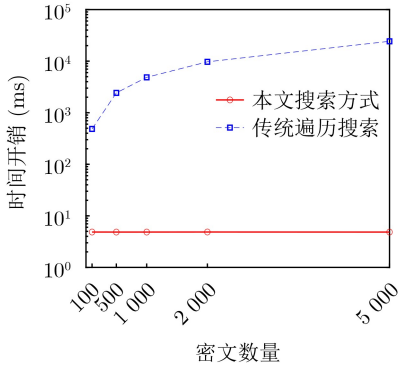

图 4 关键词搜索机制效率对比

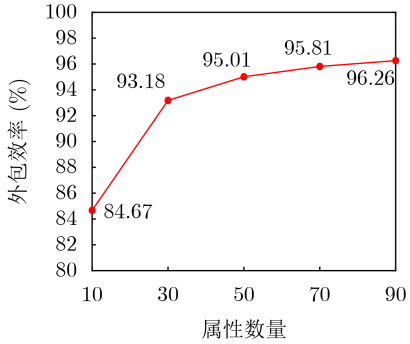

图 5 计算外包效率变化趋势

表 4　解签密计算任务外包效率分析

属性数量	10	30	50	70	90
T_{t}(ms)	108.71	306.66	504.64	702.63	900.60
T_{r}(ms)	16.66	20.92	25.18	29.44	33.70
OE(%)	84.67	93.18	95.01	95.81	96.26

表 5　端到端搜索延迟构成(ms)

属性数量	10	30	50	70	90
T_{Calc}	137.31	337.86	538.43	738.99	939.55
T_{Comm}	80.00	80.00	80.00	80.00	80.00
T_{E2E}	217.31	417.86	618.43	818.99	1 019.55

下降低了边缘节点的密码学计算复杂度，实现了更高的实时响应性能。

7 结论

本文方法实现了对IoV数据的机密性保护、不可伪造性保证和细粒度访问控制。利用边缘节点的高并发处理能力，卸载解签密过程中计算复杂度较高的双线性对运算到边缘端执行，降低了终端运算复杂度且提升了系统响应速度与用户体验。本文方法在安全特性、计算开销和通信量等有明显优势，能够很好地适应边缘计算驱动下的车联网环境。

参 考 文 献

[1] LIU Jianhang, XUE Kunlei, MIAO Qinghai, *et al.* MCVCO: Multi-MEC cooperative vehicular computation offloading[J]. *IEEE Transactions on Intelligent Vehicles*, 2024, 9(1): 813–826. doi: 10.1109/TIV.2023.3299381.

[2] HADDAJI A, AYED S, and CHAARI FOURATI L. IoV security and privacy survey: Issues, countermeasures, and challenges[J]. *The Journal of Supercomputing*, 2024, 80(15): 23018–23082. doi: 10.1007/s11227-024-06269-5.

[3] TANG Chaogang, CHEN Wei, ZHU Chunsheng, *et al.* When cache meets vehicular edge computing: Architecture, key issues, and challenges[J]. *IEEE Wireless Communications*, 2022, 29(4): 56–62. doi: 10.1109/MWC.202.2100159.

[4] QUAN Haoyu, ZHANG Qingmiao, and ZHAO Junhui. Federated learning assisted intelligent IoV mobile edge computing[J]. *IEEE Transactions on Green Communications and Networking*, 2025, 9(1): 228–241. doi: 10.1109/TGCN.2024.3421357.

[5] DAMSGAARD H J, OMETOV A, and NURMI J. Approximation opportunities in edge computing hardware: A systematic literature review[J]. *ACM Computing Surveys*, 2023, 55(12): 252. doi: 10.1145/3572772.

[6] 董裕民, 张静, 谢昌佐, 等. 云边端架构下边缘智能计算关键问题综述: 计算优化与计算卸载[J]. 电子与信息学报, 2024, 46(3): 765–776. doi: 10.11999/JEIT230390.
DONG Yumin, ZHANG Jing, XIE Changzuo, *et al.* A survey of key issues in edge intelligent computing under cloud-edge-terminal architecture: Computing optimization and computing offloading[J]. *Journal of Electronics & Information Technology*, 2024, 46(3): 765–776. doi: 10.11999/JEIT230390.

[7] DENG Ningzhi, DENG Shaojiang, HU Chunqiang, *et al.* An efficient revocable attribute-based signcryption scheme with outsourced unsigncryption in cloud computing[J]. *IEEE Access*, 2020, 8: 42805–42815. doi: 10.1109/ACCESS.2019.2963233.

[8] YU Huifang and BAI Xiaoping. Identity-based searchable attribute signcryption in lattice for a blockchain-based medical system[J]. *Frontiers of Information Technology & Electronic Engineering*, 2024, 25(3): 461–471. doi: 10.1631/FITEE.2300248.

[9] 牛淑芬, 王卫芳, 董润园, 等. 云边协同下支持等值测试的属性基广播签密方案[J]. 计算机科学与探索, 2025, 19(8): 2241–2250. doi: 10.3778/j.issn.1673-9418.2410023.
NIU Shufen, WANG Weifang, DONG Runyuan, *et al.* Attribute-based broadcast signcryption scheme with equivalence testing support under cloud-edge collaboration[J]. *Journal of Frontiers of Computer Science and Technology*, 2025, 19(8): 2241–2250. doi: 10.3778/j.issn.1673-9418.2410023.

[10] 牛淑芬, 周思玮, 吕锐曦, 等. 医疗社交网络中基于云计算的属性基签密方案[J]. 电子与信息学报, 2023, 45(3): 884–893. doi: 10.11999/JEIT220070.
NIU Shufen, ZHOU Siwei, LÜ Ruixi, *et al.* Attribute-base signcryption scheme based on cloud computing in mobile medical social network[J]. *Journal of Electronics & Information Technology*, 2023, 45(3): 884–893. doi: 10.11999/JEIT220070.

[11] ELTAYIEB N, ELHABOB R, HASSAN A, *et al.* A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud[J]. *Journal of Systems Architecture*, 2020, 102: 101653. doi: 10.1016/j.sysarc.2019.101653.

[12] 万云飞, 彭长根, 谭伟杰, 等. 基于国密SM9的边云协同属性基签密方案[J]. 信息安全研究, 2025, 11(2): 115–121. doi: 10.12379/j.issn.2096-1057.2025.02.03.
WAN Yunfei, PENG Changgen, TAN Weijie, *et al.* Edge cloud collaborative attribute-based signcryption scheme based on state secret SM9[J]. *Journal of Information Security Research*, 2025, 11(2): 115–121. doi: 10.12379/j.issn.2096-1057.2025.02.03.

[13] 王惠, 王峥. 工业物联网中基于区块链的属性基签密方案[J]. 计算机工程与设计, 2024, 45(10): 2888–2896. doi: 10.16208/j.issn1000-7024.2024.10.002.
WANG Hui and WANG Zheng. Attribute based signcryption scheme based on blockchain in industrial internet of things[J]. *Computer Engineering and Design*, 2024, 45(10): 2888–2896. doi: 10.16208/j.issn1000-7024.2024.10.002.

[14] 赖建昌, 黄欣沂, 何德彪, 等. 国密SM9数字签名和密钥封装算法的安全性分析[J]. 中国科学: 信息科学, 2021, 51(11): 1900–1913. doi: 10.1360/SSI-2021-0049.
LAI Jianchang, HUANG Xinyi, HE Debiao, *et al.* Security analysis of SM9 digital signature and key encapsulation[J]. *Scientia Sinica Informationis*, 2021, 51(11): 1900–1913. doi: 10.1360/SSI-2021-0049.

[15] QIAO Zirui, CAO Lei, ZHU Yasi, *et al.* DADD: Direct

authentication with vehicles from different domains[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2025, 26(10): 16811–16825. doi: 10.1109/TITS.2025.3575535.

俞惠芳：女，教授，博导，CCF终身会员(14320S)，研究方向为密码学、数据安全等.

王庆归：男，硕士生，研究方向为密码学、边缘计算等.

王子豪：男，硕士生，研究方向为密码学、区块链等.

责任编辑：廖海贝

Edge-Cloud Collaborative Searchable Attribute-Based Signcryption Approach for Internet of Vehicles

YU Huifang[①②]　　WANG Qinggui[①]　　WANG Zihao[①]

[①](*School of Cyberspace Security, Xi'an University of Posts & Telecommunications, Xi'an* 710121, *China*)

[②](*State Key Laboratory of Blockchain and Data Security, Zhejiang University, Hangzhou* 310058, *China*)

Abstract:

Objective　The dynamic and open environment of the Internet of Vehicles (IoV) poses substantial challenges to data security and real-time performance. Large-scale data interactions are vulnerable to eavesdropping, tampering, forgery, and replay attacks. Conventional cloud computing architectures exhibit inherent latency and cannot satisfy millisecond-level real-time requirements in IoV applications, which results in inefficient data transmission and an increased risk of traffic accidents. Therefore, balancing data security and real-time performance represents a critical bottleneck for large-scale IoV deployment.

Methods　An edge-cloud collaborative searchable attribute-based signcryption method is proposed for IoV applications. A multi-layer architecture is constructed, consisting of cloud servers, edge servers, and in-vehicle terminal devices. Access control is enforced through a hybrid key-policy and ciphertext-policy mechanism derived from attribute-based signcryption and a Linear Secret Sharing Scheme (LSSS). To reduce local decryption overhead, bilinear pairing operations are outsourced to edge nodes. SM9 is adopted for trapdoor generation and signature authentication. The proposed method provides data confidentiality, signature unforgeability, and trapdoor unforgeability.

Results and Discussions　The proposed method demonstrates superior performance in an IoV edge-cloud collaborative architecture for searchable attribute-based signcryption (Tables 1 and 4). Functional characteristics are summarized in (Table 1). (Fig. 2) illustrates the variation in total computation time as the number of attributes increases. Although the total time increases slightly, the growth rate remains low. By offloading computation-intensive tasks to edge nodes, the local computational burden on user terminals is substantially reduced. This optimization is quantified by an outsourcing efficiency exceeding 96% (Table 4, Fig. 5). Instantaneous retrieval is achieved by reducing the search complexity to $O(1)$ through a hash-based index (Fig. 4). End-to-end search latency is maintained within an acceptable range for IoV applications (Table 6), which confirms suitability for real-time data access. As shown in (Fig. 3), with an increasing number of attributes, the ciphertext size variation of the proposed method remains the smallest among the compared schemes.

Conclusions　The proposed method achieves fine-grained access control, data confidentiality, data integrity, and unforgeability, while maintaining advantages in computational and communication efficiency. Through a computation offloading mechanism, the method effectively addresses resource constraints of on-board devices in dynamic, resource-sensitive, and real-time IoV environments.

Key words: Edge-cloud collaboration for internet of vehicles; Attribute-based signcryption; Keyword search; Fine-grained access control