软件学报 ISSN 1000-9825, CODEN RUXUEW
2026,37(2):934−952 [doi: 10.13328/j.cnki.jos.007490] [CSTR: 32375.14.jos.007490]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

5G 车联网中基于区块链的半分布式消息认证加密方案*

毕昌兵[1,2,3,4], 田有亮[1,2,3,4], 李 沓[1,2,3,4]

[1](公共大数据国家重点实验室 (贵州大学), 贵州 贵阳 550025)
[2](贵州大学 计算机科学与技术学院, 贵州 贵阳 550025)
[3](贵州大学 密码学与数据安全研究所, 贵州 贵阳 550025)
[4](贵州省密码学与区块链技术特色重点实验室, 贵州 贵阳 550025)
通信作者: 田有亮, E-mail: youliangtian@163.com

摘 要: 5G 车联网通过将 5G 技术应用于车联网来实现高速的信息传输. 然而, 随着车辆数量的急剧增长, 采用传统单一第三方生成密钥容易引发单点故障问题, 同时无线通信会面临消息被拦截、篡改以及大量不可信的虚假消息干扰网络等风险. 为应对这些问题, 提出一种基于区块链的半分布式消息认证加密方案. 首先, 设计基于联盟区块链的半分布式密钥生成与分布式信息共享框架, 通过 5G 基站提供全覆盖的网络, 并由各区域的车辆管理中心充当联盟链的全节点来维护区块链的正常运行, 而车辆作为轻节点加入区块链, 仅可查看区块链上存储的信息. 其次, 设计了无双线性运算的无证书签名算法, 确保消息来源可认证, 并使用反向哈希链生成信誉票证来加解密消息, 保证消息的机密性. 然后, 针对不可信的虚假消息问题, 为车辆设置信誉值, 传播虚假消息将导致其信誉值下降, 以此约束车辆行为, 进而从源头减少虚假消息数量. 最后, 安全性分析与实验结果表明, 所提方案能够保障通信安全, 并通过实现半分布式密钥获取有效缓解单点故障风险, 同时防止篡改、重放和假冒等攻击. 此外, 该方案的计算和通信开销较低, 满足车联网的时效性需求, 且执行信誉值更新合约的 Gas 成本较低, 进一步说明所提方案具备良好的实用性和可行性.

关键词: 半分布式认证; 无证书签名; 区块链; 智能合约; 车联网
中图法分类号: TP309

中文引用格式: 毕昌兵, 田有亮, 李沓. 5G车联网中基于区块链的半分布式消息认证加密方案. 软件学报, 2026, 37(2): 934–952. http://www.jos.org.cn/1000-9825/7490.htm
英文引用格式: Bi CB, Tian YL, Li T. Blockchain-based Semi-distributed Message Authentication and Encryption Scheme in 5G Internet of Vehicles. Ruan Jian Xue Bao/Journal of Software, 2026, 37(2): 934–952 (in Chinese). http://www.jos.org.cn/1000-9825/7490.htm

Blockchain-based Semi-distributed Message Authentication and Encryption Scheme in 5G Internet of Vehicles

BI Chang-Bing[1,2,3,4], TIAN You-Liang[1,2,3,4], LI Ta[1,2,3,4]

[1](State Key Laboratory of Public Big Data (Guizhou University), Guiyang 550025, China)
[2](College of Computer Science and Technology, Guizhou University, Guiyang 550025, China)
[3](Institute of Cryptography and Data Security, Guizhou University, Guiyang 550025, China)
[4](Guizhou Provincial Key Laboratory of Cryptography and Blockchain Technology, Guiyang 550025, China)

Abstract: The 5G Internet of vehicles (IoV) enables high-speed data transmission by applying 5G technology to vehicular networks. However, with the rapid growth in the number of vehicles, traditional single third-party key generation can lead to single-point failures. In

* 基金项目: 国家重点研发计划 (2021YFB3101100); 国家自然科学基金 (62272123); 贵州省高层次创新型人才项目 (黔科合平台人才[2020]6008); 贵州省科技计划 (黔科合支撑 [2022] 一般 065); 贵阳市科技计划 (筑科合 [2021]1-5, 筑科合 [2022]2-4)
收稿时间: 2023-09-07; 修改时间: 2025-03-16; 采用时间: 2025-06-15; jos 在线出版时间: 2025-10-29
CNKI 网络首发时间: 2025-10-31

addition, wireless communication faces risks such as message interception, tampering, and network disruption due to a large number of untrustworthy false messages. To address these issues, this study proposes a blockchain-based semi-distributed message authentication and encryption scheme. First, a semi-distributed key generation and distributed information-sharing framework based on a consortium blockchain is designed. The 5G base stations provide full network coverage, while regional vehicle management centers act as full nodes to maintain the blockchain's proper operation, and vehicles, as lightweight nodes, can only view the information stored on the blockchain. Second, to ensure message source authentication and confidentiality, a certificateless signature algorithm without bilinear pairing is designed, and an inverse hash chain is employed to generate reputation tokens for message encryption and decryption. To address the problem of untrustworthy false messages, a reputation-based system is introduced, where disseminating false messages leads to a decline in the vehicle's reputation value. This mechanism helps to constrain vehicle behavior and reduces the number of false messages at the source. Finally, security analysis and experimental results demonstrate that the proposed scheme ensures communication security, effectively mitigates single-point failure risks through semi-distributed key acquisition, and prevents tampering, replay, and impersonation attacks. Moreover, the proposed scheme incurs low computational and communication overhead, meets the real-time requirements of IoV, and incurs low Gas costs for executing reputation update contracts, further demonstrating the practicality and feasibility of the proposed scheme.

Key words: semi-distributed authentication; certificateless signature; blockchain; smart contract; Internet of vehicles (IoV)

车联网 (Internet of vehicles, IoV) 是车辆与互联网技术相结合的一种应用, 可以实现车辆之间、车辆与基础设施的连接和信息交互共享. 在 IoV 中, 通信方式可以分类为车辆到车辆 (vehicular to vehicular, V2V) 和车辆到基础设施 (vehicular to infrastructure, V2I)[1]. 在 V2V 通信方式中, 车辆与相邻车辆共享交通相关信息, 例如道路堵塞情况、交通事故或转向意图等[2]; 在 V2I 通信方式中, 可信机构通过图形用户界面可以与车辆共享道路相关信息, 使驾驶员能够提前做出合理的决定. 然而, 由于 IoV 中车辆数量巨多, 频繁的通信为网络带宽带来了挑战, 而第 5 代移动通信技术 (5th generation mobile communication technology, 5G) 的出现, 为移动互联网创造了巨大的机会, 特别是 IoV[3]. 5G 可提供高达 20 Gb/s 的数据传输速率, 具有高速率、低时延、广覆盖、支持设备到设备通信的优点, 可以满足 IoV 中及时通信的需求[4].

IoV 与 5G 的结合将成为现代通信时代重要的一部分, 它能够提供快速、可靠的超低延迟信息传输. 然而, 信息在开放的无线网络环境中传输易受到各种攻击, 因此需要提供强有力的安全防护措施. 目前, 在 IoV 中仍然存在如下挑战: (1) 消息以明文的形式在无线网络中传输, 这使得非法用户可以拦截消息, 并对消息进行篡改、重放或者窃取其中的隐私信息; (2) 由于车辆数量的剧增, 采用传统的单一可信第三方中心式管理, 容易出现单点故障问题; (3) 网络中充斥着大量虚假消息, 这些消息通常由熟悉网络配置细节的合法但有恶意意图的用户发送[5], 例如: 尽管某些车辆在身份上是合法的, 但若存在不诚实行为, 如发布虚假消息, 可能导致网络拥塞或误导其他车辆的行驶路线. 这类不可信的消息可能引发一系列严重后果, 包括旅程延误、交通事故[6], 甚至可能造成现实世界中的财产损失乃至人员伤亡.

针对上述挑战 (1), 对传输的消息进行数字签名并加密能保证消息的完整性、身份认证和机密性. 目前, 数字签名主要分为传统公钥密码 (public-key infrastructure, PKI)、基于身份的公钥密码 (identity-based cryptography, IBC) 和基于无证书的公钥密码 (certificateless cryptography, CLC) 这 3 类, 其中 CLC 能有效地解决 PKI 中的证书管理问题和 IBC 中的密钥托管问题, 具有极高的安全性、实用性和研究价值[7−10]. 然而, 许多 CLC 方案使用双线性配对运算, 这就在一定程度上增加了方案的计算负载[11], IoV 中车载单元的计算和存储能力低的特性使得上述构造并不能很好地在 IoV 中部署[12]. 此外, 为了兼顾消息的机密性, 有研究者提出签密方案[13,14], 即在一个逻辑步骤内同时完成签名和加密. 数字签密方案的使用能很好地保证消息的机密性与身份认证, 但采用非对称机制加密的消息只能由指定的单一用户解密, 无法加密需要与多个用户共享的广播消息. 在 IoV 中, 同一消息 (如道路通畅情况) 需要发送给多个车辆, 若使用数字签密, 发送给不同的车辆的相同消息都需要重新执行一次签密, 这将造成极大的计算开销, 故此类签密方案并不适用于 IoV 环境信息广播共享; 其次, 针对上述挑战 (2), 去中心化的区块链可以帮助我们解决这个问题. 区块链被定义为分布式、共享和防篡改的分类账本, 利用区块链代替传统的单一可信第三方, 可以实现分布式管理系统[15−18], 以及解决单点故障问题. 区块链技术的引入为 IoV 管理提供了一种新

思路, 基于区块链分布式账本的去中心化、防篡改、可追溯等优势[19−21], 结合智能合约可编程的特性, 采用基于密码学的认证方案, 可为 IoV 认证提供安全可信的运行环境和管理方案[22]; 此外, 针对挑战 (3), 对于合法但不诚实用户发布不可信的虚假消息现象, 文献 [23] 采用的方法是设置黑名单, 文献 [24] 采用撤销列表, 一旦检测到用户发布虚假消息或被举报, 就将其拉入黑名单或撤销列表, 禁止其参与后续的通信. 然而, 只参照用户发送的某一条无用或虚假消息就将该用户评判为不诚实的用户, 并将其列入黑名单或撤销列表, 这显然是不合理的, 因为用户可能发送了 1 000 条非常有用的消息而只发送了 1 条无用消息, 并且消息的有用程度依赖于接收者的主观意识, 对 A 用户有用的消息可能对 B 用户来说是无用的; 另外, 被恶意用户举报也可能导致诚实用户被错误列入黑名单或撤销列表. 其实, 若用户不诚实, 在通信时发送毫无价值或不可信的消息, 那么身份认证和数据完整性验证的努力都将是徒劳的[25].

针对 5G 背景下 IoV 中面临的上述挑战, 本文提出了一种基于区块链的半分布式认证加密方案, 以提供半分布式的密钥获取、分布式的信息共享以及传输消息的安全性保护. 具体而言, 本文的主要贡献概括如下.

(1) 设计了一种适用于 IoV 的基于联盟区块链的半分布式密钥生成框架, 由 5G 基站提供全覆盖的网络, 各区域的交通管理中心 (vehicle management centre, VMC) 充当联盟链的全节点, 通过共识机制共同维护区块链的正常运行. 区块链存储各区域的公钥及公开参数, 供车辆公开查询, 确保信息的分布式共享.

(2) 设计了高效的无证书签名算法, 确保了消息认证及完整性保护. 车辆的部分私钥的生成来自本区域的 VMC, 有效缓解单一密钥生成器导致的单点故障风险; 此外, 使用反向哈希链生成并同步信誉票证, 从而实现对消息的加密传输, 保证通信的安全性.

(3) 为车辆设计了信誉值, 并提供了信誉值更新合约. 信誉值能反映车辆历史诚实度, 车辆的不诚实行为会导致其信誉值下降, 从而有效约束车辆的不当行为. 此外, 信誉值低于给定阈值的车辆不会获得下一时间段的信誉票证, 无法参与后续的通信, 进而从源头上减少了 IoV 中虚假消息的数量.

(4) 对所提方案进行了安全性分析和实验评估, 结果表明, 本文的方案能够保证传输消息的完整性、机密性与身份认证, 防止修改、重放和假冒等攻击, 同时有效制止内部恶意用户发送不可信消息的问题. 此外, 该方案在计算开销和通信开销方面表现优越, 并且部署的智能合约 Gas 开销较低, 进一步证明该方案具有较高的实用性和可行性.

1 相关工作

数字签名能确保无线网络实体之间共享消息的完整性、身份认证和不可否认性, 而基于 CLC 的无证书签名 (certificateless signature, CLS) 因其既无需处理 PKI 的证书管理复杂性, 又避免了 IBC 的密钥托管问题, 受到研究者的广泛关注. CLS 由 Al-Riyami 等人[26]在 2003 年的亚洲密码会议 (ASIACRYPT) 上首次提出, 由于密钥由用户和 KGC 共同生成, 因此主要存在恶意用户 (类型 I) 和恶意 KGC (类型 II) 两种类型的攻击敌手. Yeh 等人[27]设计了一种用于 IoT 的 CLS 方案, 该方案不使用双线性配对运算, 具有较低的计算开销. 然而, Jia 等人[28]指出 Yeh 等人[27]的方案对两类敌手都无法实现不可伪造, 进而提出了一种改进的方案, 并将其部署于物联网 (Internet of Things, IoT) 环境. 然而, Du 等人[29]提供的证据表明, Jia 等人[28]的方案对于类型 I 敌手来说是不安全的. 此外, Xiang 等人[30]也证明了 Jia 等人[28]的方案很容易遭受恶意 KGC 发起的攻击, 即不能抵御类型 II 的敌手. Du 等人[29]和 Xiang 等人[30]提供了两种不同的改进方案. 然而, Ma 等人[7]证明了 Du 等人[29]和 Xiang 等人[30]的方案都不能抵御类型 I 敌手的伪造攻击, 其原因在于 KGC 生成的密钥和用户生成的密钥彼此独立, 类型 I 敌手可以实行公钥替换攻击. Genc 等人[8]提出了一种面向 IoV 的 CLS 方案, 提供 V2V、V2I 之间的消息认证与完整性保护, 并在随机预言机模型 (random oracle model, ROM) 下证明其能抵御两种类型的敌手攻击. 然而, Ye 等人[10]证明了其无法抵御类型 I 敌手和类型 II 敌手的伪造攻击. Yao 等人[9]设计了一种 CLS 方案, 来抵抗广播式自动相关系统的欺骗、篡改和重放等攻击. 然而, 由于在消息签名阶段没有绑定不重复的随机数, 导致签名算法是确定性的而不是非确定性的, 即: 同一私钥对同一消息多次签名会产生同样的结果. 因此任何敌手都可以从同一用户的两个签名中恢复出该用户的

私钥, 进而伪造合法用户的签名.

另外, 传输消息的机密性也对 IoV 安全通信起着至关重要的作用. 刘文浩等人[13]提出了无双线性对的无证书签密方案, 来同时满足机密性、完整性、身份认证与不可否认, 并声称该方案在 ROM 下是安全的. 然而, 何德彪[31]证明了其方案不能满足类型 I 攻击下的不可伪造, 并强调可以通过修改哈希函数的输入来增强其安全性. Pan 等人[14]提出一种签密方案, 实现消息的机密性与签名的不可伪造性. 该方案的消息由无人机签密后发出, 地面基站接收并解密, 进而获得发送方的真实身份. 然而, 地面基站是一种资源有限的基础设施, 容易受到攻击而妥协, 一旦地面基站被攻破, 将会泄露所有消息发送方的真实身份, 并且该方案只支持消息的单向传输. 签密方案的使用能很好地保证消息的完整性与机密性, 同时提供身份认证与不可否认性, 但其采用非对称机制加密的消息只能由指定的单一用户解密, 无法与多个用户共享信息. 针对该问题, Cui 等人[32]使用一个全局参数来对消息进行加密和解密, 该参数只能由合法用户从可信中心处获取, 并且设计一种签名算法来保证消息来源的可靠性. 该方案结合全局加密参数和数字签名, 同时保证了消息的机密性与身份认证. 此外, Baee 等人[33]提出了一种轻量级的匿名广播消息认证与加密方案. 该方案采用假名隐式证书进行身份认证, 并利用对称加密技术对消息进行加密, 从而实现高效的一对多广播消息认证与加密, 提升了信息共享的安全性和身份隐私保护能力.

为了解决传统集中式管理方式的局限性, 一些研究者提出将区块链技术引入分布式密钥获取机制, 以增强系统的安全性和去中心化特性, 减少对单一信任实体的依赖, 提高密钥管理的安全性和可扩展性. Wang 等人[19]提出了一种基于区块链的无配对运算的 CLS 方案, 用于增强工业 IoT 中传输消息的安全性, 该方案引入基于以太坊的去中心化智能合约替代传统中心化的 KGC, 有效避免了单点故障以及拒绝服务攻击. 然而, Yang 等人[20]证明了 Wang 等人[19]的方案是不安全的, 即任何敌手在仅知道系统公开参数而不知道目标私钥的情况下, 能成功伪造出对于任何消息的合法签名. 此外, Shim[21]也指出 Wang 等人[19]的方案对密钥恢复攻击是不安全的, 即: 敌手能够从同一用户生成的两个签名来恢复出其对应的私钥. 然后, Shim[21]设计了新的 CLS 方案来增强安全性, 然而新方案采用双线性配对运算, 导致较大的计算开销. 导致 Wang 等人[19]方案不安全的原因与 Yao 等人[9]的类似, 主要在于没有绑定随机数导致签名算法是确定性算法. 此外, 文献 [19−21] 中的方案均利用智能合约作为 KGC 进行分布式的密钥生成. 然而, 由于智能合约上的数据具有公开透明的特性, 系统主私钥及生成的部分私钥存在暴露风险. 再者, 智能合约本身不具备随机数生成能力, 这一限制进一步削弱了其安全性. Yeh 等人[11]设计了一种 CLS 方案, 并将其应用于可穿戴设备进行移动支付场景, 提供交易安全性和不可否认性. 然而, Feng 等人[34]指出类型 I 的敌手可以使用线性方程分析方法伪造签名. 基于此, Feng 等人[34]提供了一个改进的 CLS 方案, 并与区块链结合, 设计了一种面向工业 IoT 的跨域身份认证方法. 该方法支持处于不同域中 IoT 设备之间的跨域去中心化可信认证, 消除了 IoT 认证解决方案对可信第三方和中心化服务器的依赖, 然而本文并没有给出形式化的安全性证明.

除此之外, 传输消息的可信度也影响着车辆的行驶安全和司机的驾驶体验. 有研究者提出利用信誉系统来保证 IoV 中传输消息的可信度. Li 等人[6]提出了一种基于信誉系统的广播方案. 车辆拥有信誉证书, 并对共享的消息执行签名, 允许其他车辆评估信息的可信度, 进而更新共享方的信誉值. 此外, 车辆可以根据发送者当前的信誉值快速确定信息是否可靠, 因为信誉值反映了车辆之前公布可信信息的程度, 也反映了车辆之后可能公布可信信息的概率. 然而, 该方案将信任证书存储在单一的声誉服务器中, 这种集中式存储方式存在潜在的安全和可用性挑战. 另外, Yang 等人[25]提出了一种利用区块链技术评估数据可信度的信誉系统. 在该系统中, 地理上相邻的车辆组成一个车辆集群, 集群中的所有成员维护一个区块链并试图达成声誉信息的共识. 基于存储在区块链中的评级, 车辆可以通过计算发送方的声誉得分来评估消息的可信度. 然而, Li 等人[6]和 Yang 等人[25]的方案都没有考虑到 IoV 的通信安全问题.

在综述了现有的 CLS 方案、基于区块链的分布式密钥管理、签密技术以及信誉机制在 IoV 安全通信中的应用后, 可以发现, 尽管已有研究在身份认证、消息完整性和机密性方面取得了一定进展, 但仍然存在以下不足: (1) 部分 CLS 方案无法有效抵御恶意用户和恶意 KGC 的伪造攻击, 安全性仍有待提升; (2) 智能合约用于分布式密钥管理时, 可能因其透明性特性导致密钥泄露风险; (3) 现有签密方案通常采用非对称加密, 仅支持单一用户解密, 难以

满足 IoV 环境下一对多的信息共享需求; (4) 信誉机制虽然能提升消息可信度, 但往往未与安全认证机制结合, 难以抵御恶意节点的攻击. 本文在前人研究的基础上受到启发, 针对现存的一些安全问题与安全需求, 例如消息认证、完整性、机密性、可信度保证以及去中心化等, 结合区块链、CLS、信誉机制等技术, 提出一种基于区块链的半分布式认证加密方案, 该方案能有效地保证消息的完整性和身份认证, 同时还能减少内部恶意用户发布虚假信息等问题. 本文方案与其他方案的比较总结如表 1 所示.

表 1 方案功能性比较

分类	方案	年份	应用场景	身份认证	完整性	机密性	可信度	分布式	抗 $\mathcal{A}_{\mathrm{I}}$	抗 $\mathcal{A}_{\mathrm{II}}$
CLS 方案	文献[11]	2017	移动支付	√	√	×	×	×	×	√
	文献[27]	2017	IoT	√	√	×	×	×	×	×
	文献[28]	2018	IoT	√	√	×	×	×	×	×
	文献[29]	2020	IoT	√	√	×	×	×	×	√
	文献[30]	2022	IoT	√	√	×	×	×	×	√
	文献[7]	2023	IoV	√	√	×	×	×	√	√
	文献[8]	2023	IoV	√	√	×	×	×	×	×
	文献[9]	2024	广播系统	√	√	×	×	×	×	×
	文献[10]	2025	IoV	√	√	×	×	×	√	√
签名与加密方案	文献[13]	2011	理论研究	√	√	√	×	×	×	√
	文献[31]	2013	理论研究	√	√	√	×	×	×	×
	文献[32]	2019	IoV	√	√	√	√	×	无	无
	文献[14]	2022	无人机	√	√	√	×	×	无	无
	文献[33]	2022	IoV	√	√	×	×	×	无	无
分布式密钥管理	文献[19]	2021	IoT	√	√	×	×	√	×	×
	文献[20]	2023	IoT	√	√	×	×	√	√	√
	文献[21]	2024	IoT	√	√	×	×	√	√	√
	文献[34]	2024	IoT	√	√	×	×	√	√	√
信誉机制	文献[6]	2012	IoV	√	√	×	√	×	无	无
	文献[25]	2017	IoV	×	×	×	√	×	无	无
本文方案		2025	IoV	√	√	√	√	半分布式	√	√

注: “√”表示满足该属性, “×”表示不满足该属性, “无”表示无需考虑此类属性, “抗 $\mathcal{A}_{\mathrm{I}}$”表示能抵抗类型I的敌手攻击, “抗 $\mathcal{A}_{\mathrm{II}}$”表示能抵抗类型II的敌手攻击

2 预备知识

本文所提方案涉及的预备知识主要包括椭圆曲线离散对数问题、无证书签名形式化定义、区块链与智能合约, 分别介绍如下.

2.1 相关数学困难问题

椭圆曲线离散对数问题 ECDLP (elliptic curve discrete logarithm problem): 设 G 是 q 阶椭圆曲线循环群 (其中 q 是一个大素数), P 是 G 的生成元, 给定 aP, $P\in G$, 计算 $a\in Z_q^*$.

定义算法 A 成功解出 ECDLP 的概率为:

$$Succ_{Z_p^*}^{\mathrm{ECDLP}}(A)=\Pr[a\leftarrow A(aP,P)].$$

ECDLP 假设: 对于任意多项式时间算法 A, $Succ_{Z_p^*}^{\mathrm{ECDLP}}(A)$ 是可忽略的.

2.2 无证书签名形式化定义

本文所设计的无证书签名方案包括 3 种类型的参与者: 密钥生成中心 KGC (key generation center)、发送者和

接收者, 其中 KGC 由各区域的 VMC 充当, 发送者和接收者均是车辆. 无证书签名算法形式化定义为如下 7 个子算法.

1) 系统参数生成算法: 输入安全参数 τ, 返回系统参数 $params$、系统公钥 P_{Pub} 和系统私钥 sk.

2) 秘密值生成算法: 输入地址 $Addr_k$、系统参数 $params$, 返回 $Addr_k$ 的秘密值 $x_k \in Z_q^*$.

3) 部分密钥生成算法: 输入地址 $Addr_k$、系统参数 $params$ 和系统私钥 sk, 返回 $Addr_k$ 的部分私钥 py_k.

4) 私钥生成算法: 输入地址 $Addr_k$、系统参数 $params$、部分私钥 y_k 和秘密值 $x_k \in Z_q^*$, 返回 $Addr_k$ 的私钥 $SK_k = (x_k, y_k)$.

5) 公钥生成算法: 输入地址 $Addr_k$、系统参数 $params$, 部分公钥 Y_k 和秘密值 $x_k \in Z_q^*$, 返回 $Addr_k$ 的公钥 $PK_k = (X_k, Y_k)$.

6) 签名算法: 输入系统参数 $params$、消息 m_k、发送者的地址 $Addr_k$ 及其私钥 SK_k, 返回签名 σ_k.

7) 验证算法: 输入系统参数 $params$、签名 σ_k、发送者的地址 $Addr_k$ 及其公钥 PK_k, 若验证通过, 则返回 1; 否则返回 0.

2.3 安全模型

参照 Al-Riyami 等人[26]所定义的安全模型, 在无证书密码机制中, 主要面临的敌手为类型 I 的敌手 $\mathcal{A}_{\text{I}}$ 和类型 II 的敌手 $\mathcal{A}_{\text{II}}$, 通过模拟挑战者和敌手之间的两个游戏来证明方案的安全性. 两种类型的敌手分别介绍如下.

- 类型 I: 敌手 $\mathcal{A}_{\text{I}}$ 可以替换合法用户的公钥, 但不知道系统主密钥, 也指代恶意用户.
- 类型 II: 敌手 $\mathcal{A}_{\text{II}}$ 可以获得系统主密钥, 但不能替换合法用户的公钥, 也指代恶意 KGC.

游戏 1: 定义为敌手 $\mathcal{A}_{\text{I}}$ 和挑战者 $\mathcal{C}$ 之间的一个游戏. 在该游戏中, 将哈希函数 H_1 和 H_2 看作随机预言机 (random oracle, RO). 游戏包括 3 个阶段, 过程如下.

1) 初始化阶段: 挑战者 $\mathcal{C}$ 输入安全参数 τ 进行系统初始化, 生成系统公/私钥, 以及系统参数, $\mathcal{C}$ 将系统参数发送给敌手 $\mathcal{A}_{\text{I}}$.

2) 询问阶段: $\mathcal{A}_{\text{I}}$ 可以执行如下询问.

- H_1 询问: 当 $\mathcal{A}_{\text{I}}$ 选择 $(Addr, X, Y, P_{\text{Pub}})$ 执行该询问时, $\mathcal{C}$ 选择一个随机数 α, 并发送给 $\mathcal{A}_{\text{I}}$.
- H_2 询问: 当 $\mathcal{A}_{\text{I}}$ 选择 (X, Y, K, m, t) 执行该询问时, $\mathcal{C}$ 选择一个随机数 β, 并发送给 $\mathcal{A}_{\text{I}}$.
- 部分私钥询问: 当 $\mathcal{A}_{\text{I}}$ 选择 $Addr$ 执行该询问时, $\mathcal{C}$ 生成 $Addr$ 的部分私钥 (Y, cy), 并发送给 $\mathcal{A}_{\text{I}}$.
- 私钥询问: 当 $\mathcal{A}_{\text{I}}$ 选择 $Addr$ 执行该询问时, $\mathcal{C}$ 生成 $Addr$ 的私钥 SK, 并发送给 $\mathcal{A}_{\text{I}}$.
- 公钥询问: 当 $\mathcal{A}_{\text{I}}$ 选择 $Addr$ 执行该询问时, $\mathcal{C}$ 生成 $Addr$ 的公钥 PK, 并发送给 $\mathcal{A}_{\text{I}}$.
- 公钥替换询问: $\mathcal{A}_{\text{I}}$ 可以选择新的秘密值 x, 计算新公钥 PK^*, 并替换任意 $Addr$ 的原有公钥 PK_{Addr}.
- 签名询问: 当 $\mathcal{A}_{\text{I}}$ 选择 $(Addr, m)$ 执行该询问时, $\mathcal{C}$ 产生一个对消息 m 的签名, 并发送给 $\mathcal{A}_{\text{I}}$.

3) 伪造阶段: 经过概率多项式次询问后, $\mathcal{A}_{\text{I}}$ 选择一个消息 m^* 和一个目标地址 $Addr^*$, 伪造签名 σ^*, 然后向 $\mathcal{C}$ 提交 $<Addr^*, \sigma^*>$ 作为挑战. 如果下面的 3 个条件同时成立, 则称 $\mathcal{A}_{\text{I}}$ 在游戏 1 中获胜.

a) $\mathcal{A}_{\text{I}}$ 没有使用 $Addr^*$ 执行过部分私钥询问.

b) $\mathcal{A}_{\text{I}}$ 没有使用 $Addr^*$ 执行过私钥询问.

c) 伪造的签名能成功通过验证, 即: $1 \leftarrow Verify(Addr^*, m^*, \sigma^*, PK^*)$.

记 $\mathcal{A}_{\text{I}}$ 在游戏 1 中获胜的概率为:

$$Adv^{\tau}_{\mathcal{A}_{\text{I}}} = \Pr[1 \leftarrow Verify(Addr^*, m^*, \sigma^*, PK^*)].$$

定义 1. 在概率多项式时间内, 类型 I 的敌手 $\mathcal{A}_{\text{I}}$ 以可忽略的优势 $Adv^{\tau}_{\mathcal{A}_{\text{I}}}$ 在游戏 1 中取得胜利, 则称该无证书签名方案在适应性选择消息攻击下具有不可伪造性 (EUF-CMA).

游戏 2: 定义为敌手 $\mathcal{A}_{\text{II}}$ 和挑战者 $\mathcal{C}$ 之间的一个游戏, 与游戏 1 类似, 游戏 2 也包含了以下 3 个阶段.

1) 初始化阶段: 挑战者 $\mathcal{C}$ 输入安全参数 τ 进行系统初始化, 生成系统公/私钥, 以及系统参数, $\mathcal{C}$ 将系统参数及

系统私钥发送给敌手 $\mathcal{A}_{\mathrm{II}}$.

2) 询问阶段: 与游戏 1 中的询问阶段相同.

3) 伪造阶段: 经过概率多项式次询问后, 敌手 $\mathcal{A}_{\mathrm{II}}$ 选择一个目标地址 $Addr^*$, 并伪造签名 σ^*, 然后向 $\mathcal{C}$ 提交 $<Addr^*,\sigma^*>$ 作为挑战. 如果下面的 4 个条件同时成立, 则称 $\mathcal{A}_{\mathrm{II}}$ 在游戏 2 中获胜.

a) $\mathcal{A}_{\mathrm{II}}$ 没有使用 $Addr^*$ 执行过部分私钥询问.

b) $\mathcal{A}_{\mathrm{II}}$ 没有使用 $Addr^*$ 执行过私钥询问.

c) $\mathcal{A}_{\mathrm{II}}$ 没有进行过公钥替换询问.

d) 伪造的签名能成功通过验证, 即: $1 \leftarrow Verify(Addr^*, m^*, \sigma^*, PK^*)$.

记 $\mathcal{A}_{\mathrm{II}}$ 在游戏 2 中获胜的概率为:

$$Adv^{\tau}_{\mathcal{A}_{\mathrm{II}}} = \Pr[1 \leftarrow Verify(Addr^*, m^*, \sigma^*, PK^*)].$$

定义 2. 在概率多项式时间内, 若类型 II 的敌手 $\mathcal{A}_{\mathrm{II}}$ 以可忽略的优势 $Adv^{\tau}_{\mathcal{A}_{\mathrm{II}}}$ 在游戏 2 中取得胜利, 则称该无证书签名方案在适应性选择消息攻击下具有不可伪造性 (EUF-CMA).

2.4 区块链与智能合约

(1) 区块链

区块链由 Nakamoto[35]在 2008 年首次提出, 它是一种按照时间顺序将数据区块依次先后生成并连接成链且以密码学技术保证不可篡改和不可伪造的分布式账本. 在区块链中, 数据以区块的形式储存, 每一个区块记录了一段时间内发生的所有交易信息. 区块的数据结构由区块头和区块体组成, 其中区块头包含前一个区块的哈希值, 以此确保区块的顺序和不可篡改性. 区块体则包含了区块创建过程中产生的所有交易信息. 区块链可分为公有链、私有链和联盟链, 本文方案所使用的是联盟链. 联盟链是一种基于区块链技术的私有化网络, 由一组特定实体或组织共同管理和操作. 与公有链不同, 它只服务于特定组的成员, 成员只有在获得许可后才可以加入区块链, 并且参与者可以控制网络的操作和权限, 因此联盟链也叫许可链. 相比私有链, 联盟链更加灵活和开放; 相比公有链, 联盟链的读取权限受到限制, 可以更好地提供隐私保护. 联盟链中存在全节点和轻节点两种不同类型的节点, 它们具有不同的功能和角色.

a) 全节点: 联盟链的全节点是指在联盟链网络中具有完整区块链副本的节点, 它存储并维护着整个区块链的所有交易记录和状态数据. 全节点可以与其他节点进行点对点通信, 以更新自己的区块链副本, 同时也可以通过共识机制参与到区块链网络的交易验证和区块生成过程中.

b) 轻节点: 联盟链的轻节点是指在联盟链网络中不需要存储完整区块链的所有数据, 也不参与区块链的共识, 但可以通过与全节点通信来获取所需数据和验证交易的节点. 与全节点相比, 轻节点对计算资源和存储空间的需求更低, 因此更适合由车辆等资源有限的设备充当.

(2) 智能合约

智能合约是一种以代码形式编写的程序, 它能够在满足特定条件时自动执行预设的合约条款. 运行在区块链网络上的智能合约无需依赖中心化服务器或第三方机构, 从而降低信任成本, 增强系统的自主性和效率. 依托区块链的共识机制与加密技术, 智能合约具备防篡改和抗欺诈能力, 相较于传统合约更加安全可靠. 此外, 智能合约的执行过程透明可验证, 确保交易的公平性和可信度. 通过智能合约, 参与者能够在一个去信任、透明且不可篡改的区块链环境中实现自动化交易与协议执行. 本方案为车辆设置信誉值, 并将信誉值存储到区块链上, 并设计了如算法 1 所示的信誉值更新合约.

算法 1. 信誉值更新合约.

输入: t_i: 时间戳; $RS^{c}_{i,k}$: 被评车辆的当前信誉值; $Addr_{i,k}$: 被评车辆的区块链地址; $S = \{RS_{i,k} | i = 1,2,\ldots,N; k = 1,2,\ldots,n\}$: 参评车辆信誉值集合; $W = \{w_{i,k} | i = 1,2,\ldots,N; k = 1,2,\ldots,n\}$: 评价反馈等级集合, $w_{i,k}$ 表示来自 $V_{i,k}$ 的评价;
输出: $RS^{c+1}_{i,k}$: 被评车辆更新后的信誉值.

1. 步骤 1: 计算所共享消息的加权评价反馈得分
2. **While** $(T_c - t_i < \Delta t)$ **do** // T_c 表示当前时间, Δt 表示设定的阈值
3. $Num+ = RS_{i,k} \cdot w_{i,k}$
4. $Den+ = RS_{i,k}$
5. $Value = Num/Den$
6. **End while**
7. 步骤 2: 计算最新信誉值
8. $RS_{i,k}^{c+1} = RS_{i,k}^{c} + Value$
9. **If** $RS_{i,k}^{c+1} < RSthld$ **then**
10. Let $Addr_{i,k}$ into Blacklist //若车辆更新后的信誉值小于给定阈值, 则将其加入黑名单
11. **End if**
12. **Return** $RS_{i,k}^{c+1}$ //返回用户最新信誉值

说明: 信誉值可以衡量用户的诚实度, 它可以暗示用户发送消息的可信度与准确性. 接收消息的车辆可以根据该消息的有用性对该条消息进行评价反馈. 例如, 可以设定阈值为 $RSthld = 60$, 评价反馈等级的集合为 $w_i \in \{-2,-1,0,1,2\}$, 依次代表恶意、没有帮助、不确定、有帮助和非常有帮助这 5 个等级. 参评车辆将评分反馈结果发送给 VMC, 收到消息并验证参评者身份合法性后, VMC 调用部署在区块链上的信誉值更新合约来更新被评车辆的信誉值.

3 系统模型

3.1 网络模型

本方案的网络模型如图 1 所示, 其中包括车辆、交通管理中心、区块链和 5G 基站这 4 种类型的实体, 对参与网络的各实体的功能和细节描述如下.

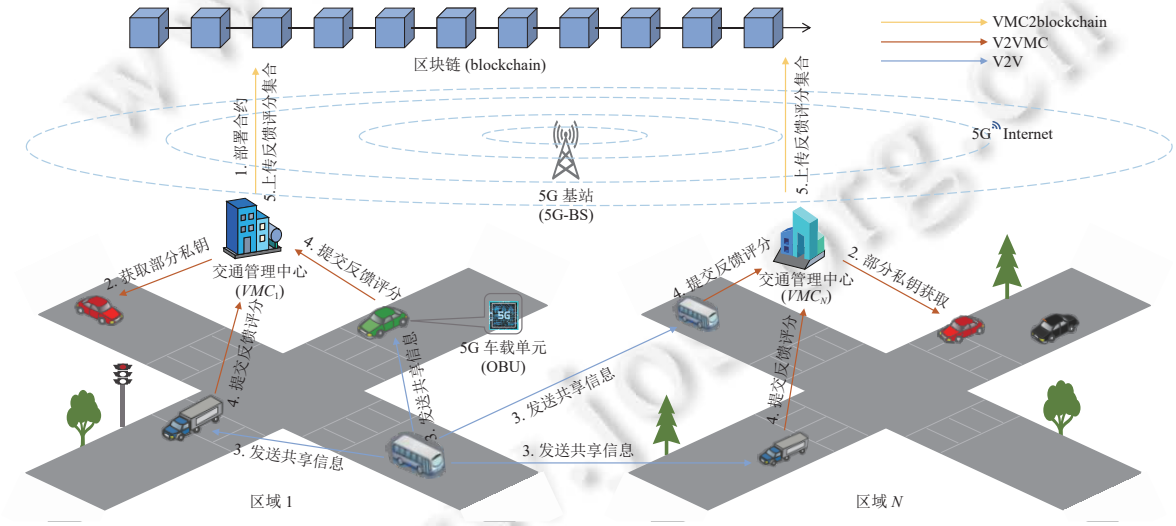

图 1 网络模型图

(1) 交通管理中心 (VMC): VMC 分布在各区域, 具有强大的计算和存储能力. 各区域的 VMC 作为全节点加入区块链, 共同维护联盟区块链, VMC 主要有以下 4 个功能.

a) 系统初始化: 各区域的 VMC 通过共识算法协商出系统所需参数, 进行系统初始化. 此外, VMC 需要将信誉值更新合约部署到区块链上.

b) 为本区域车辆生成部分私钥: 当车辆发送真实身份 RID 向本地 VMC 请求生成部分密钥时, 在确认了 RID 的合法性后, 为其分配区块链地址、生成部分私钥以及设定初始信誉值, 并上传到区块链. 此外, VMC 在本地数据库存储车辆地址和真实身份的键值对列表 $<Addr,RID>$, 保证方案的可追溯性.

c) 信誉票证 CT 发放: 为保证传输信息的机密性, 本文设计全局加密信誉票证 CT, 并设置了短暂的时间窗口. 在不同的时间段, VMC 需要为信誉值大于阈值的车辆发放最新的信誉票证.

d) 反馈结果收集: VMC 需要收集来自车辆的评价反馈结果, 并在验证反馈者身份的合法性后将反馈结果上传到区块链上, 调用部署在区块链上的智能合约计算出车辆最新的信誉值.

(2) 车辆 V_k (vehicle): 车辆装有内置的车载单元 OBU (on board unit), 具备一定的计算和存储能力, 可以存储车辆的隐私数据, 并提供简单的密码运算. 假设 OBU 支持 5G 网络协议, 是一种防篡改的设备, 它为车辆提供无线通信能力. 每个车辆作为轻节点加入区块链, 具有访问区块链上数据的权限.

(3) 区块链 (blockchain): 本文采用区块链的类型是联盟链, 它由每个区域的 VMC 共同维护, 区块链上存储有 $<Addr,RS>$ 列表, 通过区块链的共识算法, 每个区域的 VMC 能同步车辆的 $<Addr,RS>$ 信息以及每个域的 VMC 公钥. 另外, 通过区块链上部署的智能合约可以实现信誉值更新等.

(4) 5G 基站 (5G base station, 5G-BS): 为 IoV 提供高速率的信息传输, 由于 5G 基站的存在, 可以实现 V2VMC 和 V2V 之间的快速通信. 假设 5G 网络能够很好地覆盖所有区域, 且传输速度足够快.

3.2 系统假设

本文提出的半分布式认证加密方案基于一些合理的假设, 在一定条件下可以满足. 这些假设分别如下.

(1) 存储在车辆 OBU 中的秘密数据不可能被其他人获得, 也不能被篡改.

(2) 由 5G-BS 提供的 5G 网络足以覆盖所有地域, IoV 的各部分时间保持同步.

(3) 大部分车辆在与其他车辆通信后做出的反馈是客观诚实的.

4 方案设计

本文所提的方案总共包括系统初始化、密钥生成、加密签名、解密验证和信誉值更新这 5 个阶段. 方案整体流程如后文图 2 所示. 本文中使用的符号见后文表 2.

4.1 系统初始化

(1) 假设共有 N 个 VMC, 组成的集合表示为 $\{VMC_i|i=1,2,\ldots,N\}$. 各区域的 VMC 通过共识机制协商生成椭圆曲线 E、安全参数 τ、大素数 p和q, 随机种子 $Seed$ 以及 3 个抗碰撞 Hash 函数 H_1, H_2, h.

(2) VMC_i 选择随机数 $sk_i \in Z_q^*$ 作为自己的私钥, 计算对应的公钥 $P_{\text{Pub-}i}=sk_iP$. 初始化生成的系统公开参数为 $SP=\{p,q,P,H_1,H_2,h,P_{\text{Pub-1}},P_{\text{Pub-2}},\ldots,P_{\text{Pub-}i}\}$.

(3) 各方 VMC 通过共识算法选举代表成员 (假设选择 VMC_1) 部署如算法 1 所示的信誉值更新合约, 将系统参数 SP 上传到区块链.

(4) 各区域的 VMC 利用协商的随机种子 $Seed$, 使用如图 3 所示的反向哈希链生成信誉票证集合 $\{CT_i|i=1,2,\ldots,n\}$, 其中 $h^i(Seed)$ 表示对 $Seed$ 执行过 i 次哈希运算, 如 $h^2(Seed)=h(h(Seed))=CT_{n-1}$. 另外, 为了加密的安全性, CT_i 仅在时间范围内有效, 例如在时间 T_0-T_1 内的有效信誉票证为 CT_1. VMC 定期为信誉值大于阈值的合法用户发放最新的信誉票证 CT_i, 用户可以通过检查等式 $h^{i-(i-k)}(CT_i)=CT_{i-k}$ 是否成立来检查 VMC 更新的 CT_i 是否有效. 当 CT_i 全部耗尽的时候, VMC 协商新的 $Seed'$ 执行相同的操作进行下一轮的加密通信.

4.2 密钥生成

车辆集合定义为 $\{V_{i,k}|i=1,2,\ldots,N;k=1,2,\ldots,n\}$, 其中 i 表示车辆所属的域, k 表示车辆的序号. 假设每个 $V_{i,k}$ 拥有唯一且不重复的真实身份标识 $RID_{i,k}$, $RID_{i,k}$ 由汽车出厂商在生产时为车辆设置. $V_{i,k}$ 生成密钥的步骤如下.

1) $V_{i,k}$ 发送 $RID_{i,k}$ 给当地的 VMC_i, VMC_i 检查 $RID_{i,k}$ 的合法性. 若合法, 则进入下一步; 否则终止.

图 2　方案流程图

表 2　符号定义

符号	描述
$P_{Pub\text{-}i}$	区域 i 中 VMC_i 的公钥
sk_i	区域 i 中 VMC_i 的私钥
$RID_{i,k}$	区域 i 中第 k 个车辆的真实身份
$Addr_{i,k}$	区域 i 中第 k 个车辆的区块链地址
$SK_{i,k}=(x_{i,k}, py_{i,k})$	区域 i 中第 k 个车辆的私钥
$PK_i=(X_i, Y_i)$	区域 i 中第 k 个车辆的公钥
m_i	消息
σ_i	对消息 m_i 的签名
CT_i	信誉票证
$RS_{i,k}$	区域 i 中车辆 k 的信誉值
t_i	时间戳

2) VMC_i 为 $RID_{i,k}$ 分配区块链地址 $Addr_{i,k}$, 允许其作为轻节点加入区块链.

3) $V_{i,k}$ 选择随机数 $x_{i,k} \in Z_q^*$ 作为秘密值, 计算 $X_{i,k}=x_{i,k}P$, 并发送 $X_{i,k}$ 和 $Addr_{i,k}$ 给本地 VMC_i.

4) VMC_i 选择 $y_{i,k} \in Z_q^*$, 计算 $Y_{i,k}=y_{i,k}P$, $py_{i,k}=(y_{i,k}+sk_i \cdot H_1(Addr_{i,k},X_{i,k},Y_{i,k},P_{\text{Pub-}i})) \bmod q$ 和 $cpy_{i,k}=py_{i,k} \oplus H_3(sk_iX_{i,k})$, 返回部分公钥和加密后的部分私钥 $(Y_{i,k},cpy_{i,k})$ 对给 $V_{i,k}$.

5) 收到消息后, $V_{i,k}$ 解密得 $py_{i,k}=cpy_{i,k} \oplus H_3(sk_iX_{i,k})$, 生成完整私钥 $SK_{i,k}=(x_{i,k},py_{i,k})$ 和完整公钥 $PK_{i,k}=(X_{i,k},Y_{i,k})$. 此外, $V_{i,k}$ 可以通过检查等式 $Y_{i,k}=H_1(Addr_{i,k},X_{i,k},Y_{i,k},P_{\text{Pub-}i})P_{\text{Pub-}i}+py_{i,k}P$ 是否成立来判断收到密钥的正确性;

6) VMC_i 为 $V_{i,k}$ 生成初始信誉值 $RS_{i,k}$, 上传 $<Addr_{i,k},PK_{i,k},RS_{i,k}>$ 到区块链, 并返回最新的 CT_i 给 $V_{i,k}$.

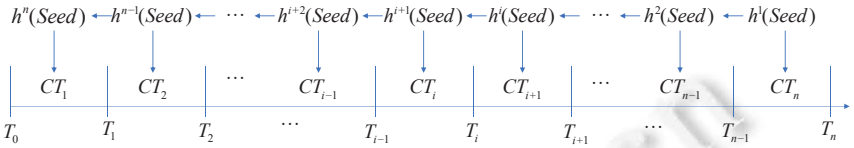

图 3 反向哈希链生成信誉票证

4.3 加密签名

为了同时保证消息的机密性、完整性和身份认证, 当车辆 $V_{i,k}$ (发送者) 给邻车 (接收者, 来自不同的域) 发送共享信息 m_i 时, 需要对 m_i 进行签名和加密, 具体执行步骤如下.

1) $V_{i,k}$ 选择随机数 $l_{i,k} \in Z_q^*$, 计算 $L_{i,k}=l_{i,k}P$, $\beta_{i,k}=H_2(X_{i,k},Y_{i,k},K_{i,k},m_i,t_i)$, $C_1=L_{i,k} \oplus CT_i$ 和 $C_2=m_i \oplus CT_i$, 其中 t_i 表示时间戳. 然后生成签名 $\sigma_{i,k}=l_{i,k}+(x_{i,k}+cy_{i,k})\beta_{i,k}$.

2) $V_{i,k}$ 发送 $\{Addr_{i,k},C_1,C_2,\sigma_{i,k},t_i\}$ 给接收者.

4.4 解密验证

为了确保消息的完整性以及消息来源的可靠性, 接收者需要对消息进行解密并验证签名的正确性, 具体执行步骤如下.

1) 收到消息 $\{Addr_{i,k},C_1,C_2,\sigma_{i,k},t_i\}$ 后, 接收者首先检查时间戳 t_i 的有效性, 若时间戳无效, 则丢弃该消息, 否则执行下一步.

2) 接收者使用 CT_i 分别计算 $L_i=CT_i \oplus C_1$ 和 $m_i=CT_i \oplus C_2$ 获得 $L_{i,k}$ 和 m_i.

3) 接收者计算 $\alpha_{i,k}=H_1(Addr_{i,k},X_{i,k},Y_{i,k})$ 和 $\beta_{i,k}=H_2(X_{i,k},Y_{i,k},L_{i,k},m_i,t_i)$, 然后验证公式 (1) 是否成立, 若成立, 则说明消息完整且来源可靠, 接收消息, 否则拒绝.

$$\sigma_{i,k}P=L_{i,k}+\beta_{i,k}(X_{i,k}+Y_{i,k})+\alpha_{i,k}\beta_{i,k}P_{\text{Pub-}i} \tag{1}$$

4.5 信誉值更新

车辆可以根据接收消息的有用性为其评价, 并将反馈结果发送给 VMC. VMC 调用部署在区块链上的算法 1 所示的信誉值更新合约, 更新车辆的信誉值.

此外, 为了鼓励车辆积极参与评价反馈, 可以设置激励机制, 如: 参与评价反馈可以获得额外信誉值、信誉值高于某个阈值的车辆可以享受车险优惠或修理优惠等.

5 安全性证明与分析

在本节中, 对本文方案做了形式化的安全性证明和非形式化的安全性分析 (每个区域的算法相同, 证明和分析方法也相同, 故以一个区域为例进行证明).

5.1 安全性证明

定理 1. 在基于 ECDLP 假设和 ROM 的帮助下, 若敌手 $\mathcal{A}_{\text{I}}$ 能在概率多项式时间内, 以不可忽略的优势 $\varepsilon \geqslant 10(q_s+1)(q_s+q_2)/2^k$ 赢得游戏 1 (假设最多进行 q_i 次 H_i 询问, q_s 次签名询问), 则挑战者 $\mathcal{C}$ 能在概率多项式时间内, 以不可忽略的优势 $1/(9q_1q_2)$ 解决 ECDLP 假设.

证明: 假设挑战者 $\mathcal{C}$ 想解决 ECDLP 假设, 其输入是 $(ss\cdot P,P)$, 若他能计算出 ss 作为该问题的解. 则称挑战者 $\mathcal{C}$ 可以解决 ECDLP 假设.

初始化阶段: 挑战者 $\mathcal{C}$ 输入安全参数 τ 进行系统初始化, 产生系统参数 $\{p,q,P,P_{\text{Pub}},H_1,H_2\}$, 其中 $P_{\text{Pub}}=ss\cdot P$. 挑战者 $\mathcal{C}$ 发送系统参数给敌手 $\mathcal{A}_{\text{I}}$. 安全模型将哈希函数 H_1, H_2 看成 RO.

询问阶段: $\mathcal{A}_{\text{I}}$ 可以自适应地向 $\mathcal{C}$ 发起下列询问.

1) H_1 询问: 挑战者 $\mathcal{C}$ 维护列表 L_1, 列表结构为 $<Addr,X,Y,P_{\text{Pub}},\alpha>$ 且初始化为空. 当敌手 $\mathcal{A}_{\text{I}}$ 使用元组 $<Addr_i,X_i,Y_i,P_{\text{Pub}}>$ 进行 H_1 询问时, 如果元组已经存在列表 L_1 中, 则返回 α_i; 否则, $\mathcal{C}$ 随机选择 $\alpha_i\in Z_q^*$, 将 $<Addr_i,X_i,Y_i,\alpha_i>$ 加入列表 L_1, 并返回 α_i 给 $\mathcal{A}_{\text{I}}$.

2) H_2 询问: 挑战者 $\mathcal{C}$ 维护列表 L_2, 列表结构为 $<X,Y,L,m,t,\beta>$ 且初始化为空. 当敌手 $\mathcal{A}_{\text{I}}$ 使用元组 $<X_i,Y_i,L_i,m_i,t_i>$ 进行 H_2 询问时, 如果元组已经存在列表 L_2 中, 则返回 β_i; 否则, $\mathcal{C}$ 随机选择 $\beta_i\in Z_q^*$, 将 $<X_i,Y_i,K_i,m_i,t_i>$ 加入列表 L_2, 并返回 β 给 $\mathcal{A}_{\text{I}}$.

3) 部分私钥询问: 挑战者 $\mathcal{C}$ 维护列表 L_{py}, 列表结构为 $<Addr,py,Y,c>$ 且初始为空. 当敌手 $\mathcal{A}_{\text{I}}$ 使用 $Addr_i$ 进行密钥提取询问时, 若元组已经存在列表中, 则返回给 $\mathcal{A}_{\text{I}}$; 否则, $\mathcal{C}$ 抛掷偏心硬币 $c\in\{0,1\}$ ($\Pr[c=1]=\dfrac{1}{q_1+1}$, $\Pr[c=0]=\dfrac{q_1}{q_1+1}$), 当 $c=1$ 时, 令 $py=\perp$, 返回 $\perp$ 给 $\mathcal{A}_{\text{I}}$; 当 $c=0$ 时, $\mathcal{C}$ 随机选择 $py_i\in Z_q^*$ 计算 $Y_i=py_iP-\alpha_iP_{\text{Pub}}$, 将 $<Addr_i,py_i,Y_i>$ 加入列表 L_{py}, 并返回 $<py_i,Y_i>$ 给 $\mathcal{A}_{\text{I}}$.

4) 私钥询问: 挑战者 $\mathcal{C}$ 维护列表 L_{SK}, 列表结构为 $<Addr,x,py>$ 且初始为空. 当敌手 $\mathcal{A}_{\text{I}}$ 使用 $Addr_i$ 进行私钥提取询问时, 若元组已经存在列表 L_{SK} 中, 则返回给 $\mathcal{A}_{\text{I}}$; 否则, $\mathcal{C}$ 询问列表 L_{py}, 若 $c=1$, 则终止; 否则, $\mathcal{C}$ 随机选择 $x_i,py_i\in Z_q^*$, 将 $<Addr_i,x_i,py_i>$ 加入列表 L_{SK}, 并返回 $<x_i,py_i>$ 给 $\mathcal{A}_{\text{I}}$.

5) 公钥询问: 挑战者 $\mathcal{C}$ 维护列表 L_{PK}, 列表结构为 $<Addr,X,Y>$ 且初始为空. 当敌手 $\mathcal{A}_{\text{I}}$ 使用 $Addr_i$ 进行公钥提问时, 若元组已经存在列表 L_{PK} 中, 则返回给 $\mathcal{A}_{\text{I}}$; 否则, $\mathcal{C}$ 询问列表 L_{py}, 若 $c=1$, $\mathcal{C}$ 随机选择 $x_i,y_i\in Z_q^*$, 计算 $X_i=x_iP$ 和 $Y_i=y_iP$, 将 $<Addr_i,X_i,Y_i,c>$ 加入列表 L_{PK}, 并返回给 $\mathcal{A}_{\text{I}}$; 若 $c=0$, 运行部分私钥询问, 从 L_{cy} 中获得 $<Y_i,py_i>$. 然后, $\mathcal{C}$ 随机选择 $x_i\in Z_q^*$, 将 $<Addr_i,py_i,x_i>$ 和 $<Addr_i,X_i,Y_i>$ 分别加入到 L_{SK} 列表和 L_{PK} 列表, 并返回给 $\mathcal{A}_{\text{I}}$.

6) 公钥替换询问: 敌手 $\mathcal{A}_{\text{I}}$ 可以进行公钥替换, 即使用 $<Addr_i,X_i',Y_i'>$ 替换 $<Addr_i,X_i,Y_i>$.

7) 签名询问: 当 $\mathcal{A}_{\text{I}}$ 使用 $<Addr_i,m_i>$ 进行该询问时, $\mathcal{C}$ 先在列表 L_{py} 中查询 $<Addr_i,py_i,Y_i,c>$, 若 $c=1$, 则终止; 否则 $\mathcal{C}$ 在列表 L_{SK} 中查询得到 $<Addr_i,x_i,py_i>$. 然后 $\mathcal{C}$ 选择随机数 $l_i\in Z_q^*$, 计算 $L_i=l_iP$, $\alpha_i=H_1(Addr_i,X_i,Y_i)$, $\beta_i=H_2(X_i,Y_i,L_i,m_i,t_i)$, $\sigma_i=l^{-1}(x_i+py_i+\beta_i)$, 返回签名 σ_i 给 $\mathcal{A}_{\text{I}}$.

伪造阶段: 经过概率多项式次数询问后, 敌手 $\mathcal{A}_{\text{I}}$ 成功伪造对 $Addr'$ 的两个合法签名 σ_1 和 σ_2, 若签名伪造成功, 说明等式 $\sigma_1P=L+\beta(X'+Y')+\alpha_1\beta P_{\text{Pub}}$ 和 $\sigma_2P=L+\beta(X'+Y')+\alpha_2\beta P_{\text{Pub}}$ 成立.

根据叉子引理 (forking lemma)[36], $\mathcal{C}$ 可以计算出 $ss=(\sigma_1-\sigma_2)/\beta(\alpha_1-\alpha_2)$ 作为 ECDLP 假设的解; 否则, $\mathcal{C}$ 没有解决 ECDLP 假设. 若 $\mathcal{A}_{\text{I}}$ 对 $Addr'$ 进行过部分私钥询问或者私钥询问, 则 $\mathcal{C}$ 失败. $\mathcal{A}_{\text{I}}$ 不进行这种询问的概率至少是 $1/q_1^2$; 若 $\mathcal{A}_{\text{I}}$ 对 L^* 进行过 H_2 询问, 则 $\mathcal{C}$ 失败, $\mathcal{A}_{\text{I}}$ 不进行这种询问的概率大于 $1/q_2$; 利用预言机重放技术产生两个或以上有效签名时, 失败的概率小于 1/9. 因此, 解决 ECDLP 假设的优势为:

$$Adv_{\mathcal{A}_{\text{I}}}^{\tau}\geqslant 1/9q_1^2q_2.$$

定理 2. 在基于 ECDLP 假设和 ROM 的帮助下, 若敌手 $\mathcal{A}_{\text{II}}$ 能在概率多项式时间内, 以不可忽略的优势 $\varepsilon\geqslant 10(q_s+1)(q_s+q_2)/2^k$ 赢得游戏 2 (假设最多进行 q_i 次 H_i 询问, q_s 次签名询问), 则挑战者 $\mathcal{C}$ 能在概率多项式时间内, 以不可忽略的优势 $1/(9q_1q_2)$ 解决 ECDLP 假设.

证明: 假设挑战者 $\mathcal{C}$ 想解决 ECDLP 假设, 其输入是 $(xx\cdot P,P)$, 若他能计算出 xx 作为该问题的解. 则称挑战者 $\mathcal{C}$ 可以解决 ECDLP 假设.

初始化阶段: 挑战者 $\mathcal{C}$ 输入安全参数 τ 进行系统初始化, 产生系统参数 $\{p,q,P,P_{\text{Pub}},H_1,H_2\}$, 其中 $P_{\text{Pub}}=ss\cdot P$. 挑战者 $\mathcal{C}$ 发送系统参数和 ss 给敌手 $\mathcal{A}_{\text{I}}$. 安全模型将哈希函数 H_1和H_2 看成 RO.

询问阶段: 敌手 $\mathcal{A}_{\mathrm{II}}$ 可以进行定理 1 中除“签名验证”和“公钥替换”之外的所有询问.

伪造阶段: 经过概率多项式次数询问后, 敌手 $\mathcal{A}_{\mathrm{II}}$ 成功伪造对 $Addr'$ 的两个合法签名 σ_1 和 σ_2, 若签名伪造成功, 说明等式 $\sigma_1 P = L + \beta(X' + Y') + \alpha_1 \beta P_{\mathrm{Pub}}$ 和 $\sigma_2 P = L + \beta(X' + Y') + \alpha_2 \beta P_{\mathrm{Pub}}$ 成立.

$\mathcal{C}$ 知道系统主密钥 ss, 因此 $\mathcal{C}$ 可以计算出 $(xx + py) = ((\sigma_1 - \sigma_2) - (\alpha_2\beta_2 - \alpha_1\beta_1)ss)/(\beta_1 - \beta_2)$, 然后通过检索列表 L_{SK} 得到 xx 作为 ECDLP 假设的解; 否则, $\mathcal{C}$ 没有解决 ECDLP 假设. 若 $\mathcal{A}_{\mathrm{II}}$ 对 $Addr'$ 进行过部分私钥询问或者私钥询问, 则 $\mathcal{C}$ 失败. $\mathcal{A}_{\mathrm{II}}$ 不进行这种询问的概率至少是 $1/q_1^2$; 若 $\mathcal{A}_{\mathrm{II}}$ 对 L 进行过 H_2 询问, 则 $\mathcal{C}$ 失败, $\mathcal{A}_{\mathrm{II}}$ 不进行这种询问的概率大于 $1/q_2$; 利用预言机重放技术产生两个或以上有效密文时, 失败的概率小于 1/9. 因此, 解决 ECDLP 假设的优势为:

$$Adv^{\tau}_{\mathcal{A}_{\mathrm{II}}} \geqslant 1/9q_1^2q_2.$$

5.2 安全性分析

本节将分析本文方案如何满足 IoV 的安全需求, 并探讨其能够抵抗的常见攻击类型, 具体论述如下.

(1) 消息认证: 所传输的共享消息均由发送者使用私钥进行签名, 由于 ECDLP 假设的存在, 敌手无法伪造合法用户的签名, 当且仅当公式 (1) 成立, 证明消息来自于合法的发送者.

(2) 完整性: 在签名阶段, 所传输的共享消息 m 被嵌入到 $\beta = H_2(X, Y, L, m, t)$ 中, 若消息 m 被篡改, 则 β 发生变化, 导致公式 (1) 不成立, 进而无法通过认证, 因此方案能保证消息的完整性.

(3) 机密性: 所有共享的消息 m 都用 CT_i 加密传输, 只有合法且信誉值大于阈值的车辆才能获得 CT_i 解密出明文 m, 且 CT_i 的短暂生命周期进一步保证了消息的机密性.

(4) 匿名性: 区块链为车辆分配区块链地址 $Addr$, 根据地址无法推断出车辆的真实身份 RID, 基于区块链地址而非真实身份进行信息共享, 保证了车辆的匿名性.

(5) 可追溯性: 车辆的真实身份 RID 保存在 VMC 中, 一旦车辆发送恶意消息而被举报, VMC 可以根据区块链地址 $Addr$ 匹配到车辆真实身份 RID, 进而追溯到车辆的真实身份.

(5) 不可否认性: 车辆发送的每条共享消息都进行了签名, 安全性证明表示, 敌手无法伪造合法用户的签名, 且签名具有不可否认性, 故任何人都无法否认所发送过的消息.

(7) 缓解单点故障: 本文采用区域中心化管理方式替代传统的完全中心化管理, 各区域的车辆在本区域内注册并生成私钥, 而各区域的密钥可在全局范围内可使用, 从而实现半分布式的密钥管理. 这种机制减少了对单一中心节点的依赖, 提高了系统的可靠性和安全性.

(8) 抗普通攻击: 本方案能够抵御 IoV 场景中常见的攻击类型, 具体描述如下.

a) 抗重放攻击: 指攻击者通过拦截和重复发送过时的信息, 欺骗系统执行未授权操作. 在本文的方案中, 每条共享的消息 m 都包含时间戳 t, 且被嵌入 $\beta = H_2(X, Y, L, m, t)$, 既保证了时间戳的完整性, 也绑定了 m. 通过检查时间戳的有效性, 接收者可以发现重放的消息, 因此本文的方案能抵御重放攻击.

b) 抗修改攻击: 指攻击者通过截取信道中所传输的信息, 修改部分内容后重新发送给其他车辆. 本文对所传输的共享消息都做了签名操作, 一旦消息内容被攻击者修改, 这将导致公式 (1) 不成立, 敌手无法对其进行修改.

c) 抗中间人攻击: 指敌手通过虚拟出一个中间节点, 放置在通信双方中间, 使得通信双方误以为他们正在直接进行通信, 从而能够窃取、篡改或伪造通信内容. 因为本文的方案能够实现消息认证、完整性和不可否认性, 所以该方案能够抵御中间人攻击.

d) 降低 DoS 攻击: 指攻击者通过大量无效请求过载目标系统, 导致正常服务无法进行. 本文采用半分布式密钥管理机制, 将密钥生成和管理分散到多个区域, 减少了对单一中心节点的依赖. 即使某个区域受到攻击, 其他区域仍能继续提供服务, 从而提高了系统的可靠性和抗攻击能力, 有效缓解了 DoS 攻击的影响.

6 实验评估

为评估本方案的可行性, 本节分别对其计算开销和通信开销进行分析与对比, 并对所部署的智能合约的 Gas

消耗情况进行评估. 为了保证方案的安全性以及对比的公平性, 本文选择了相同的非奇异椭圆曲线 E: $y^2 = x^3 + ax + b \bmod q$, 其中 $a,b \in Z_q^*$, G 是 E 上的 q 阶加法群, p 和 q 是两个长度为 256 bits (32 Bytes) 的大素数. 基于 MIRACL 库, 将本实验部署在硬件设备配置为 Intel(R) Core(TM) i5-9500 CPU 3.00 GHz 的处理器、8.00 GB 的 RAM 和 Windows 10 系统上, 该硬件配置和车辆的 OBU 配置几乎相似. 相关密码运算符号及开销如表 3 所示. 其中密码运算时间取 1 000 次运算的平均值.

表 3　相关操作开销或长度

符号	说明	时间或长度开销
T_{pa}	执行一次ECC上的点加法操作的时间开销	0.016 ms
T_{sm}	执行一次ECC上的标量乘法操作的时间开销	3.052 ms
T_{inv}	执行一次模逆运算的时间开销	0.021 ms
T_h	执行一次哈希运算的时间	0.002 ms
$\|G\|$	ECC群中元素的长度	40 Bytes
$\|Z_q^*\|$	整数群中元素的长度	20 Bytes

6.1　计算开销

本文方案在执行单次消息签名、单次签名验证, 以及单次签名与验证的总开销等方面, 与多种均不使用双线性配对运算的无证书签名方案的对比结果如表 4 所示.

表 4　各方案计算开销对比

方案	消息签名开销	签名验证开销	总开销	抗 $\mathcal{A}_{\mathrm{I}}$ 攻击	抗 $\mathcal{A}_{\mathrm{II}}$ 攻击
文献[7]	$1T_{sm}+2T_h$	$4T_{sm}+3T_{pa}+3T_h$	$5T_{sm}+3T_{pa}+5T_h$	√	√
文献[8]	$3T_{sm}+1T_{pa}+2T_h$	$2T_{sm}+2T_{pa}+1T_h$	$5T_{sm}+3T_{pa}+3T_h$	×	×
文献[9]	$1T_{sm}+1T_{inv}$	$3T_{sm}+2T_{pa}+2T_h$	$4T_{sm}+2T_{pa}+2T_h+1T_{inv}$	×	×
文献[10]	$1T_{sm}+1T_h$	$3T_{sm}+3T_{pa}+2T_h$	$4T_{sm}+3T_{pa}+3T_h$	√	√
文献[11]	$1T_{sm}+1T_h$	$4T_{sm}+3T_{pa}+2T_h$	$5T_{sm}+3T_{pa}+3T_h$	×	√
文献[19]	$1T_h$	$3T_{sm}+2T_{pa}+2T_h$	$3T_{sm}+2T_{pa}+3T_h$	×	×
文献[20]	$1T_{sm}+2T_h$	$4T_{sm}+3T_{pa}+3T_h$	$5T_{sm}+3T_{pa}+5T_h$	√	√
文献[27]	$1T_{sm}+1T_h$	$3T_{sm}+2T_{pa}+2T_h$	$4T_{sm}+2T_{pa}+3T_h$	×	×
文献[28]	$1T_{sm}+2T_h+1T_{inv}$	$4T_{sm}+2T_{pa}+2T_h$	$5T_{sm}+2T_{pa}+2T_h+1T_{inv}$	×	×
文献[29]	$1T_{sm}+2T_h+1T_{inv}$	$4T_{sm}+2T_{pa}+3T_h$	$5T_{sm}+2T_{pa}+5T_h+1T_{inv}$	×	√
文献[30]	$1T_{sm}+2T_h+1T_{inv}$	$4T_{sm}+2T_{pa}+3T_h$	$5T_{sm}+2T_{pa}+5T_h+1T_{inv}$	×	√
文献[34]	$1T_{sm}+2T_h+1T_{inv}$	$4T_{sm}+3T_{pa}+3T_h$	$5T_{sm}+3T_{pa}+5T_h+1T_{inv}$	√	√
本文	$1T_{sm}+1T_h$	$3T_{sm}+3T_{pa}+2T_h$	$4T_{sm}+3T_{pa}+3T_h$	√	√

以文献 [7] 为例进行分析, 发送者在消息签名阶段需要执行 1 次 ECC 上的标量乘法操作和 2 次哈希运算, 即发送者进行一次签名所需要的计算开销是 $1T_{sm}+2T_h \approx 3.056$ ms; 接收者在签名验证阶段需要执行 4 次 ECC 上的标量乘法操作、3 次 ECC 上的点加法操作和 3 次哈希运算, 即接收者进行一次签名验证所需的计算开销是 $4T_{sm}+3T_{pa}+3T_h \approx 12.262$ ms.

在本文的方案中, 发送者在签名阶段需要执行 1 次 ECC 上的标量乘法操作和 1 次哈希运算, 即发送者进行一次签名所需要的计算开销是 $1T_{sm}+1T_h+1T_{inv} \approx 3.054$ ms; 接收者在签名验证阶段需要执行 3 次 ECC 上的标量乘法操作、3 次 ECC 上的点加法操作和 2 次哈希运算, 即接收者进行一次签名验证所需的计算开销是 $3T_{sm}+3T_{pa}+2T_h \approx 9.208$ ms. 其余方案的分析方法均相同, 故不再赘述.

各方案的消息签名、签名验证和总开销可视化对比如图 4 所示. 由图 4 可以看出, 在消息签名方面, 除了文献 [9,19] 因其未绑定随机数 (方案均不安全) 而具有极低的时间开销外, 其他方案的时间开销波动不大; 在签名验

证方面, 文献 [8] 具有最低的开销, 本文的方案与文献 [9,10,19,27] 的开销相当, 但均低于文献 [7,11,20,28−30,34]; 然而, 从一轮签名和签名验证的总开销来看, 虽然文献 [9,19] 明显由于其他方案, 但这两个文献所提供的方案都被证明了是不安全的, 而本文的方案与文献 [10,27] 的开销相当, 且均低于文献 [7,8,11,20,28−30,34]. 鉴于其他方案均已被证明无法完全抵御两种类型的敌手攻击, 我们应重点关注能够同时抵御这两类攻击的方案[7,10,20,34], 分析表明, 本文方案与文献 [10] 的总开销相当, 且均低于文献 [7,10,20,34].

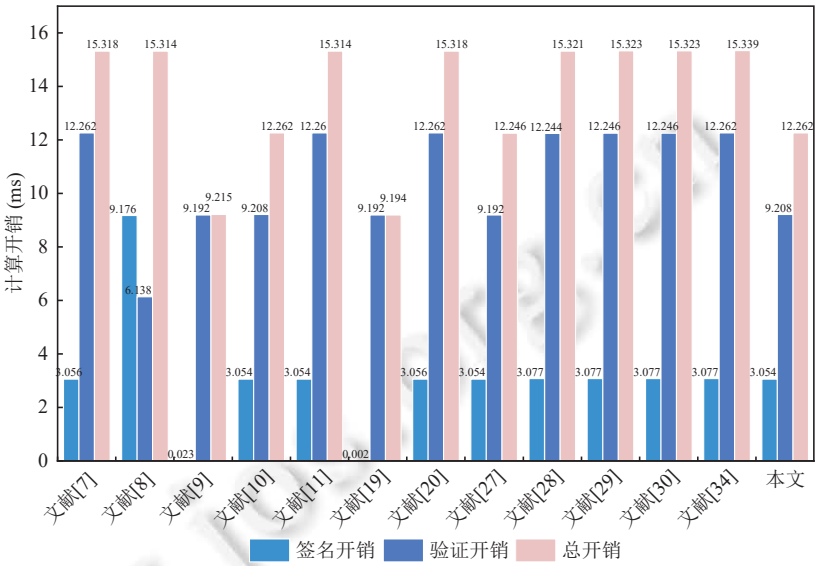

图 4 各方案计算开销对比图

6.2 通信开销

本文方案在签名长度、私钥长度、公钥长度和公/私钥总长度等方面, 与多种均不使用双线性配对运算的无证书签名方案的对比结果如表 5 所示.

表 5 各方案通信开销对比

方案	签名长度	私钥长度	公钥长度	公/私钥总长度	抗 $\mathcal{A}_{\mathrm{I}}$ 攻击	抗 $\mathcal{A}_{\mathrm{II}}$ 攻击
文献[7]	$1\|G\|+1\|Z_q^*\|$	$2\|Z_q^*\|$	$2\|G\|$	$2\|Z_q^*\|+2\|G\|$	√	√
文献[8]	$1\|Z_q^*\|$	$1\|Z_q^*\|$	$1\|G\|$	$1\|Z_q^*\|+1\|G\|$	×	×
文献[9]	$1\|Z_q^*\|$	$2\|Z_q^*\|$	$2\|G\|$	$2\|Z_q^*\|+2\|G\|$	×	×
文献[10]	$1\|G\|+1\|Z_q^*\|$	$2\|Z_q^*\|$	$2\|G\|$	$2\|Z_q^*\|+2\|G\|$	√	√
文献[11]	$1\|G\|+1\|Z_q^*\|$	$2\|Z_q^*\|$	$1\|G\|$	$2\|Z_q^*\|+1\|G\|$	×	√
文献[19]	$2\|G\|+1\|Z_q^*\|$	$2\|Z_q^*\|$	$2\|G\|$	$2\|Z_q^*\|+2\|G\|$	×	×
文献[20]	$1\|G\|+1\|Z_q^*\|$	$2\|Z_q^*\|$	$2\|G\|$	$2\|Z_q^*\|+2\|G\|$	√	√
文献[27]	$1\|G\|+1\|Z_q^*\|$	$2\|Z_q^*\|$	$1\|G\|$	$2\|Z_q^*\|+1\|G\|$	×	×
文献[28]	$1\|G\|+1\|Z_q^*\|$	$2\|Z_q^*\|$	$2\|G\|$	$2\|Z_q^*\|+2\|G\|$	×	×
文献[29]	$1\|G\|+1\|Z_q^*\|$	$2\|Z_q^*\|$	$2\|G\|$	$2\|Z_q^*\|+2\|G\|$	×	√
文献[30]	$1\|G\|+1\|Z_q^*\|$	$2\|Z_q^*\|$	$2\|G\|$	$2\|Z_q^*\|+2\|G\|$	×	√
文献[34]	$\|G\|+1\|Z_q^*\|$	$2\|Z_q^*\|$	$1\|G\|$	$2\|Z_q^*\|+1\|G\|$	√	√
本文	$1\|Z_q^*\|$	$2\|Z_q^*\|$	$2\|G\|$	$2\|Z_q^*\|+2\|G\|$	√	√

以文献 [7] 为例进行分析, 文献 [7] 生成的签名是 $\delta=(T,\sigma)$, 其中 $T\in G$, $\sigma\in Z_q^*$, 因此签名的长度为 $1|G|+1|Z|=60$ Bytes; 发送者的私钥是 $SK=(x,d)$, 其中 $x,d\in Z_q^*$, 因此私钥长度为 $2|Z|=40$ Bytes; 发送者的公钥是

$PK=(X,R)$, 其中 $X,R\in G$, 因此公钥长度为 $2|G|=80$ Bytes.

在本文方案中, 生成的签名是 σ, 其中 $\sigma\in Z_q^*$, 因此签名的长度为 $1|Z|=20$ Bytes; 发送者的私钥是 $SK=(x,py)$, 其中 $x,py\in Z_q^*$, 因此私钥长度为 $2|Z|=40$ Bytes; 发送者的公钥是 $PK=(X,Y)$, 其中 $X,Y\in G$, 因此公钥长度为 $2|G|=80$ Bytes. 其余方案的分析方法均相同, 故不再赘述.

各方案在签名长度、私钥、公钥和公/私钥总长度可视化对比如图 5 所示, 由图可知, 在签名长度方面, 本文与文献 [8,9] 具有最短的签名长度, 相较于文献 [19] 节约了 80%, 相较于除了文献 [19] 之外的方案节约了 66.7%; 在私钥长度方面, 文献 [8] 具有最短的私钥长度, 本文与文献 [7,10,19,20,27,28,30,34] 的私钥长度一样, 但相较于文献 [9,11,29] 节约 50%; 在公钥长度方面, 文献 [8,11,27,34] 拥有最短的公钥长度, 均优于本文方案与剩余的方案; 在公/私钥总长度方面, 文献 [8] 最占优势, 其次是文献 [27,34], 然后是本文与文献 [7,10,11,19,20,28,30], 最后是文献 [9,29]. 鉴于其他方案均已被证明无法完全抵御两种类型的敌手攻击, 我们应重点关注能够同时抵御这两类攻击的文献 [7,10,20,34]. 分析表明, 本文的方案在与文献 [7,10,20,34] 的方案保持相同私钥长度的前提下, 实现了最短的签名长度.

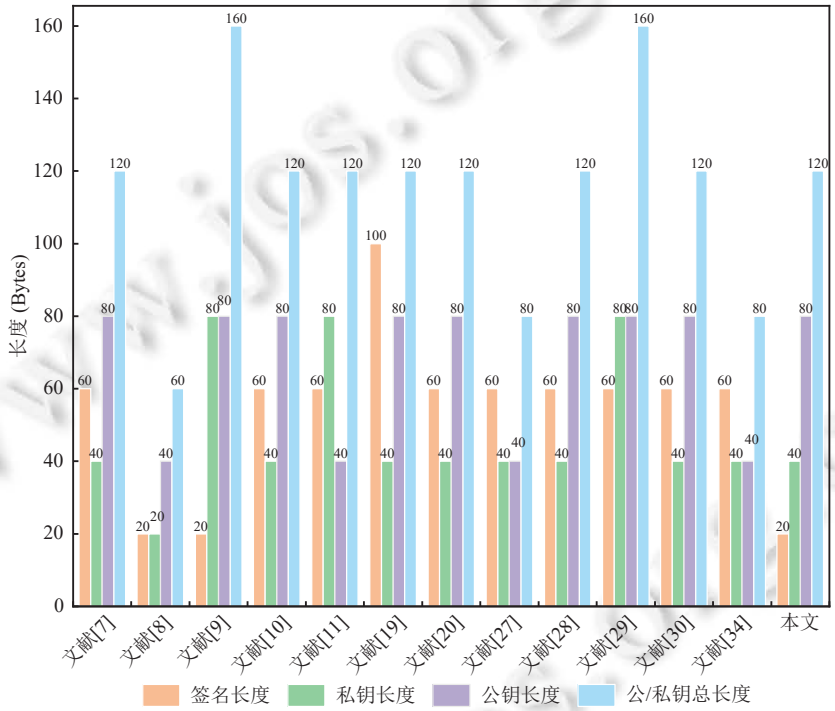

图 5 各方案通信开销对比图

6.3 智能合约 Gas 消耗

基于 elliptic-curve-solidity 库, 本文将信誉值更新合约部署到 Remix IDE 以测量智能合约的 Gas 消耗. 通过调用该合约并上传不同的参数进行测试, 统计并分析了其 Gas 消耗情况.

本文参考了 2025 年 3 月 27 日的兑换参数, 即: 1 ETH = \$1710.6 USD; 1 Gas = 1.335 GWEI, 1 RMB = 0.1379 USD, 并计算了传入不同数量的评价反馈消息的花销, 结果详细列于表 6. 结果显示, 虽然部署合约的消耗最大, 高达 419655 Gas = 6.952126199 RMB, 但考虑到部署合约仅需执行一次, 这一开销是完全可以接受的. 而合约部署成功后, 其内部函数可以重复执行, 单次处理 50 条评价反馈消息的开销不超过 1.2 RMB, 这远远低于采用第三方模式所产生的维护和管理成本.

表 6 合约开销

操作	Gas	ETH	RMB	USD
部署合约	419 655	549.33	6.952 126 199	0.958 345 560
处理1条评价反馈消息	3 341	4.373 4	0.055 347 973	0.007 629 678
处理5条评价反馈消息	8 969	11.740 4	0.148 583 050	0.020 482 066
处理10条评价反馈消息	16 005	20.951	0.265 143 463	0.036 549 834
处理50条评价反馈消息	72 306	94.649	1.197 842 125	0.165 121 669

7 总 结

针对 5G IoV 中存在的一些挑战, 首先, 本文设计了一种面向 5G IoV 的基于联盟区块链的半分布式消息认证加密框架, 由各区域的 VMC 共同维护区块链, 而车辆作为轻节点加入区块链, 并且由 5G 基站提供快速的信息传输. 通过结合区块链与智能合约, 实现分布式密钥获取, 解决传统第三方中心化管理引起的单点故障问题. 其次, 在本文中使用 CLS 与对称加密的方式结合, 保证了传输消息的完整性及消息来源的可验证, 从而保障了 IoV 的安全通信. 然后, 本文还设置信誉值约束车辆乱发虚假消息等恶意行为, 可以从源头减少网络中虚假消息的数量. 最后, 形式化的安全性证明和详细的安全性分析表明, 该协议不仅能达到 IoV 的安全需求, 而且能够抵抗各种常见的攻击. 该方案基于椭圆曲线密码体制, 通过实验证明了其具有较低的计算开销和通信开销.

References

[1] Dong S, Su HD, Xia YJ, Zhu F, Hu XR, Wang BC. A comprehensive survey on authentication and attack detection schemes that threaten it in vehicular ad-hoc networks. IEEE Trans. on Intelligent Transportation Systems, 2023, 24(12): 13573–13602. [doi: 10.1109/TITS.2023.3297527]

[2] Yoshizawa T, Singelée D, Muehlberg JT, Delbruel S, Taherkordi A, Hughes D, Preneel B. A survey of security and privacy issues in V2X communication systems. ACM Computing Surveys, 2023, 55(9): 185. [doi: 10.1145/3558052]

[3] Dong P, Zheng T, Yu S, Zhang HK, Yan XY. Enhancing vehicular communication using 5G-enabled smart collaborative networking. IEEE Wireless Communications, 2017, 24(6): 72–79. [doi: 10.1109/MWC.2017.1600375]

[4] Elsayed MM, Hosny KM, Fouda MM, Khashaba MM. Vehicles communications handover in 5G: A survey. ICT Express, 2023, 9(3): 366–378. [doi: 10.1016/j.icte.2022.01.005]

[5] Al-Shareeda MA, Anbar M, Hasbullah IH, Manickam S. Survey of authentication and privacy schemes in vehicular ad hoc networks. IEEE Sensors Journal, 2021, 21(2): 2422–2433. [doi: 10.1109/JSEN.2020.3021731]

[6] Li Q, Malip A, Martin KM, Ng SL, Zhang J. A reputation-based announcement scheme for VANETs. IEEE Trans. on Vehicular Technology, 2012, 61(9): 4095–4108. [doi: 10.1109/TVT.2012.2209903]

[7] Ma K, Zhou YW, Wang Y, Dong CS, Xia Z, Yang B, Zhang MW. An efficient certificateless signature scheme with provably security and its applications. IEEE Systems Journal, 2023, 17(4): 5636–5647. [doi: 10.1109/JSYST.2023.3269597]

[8] Genc Y, Aytas N, Akkoc A, Afacan E, Yazgan E. ELCPAS: A new efficient lightweight certificateless conditional privacy preserving authentication scheme for IoV. Vehicular Communications, 2023, 39: 100549. [doi: 10.1016/j.vehcom.2022.100549]

[9] Yao C, Zhang XJ, Liu YZ, Zhao BY, Wu QH, Susilo W. Blockchain-based secure and efficient ADS-B authentication via certificateless signature with packet loss tolerance. IEEE Internet of Things Journal, 2025, 12(8): 10574–10588. [doi: 10.1109/JIOT.2024.3511627]

[10] Ye FX, Wu WQ. A security-enhanced certificateless conditional privacy-preserving authentication scheme with collusion-resistance for IoV. Computer Networks, 2025, 259: 111084. [doi: 10.1016/j.comnet.2025.111084]

[11] Yeh KH. A secure transaction scheme with certificateless cryptographic primitives for IoT-based mobile payments. IEEE Systems Journal, 2018, 12(2): 2027–2038. [doi: 10.1109/JSYST.2017.2668389]

[12] Qiao ZR, Yang QL, Zhou YW, Yang B, Gu CX, Zhang MW, Xia Z. An efficient authentication key agreement protocol with provable security for VANET. Chinese Journal of Computers, 2023, 46(5): 929–944 (in Chinese with English abstract). [doi: 10.11897/SP.J.1016.2023.00929]

[13] Liu WH, Xu CX. Certificateless signcryption scheme without bilinear pairing. Ruan Jian Xue Bao/Journal of Software, 2011, 22(8): 1918–1926 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3891.htm [doi: 10.3724/SP.J.1001.2011.03891]

[14] Pan XY, Jin YQ, Wang ZQ, Li FG. A pairing-free heterogeneous signcryption scheme for unmanned aerial vehicles. IEEE Internet of

Things Journal, 2022, 9(19): 19426–19437. [doi: 10.1109/JIOT.2022.3167102]

[15] Wang WZ, Huang HK, Zhang LJ, Su CH. Secure and efficient mutual authentication protocol for smart grid under blockchain. Peer-to-peer Networking and Applications, 2021, 14(5): 2681–2693. [doi: 10.1007/s12083-020-01020-2]

[16] Zhang LJ, Zhang ZJ, Wang WZ, Jin ZL, Su YS, Chen HL. Research on a covert communication model realized by using smart contracts in blockchain environment. IEEE Systems Journal, 2022, 16(2): 2822–2833. [doi: 10.1109/JSYST.2021.3057333]

[17] Zhang LJ, Zou YF, Wang WZ, Jin ZL, Su YS, Chen HL. Resource allocation and trust computing for blockchain-enabled edge computing system. Computers & Security, 2021, 105: 102249. [doi: 10.1016/j.cose.2021.102249]

[18] Alnasser A, Sun HJ, Jiang J. Recommendation-based trust model for vehicle-to-everything (V2X). IEEE Internet of Things Journal, 2020, 7(1): 440–450. [doi: 10.1109/JIOT.2019.2950083]

[19] Wang WZ, Xu H, Alazab M, Gadekallu TR, Han ZY, Su CH. Blockchain-based reliable and efficient certificateless signature for IIoT devices. IEEE Trans. on Industrial Informatics, 2022, 18(10): 7059–7067. [doi: 10.1109/TII.2021.3084753]

[20] Yang XD, Wang WJ, Tian T, Wang CF. Cryptanalysis and improvement of a blockchain-based certificateless signature for IIoT devices. IEEE Trans. on Industrial Informatics, 2024, 20(2): 1884–1894. [doi: 10.1109/TII.2023.3282317]

[21] Shim KA. A secure certificateless signature scheme for cloud-assisted industrial IoT. IEEE Trans. on Industrial Informatics, 2024, 20(4): 6834–6843. [doi: 10.1109/TII.2023.3343437]

[22] Cheng GJ, Deng SG, Wen YY, Yan XQ, Zhao MY. Survey on blockchain-based Internet of Things authentication mechanisms. Ruan Jian Xue Bao/Journal of Software, 2023, 34(3): 1470–1490 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6778.htm [doi: 10.13328/j.cnki.jos.006778]

[23] Yang YH, Wei LJ, Wu J, Long CN, Li B. A blockchain-based multidomain authentication scheme for conditional privacy preserving in vehicular ad-hoc network. IEEE Internet of Things Journal, 2022, 9(11): 8078–8090. [doi: 10.1109/JIOT.2021.3107443]

[24] Yao YY, Chang XL, Mišić J, Misic VB, Li L. BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services. IEEE Internet of Things Journal, 2019, 6(2): 3775–3784. [doi: 10.1109/JIOT.2019.2892009]

[25] Yang Z, Zheng K, Yang K, Leung VCM. A blockchain-based reputation system for data credibility assessment in vehicular networks. In: Proc. of the 28th IEEE Annual Int'l Symp. on Personal, Indoor, and Mobile Radio Communications. Montreal: IEEE, 2017. 1–5. [doi: 10.1109/PIMRC.2017.8292724]

[26] Al-Riyami SS, Paterson KG. Certificateless public key cryptography. In: Proc. of the 9th Int'l Conf. on the Theory and Application of Cryptology and Information Security. Taipei: Springer, 2003. 452–473. [doi: 10.1007/978-3-540-40061-5_29]

[27] Yeh KH, Su CH, Choo KKR, Chiu W. A novel certificateless signature scheme for smart objects in the Internet-of-Things. Sensors, 2017, 17(5): 1001. [doi: 10.3390/s17051001]

[28] Jia XY, He DB, Liu Q, Choo KKR. An efficient provably-secure certificateless signature scheme for Internet-of-Things deployment. Ad Hoc Networks, 2018, 71: 78–87. [doi: 10.1016/j.adhoc.2018.01.001]

[29] Du HZ, Wen QY, Zhang SS, Gao MC. A new provably secure certificateless signature scheme for Internet of Things. Ad Hoc Networks, 2020, 100: 102074. [doi: 10.1016/j.adhoc.2020.102074]

[30] Xiang DM, Li XL, Gao JT, Zhang XC. A secure and efficient certificateless signature scheme for Internet of Things. Ad Hoc Networks, 2022, 124: 102702. [doi: 10.1016/j.adhoc.2021.102702]

[31] He DB. Security analysis of a certificateless signcryption scheme. Ruan Jian Xue Bao/Journal of Software, 2013, 24(3): 618–622 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4245.htm [doi: 10.3724/SP.J.1001.2013.04245]

[32] Cui J, Zhang XY, Zhong H, Ying ZB, Liu L. RSMA: Reputation system-based lightweight message authentication framework and protocol for 5G-enabled vehicular networks. IEEE Internet of Things Journal, 2019, 6(4): 6417–6428. [doi: 10.1109/JIOT.2019.2895136]

[33] Baee MAR, Simpson L, Boyen X, Foo E, Pieprzyk J. ALI: Anonymous lightweight inter-vehicle broadcast authentication with encryption. IEEE Trans. on Dependable and Secure Computing, 2023, 20(3): 1799–1817. [doi: 10.1109/TDSC.2022.3164436]

[34] Feng LB, Qiu F, Hu K, Yu B, Lin JY, Yao SW. CABC: A cross-domain authentication method combining blockchain with certificateless signature for IIoT. Future Generation Computer Systems, 2024, 158: 516–529. [doi: 10.1016/j.future.2024.04.042]

[35] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008. https://bitcoin.org/en/bitcoin-paper

[36] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures. Journal of Cryptology, 2000, 13(3): 361–396. [doi: 10.1007/s001450010003]

附中文参考文献

[12] 乔子芮, 杨启良, 周彦伟, 杨波, 顾纯祥, 张明武, 夏喆. 可证明安全的高效车联网认证密钥协商协议. 计算机学报, 2023, 46(5):

929–944. [doi: 10.11897/SP.J.1016.2023.00929]
[13] 刘文浩, 许春香. 无双线性配对的无证书签密方案. 软件学报, 2011, 22(8): 1918–1926. http://www.jos.org.cn/1000-9825/3891.htm [doi: 10.3724/SP.J.1001.2011.03891]
[22] 程冠杰, 邓水光, 温盈盈, 严学强, 赵明宇. 基于区块链的物联网认证机制综述. 软件学报, 2023, 34(3): 1470–1490. http://www.jos.org.cn/1000-9825/6778.htm [doi: 10.13328/j.cnki.jos.006778]
[31] 何德彪. 无证书签密机制的安全性分析. 软件学报, 2013, 24(3): 618–622. http://www.jos.org.cn/1000-9825/4245.htm [doi: 10.3724/SP.J.1001.2013.04245]

作者简介

毕昌兵, 硕士, 主要研究领域为密码学, 身份认证, 区块链.
田有亮, 博士, 教授, 博士生导师, CCF 杰出会员, 主要研究领域为博弈论, 密码学与安全协议, 大数据隐私保护.
李沓, 博士, 主要研究领域为密码学, 安全多方计算, 区块链, 联邦学习.