VANET 中基于区块链的分布式匿名认证方案

冯霞[1]，崔凯平[1]，谢晴晴[2]，王良民[3]

（1. 江苏大学汽车与交通工程学院，江苏 镇江 212013；2. 江苏大学计算机科学与通信工程学院，江苏 镇江 212013；
3. 东南大学网络空间安全学院，江苏 南京 211110）

摘 要：身份认证是阻止恶意车辆传播虚假交通信息的第一道防线。然而由于车载自组网（VANET）中网络带宽和计算能力有限，现有方案不能满足对车辆身份的高效认证需求，也无法实现对恶意车辆的快速匿名追溯。鉴于此，提出一种基于区块链的分布式匿名认证方案。该方案利用零知识证明对 VANET 中车辆进行快速匿名认证，并采用非线性对的聚合签名实现快速批量认证，有效减少认证过程中产生的计算量。另外，区域性可信机构（RTA）可以实现对恶意车辆身份的匿名追溯，并基于区块链对其身份进行快速撤销；还可以基于本地密钥对车辆的短期匿名身份进行及时更新，保证车辆的匿名性和签名的新鲜性。安全分析与仿真实验表明，所提方案能够满足匿名性、不可链接性等多种安全需求，并能有效降低计算与通信开销，比同类方案在性能上至少提升 27.28%。

关键词：车载自组网；匿名认证；区块链；零知识证明；非线性对

中图分类号：TN915.08

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2022167

Distributed anonymous authentication scheme based on the blockchain in VANET

FENG Xia[1], CUI Kaiping[1], XIE Qingqing[2], WANG Liangmin[3]

1. School of Automotive and Traffic Engineering, Jiangsu University, Zhenjiang 212013, China

2. School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China

3. School of Cyber Science and Engineering, Southeast University, Nanjing 211110, China

Abstract: Identity authentication is the first line of defense against malicious vehicles spreading false traffic information. However, due to the limited network bandwidth and computing power in the vehicle ad-hoc network (VANET), the existing schemes cannot meet the requirements of efficient authentication, nor can achieve fast and anonymous traceability of malicious vehicles. In view of this, a distributed anonymous authentication scheme based on the blockchain was proposed. The zero-knowledge proof was used to quickly and anonymously authenticate the identity of vehicles in VANET, and the pairing-free-based aggregating signature was used to provide fast batch verification, effectively reducing the computational burden generated during the authentication process. In addition, the regional trusted authority (RTA) could realize the anonymous traceability of malicious vehicle identities, and quickly revoke their identities by using the block chain. It could also update the short-term anonymous identities of vehicles based on local keys in time to ensure that vehicles anonymity and freshness of signatures. Security analysis and simulation show that the proposed scheme can satisfy various security requirements such as anonymity and unlinkability, and can effectively reduce computing and communication overhead, which is at least 27.28% higher in performance than similar schemes.

Keywords: VANET, anonymous authentication, blockchain, zero-knowledge proof, pairing-free

收稿日期：2022−05−23；**修回日期：**2022−08−17

基金项目：国家自然科学基金资助项目（No.61902157, No.62002139）

Foundation Item: The National Natural Science Foundation of China (No.61902157, No.62002139)

0　引言

车载自组网（VANET, vehicular ad-hoc network）作为智能交通系统（ITS, intelligent transportation system）的重要组成部分，能够有效促进实时交通信息的传播，成为缓解现有交通问题的关键技术。在实际交通场景中，车辆能够通过 VANET 实时获取与安全相关的交通信息（如周围车辆的速度和方向、危险路况等）来提高驾驶体验与行车安全性。然而，VANET 具有动态拓扑结构、节点分布不均匀、网络规模庞大及移动轨迹可预测等特点[1]，使其更容易受到窃听攻击、中间人攻击、篡改攻击等，因此隐私安全问题成为制约 VANET 发展的重要因素[2]。匿名认证是解决隐私安全问题的有效手段之一。传统的匿名认证算法比较复杂，尤其是车辆在高密度交通条件下同时发送认证消息时，认证效率相对较低[3]。并且，在网络带宽和计算能力有限的情况下，大量的消息传输会产生较大的计算开销和通信开销[4-6]。因此，提高匿名认证效率、降低计算与通信开销是 VANET 认证方案的必然要求。

针对 VANET 匿名认证方案中的效率与计算开销问题，研究者提出了一系列批量认证与轻量级认证方案[7-12]。Zhang 等[7]提出了一种用于路侧单元（RSU, road side unit）和车载单元（OBU, on board unit）之间通信的批量认证方案，使 RSU 能够同时对多个车辆进行身份认证，但该方案对 OBU 的安全性和算力要求较高。Chim 等[8]提出了一种基于隐私保护的批量认证方案，允许完成身份认证的车辆在没有 RSU 的参与下以群组的方式进行车与车之间的安全通信，但该方案无法抵御伪造攻击，攻击者能够伪装成合法车辆发布交通信息或者与其他车辆进行通信。Jiang 等[9]基于二进制认证树实现了一种针对消息签名的批量认证方案，但该方案需要依赖半可信 RSU 的参与。Jiang 等[10]在批量认证方案中提出使用哈希消息验证码（HMAC, hash message authentication code）来代替证书撤销列表（CRL, certificate revocation list），该方案虽然克服了检索 CRL 导致的认证开销，但却过分依赖于公钥基础设施（PKI, public key infrastructure）。Ying 等[11]提出了一种轻量级的认证方案，利用哈希函数能够快速计算的特点，实现了 OBU、RSU 及可信机构（TA, trusted authority）三者之间的相互认证，但该方案无法有效抵御重放攻击与篡改攻击。Cui 等[12]提出了一种基于雾的身份认证方案，利用雾节点来代替 RSU 实现 OBU 与 TA 之间的认证，但无法实现对恶意车辆身份的快速追溯。另外，针对聚合签名技术也有许多研究[13-17]，然而它们都存在计算开销较大的问题。

区块链[18]具有去中心化、可扩展及匿名性等特点。利用区块链技术可以建立分布式系统架构，能够有效解决 VANET 中的广播冲突、资源调度和隐私保护等诸多问题[19]。国内外许多学者提出了基于区块链的认证方案[20-23]。然而，现有基于区块链的认证方案在应用过程中仍存在三方面的不足：1) 验证者利用智能合约完成消息认证，在共识阶段会产生额外的时间开销；2) 缺乏信誉评估机制，无法实现对车辆行为的有效约束；3) 部分方案在缺乏有效身份管理机制的情况下将数字证书存储在区块链上，造成了存储资源的浪费。

综上所述，现有研究提出的认证方案大多不能满足 VANET 的高效认证需求，并且对车辆匿名性、可追溯性及有效撤销等安全问题考虑不够全面。本文针对已有研究的不足，提出了一种基于区块链的分布式匿名认证方案。本文主要的研究工作如下。

1) 提出一种基于区块链的分布式匿名认证方案。该方案能够利用零知识证明对 VANET 中车辆进行快速匿名认证，并采用非线性对的聚合签名来实现快速批量认证，有效减少认证过程中产生的计算量，提高消息认证效率。

2) 在认证安全方面，本文方案可以实现对恶意车辆身份的匿名追溯，并基于区块链对其身份进行快速撤销；还可以基于本地密钥对车辆的短期匿名身份进行及时更新，保证车辆的匿名性和签名的新鲜性。

3) 安全分析结果表明，和现有研究相比，本文提出的基于区块链的分布式匿名认证方案在 VANET 拓扑动态变化特性的基础上，对消息认证性、身份隐私性及不可否认性等安全问题考虑得更加全面。仿真结果表明，相较于现有同类方案，本文方案能有效降低计算开销与通信开销，并显著提高认证效率。

1　预备知识

1.1　椭圆曲线密码学

基于有限域 $Z_q^* = \{1,2,\cdots,q-1\}$ 定义椭圆曲线 $E: y^2 = x^3 + \lambda x + \mu (\mathrm{mod}\ p)$。其中，$\lambda, \mu \in Z_q^*$ 且满

足 $(4\lambda^3+27\mu^2)(\mathrm{mod}\ p)\neq 0$。椭圆曲线 E 上的点及无穷远点 Θ 构成一个椭圆曲线加法群 G_p。该椭圆曲线加法群具有以下性质。

1) 几何加法。假设曲线 E 上存在 2 个随机点 P_1 和 P_2，若 $P_1\neq P_2$，P_1 与 P_2 的连线和曲线 E 相交于点 $-P_3$，则有 $P_1+P_2=P_3$；反之，若 $P_1=P_2$，则有 $2P_1=P_3$。

2) 标量乘法。定义椭圆曲线 E 上的标量乘法为 $nP=P+P+\cdots+P$（$n-1$ 次加法），其中，$n\in Z_q^*$，$n>0$。

3) 椭圆曲线点的阶。定义椭圆曲线上一点 P 的阶为满足 $nP=\Theta$ 的最小正整数 n。

1.2 安全性假设

本文提出的分布式匿名认证方案基于 2 种难破解问题，即椭圆曲线离散对数问题（ECDLP, elliptic curve discrete logarithm problem）[24]和椭圆曲线计算 Diffie- Hellman 问题（ECDHP, computational Diffie-Hellman problem）[25]。

椭圆曲线离散对数问题（ECDLP）。给定素数 q 和椭圆曲线 E，选定曲线 E 上任意一点 Q，且满足 $Q=xP$。其中，整数 $x,y\in[2,q-1]$，$P,Q\in G$，G 为 q 阶加法循环群，P 为群的生成元。攻击者在已知 P,Q 的情况下计算 x 是困难的。

椭圆曲线计算 Diffie-Hellman 问题（ECDHP）。给定素数 q 和椭圆曲线 E，选定曲线 E 上任意两点 Q,V，且满足 $Q=xP$ 和 $V=yP$。其中，整数 $x,y\in[2,q-1]$，$P,Q,V\in G$，G 为 q 阶加法循环群，P 为群的生成元。在随机数 x,y 未知的情况下，攻击者在概率多项式时间内计算得到 $xyP\in G$ 是困难的。

1.3 系统模型

如图 1 所示，本文提出的匿名认证方案的系统架构分为两层，主要由区块链和 4 种实体组成，即根机构（RA, root authority）、区域性可信机构（RTA, regional trusted authority）、RSU 和 OBU。架构上层主要由 RA 和 RTA 组成，它们之间能够进行安全通信，并负责维护区块链网络。架构下层主要由车辆和 RSU 组成，车辆可以利用 OBU 通过专用短程通信（DSRC, dedicated short range communication）技术与 RSU 通信，RSU 能够通过安全传输协议（如有线传输层安全协议）与 RTA 通信[3]。

1) RA。RA 是一个完全可信的机构，且拥有强大的计算与存储能力。在 VANET 系统中，RA 主要负责生成系统参数、对 OBU 和 RSU 进行注册以及维护区块链网络。RA 是唯一存储车辆真实身份信息以及能够揭露车辆真实身份的机构。当有注册车辆发生恶意行为时，RA 会对该车辆的身份进行准确追溯和有效撤销。另外，本文假设 RA 不会妥协

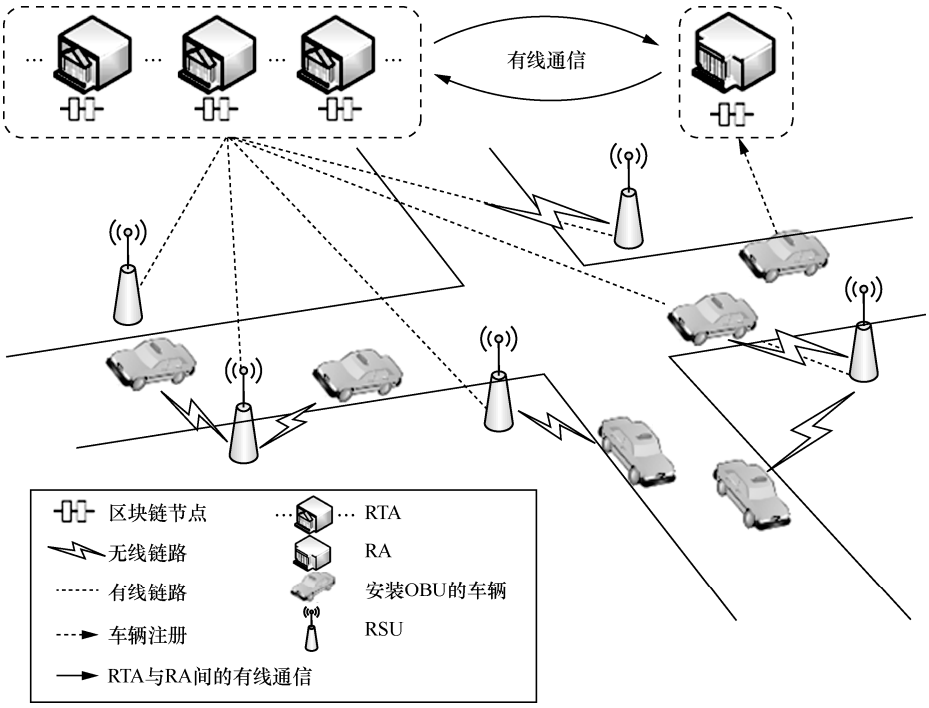


图 1 系统架构

以及与任何实体进行合谋。

2) RTA。RTA 是完全可信的机构，且拥有足够的计算与存储能力。在 VANET 系统中，RTA 负责验证、分析来自 RSU 和车辆的消息，从而准确预测交通分布以优化实时交通信号灯控制等。RTA 受 RA 的监督，尤其当 RTA 检测到恶意车辆时，RTA 需要将该车辆的匿名身份信息上传至 RA，以实现 RA 对该恶意车辆身份的准确追溯。同时，RTA 和 RA 作为区块链共识节点，共同负责维护区块链网络。另外，本文假设 RTA 不会妥协以及与任何实体进行合谋。

3) RSU。RSU 是一个固定在路边且拥有计算与通信能力的装置。它比 OBU 具有更多的计算能力，与 OBU 共同负责收集实时的车辆及路况信息。本文假设 RSU 为半可信装置，并在通信环境较差时辅助车辆向 RTA 提交交通信息。

4) OBU。在 VANET 系统中，每辆车都配备 OBU。OBU 是一种防篡改设备，可以防止攻击者获取存储在其中的数据。OBU 具备有限的计算能力，与 RSU 共同负责收集实时路况信息。

5) 区块链。在本文方案中，RA 与 RTA 作为区块链的共识节点，负责维护区块链网络。区块链技术主要应用于车辆身份管理与认证信息检索，并且可以有效实现车辆信息共享与跨区域认证。在车辆身份管理方面，RA 将车辆的匿名身份存储在区块链状态数据库中。匿名身份的更新与撤销需要 RTA 在该数据库中对车辆匿名身份的状态标识进行修改（见 2.5 节和 2.6 节）。在认证信息检索方面，RTA 根据车辆提供的匿名身份检索区块链状态数据库，以获得该匿名身份对应的认证参数，从而完成零知识证明过程（见 2.3 节）。另外，本文利用智能合约实现对区块链状态数据库的读写以及车辆匿名身份的更新和撤销。因此，RTA 能够通过调用部署在区块链上的智能合约来完成车辆身份更新及认证信息检索过程。

1.4　安全需求

为确保 VANET 的通信安全，认证方案应该具备完整性、匿名性及不可链接性等属性。本文应满足以下安全要求。

1) 匿名性。VANET 具有开放性，因此车辆在通信过程中必须以匿名的方式与其他实体进行信息交互，并且网络内的任何实体（RA 除外）都无法获得某个网络参与者的真实身份，即参与者的真实身份对 RA 以外的任何实体都是机密的。

2) 可追溯性。车辆以匿名的方式与其他实体进行通信。当车辆发生恶意行为时，例如广播虚假路况信息以扰乱正常的交通秩序，RA 能够对车辆的真实身份进行准确追溯并拒绝其再次访问系统。

3) 不可链接性。任何实体都无法将接收到的 2 个或多个消息链接到同一车辆。

4) 消息验证及完整性。RTA 验证消息发送主体的身份合法性，并确保消息没有被其他实体修改。

同时，本文方案应确保能抵御以下常见攻击[26]。

1) 重放攻击。攻击者将先前获得的合法消息重新发送给接收者。通过重新发送消息，攻击者能够利用之前的消息误导其他车辆并扰乱正常的交通秩序。

2) 伪造攻击。攻击者通过伪造授权车辆的签名以冒充合法车辆。攻击者使用虚假的合法身份向其他车辆/基础设施发送伪造信息，进而造成交通事故或交通拥堵以及扰乱交通秩序等。

3) 篡改攻击[27]。攻击者对验证消息进行删除、修改等，导致合法车辆认证失败或令恶意车辆成功欺骗认证者。

4) 中间人攻击。攻击者同时与相互通信的双方保持通信连接，并且使相互通信的双方相信彼此在一个安全的连接中进行信息交互，从而获得有用信息，以达到攻击的目的[28]。另外，攻击者还可能会拦截认证请求者发送的消息，然后将伪造的消息发送给接收者。中间人攻击会导致严重的通信数据泄露。

2　基于区块链的分布式匿名认证方案

为满足 VANET 通信过程中的安全与隐私保护需求，本文提出的基于区块链的分布式匿名认证方案包含 6 个阶段，即系统初始化阶段、匿名身份生成阶段、签名及认证阶段、信誉评估阶段、匿名身份更新阶段、匿名身份撤销阶段，如图 2 所示。方案涉及的参数及定义如表 1 所示。

2.1　系统初始化阶段

RA 与 RTA 负责系统初始化，详细步骤如下。

1) RA 设定安全参数 λ。如 1.1 节所述，RA 基于椭圆曲线 E 上的点及无穷远点 Θ 构建一个椭圆曲线加法群 G_p。加法群 G_p 的阶为 q，生成元为 P。

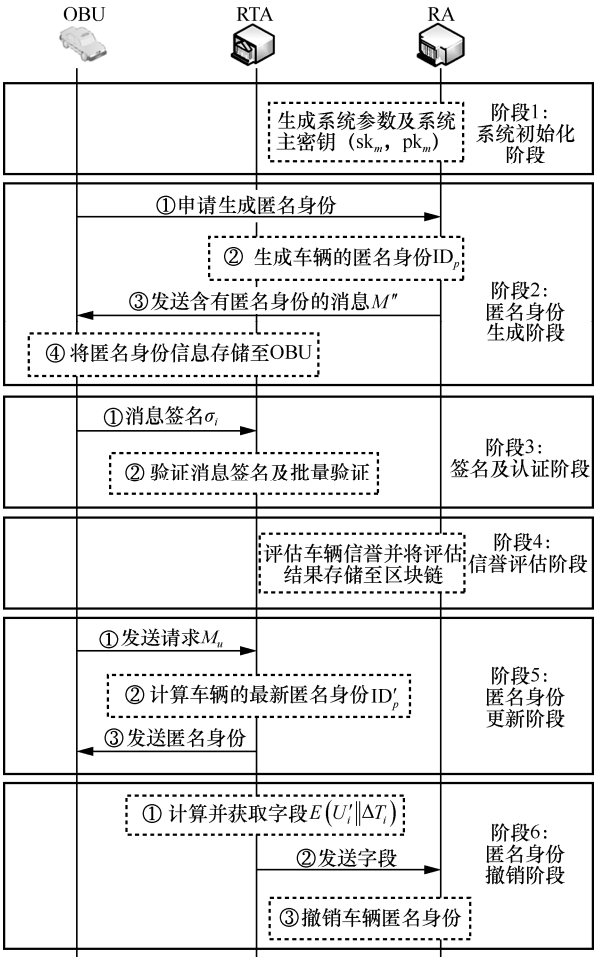


图 2　方案流程

表 1　　方案涉及的参数及定义

参数	含义
p,q	大素数
P	加法群 G_p 的生成元
E	椭圆曲线：$y^2 = x^3 + \lambda x + \mu \mod q$
G_p	基于椭圆曲线生成的加法群
Z_q^*	有限域
sk_m, pk_m	RA 的私钥与公钥
sk_r, pk_r	RTA 的私钥与公钥
sk_v, pk_v	车辆的私钥与公钥
sk_{vr}	车辆的部分签名私钥
t	时间戳
RC	车辆所在区域代码
ΔT	匿名身份有效期
ID_p	车辆的匿名身份
ID	车辆的真实身份
Cr	车辆的信誉值
$E(X)$	椭圆曲线加密函数

2) RA 生成系统主密钥用于加密车辆真实身份。RA 选取随机数 $a \in Z_p^*$ 作为系统私钥 sk_m，并计算相应公钥 pk_m。RTA 同样生成本地密钥对用于认证车辆身份。RTA 选取随机数 $b \in Z_p^*$ 作为本地私钥 sk_r，并计算相应公钥 pk_r。

3) RA 选取一个安全的哈希函数 $h:\{0,1\}^* \to Z_p^*$，并且向网络广播参数集合 $\{P, p, q, E, G_p, h, pk_m\}$。车辆将该参数集合及所在区域的 RTA 公钥存储在 OBU 中。

4) 车辆 v_i 基于参数集合向 RA 发送包含真实身份 ID_i 的注册信息，RA 与 RTA 将为车辆生成匿名身份（见 2.2 节）。同时，RSU 也在初始化阶段注册，并以安全的方式获取系统参数。

2.2　匿名身份生成阶段

RA 与 RTA 为车辆生成匿名身份。在消息认证过程中，车辆将以匿名身份发送认证信息，以保护其真实身份信息不被泄露。同时，通过匿名身份，系统可以实现有条件的隐私保护。在必要时，RA 可以通过认证消息揭露车辆的真实身份。车辆匿名身份生成过程如图 3 所示，其具体流程如下。

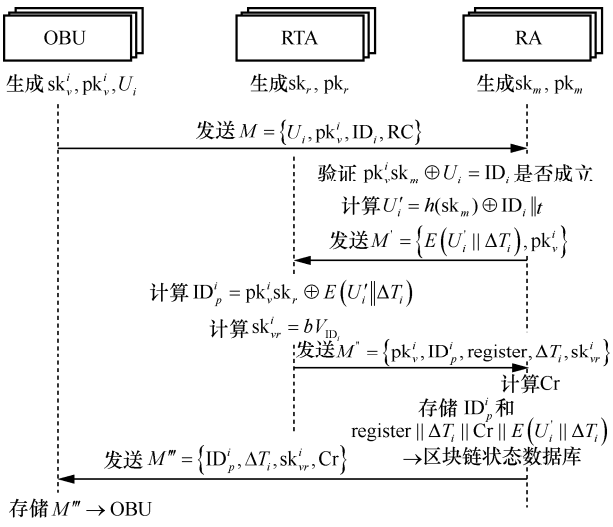


图 3　车辆匿名身份生成过程

1) 车辆 v_i 选取随机数 $x_i \in Z_p^*$ 作为私钥 sk_v^i，并计算对应公钥 pk_v^i，基于公钥计算参数 $U_i = sk_v^i pk_m \oplus ID_i$，然后向 RA 发送消息 $M = \{U_i, pk_v^i, ID_i, RC\}$。

2) RA 接收到消息 M 后首先确认等式 $pk_v^i sk_m \oplus U_i = ID_i$ 是否成立并验证此身份的有效

性，即确保此车辆合法且未注册。若等式不成立，则验证失败，RA 将直接丢弃该消息；若等式成立，RA 计算参数 $U_i^{'}=h(\mathrm{sk}_m)\oplus \mathrm{ID}_i \| t$。然后，RA 利用私钥 sk_m 生成加密值 $E\left(U_i^{'} \| \Delta T_i\right)$，并向区域代码 RC 对应的 RTA 转发消息 $M^{'}=\left\{E\left(U_i^{'} \| \Delta T_i\right), \mathrm{pk}_v^i\right\}$，其中，$\Delta T_i$ 为匿名身份的有效期。

3) RTA 接收到消息 $M^{'}$ 后，计算匿名身份 $\mathrm{ID}_p^i=\mathrm{pk}_v^i \mathrm{sk}_r \oplus E\left(U_i^{'} \| \Delta T_i\right)$。另外，RTA 计算参数 $V_{\mathrm{ID}_i}=h\left(\mathrm{ID}_p^i\right)$ 和 $C_i=V_{\mathrm{ID}_i} \mathrm{pk}_r$，从而计算出车辆的部分签名私钥 $\mathrm{sk}_{vr}^i=bV_{\mathrm{ID}_i}$。然后，RTA 将消息 $M^{''}=\left\{\mathrm{pk}_v^i, \mathrm{ID}_p^i, \mathrm{register}, \Delta T_i, \mathrm{sk}_{vr}^i\right\}$ 返回给 RA。

4) RA 设置车辆的初始信誉值 Cr，并将 ID_p^i 和 $\mathrm{register} \| \Delta T_i \| \mathrm{Cr} \| E\left(U_i^{'} \| \Delta T_i\right)$ 字段以键值对的形式存储在区块链状态数据库中。RA 将含有匿名身份的消息 $M^{'''}=\left\{\mathrm{ID}_p^i, \Delta T_i, \mathrm{sk}_{vr}^i, \mathrm{Cr}\right\}$ 发送给车辆 v_i。车辆将 $M^{'''}$ 存储在 OBU 中。

2.3　签名及认证阶段

在认证过程中，为保证消息的真实性和完整性，车辆必须对发送的认证进行签名。具体来说，车辆 v_i 基于匿名身份 ID_i 利用签名私钥 $\mathrm{sk}_v^i, \mathrm{sk}_{vr}^i$ 对消息 M_i 进行签名，其过程如图 4 所示，具体流程如下。

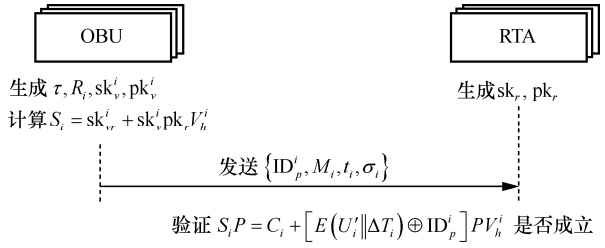


图 4　消息签名及认证过程

1) 车辆 v_i 选取一个随机数 $\tau \in Z_p^*$，并且计算 $R_i=\tau P$。

2) 车辆 v_i 基于本地匿名身份与时间戳 t_i 计算哈希值 $V_h^i=h\left(M_i \| \mathrm{ID}_p^i \| R_i \| t_i\right)$。然后，车辆 v_i 利用签名私钥计算 $S_i=\mathrm{sk}_{vr}^i+\mathrm{sk}_v^i \mathrm{pk}_r V_h^i$，进而生成消息 M_i 对应的签名 $\sigma_i=\left(R_i \| S_i\right)$。

3) 车辆 v_i 向 RTA 发送包含交通信息的认证消息 $\left\{\mathrm{ID}_p^i, M_i, t_i, \sigma_i\right\}$。

4) RTA 通过接收到的消息 $\left\{\mathrm{ID}_p^i, M_i, t_i, \sigma_i\right\}$ 来验证 M_i 的有效性与车辆身份的合法性。首先，RTA 基于认证消息中的各项参数计算哈希值 $V_h^i=h\left(M_i \| \mathrm{ID}_p^i \| R_i \| t_i\right)$ 和 $V_{\mathrm{ID}_i}=h\left(\mathrm{ID}_p^i\right)$；其次，RTA 利用智能合约在区块链状态数据库中检索 ID_p^i，从而获取椭圆曲线加密值参数 $E\left(U_i^{'} \| \Delta T_i\right)$；最后，RTA 计算参数 $C_i=V_{\mathrm{ID}_i} \mathrm{pk}_r$ 并检验等式 $S_iP=C_i+\left[E\left(U_i^{'} \| \Delta T_i\right) \oplus \mathrm{ID}_p^i\right] PV_h^i$ 是否成立。若等式成立，则验证通过，消息 M_i 被 RTA 接收；反之，则验证失败，消息 M_i 被 RTA 丢弃。

在上述认证过程中，验证者利用零知识证明来验证目标车辆是否拥有合法身份。匿名身份 ID_p^i 是基于车辆公钥 pk_v^i 与加密值参数 $E\left(U_i^{'} \| \Delta T_i\right)$ 并通过计算 $\mathrm{ID}_p^i=\mathrm{pk}_v^i \mathrm{sk}_r \oplus E\left(U_i^{'} \| \Delta T_i\right)$ 生成的，而参数 $U_i^{'}$ 是基于车辆的真实身份 ID_i 生成的。验证者通过计算相关密钥 $\left[E\left(U_i^{'} \| \Delta T_i\right) \oplus \mathrm{ID}_p^i\right] P=\mathrm{pk}_v^i \mathrm{pk}_r$ 参与消息认证的等式验证过程。具体而言，若该计算结果使等式 $S_iP=C_i+\left[E\left(U_i^{'} \| \Delta T_i\right) \oplus \mathrm{ID}_p^i\right] PV_h^i$ 成立，则证明该验证者持有匿名身份 ID_p^i 对应的真实身份 ID_i 和密钥对 $(\mathrm{sk}_v^i, \mathrm{pk}_v^i)$；反之，则代表车辆利用非法匿名身份 ID_p^i 发送认证消息。

在认证过程中，RTA 可能同时收到来自不同车辆的签名。通过聚合签名可以有效提高 RTA 对签名的验证效率，其过程如图 5 所示，具体流程如下。

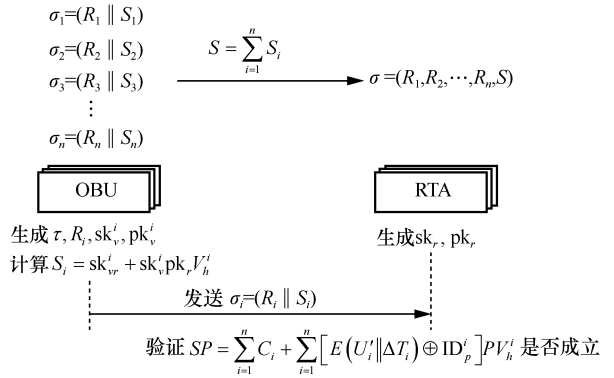


图 5　基于聚合签名的消息认证过程

1) 当 RTA 同时接收到来自不同车辆的验证消息时，即 $\left\{\mathrm{ID}_p^i, M_i, t_i, \sigma_i\right\}$，$i \in \{1,2,3,\cdots,n\}$。RTA 利用智能合约在区块链状态数据库中检索 ID_p^i，从而获取椭圆曲线加密值参数 $E\left(U_i^{'} \| \Delta T_i\right)$。

2) RTA 计算 $S=\sum_{i=1}^{n} S_i$，故车辆 $(v_1, v_2, v_3, \cdots,$

v_n) 基于匿名身份 $\left(\mathrm{ID}_p^1, \mathrm{ID}_p^2, \mathrm{ID}_p^3, \cdots, \mathrm{ID}_p^n\right)$ 生成的签名可以聚合为 $\sigma = \left(R_1, R_2, R_3, \cdots, R_n, S\right)$。RTA 计算参数 $V_{\mathrm{ID}_i} = h\left(\mathrm{ID}_p^i\right)$ 以及哈希值 $V_h^i = h\left(M_i \| \mathrm{ID}_p^i \| R_i \| t_i\right)$，$i \in \{1, 2, 3, \cdots, n\}$。

3) RTA 基于以上计算参数检验等式 $SP = \sum_{i=1}^{n} C_i + \sum_{i=1}^{n}\left[E\left(U_i^{'} \| \Delta T_i\right) \oplus \mathrm{ID}_p^i\right] PV_h^i$。其中，$C_i = V_{\mathrm{ID}_i}\mathrm{pk}_r$。若等式成立，RTA 接收所有的消息。

4) 当出现无效签名导致聚合签名验证失效时，可以通过二进制搜索来验证聚合签名[23]，即 RTA 先将接收到的签名进行排序，并将签名均分为两部分；然后，将这两部分的签名分别进行聚合、验证。对验证失败的那部分签名重复进行均分、聚合、验证操作，直至找到全部无效的签名。该方法可以有效避免聚合验证失败后所有签名都被判定为无效的问题。

2.4 信誉评估阶段

为了对车辆行为进行有效约束，本文方案在区块链架构的基础上引入了信誉评估机制[29]。RA 首先设置一个信誉阈值并广播。基于信誉评估机制，当车辆提供有效交通信息时，其信誉值会增加；反之其信誉值会被扣除。当车辆的信誉值低于信誉阈值时，车辆的匿名身份会被撤销。具体而言，针对车辆 v_i 提供的交通信息，只有当 n 辆车提供与之相同或相似的交通信息时，车辆 v_i 提供的交通信息才会被 RTA 接收。另外，本文设定 $\frac{1}{n} \propto \mathrm{Cr}_i$，即车辆 v_i 信誉值越低，就需要越多的其他车辆提供与之相同或相似的交通信息；车辆 v_i 提供的交通信息越难被接收，车辆的信誉值就越难恢复，以此有效约束车辆行为。

本文方案中的信誉值计算方法为

$$\mathrm{Cr}_i = \lambda_1 \mathrm{Cr}_i^{\mathrm{P}} + \lambda_2 \mathrm{Cr}_i^{\mathrm{N}} \tag{1}$$

其中，$\mathrm{Cr}_i^{\mathrm{P}}$ 表示正向影响值；$\mathrm{Cr}_i^{\mathrm{N}}$ 表示负向影响值；λ_1 和 λ_2 分别表示两部分的权重。参数 $\mathrm{Cr}_i^{\mathrm{P}}$ 与 $\mathrm{Cr}_i^{\mathrm{N}}$ 的计算过程如下。

1) 参数 $\mathrm{Cr}_i^{\mathrm{P}}$ 的值与车辆在单位时间提交有效交通信息的数量呈正相关，通过车辆的活跃度来衡量，即

$$\mathrm{Cr}_i^{\mathrm{P}} = \frac{\sum_{j=1}^{n_i} \omega_j}{\Delta T_c} \tag{2}$$

其中，n_i 表示车辆在单位时间内车辆提交有效交通信息的数量，ΔT_c 表示一个单位时间，ω_j 表示第 j 个交通信息的权重，该值由 RTA 进行计算。

2) 参数 $\mathrm{Cr}_i^{\mathrm{N}}$ 的值与车辆的恶意行为数量呈负相关，定义为

$$\mathrm{Cr}_i^{\mathrm{N}} = -\sum_{j=1}^{m_i} \alpha(\beta) \frac{\Delta T_c}{t - t_j} \tag{3}$$

其中，m_i 表示车辆 i 的恶意行为总数，t 表示目前时间，t_j 表示车辆 i 第 j 次恶意行为的时间，$\alpha(\beta)$ 表示惩罚系数。

在进行消息验证后，RTA 基于车辆提供的交通信息的有效性重新评估车辆的信誉值，并将包含车辆最新信誉值 $\mathrm{Cr}^{'}$ 的字段与参数 ID_p 重新存储在区块链状态数据库中。

2.5 匿名身份更新阶段

当车辆的匿名身份失效时，车辆需要对匿名身份进行更新，具体流程如下。

1) 车辆 v_i 选取随机数 $x_i^{'} \in Z_p^*$ 作为新私钥 $\mathrm{sk}_v^{i'}$，并计算对应公钥 $\mathrm{pk}_v^{i'}$。另外，车辆基于 RTA 公钥计算参数 $D_i = \mathrm{sk}_v^{i'}\mathrm{pk}_r \oplus \mathrm{ID}_p^i$，然后向 RTA 发送消息 $M_u = \left\{\mathrm{update}, D_i, \mathrm{pk}_v^{i'}, \mathrm{pk}_v^i, \mathrm{ID}_p^i\right\}$。

2) RTA 接收到更新请求消息后，首先，计算 $E\left(U_i^{'} \| \Delta T_i\right) = \mathrm{pk}_v^i \mathrm{sk}_r \oplus \mathrm{ID}_p^i$ 并检验车辆最新密钥的合法性，即计算 $\mathrm{ID}_p^i = \mathrm{pk}_v^{i'}\mathrm{sk}_r \oplus D_i$。然后，RTA 利用智能合约在区块链状态数据库中检索 ID_p^i，以确认该车辆是否为合法授权车辆并确定匿名身份 ID_p^i 的有效期。在确定车辆为已注册车辆且匿名身份失效后，RTA 重新计算匿名身份 $\mathrm{ID}_p^{i'} = \mathrm{pk}_v^{i'}\mathrm{sk}_r \oplus E\left(U_i^{'} \| \Delta T_i^{'}\right)$。

3) RTA 将 $\mathrm{ID}_p^{i'}$ 和 $\mathrm{update} \| \Delta T_i^{'} \| \mathrm{Cr} \| E\left(U_i^{'} \| \Delta T_i\right)$ 字段以键值对的形式存储在区块链状态数据库中，并将含有最新匿名身份的消息 $\mathrm{ID}_p^{i'}, \Delta T_i^{'}$ 发送给车辆 v_i，从而完成匿名身份的更新过程。

基于该匿名身份更新机制，本文方案可以采用预加载若干匿名身份的方法来抵抗可链接性。车辆可以基于较短的匿名身份有效期 ΔT 加载一个匿名身份池，匿名身份池中装载的匿名身份在失效时能够进行及时的更新。

2.6 匿名身份撤销阶段

当车辆进行恶意行为时，RTA 与 RA 能够对车

辆身份进行有效追溯，并对其全部的匿名身份进行撤销，具体流程如下。

1) RTA 通过计算 $\mathrm{pk}_v^i \mathrm{sk}_r \oplus \mathrm{ID}_p^i$ 获得字段 $E\left(U_i^{'} \| \Delta T_i^{'}\right)$，并将该字段转发至 RA。

2) RA 基于本地私钥从字段 $E\left(U_i^{'} \| \Delta T_i^{'}\right)$ 恢复出参数 $U_i^{'}$，并计算 $\mathrm{ID}_i \| t = h(\mathrm{sk}_m) \oplus U_i^{'}$ 从而揭露恶意车辆的真实身份，并对车辆的匿名身份进行撤销，将 ID_p^i 和 revoke 字段以键值对的形式重新存储在区块链状态数据库中。

另外，当车辆主动申请撤销某一匿名身份时，RTA 与 RA 需要验证车辆密钥的合法性，具体流程如下。

1) 车辆 v_i 计算参数 $B_i = \mathrm{sk}_v^i \mathrm{pk}_r \oplus \mathrm{ID}_p^i$，然后向 RTA 发送消息 $M_r = \left\{\mathrm{revoke}, B_i, \mathrm{pk}_v^i, \mathrm{ID}_p^i\right\}$。

2) RTA 收到更新请求消息后，首先，计算 $E\left(U_i^{'} \| \Delta T_i\right) = \mathrm{pk}_v^i \mathrm{sk}_r \oplus \mathrm{ID}_p^i$ 并检验车辆密钥的合法性，即计算 $\mathrm{ID}_p^i = \mathrm{pk}_v^i \mathrm{sk}_r \oplus B_i$。然后，RTA 利用智能合约在区块链状态数据库中检索 ID_p^i，以确认该车辆是否为合法授权车辆。在确定车辆为已注册车辆后，RTA 将 ID_p^i 与 revoke 字段以键值对的形式重新存储在区块链状态数据库中，以完成匿名身份撤销过程。

3　方案分析

针对所提方案在消息认证过程中的具体实现，本节从正确性与安全性的角度对其进行验证和分析。

3.1　正确性分析

本节将分析在消息认证过程中涉及的单一认证的正确性和批量认证的正确性。RTA 通过检验 $S_i P = C_i + \left[E\left(U_i^{'} \| \Delta T_i\right) \oplus \mathrm{ID}_p^i\right] PV_h^i$ 来确认单一签名消息的有效性与车辆身份的合法性。在单一认证过程中，基于参数 $S_i = \mathrm{sk}_{vr}^i + \mathrm{sk}_v^i \mathrm{pk}_r V_h^i$、$\mathrm{sk}_{vr}^i = bV_{\mathrm{ID}_i}$ 和 $V_{\mathrm{ID}_i} = h\left(\mathrm{ID}_p^i\right)$，可以得到等式 $S_i P = C_i + \left[E\left(U_i^{'} \| \Delta T_i\right) \mathrm{ID}_p^i\right] PV_h^i$ 成立的基本细节，即

$$\begin{aligned} & S_i P = \left(\mathrm{sk}_{vr}^i + \mathrm{sk}_v^i \mathrm{pk}_r V_h^i\right) P = \\ & \mathrm{sk}_{vr}^i P + \mathrm{sk}_v^i \mathrm{pk}_r V_h^i P = \\ & bh\left(\mathrm{ID}_p^i\right) P + \mathrm{pk}_v^i \mathrm{pk}_r V_h^i = \\ & bh\left(\mathrm{ID}_p^i\right) P + \mathrm{pk}_v^i \mathrm{sk}_r P V_h^i = \\ & C_i + \left[E\left(U_i^{'} \| \Delta T_i\right) \oplus \mathrm{ID}_p^i\right] PV_h^i \end{aligned} \tag{4}$$

在批量认证过程中，RTA 通过验证等式 $SP = \sum_{i=1}^{n} C_i + \sum_{i=1}^{n}\left[E\left(U_i^{'} \| \Delta T_i\right) \oplus \mathrm{ID}_p^i\right] PV_h^i$ 来确认签名消息的有效性。因此，对于批量认证的正确性证明，主要通过验证上述等式是否成立来实现。基于已知计算参数 $\mathrm{sk}_{vr}^i = bV_{\mathrm{ID}_i}$、$S = \sum_{i=1}^{n} \mathrm{sk}_{vr}^i + \mathrm{sk}_v^i V_h^i\ \mathrm{pk}_r = \sum_{i=1}^{n} S_i$、$V_{\mathrm{ID}_i} = h\left(\mathrm{ID}_p^i\right)$ 以及 $C_i = V_{\mathrm{ID}_i} \mathrm{pk}_r$，可以进一步得到等式 $SP = \sum_{i=1}^{n} C_i + \sum_{i=1}^{n}\left[E\left(U_i^{'} \| \Delta T_i\right) \oplus \mathrm{ID}_p^i\right] PV_h^i$ 成立的基本细节，即

$$\begin{aligned} & SP = \sum_{i=1}^{n} S_i P = \sum_{i=1}^{n}\left(\mathrm{sk}_{vr}^i + \mathrm{sk}_v^i \mathrm{pk}_r V_h^i\right) P = \\ & \sum_{i=1}^{n}\left(\mathrm{sk}_{vr}^i P + \mathrm{sk}_v^i \mathrm{pk}_r V_h^i P\right) = \\ & \sum_{i=1}^{n} bh\left(\mathrm{ID}_p^i\right) P + \sum_{i=1}^{n} \mathrm{pk}_v^i V_h^i \mathrm{pk}_r = \\ & \sum_{i=1}^{n} bh\left(\mathrm{ID}_p^i\right) P + P\sum_{i=1}^{n} \mathrm{pk}_v^i V_h^i \mathrm{sk}_r = \\ & \sum_{i=1}^{n} C_i + P\sum_{i=1}^{n}\left[E\left(U_i^{'} \| \Delta T_i\right) \oplus \mathrm{ID}_p^i\right] V_h^i \end{aligned} \tag{5}$$

3.2　安全性分析

本节将从安全要求与抵御攻击两方面对本文协议进行安全性分析。针对安全要求，本节将从匿名性、可追溯性、不可链接性以及消息验证及完整性等方面展开。同时，考虑到密钥更新的安全性，本文还对密钥生成过程中涉及的前向和后向安全性进行分析。针对安全要求的分析细节如下。

1) 匿名性。在本文方案中，车辆使用匿名身份 $\mathrm{ID}_p^i = \mathrm{pk}_v^i \mathrm{sk}_r \oplus E\left(U_i^{'} \| \Delta T_i\right)$ 参与消息认证过程。其中，$U_i^{'} = h(\mathrm{sk}_m) \oplus \mathrm{ID}_i \| t$。为获取车辆的真实身份，攻击者首先需要进行 3 个计算步骤。①攻击者计算 $E\left(U_i^{'} \| \Delta T_i\right) = \mathrm{pk}_v^i \mathrm{sk}_r \oplus \mathrm{ID}_p^i$ 或者 $E\left(U_i^{'} \| \Delta T_i\right) = \mathrm{sk}_v^i\ \mathrm{pk}_r \oplus \mathrm{ID}_p^i$，获取字段 $E\left(U_i^{'} \| \Delta T_i\right)$。②攻击者需要从加密字段 $E\left(U_i^{'} \| \Delta T_i\right)$ 恢复出参数 $U_i^{'}$。③攻击者需要计算 $\mathrm{ID}_i \| t = h(\mathrm{sk}_m) \oplus U_i^{'}$，从而获取车辆的真实身份。在步骤①中，攻击者需要获取签名者或者 RTA 的私钥。在步骤②~步骤③中，攻击者需要获取 RA 的私钥。然而，基于 ECDLP，攻击者无法由公钥推算出私钥，进而无法通过消息获取车辆的真实身份，从而实现了对车辆匿名性的保护。

2) 可追溯性。本文方案中，只有 RA 可以揭露车辆的真实身份。RTA 根据恶意车辆的匿名身份可以计算得到 $E\left(U_i^{'} \| \Delta T_i\right)=\mathrm{pk}_v^i \mathrm{sk}_r \oplus \mathrm{ID}_p^i$。RTA 向 RA 发送加密字段 $E\left(U_i^{'} \| \Delta T_i\right)$，RA 基于本地私钥从该字段中恢复出参数 $U_i^{'}$，并通过计算等式 $\mathrm{ID}_i \| t=h(\mathrm{sk}_m) \oplus U_i^{'}$ 最终得到车辆的真实身份 ID_i。因此，本文方案可以有效实现对恶意车辆的身份追溯。

3) 不可链接性。车辆在认证过程中首先选取一个随机数 $\tau \in Z_p^*$，并且计算 $R_i=\tau P$。由于参数 τ 使签名具有随机性，攻击者无法链接多个验证信息 $\left\{\mathrm{ID}_p^i, M_i, t_i, \sigma_i\right\}$ 至同一车辆。另外，基于匿名身份的更新机制，匿名身份池里具备多个匿名身份，攻击者同样无法链接多个匿名身份至同一车辆。

4) 消息验证及完整性。RTA 基于接收到的消息计算 $E\left(U_i^{'} \| \Delta T_i\right)=\mathrm{pk}_v^i \mathrm{sk}_r \oplus \mathrm{ID}_p^i$，并利用智能合约在区块链状态数据库中检索 ID_p^i。然后，RTA 通过计算 $C_i=V_{\mathrm{ID}_i} \mathrm{pk}_r$，并基于零知识证明检验等式 $S_i P=C_i+\left[E\left(U_i^{'} \| \Delta T_i\right) \oplus \mathrm{ID}_p^i\right] PV_h^i$ 是否成立来验证消息的完整性与车辆身份的合法性。

5) 前向和后向安全性。在密钥生成过程中，车辆 v_i 选取随机数 $x_i \in Z_p^*$ 作为当前私钥 sk_v^t，并计算对应公钥 pk_v^t。因此，sk_v^t 和 sk_v^t 都是车辆通过选择随机数计算的，攻击者无法通过当前 sk_v^t 推导出 sk_v^{t-1} 或 sk_v^{t+1}。

本节对常见的抵御攻击进行分析，主要包括重放攻击、伪造攻击、篡改攻击及中间人攻击，其分析细节如下。

1) 重放攻击。车辆在验证消息中添加时间戳 t_i 即 $\left\{\mathrm{ID}_p^i, M_i, t_i, \sigma_i\right\}$，并对其签名以确保其为最新消息。RTA 能够基于时间戳检测重放攻击。因此本文方案能够有效抵御重放攻击。

2) 伪造攻击。根据前文的证明，基于 ECDLP，攻击者无法获取 RTA 或签名者的私钥。因此，攻击者无法假冒签名者的身份来伪造验证消息 $\left\{\mathrm{ID}_p^i, M_i, t_i, \sigma_i\right\}$ 并使该消息满足等式 $S_i P=C_i+\left[E\left(U_i^{'} \| \Delta T_i\right) \oplus \mathrm{ID}_p^i\right] PV_h^i$。

3) 篡改攻击。在消息的验证过程中，攻击者篡改消息 $\left\{\mathrm{ID}_p^i, M_i, t_i, \sigma_i\right\}$ 的任何内容都会导致等式 $S_i P=C_i+\left[E\left(U_i^{'} \| \Delta T_i\right) \oplus \mathrm{ID}_p^i\right] PV_h^i$ 不成立。验证者能够通过计算该等式来检查验证消息是否被篡改。因此，本文方案能够有效抵御篡改攻击。

4) 中间人攻击。当攻击者在 OBU 与 RTA 之间进行中间人攻击时，需要假冒成 OBU 向 RTA 发送验证消息，同时假冒成 RTA 向 OBU 发送反馈消息。然而，所提方案能够有效抵御伪造攻击，因此攻击者无法仿冒为其他合法实体。另外，由于消息签名的存在，攻击者只能截获和转发消息，而无法篡改消息。

4 仿真与性能对比分析

VANET 系统具有车辆移动速度快、动态网络拓扑等特点，下面将从安全性、计算开销和通信开销等方面对本文方案进行有效分析。

4.1 实验预设

本文使用 AMD Ryzen 7 5800H、Radeon Graphics CPU @ 3.20 GHz CPU 、16 GB RAM 进行仿真实验，并基于 Hyperledger Fabric v2.0.0 搭建联盟链网络。本文在区块链网络中使用 Raft 共识机制，并基于 Golang 编写智能合约。基于本文方案架构，本文在 Fabric 联盟链中构建了 2 个组织，组织内的节点分别代表 RA 和 RTA。RA 和 RTA 作为背书节点，当来自背书节点的有效签名数量超过 2*n*+1 个时，网络内的交易将被提交至排序节点，进而被打包至区块。本文实验构建了单通道下的 4 个 peer 节点（分别属于 2 个组织，即 org_1 和 org_2）、3 个 order 节点和一个客户端节点。此外，由于车辆的移动性和有限的计算能力，车辆不会作为背书节点并且无权访问区块链通道。

4.2 安全性分析

安全性是 VANET 系统中车辆利用通信协议与其他实体进行信息交互的最基本需求。本节将所提方案与几种 VANET 系统中的认证方案进行了对比，具体包括 Kamil 方案[30]，Gayathri 方案[31]，Liu 方案[32]、Sikarwar 方案[33]、Wang 方案[34]及 Yang 方案[35]。本文方案与其他方案主要在匿名性、可追溯性、可撤销性及抵御攻击等方面进行比较，具体比较细节如表 2 所示。其中，Kamil 方案能够实现匿名性、可追溯性以及批量认证等，且能够有效抵御重放攻击、中间人攻击、篡改攻击以及伪造攻击等，但该方案缺乏对车辆身份可撤销性的分析。Gayathri 方案和 Liu 方案能够有效实现匿名性、可撤销性及可追溯性，但没有分析是否能够有效抵御重放攻击以及中间人攻击。Sikarwar 方案能够有效实现匿名性、可追溯性等，但不能满足可撤销性。Wang 方案能够满足常见的安全需求，但不支持高

表 2　　本文方案与其他方案的安全性对比

安全性	Kamil 方案	Gayathri 方案	Liu 方案	Sikarwar 方案	Wang 方案	Yang 方案	本文方案
身份认证性	√	√	√	√	√	√	√
匿名性	√	√	√	√	√	√	√
可撤销性	×	√	√	×	√	√	√
可追溯性	√	√	√	√	√	√	√
批量认证	√	√	√	√	×	√	√
抵御重放攻击	√	×	×	√	√	√	√
抵御中间人攻击	√	×	×	√	√	×	√
抵御篡改攻击	√	√	√	√	√	√	√
抵御伪造攻击	√	√	√	√	√	√	√
前向和后向安全性	√	√	√	√	√	√	√

效的批量认证。Yang 方案能够满足可撤销性、可追溯性以及批量认证等，且能够有效抵御篡改攻击及伪造攻击等，但该方案没有对中间人攻击等其他常见攻击进行分析。通过与其他方案比较，本文方案满足常见的安全需求，且能够实现高效的批量认证。

4.3　计算开销分析

为了更有效地分析本文方案的计算开销，且考虑到需要与不同类型的方案进行对比，本文选择 2 种基于双线性配对的方案，即 Liu 方案与 Sikarwar 方案；以及 4 种基于非双线性配对的方案，即 Gayathri 方案、Kamil 方案、Wang 方案和 Yang 方案作为对比方案。本文使用 C/C++密码学库 MIRACL 对几种方案设计的密码学操作进行了模拟测试。考虑到测试的准确性，每一种密码学操作都基于 1 000 次计算并取平均值作为最终结果，具体如表 3 所示。其中，T_{bp}、T_{sbp}、T_{mtp}、T_{pbp}、T_{sec}、T_{pec}、T_{h} 分别表示进行一次双线性配对操作、基于双线性配对的标量乘法计算、基于双线性配对的 MapToPoint 哈希操作、基于双线性配对的点加操作、基于椭圆曲线的标量乘操作、基于椭圆曲线的点加操作、哈希运算的执行时间。

表 3　　密码学运算的平均执行时间

密码学运算	平均执行时间/ms
T_{bp}	3.786
T_{sbp}	0.336
T_{mtp}	0.101
T_{pbp}	0.001
T_{sec}	0.162
T_{pec}	0.002
T_{h}	0.001

表 4 给出了各方案在身份认证过程中的计算开销。Kamil 方案生成签名的计算开销为 $3T_{\mathrm{sec}}+2T_{\mathrm{pec}}+3T_{\mathrm{h}}\approx 0.493$ ms，进行单一认证的计算开销为 $4T_{\mathrm{sec}}+3T_{\mathrm{pec}}+3T_{\mathrm{h}}\approx 0.657$ ms，批量认证的计算开销为 $(3n+1)T_{\mathrm{sec}}+3nT_{\mathrm{pec}}+3nT_{\mathrm{h}}$。Gayathri 方案生成签名的计算开销为 $2T_{\mathrm{sec}}\approx 0.324$ ms，进行单一认证的计算开销为 $5T_{\mathrm{sec}}+3T_{\mathrm{pbp}}\approx 0.813$ ms，批量认证的计算开销为 $5nT_{\mathrm{sec}}+3nT_{\mathrm{pbp}}$。Liu 方案生成签名的计算开销为 $3T_{\mathrm{sec}}+3T_{\mathrm{h}}\approx 0.489$ ms，进行单一认证的计算开销为 $2T_{\mathrm{bp}}+2T_{\mathrm{sbp}}+2T_{\mathrm{h}}\approx 8.246$ ms，批量认证的计算开销为 $2T_{\mathrm{bp}}+(n+1)T_{\mathrm{sbp}}+2nT_{\mathrm{h}}$。Sikarwar 方案生成签名的计算开销为 $T_{\mathrm{sec}}+T_{\mathrm{h}}\approx 0.163$ ms，进行单一认证的计算开销为 $3T_{\mathrm{bp}}+T_{\mathrm{sbp}}+T_{\mathrm{h}}\approx 11.695$ ms，批量认证的计算开销为 $3T_{\mathrm{bp}}+nT_{\mathrm{sbp}}+3nT_{\mathrm{pbp}}+nT_{\mathrm{h}}$。Wang 方案生成签名的计算开销为 $4T_{\mathrm{sec}}+T_{\mathrm{pec}}+5T_{\mathrm{h}}\approx 0.655$ ms，进行单一认证的计算开销为 $4T_{\mathrm{sec}}+T_{\mathrm{pec}}+6T_{\mathrm{h}}\approx 0.656$ ms，批量认证的计算开销为 $4nT_{\mathrm{sec}}+nT_{\mathrm{pec}}+6nT_{\mathrm{h}}$。Yang 方案生成签名的计算开销为 $2T_{\mathrm{sec}}+T_{\mathrm{pec}}+4T_{\mathrm{h}}\approx 0.33$ ms，进行单一认证的计算开销为 $4T_{\mathrm{sec}}+2T_{\mathrm{pec}}+4T_{\mathrm{h}}\approx 0.656$ ms，批量认证的计算开销为 $4nT_{\mathrm{sec}}+2nT_{\mathrm{pec}}+4nT_{\mathrm{h}}$。本文方案生成签名的计算开销为 $2T_{\mathrm{sec}}+T_{\mathrm{h}}\approx 0.325$ ms，进行单一认证的计算开销为 $4T_{\mathrm{sec}}+T_{\mathrm{pec}}+2T_{\mathrm{h}}\approx 0.652$ ms，进行批量认证的计算开销为 $(2n+2)T_{\mathrm{sec}}+(2n-1)T_{\mathrm{pec}}+2nT_{\mathrm{h}}$。

当车辆数量分别为 20、40、60、80、100、120 时，各方案进行批量认证的计算开销如图 6 所示。从图 6 中可以看出，随着车辆数量的不断增加，各方案的计算开销也逐渐增大。其中，Gayathri 方案的计算

表 4 各方案在身份认证过程中的计算开销

认证方案	生成签名/ms	单一认证/ms	批量认证/ms
Kamil 方案	$3T_{\text{sec}}+2T_{\text{pec}}+3T_{\text{h}}$	$4T_{\text{sec}}+3T_{\text{pec}}+3T_{\text{h}}$	$(3n+1)T_{\text{sec}}+3nT_{\text{pec}}+3nT_{\text{h}}$
Gayathri 方案	$2T_{\text{sec}}$	$5T_{\text{sec}}+3T_{\text{pbp}}$	$5nT_{\text{sec}}+3nT_{\text{pbp}}$
Liu 方案	$3T_{\text{sec}}+3T_{\text{h}}$	$2T_{\text{bp}}+2T_{\text{sbp}}+2T_{\text{h}}$	$2T_{\text{bp}}+(n+1)T_{\text{sbp}}+2nT_{\text{h}}$
Sikarwar 方案	$T_{\text{sec}}+T_{\text{h}}$	$3T_{\text{bp}}+T_{\text{sbp}}+T_{\text{h}}$	$3T_{\text{bp}}+nT_{\text{sbp}}+3nT_{\text{pbp}}+nT_{\text{h}}$
Wang 方案	$4T_{\text{sec}}+T_{\text{pec}}+5T_{\text{h}}$	$4T_{\text{sec}}+T_{\text{pec}}+6T_{\text{h}}$	$4nT_{\text{sec}}+nT_{\text{pec}}+6nT_{\text{h}}$
Yang 方案	$2T_{\text{sec}}+T_{\text{pec}}+4T_{\text{h}}$	$4T_{\text{sec}}+2T_{\text{pec}}+4T_{\text{h}}$	$4nT_{\text{sec}}+2nT_{\text{pec}}+4nT_{\text{h}}$
本文方案	$2T_{\text{sec}}+T_{\text{h}}$	$4T_{\text{sec}}+T_{\text{pec}}+2T_{\text{h}}$	$(2n+2)T_{\text{sec}}+(2n-1)T_{\text{pec}}+2nT_{\text{h}}$

开销最大，本文方案的计算开销最低。当车辆数量为 100 时，本文方案的计算开销分别比 Kamil 方案、Gayathri 方案、Liu 方案、Sikarwar 方案、Wang 方案及 Yang 方案减少了约 32.9%、59.01%、20.1%、26.54%、49.2%及 49.2%。

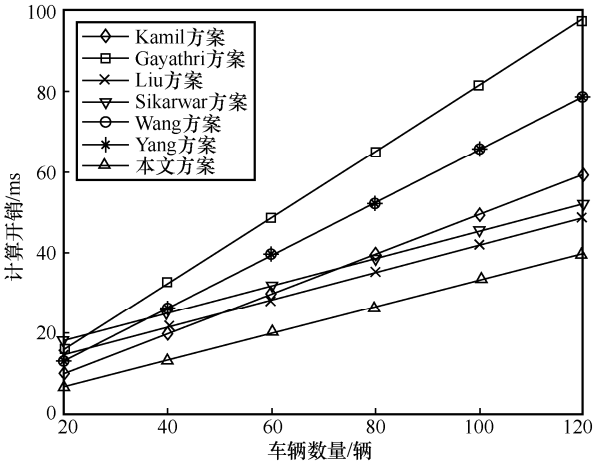


图 6 各方案进行批量认证的计算开销

4.4 通信开销分析

本文构建双线性配对为 $e:G_1\times G_1\to G_2$。G_1 为加法循环群，该群元素的大小为 $64\times 2=128$ byte。基于椭圆曲线 E 上的点及无穷远点 Θ 构建椭圆曲线加法群 G，该群元素大小为 $20\times 2=40$ byte。时间戳大小为 4 byte，哈希值大小为 20 byte，整数域 Z_q^* 中的元素大小为 20 byte。各方案在认证过程中的通信开销如表 5 所示。

Kamil 方案在认证过程中需要传输一个消息元组 $\{\text{PID}_{y,k},PK_k,\ \omega_k,R_k,\upsilon_k,T_k,\nabla,A_k,\Omega_k\}$。在该元组中，$\{\text{PK}_k,R_k,A_k,\Omega_k\}\in G$，$\{\text{PID}_{y,k},\omega_k,\upsilon_k,\nabla\}\in Z_q^*$，$T_k$ 为时间戳。因此，Kamil 方案的通信开销为 $4|G|+4|Z_q^*|+4=244$ byte。Gayathri 方案在认证过程中需要传输假名信息 $\text{ID}_i=(\text{ID}_{1i},\text{ID}_{2i},T_i)$、签名 $\sigma_i=(R_i,Y_{1i},u_i,w_i)$、公钥 $X_i\in G$ 以及部分私钥 $d_i\in Z_q^*$，并且 $\text{ID}_i,\sigma_i,X_i\in G$。因此，Gayathri 方案在认证过程中产生的总通信开销约为 $4|G|+4|Z_q^*|+4=244$ byte。Liu 方案在认证过程中需要传输一个匿名身份 $\text{ID}_i=\{\text{ID}_{i1},\text{ID}_{i2}\}$ 和签名 $\sigma_i=(r_2,U_i)$。其中，$\text{ID}_{i1}\in G$，ID_{i2} 和 r_2 为单个哈希值大小，$U_i\in G_1$。因此，通信开销约为 $|G|+|G_1|+40=128+40+40=208$ byte。Sikarwar 方案在认证过程中需要传输一个消息元组 $\{P_{\text{ID}}^i,M_i,\text{sign}_i,T_i\}$。其中，$\{P_{\text{ID}}^i,M_i,\text{sign}_i\}\in G_1$，$T_i$ 为时间戳。因此，Sikarwar 方案的通信开销为 $3|G_1|+4=128\times 3+4=388$ byte。同理，Wang 方案的通信开销为 $3|G|+2|Z_q^*|+8=168$ byte；Yang 方案的通信开销为 $2|G|+2|Z_q^*|+8=128$ byte。本文方案需要向 RTA 发送消息元组 $\{\text{ID}_p,t_i,\sigma_i\}$。其中，$\sigma_i\in G$，$\text{ID}_p$ 为单个哈希值大小，t_i 为时间戳。所以，本文方案的通信开销约为 $2|G|+20+4=108$ byte。

表 5 各方案在认证过程中的通信开销

认证方案	单一认证/byte	批量认证/byte
Kamil 方案	244	244*n*
Gayathri 方案	244	244*n*
Liu 方案	208	208*n*
Sikarwar 方案	388	388*n*
Wang 方案	168	168*n*
Yang 方案	128	128*n*
本文方案	108	108*n*

各方案认证过程中通信开销对比如图 7 所示。从图 7 中可以看出，本文方案的通信开销低

于其他方案。这是由于本文方案在认证过程中没有依赖于双线性配对操作，且基于区块链使用更少计算步骤完成身份认证过程，因此相较于其他方案，本文方案需要传输的消息元组体积更小，通信开销也相对较少。

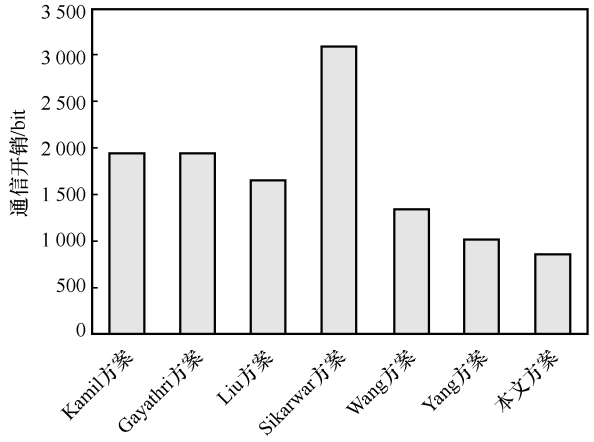


图 7　各方案认证过程中通信开销对比

4.5　认证时延分析

为了更好地分析车载自组网场景下的实际需求，本文进一步考虑了通信时延对认证开销的影响。因此，基于实际车载自组网场景利用 Network Simulator 2 对各方案的通信模块进行了仿真，结果如图 8 所示。当车辆数量分别为 20、40、60、80、100 时，Kamil 方案的通信时延为 46.641 ms、90.732 ms、137.112 ms、182.839 ms、228.139 ms；Gayathri 方案的通信时延分别为 46.991 ms、91.332ms、137.055 ms、182.982 ms、228.147 ms；Liu 方案的通信时延分别为 39.445 ms、78.245 ms、116.646 ms、156.105 ms、193.479 ms；Sikarwar 方案的通信时延分别为 73.805 ms、145.039ms、217.473 ms、289.726 ms、360.320 ms；Wang 方案的通信时延分别为 32.265 ms、63.798 ms、94.232 ms、125.265 ms、157.385 ms；Yang 方案的通信时延分别为 24.398 ms、49.652 ms、73.745 ms、94.532 ms、120.645 ms；本文方案的通信时延分别为 21.182 ms、40.191 ms、61.845 ms、80.534 ms、102.276 ms。在通信时延方面，本文方案具有相较于其他方案更短的通信时延。这是由于本文方案的通信开销低于其他方案，因此会产生更短的通信时延。

在考虑通信时延的情况下，本文计算了各方案的实际认证开销，如图 9 所示。从图 9 中可以看出，各方案的认证时延与车辆数呈近线性关系。其中，当车辆数量为 100 时，Sikarwar 方案认证开销最高，而本文方案的总体认证开销分别比 Kamil 方案、Gayathri 方案、Liu 方案、Sikarwar 方案、Wang 方案及 Yang 方案减少了约 40.54%、56.23%、42.41%、66.61%、39.26%及 27.28%。这是因为本文方案在计算复杂度与通信复杂度方面均优于其他方案。在计算复杂度方面，本文方案没有使用计算成本较高的双线性配对操作，并且相较于其他方案具有更少的计算步骤。因此，本文方案具有更少的计算开销。在通信复杂度方面，本文方案基于区块链实现，验证者通过检索区块链状态数据库获得部分认证参数，有效减少了车辆在实际认证过程中的数据通信需求。因此，本文方案具有更少的通信开销。综上，在车载自组网实际应用场景中，本文方案具有更低的总体认证开销。

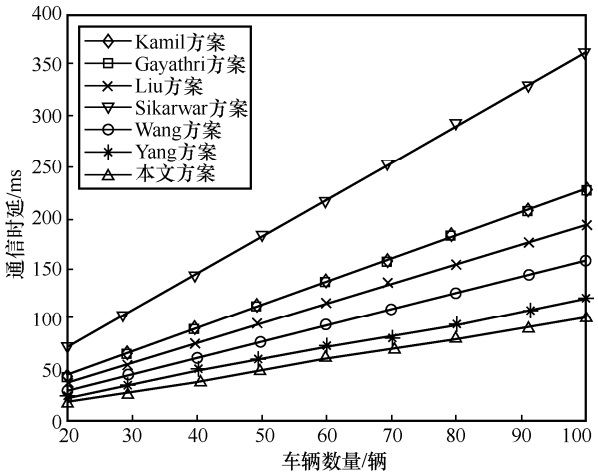


图 8　各方案通信时延对比

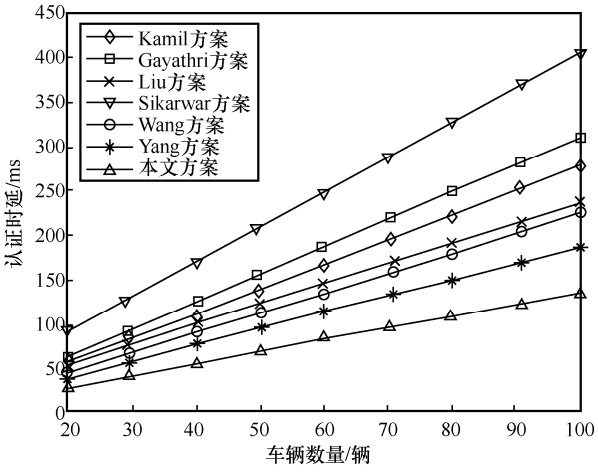


图 9　各方案认证时延对比

4.6　信誉评估机制分析

为了更加清晰地分析本文方案中的信誉评估机制，本文选取参数 $\lambda_1=1$，$\lambda_2=0.5$，$\Delta T_c=20\,\mathrm{s}$，

$\alpha(\beta)=0.5$。交通信息权重值ω需要由 RTA 进行评定计算，这里本文只做举例。假设在消息认证过程中，车辆v_i在 18 s 时进行了一次恶意行为。由图 10 可知，当时间为 0~18 s 时，车辆v_i无恶意行为，此时负向影响值$\mathrm{Cr}_i^{\mathrm{N}}=0$，正向影响值曲线与信誉值曲线重合。当时间为 18 s 时，车辆在消息认证过程中进行了一次恶意行为，导致负向影响值绝对值$\left|\mathrm{Cr}_i^{\mathrm{N}}\right|$急剧增大，同时，该车辆$v_i$的信誉值也随之下降。恶意行为导致车辆$v_i$在时间为 19~40 s 时提供的交通信息较少地被 RTA 接收，正向影响值也随之下降，车辆v_i的信誉值此时处于较低的水平。当时间为 40~60 s 时，车辆v_i的正向影响值逐渐升高，负向影响值绝对值$\left|\mathrm{Cr}_i^{\mathrm{N}}\right|$逐渐降低，此时车辆$v_i$的信誉值逐渐恢复到正常水平。当车辆出现较多恶意行为时，信誉值恢复至正常水平的时间将会大幅增加；当车辆的信誉值低于信誉阈值时，车辆的匿名身份将会被撤销。因此，本文方案的信誉值评估机制能够有效约束车辆行为。

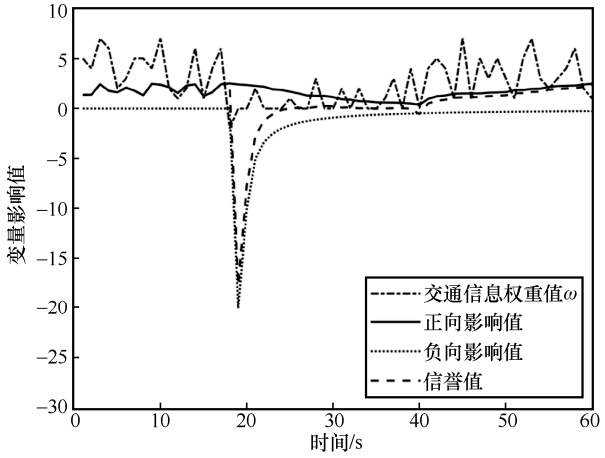


图 10 信誉评估分析

5 结束语

本文提出一种基于区块链的分布式匿名认证方案。车辆利用签名私钥对认证消息进行签名，而区域性可信机构能够利用零知识证明对签名消息进行快速认证。另外，区域性可信机构能够利用签名聚合机制可以将来自不同车辆的单一签名聚合为一个短签名进行批量认证。在认证安全方面，本文方案能够利用签名信息对恶意车辆身份进行准确追溯，并通过区块链状态数据库对车辆身份实现快速撤销。另外，该方案在区块链架构的基础上引入了信誉评估机制，实现对车辆行为的有效约束。最后，安全分析与仿真实验表明，本文方案能够满足匿名性、不可链接性等多种安全需求，且相较于现有同类方案，本文方案能有效降低计算与通信开销，并显著提高认证效率。本文虽然已经涉及车辆信誉评估，但是缺少具体的激励机制，基于所提方案，考虑如何设置合理的激励机制是下一步的主要工作方向。

参考文献：

[1] 张海波, 陈舟, 黄宏武, 等. VANET 系统中基于中国剩余定理的群内相互认证密钥协商协议[J]. 通信学报, 2022, 43(1): 182-193.
ZHANG H B, CHEN Z, HUANG H W, et al. Intra-group mutual authentication key agreement protocol based on Chinese remainder theorem in VANET system[J]. Journal on Communications, 2022, 43(1): 182-193.

[2] SUN Y C, WU L, WU S Z, et al. Security and privacy in the Internet of vehicles[C]//Proceedings of 2015 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI). Piscataway: IEEE Press, 2015: 116-121.

[3] HAN Y B, SONG W, ZHOU Z B, et al. eCLAS: an efficient pairing-free certificateless aggregate signature for secure VANET communication[J]. IEEE Systems Journal, 2022, 16(1): 1637-1648.

[4] ZHANG L, WU Q H, SOLANAS A, et al. A scalable robust authentication protocol for secure vehicular communications[J]. IEEE Transactions on Vehicular Technology, 2010, 59(4): 1606-1617.

[5] ZHANG J H, SUN Z B, LIU S, et al. On the security of a threshold anonymous authentication protocol for VANETs[C]//Security, Privacy, and Anonymity in Computation, Communication, and Storage. Berlin: Springer, 2016: 145-155.

[6] YAO L, LIN C, WU G W, et al. An anonymous authentication scheme in data-link layer for VANETs[J]. International Journal of Ad Hoc and Ubiquitous Computing, 2016, 22(1): 1.

[7] ZHANG C, LU R, LIN X, et al. An efficient identity-based batch verification scheme for vehicular sensor networks[C]//Proceedings of the 27th Conference on Computer Communications. Piscataway: IEEE Press, 2008: 246-250.

[8] CHIM T W, YIU S M, HUI L C K, et al. SPECS: secure and privacy enhancing communications schemes for VANETs[C]/Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Berlin: Springer, 2009: 160-175.

[9] JIANG Y X, SHI M H, SHEN X M, et al. BAT: a robust signature scheme for vehicular networks using binary authentication tree[J]. IEEE Transactions on Wireless Communications, 2009, 8(4): 1974-1983.

[10] JIANG S R, ZHU X Y, WANG L M. An efficient anonymous batch authentication scheme based on HMAC for VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(8): 2193-2204.

[11] YING B D, NAYAK A. Anonymous and lightweight authentication for secure vehicular networks[J]. IEEE Transactions on Vehicular Technology, 2017, 66(12): 10626-10636.

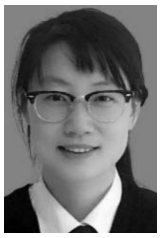
[12] CUI J, WANG Y L, ZHANG J, et al. Full session key agreement scheme based on chaotic map in vehicular ad hoc networks[J]. IEEE Transactions on Vehicular Technology, 2020, 69(8): 8914-8924.

[13] LI Y S, LUO Q, LIU J J, et al. TSP security in intelligent and connected vehicles: challenges and solutions[J]. IEEE Wireless Communications, 2019, 26(3): 125-131.

[14] MEI Q, XIONG H, CHEN J H, et al. Efficient certificateless aggregate

signature with conditional privacy preservation in IoV[J]. IEEE Systems Journal, 2021, 15(1): 245-256.
[15] ZHONG H, HAN S S, CUI J, et al. Privacy-preserving authentication scheme with full aggregation in VANET[J]. Information Sciences, 2019, 476: 211-221.
[16] CUI J, ZHANG J, ZHONG H, et al. An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks[J]. Information Sciences, 2018, 451/452: 1-15.
[17] HUANG J L, YEH L Y, CHIEN H Y. ABAKA: an anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks[J]. IEEE Transactions on Vehicular Technology, 2011, 60(1): 248-262.
[18] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB].2008.
[19] 张海波, 黄宏武, 刘开健, 等. 车联网中可证安全的匿名可追溯快速组认证协议[J]. 通信学报, 2021, 42(6): 213-225.
ZHANG H B, HUANG H W, LIU K J, et al. Verifiably secure fast group authentication protocol with anonymous traceability for Internet of vehicles[J]. Journal on Communications, 2021, 42(6): 213-225.
[20] LU Z J, WANG Q, QU G, et al. A blockchain-based privacy-preserving authentication scheme for VANETs[J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2019, 27(12): 2792-2801.
[21] LIN C, HE D B, HUANG X Y, et al. BCPPA: a blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(12): 7408-7420.
[22] MAIO V D, URIARTE R B, BRANDIC I. Energy and profit-aware proof-of-stake offloading in blockchain-based VANETs[C]//Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing. New York: ACM Press, 2019: 177-186.
[23] LUO B, LI X H, WENG J, et al. Blockchain enabled trust-based location privacy protection scheme in VANET[J]. IEEE Transactions on Vehicular Technology, 2020, 69(2): 2034-2048.
[24] 马铭鑫, 李凤华, 史国振, 等. 物联网感知层中基于 ECC 的分层密钥管理方案[J]. 通信学报, 2018, 39(S2): 1-8.
MAM X, LIFH, SHIZG, et al. ECC based hierarchical key management scheme for perceptual layer of IoT[J]. Journal on Communications, 2018, 39(S2): 1-8.
[25] KUSHWAHA P. Towards the equivalence of Diffie-Hellman problem and discrete logarithm problem for important elliptic curves used in practice[C]//Proceedings of 2017 ISEA Asia Security and Privacy (ISEASP). Piscataway: IEEE Press, 2017: 1-4.
[26] LI X H, JING T, LI R N, et al. BDRA: blockchain and decentralized identifiers assisted secure registration and authentication for VANETs[J]. IEEE Internet of Things Journal, 2022: doi.org/10.1109/JIOT.2022.3164147.
[27] HEZAM A J M A, SYED A A, MOHD W M N, et al. Classification of security attacks in VANET: a review of requirements and perspectives[J]. MATEC Web of Conferences, 2018, 150: 06038.
[28] 宋成, 张明月, 彭维平, 等. 基于双线性对的车联网批量匿名认证方案研究[J]. 通信学报, 2017, 38(6): 49-57.
SONG C, ZHANG M Y, PENG W P, et al. Research on batch anonymous authentication scheme for VANET based on bilinear pairing[J]. Journal on Communications, 2017, 38(6): 49-57.
[29] HUANG J Q, KONG L H, CHEN G H, et al. Towards secure industrial IoT: blockchain system with credit-based consensus mechanism[J]. IEEE Transactions on Industrial Informatics, 2019, 15(6): 3680-3689.
[30] KAMIL I A, OGUNDOYIN S O. An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks[J]. Journal of Information Security and Applications, 2019, 44: 184-200.
[31] GAYATHRI N B, THUMBUR G, REDDY P V, et al. Efficient pairing-free certificate less authentication scheme with batch verification for vehicular ad-hoc networks[J]. IEEE Access, 2018, 6: 31808-31819.
[32] LIU Y W, HE Z J, ZHAO S J, et al. An efficient anonymous authentication protocol using batch operations for VANETs[J]. Multimedia Tools and Applications, 2016, 75(24): 17689-17709.
[33] SIKARWAR H, NAHAR A, DAS D. LABVS: lightweight authentication and batch verification scheme for universal Internet of vehicles (UIoV)[C]//Proceedings of 2020 IEEE 91st Vehicular Technology Conference. Piscataway: IEEE Press, 2020: 1-6.
[34] WANG J, WU L B, CHOO K K R, et al. Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure[J]. IEEE Transactions on Industrial Informatics, 2020, 16(3): 1984-1992.
[35] YANG J N, LIU J, SONG H X, et al. Blockchain-based conditional privacy-preserving authentication protocol with implicit certificates for vehicular edge computing[C]//Proceedings of 2022 7th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA). Piscataway: IEEE Press, 2022: 210-216.

[作者简介]



冯霞（1983− ），女，江苏镇江人，博士，江苏大学副教授、硕士生导师，主要研究方向为物联网安全认证、区块链、应用密码学等。

崔凯平（1997− ），男，山东潍坊人，江苏大学硕士生，主要研究方向为车联网安全认证、区块链、应用密码学等。

谢晴晴（1990− ），女，安徽宿州人，博士，江苏大学副教授、硕士生导师，主要研究方向为云计算、区块链、应用密码学等。

王良民（1977− ），男，安徽潜山人，博士，东南大学教授、博士生导师，主要研究方向为信息安全、区块链、物联网、密码学等。