基于双层分片区块链的车联网跨信任域高效认证方案

刘雪娇[1]，钟强[1]，夏莹杰[2]

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

摘 要：为解决车联网跨信任域消息认证中拓展性差、认证信息同步慢和认证开销大的问题，提出了基于双层分片区块链的车联网跨信任域高效认证方案。设计了一种面向大量跨信任域消息认证的双层分片区块链架构，通过在全域不同实体层级上构建区块链，提升系统的拓展性，确保跨域信息安全高效的共享；提出了一种基于 Metis 图划分算法的车联网区块链分片方法，通过均衡各分片的负载，适应车联网中各路段认证信息不均的情形，提高大量认证信息上链同步的效率；提出了基于无证书公钥密码的跨域批量认证方案，实现对不同信任域消息的批量认证，降低了跨域消息的认证开销。实验表明，所提方案有效地提升了跨信任域消息的认证效率，相比于其他方案，在大量跨域消息认证上降低了 26.4%以上的计算开销。

关键词：车联网；批量认证；跨信任域；分片区块链；高效

中图分类号：TN92

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2023080

Efficient authentication scheme for cross-trust domain of IoV based on double-layer shard blockchain

LIU Xuejiao[1], ZHONG Qiang[1], XIA Yingjie[2]

1. School of Information Science and Technology, Hangzhou Normal University, Hangzhou 311121, China

2. College of Computer Science and Technology, Zhejiang University, Hangzhou 310027, China

Abstract: To solve the problems of poor scalability, slow synchronization of authentication information, and high authentication overhead in cross-trust domain message authentication in the Internet of vehicles (IoV), an efficient authentication scheme for cross-trust domain of IoV based on a double-layer shard blockchain was proposed. A double-layer shard blockchain architecture was designed for lots of cross-trust domain message authentication by constructing blockchains on different entity levels in all domains to improve the scalability of the system and ensure secure and efficient sharing of cross-domain information. A blockchain sharding method based on the Metis graph partitioning algorithm for IoV was proposed to balance loads of each shard and adapt to the uneven distribution of authentication information on different road segments in IoV, thereby improving the efficiency of synchronizing a large number of authentication information on the chain. A batch authentication scheme based on certificateless public-key cryptography (CL-PKC) was proposed, which reduced the authentication overhead of cross-domain messages by enabling batch authentication of messages from different trust domains. Experimental results show that the proposed scheme effectively improves the authentication efficiency of cross-trust domain messages. Compared with other schemes, the proposed scheme reduces the computational overhead of a large number of cross-domain message authentication by more than 26.4%.

Keywords: Internet of vehicles, batch authentication, cross-trust domain, shard blockchain, efficient

---

收稿日期：2023−01−09；**修回日期：**2023−03−21

通信作者：夏莹杰，xiayingjie@zju.edu.cn

基金项目：浙江省自然科学基金资助项目（No.LZ22F030004）；浙江省电子信息产品检验研究院（浙江省信息安全重点实验室）（No.KF202303）

Foundation Items: The Natural Science Foundation of Zhejiang Province (No.LZ22F030004), Zhejiang Electronic Information Products Inspection and Research Institute(Key Laboratory of Information Security of Zhejiang Province) (No.KF202303)

0 引言

车联网是一种多信任域构建的自治网络，基础设施根据网络中不同信任域传输的消息，为车辆跨域出行提供实时可靠的消息服务[1-3]，如路况状态、路径规划等。由于各信任域之间并不完全相互信任、实时消息的有效期短，以及传输过程中容易被截获和篡改，因此对跨域消息进行快速认证尤为重要[4]。然而，随着接收到的跨域消息数量的增加，跨域消息的认证时间成倍增长[5]，导致跨域消息的认证效率不断降低。

区块链技术通过在多个信任域间构建可靠的信任关系，确保认证信息的安全跨域共享，接收者则根据链上共享的跨域认证信息，实现对跨域消息的认证[6-8]。在这个过程中，各信任域的可信机构（TA, truth authority）不仅需要协助完成跨域认证，还需要管理域内车辆和其他基础设施，使整个系统的拓展性较低，难以适用于网络规模化拓展和大量车辆接入的车联网场景。此外，随着划分区域数量的增加，分片技术能够近乎线性地提升区块链吞吐量[9]，有效地适用于车联网中多信任域内大量认证信息上链的处理需求。但传统的随机分片生成方法容易出现热分片，即大部分交易聚集在个别分片上的现象[10-11]，难以适应车联网中不同域内各路段的认证信息负载分布不均的情形，进而导致分片区块链的并行上传认证信息能力降低。因此，如何设计一种适用于车联网多信任域场景和大量认证信息上链需求的分片区块链，是一个值得进一步探索的问题。

另一方面，现有的车联网跨域消息认证方案大多采用基于公钥基础设施（PKI, public key infrastructure）和基于身份密码（IBC, identity-based cryptograph）这2种认证体系[12-13]。而基于无证书公钥密码（CL-PKC, certificateless public-key cryptography）的认证体系有效地解决了PKI的复杂证书管理机制和IBC的密钥托管的固有缺陷，确保密钥生成中心无法拥有车辆的完整私钥，拥有更高的安全性[14]。此外，由于各个信任域的可信机构拥有完全不同的域公私钥对，跨域消息中的密钥和签名也都源自各域的域公私钥对，验证者只能逐一验证各域的消息签名，签名的验证开销也将随着消息数量的增加而线性增长，导致跨域消息验证效率降低。因此，设计一种适用于大量跨域消息认证需求的批量认证方案是一个重要的挑战。

为解决上述的问题与挑战，本文设计了一种适用于车联网大量跨域消息的高效认证方案，采用区块链技术在不同实体层级上进行跨域信息的安全共享，并从跨域认证信息上链的处理性能和跨域消息的认证开销两部分进行改进，以提高跨域消息的认证效率，相应贡献点如下。

1) 设计了一种面向车联网大量跨域认证需求的双层分片区块链架构。该架构维护不同域的基础设施之间的信任关系，确保跨域信息的安全共享，并能有效地利用车联网中不同基础设施的计算能力，提升系统的可拓展性。

2) 设计了一种基于Metis图划分算法的车联网区块链分片方法。该方法有效地适用于车联网中不同信任域内各路段认证信息上链需求分布差异的情形，实现对区块链各分片的负载均衡，进而确保各分片内认证信息上链和同步的并行处理性能。

3) 提出了基于无证书公钥密码的车联网跨信任域批量认证方案。方案实现了对不同信任域消息的批量验证，有效地降低了对大量跨域消息的验证开销，提升了跨信任域消息的认证效率。

1 相关工作

为满足跨域消息认证的高效性需求，已有大量的研究工作被提出。本节将从车联网中提升信息上链效率的分片区块链，以及降低跨域认证开销的跨域消息认证方案2个方面展开介绍。

1.1 车联网中的分片区块链研究

分片区块链凭借链上水平拓展的特性，能够有效地解决区块链低吞吐量和低同步效率的固有缺陷[15]。为此，研究者尝试将分片区块链应用在车联网中，以满足大量跨域信息通过区块链进行安全共享的处理需求。

实际上，分片区块链中各分片区域互不干扰、并行处理的思想，能有效地适用于车联网中按基础设施的通信和管理范围划分区域的场景。Singh等[16]提出一种基于分片区块链的车联网自适应信誉管理机制，按节点地理位置进行分片划分，各分片并行更新区域内车辆的信誉，以此提升全域数据的上链效率。研究者结合车辆动态移动的特性，使分片区块链应用更加贴合车联网场景。Zhang等[17]提出基于分片的车辆区块链高效数据共享方案，由路侧单元（RSU, road side unit）和通信范围内的车辆构成动态分片，通过结合信誉辅助的分片内共识和车辆协助的分片间共识机制，进行局部数据的移动共享，提升了分片共识的效

率。Wang 等[18]提出了一种基于多分片区块链协议的车联网高效数据共享方案，多分片协议中共识节点可以维护多个分片，并直接处理车辆移动产生的跨分片事务，提升了跨分片数据区块的生成效率。Naresh 等[19]提出了一种基于物联网联盟（IOTA, Internet of things alliance）分片的车联网安全组通信方案，通过分片区块链实现群组间的安全通信，有效地提高了区块链处理信息的吞吐量。

目前，分片区块链已在车联网的跨域数据共享、跨域信誉管理等领域取得了一定的研究成果和应用。但现有研究没有考虑在车联网大量跨域消息认证场景中更容易出现热分片的问题，导致各分片并行上链的效率降低。

1.2　高效的跨域消息认证方案

随着应用场景的扩展和跨域消息的频繁传输，跨域认证的效率将随着消息数量增加而降低[20]，因此，跨域消息认证方案的高认证开销问题也吸引了大量研究人员的关注。

Shen 等[21]提出一种区块链辅助的物联网设备安全跨域认证机制，通过云上存储跨域认证信息和链上存储认证信息哈希值相结合的链上验证方式，有效地降低了跨域消息的验证开销。Tong 等[22]提出了基于联盟区块链的物联网完全跨域认证方案，允许异构域拥有各自的认证机制，以降低不同域设备资源交互的认证开销。Yang 等[23]提出一种基于区块链的车联网多域认证方案，所设计的 RSU 代理的两阶段假名生成机制中，车辆根据假名生成材料自行生成假名和密钥，降低了假名和密钥生成的计算开销。上述方案在不同程度上降低了跨域消息的认证开销，但只能对不同信任域的消息进行逐一验证，对大量消息的验证开销较大。

Shen 等[24]提出一种面向车辆云的车联网实时交通数据聚合认证方案，通过采用消息恢复签名技术，在验证签名的同时恢复了消息内容，降低了消息的批量验证开销。Lin 等[6]提出了一种基于重构密钥派生的车联网高效认证方案，采用知识签名算法降低签名验证开销，并在批量验证上拥有较低的开销。然而，这些方案仅实现了同一个信任域内不同管理域（如跨 RSU）的批量验证。Chen 等[25]提出了一种基于 IBC 的跨信任域组批量认证方案，通过在不同域组成员之间进行组密钥协商，实现跨域组内的批量验证。但车辆在维持这种跨域群组结构时，需要可信机构协助并产生大量的通信开销。因此，本文设计了一种高效的车联网跨信任域批量认证方案，不需要构建跨域群组，即可实现对不同信任域车辆消息的批量验证。

2　基于双层分片区块链的车联网跨信任域认证架构

本节将介绍适用于车联网大量跨信任域消息认证需求的双层分片区块链架构，以及区块链中基于 Metis 图划分算法的车联网区块链分片方法。

2.1　双层分片区块链架构

如图 1 所示，双层分片区块链架构由 TA 层、多接入边缘计算（MEC, multi-access edge computing）层、感知层组成，包括各信任域 TA、MEC、RSU 和车辆等实体。TA 区块链和 MEC 区块链分别构建不同实体层级之间的信任传递关系，确保系统中关键信息的安全共享。具体而言，各层级和各实体功能如下。

TA 层。由各个信任域的 TA 构成，TA 负责域内车辆的注册、假名和部分私钥生成，并与其他信任域的 TA 共同维护 TA 区块链，管理全域关键参数和定期更新系统密钥，以及协助分片生成。

MEC 层。由所有信任域内半可信的 MEC 构成，每个 MEC 管理数量不等的多个 RSU，所有 MEC 构成 MEC 区块链，并将 MEC 区块链划分为多个分片。MEC 区块链负责维护各域的公共参数、公钥和假名等认证信息，协助 MEC 对跨域消息进行验证。特别地，各域的 MEC 构成 MEC 区块链的前提是所在域的 TA 已成为构成 TA 链的节点。

感知层。由 RSU 和车辆构成，RSU 为道路两侧的通信中继，负责车辆与其他基础设施之间的信息传输，车辆为车流量和路况信息等消息产生的主体。

2.2　基于Metis图划分算法的车联网区块链分片方法

考虑到各分片的安全性和跨信任域分片管理的复杂性，各信任域要求所构成分片区块链的 MEC 节点是半可信的（即对数据好奇但不泄露和篡改数据），并且不存在跨域分片的现象。具体的分片方法如下。

一个信任域内的划分示例如图 2 所示。由信任域内各 RSU 统计周期 T 内的路段车流量数据，各 MEC 收集通信范围内 RSU 的统计数据，并由 TA 根据各 MEC 的位置和统计的车流量数据生成顶点加权图。

在该顶点加权图中，每个顶点代表一个 MEC 节点，各个顶点的拓扑关系和权重信息以(w_i,v_1,e_1, v_2,e_2,$\cdots$,v_k,e_k)的形式进行存储，其中，顶点权值 w_i 为 MEC 内的车流量，(v_k,e_k)为邻接顶点和与邻接顶

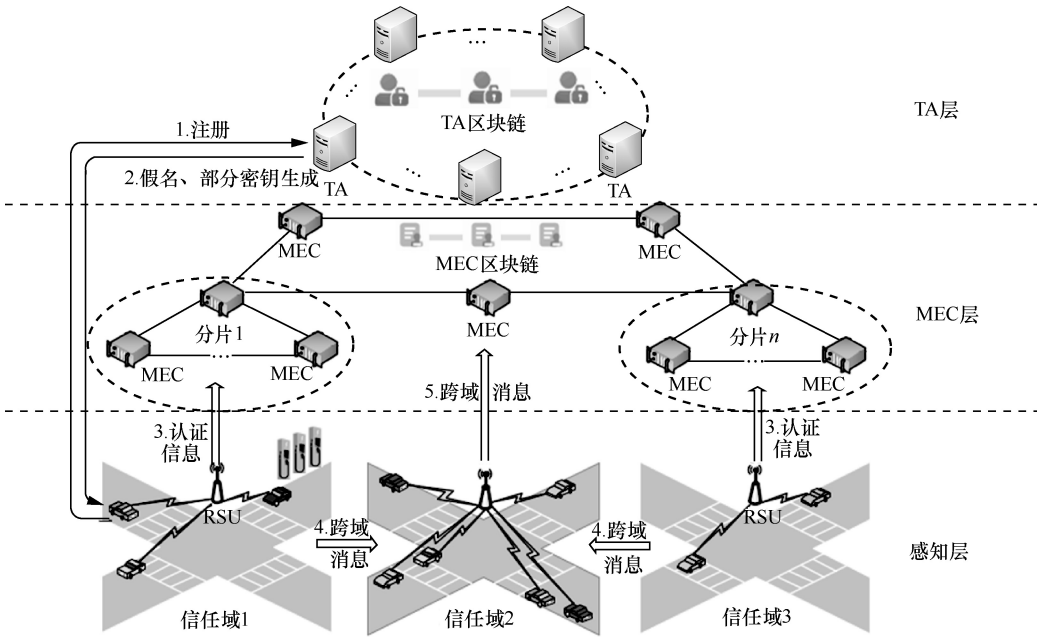

图 1　双层分片区块链架构

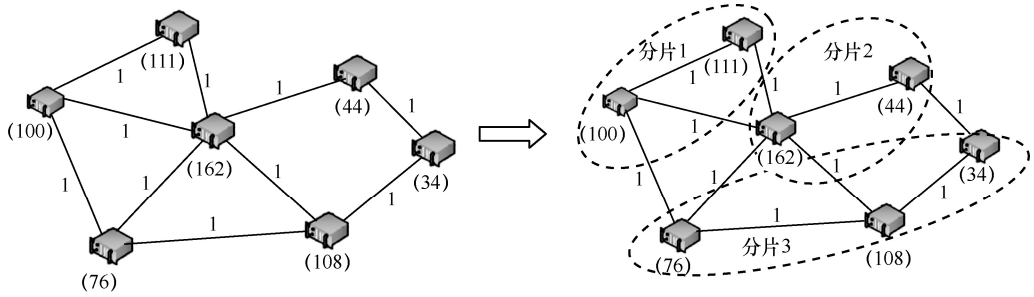

图 2　一个信任域内的划分示例

点之间的边权值（默认为 1）。转换拓扑文件格式为 Metis 可调用的 CSR 格式（CSR 格式广泛用于图的存储，也是 Metis 可处理的标准格式），TA 使用 Metis 对图进行划分，使划分后的各子图之间的顶点权值之和相近。其中，Metis 是一种有效的图划分算法[26]。具体的分片生成算法如算法 1 所示。

算法 1　基于 Metis 的分片生成算法

输入　MEC 节点数 N，域内 MEC 位置和车流量数据 Data

输出　划分结果

1) Topo.brite = Brite(N, Data)
　　//通过拓扑生成器 Brite 生成网络拓扑文件
2) Topo = transform(Topo.brite)
　　//拓扑文件格式转换为 CSR
3) for $i = 0$ to N //读取拓扑数据
4) 　node[i].vwget = Topo.data[$i+1$].w_i
5) 　for $j = 1$ to k
6) 　　node[i].adjncy[j] = Topo.data[$i+1$].v_j
7) 　　node[i].adjwgt[j] = Topo.data[$i+1$].e_j
8) 　end for
9) end for
10) execute metis node N, npart //图划分
11) for $i = 0$ to k //节点所属子图序号
12) 　node[i].part
13) end for

各 TA 通过加入构建和维护 TA 区块链来构建跨域信息共享的信任关系，相应地，这些信任域内的所有 MEC 构成 MEC 区块链，并由各 TA 根据域内图的划分结果对 MEC 区块链进行分片，每个子图对应一个区块链分片，最终生成具有负载均衡特性的分片区块链。

相对于传统的车联网区块链分片方法，本文所提分片方法考虑了实际场景中各区域内 MEC 节点的位置和认证信息处理数量的差异，有效地均衡了各分片

的工作负载，以确保分片区块链的高效并行处理性能，更加适应实际的车联网应用场景和认证需求。

3　基于无证书公钥密码的车联网跨信任域批量认证方案

所提方案采用椭圆曲线密码（ECC, elliptic curve cryptography）技术，并基于椭圆曲线的离散对数问题（ECDLP, elliptic curve discrete logarithm problem）[27]进行设计。具体来说，在由椭圆曲线上的点和一个无穷远点的集合构成的加法群 $\mathbb{G}$ 中，阶为 q，生成元为 P，给定 $W,P\in\mathbb{G}$，由 $W=kP$ 计算出 $k\in Z_q^*$ 对于任何一个概率多项式时间算法都是困难的。

跨域消息认证流程如图 3 所示，整个认证方案包括 6 个阶段：初始化、假名生成、部分私钥生成、完整公私钥对生成、跨域消息签名和跨域消息验证。

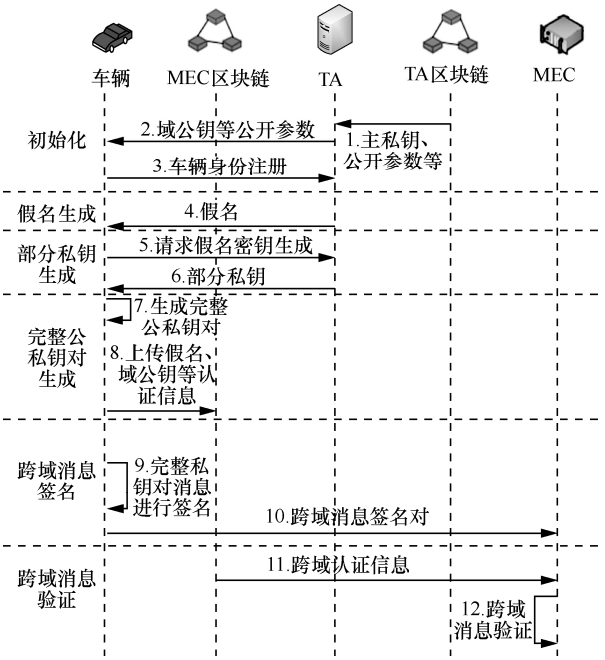

图 3　跨域消息认证流程

3.1　初始化

TA 根据安全参数 λ 生成循环加法群 $\{\mathbb{G},P,q\}$，生成系统主私钥 $r\in Z_q^*$ 和主公钥 $P_r=rP$，并定义认证过程中所需的 3 个安全哈希函数 $H_0:\{0,1\}^*\times\mathbb{G}\to Z_q^*$、$H_1:\{0,1\}^*\times\mathbb{G}\times\mathbb{G}\to Z_q^*$ 和 $H_2:\{0,1\}^*\times\{0,1\}^*\times\mathbb{G}\times\{0,1\}^*\to Z_q^*$，然后将系统参数 $\{\mathbb{G},P,q,P_r,r,H_0,H_1,H_2\}$ 发布到 TA 区块链上，由各信任域的 TA 共同维护系统参数，并定期由 TA 区块链上的智能合约更新系统主私钥和主公钥。各个信任域的 TA 分别进行系统初始化。

TA_j 随机选择 $c_j\in Z_q^*$，计算 $C_j=c_jP$ 和 $\mu_j=H_1(\mathrm{TA}_j,C_j,P_r)$，其中，$\mathrm{TA}_j$ 为 TA 身份标识，各域 TA 都拥有全域 TA 的标识并广播给全域 MEC。然后，计算 $s_j=(c_j+\mu_j r)\bmod q$ 作为域私钥，以及计算得出相应的域公钥 $P_j=s_jP$。各域 TA 广播公开参数 $\{\mathbb{G},P,q,C_j,P_j,H_0,H_1,H_2\}$ 给域内所有实体。

任何进入车联网并需要与网络中基础设施互相进行信息传输的车辆，都需要将真实身份和其他关键身份凭据（如车牌号）通过安全信道发送给本域 TA 进行身份注册，TA 为车辆注册后存储车辆的相应身份信息。

3.2　假名生成

注册有效的车辆为确保发送消息时的匿名性，需要由注册域 TA 根据车辆的真实身份生成车辆的假名，并且 TA 会为车辆预先生成一批假名，以确保每条消息都以不同的假名身份产生和发送，假名生成的具体步骤如下。

车辆 i 随机选择 $r_i\in Z_q^*$ 并计算 $\mathrm{PID}_{i,1}=r_iP$，将 $\{\mathrm{RID}_i,\mathrm{PID}_{i,1},T_i\}$ 通过安全通道发送给 TA，其中，T_i 为申请假名的时间戳。

TA_j 接收到车辆 i 身份信息后通过查询存储的身份数据库对车辆 i 的真实身份 RID_i 进行验证，在确保身份已注册且合法有效后计算 $\mathrm{PID}_{i,2}=\mathrm{RID}_i\oplus H_0(s_j\mathrm{PID}_{i,1},P_j,T_i)$，进而生成假名 $\mathrm{PID}_i=\{\mathrm{PID}_{i,2},T_{\mathrm{pub}}\}$，并通过安全信道发送给车辆 i（T_{pub} 为假名的有效期）。

3.3　部分私钥生成

在该阶段，TA 计算生成车辆的部分私钥，车辆通过安全信道发送身份信息 $\{\mathrm{RID}_i,\mathrm{PID}_i,T_{\mathrm{pub}}\}$ 给 TA，并请求生成相应的部分私钥。TA 检查身份信息中的假名是否存在于假名列表中，若不存在，则忽略该私钥生成请求，若存在，则进行以下操作。

TA_j 随机选择 $k_i\in Z_q^*$ 计算 $U_i=k_iP$，并计算 $w_i=H_1(\mathrm{PID}_i,U_i,P_j)$、$Q_i=(k_i+w_is_j)\bmod q$。然后，$\mathrm{TA}_j$ 把假名对应的部分私钥 $\mathrm{ppk}_i=\{Q_i,U_i\}$ 发送给车辆 i，车辆 i 生成随机秘密值 $x_i\in Z_q^*$ 并计算 $X_i=x_iP$。

3.4　完整公私钥对生成

在该阶段，车辆根据部分私钥和其他相关信息生成完整公私钥对，具体步骤如下。

车辆 i 验证接收到的 $\{Q_i, U_i\}$，验证 $Q_iP = U_i + w_iP_j$ 是否成立，若成立则计算 $K_i = U_i + w_iX_i$，并计算出完整私钥 $\mathrm{sk}_i = Q_i + w_ix_i$，以及相应公钥 $\mathrm{pk}_i = \{K_i, U_i\}$。

车辆 i 将信息 $\{\mathrm{PID}_i, \mathrm{pk}_i, T_i\}$ 发送给附近的 MEC，由 MEC 根据本域的公开参数生成车辆认证信息 $\{C_j, P_j, \mathrm{PID}_i, \mathrm{pk}_i, T_i\}$，并通过分片内共识将其上传到相应的分片上。分片内随机选择的主节点经过全局共识上传到 MEC 区块链上。

3.5 消息签名生成

在该阶段，车辆根据所要发送的消息生成相应的签名，签名过程分为两部分，第一部分由车辆预先执行部分计算操作，第二部分由车辆对消息进行签名。车辆并不知道需要生成签名的消息内容，因此可以预先进行离线签名的计算过程。签名生成的具体步骤如下。

1) 离线签名。车辆预先进行与消息内容无关的操作，车辆 i 随机选择 $a_i \in Z_q^*$ 并计算 $A_i = a_iP$。

2) 在线签名。当车辆 i 需要发送跨域消息 M_i 时，首先计算 $h_{i,1} = H_2(M_i, \mathrm{PID}_i, \mathrm{pk}_i, A_i, P_j, T_s)$，其中 T_s 为消息的新鲜度，进而计算得到 $\mathrm{sig}_i = a_i + h_{i,1}\mathrm{sk}_i$，生成消息对应的签名 $\sigma_i = \{\mathrm{sig}_i, A_i\}$；车辆 i 的每条消息签名对都以 $\{M_i, \mathrm{PID}_i, w_i, \sigma_i, T_s\}$ 的形式发送出去。

3.6 跨域消息验证

1) 消息验证。当 MEC 接收到来自其他域的车辆发送的消息签名对 $\{M_i, \mathrm{PID}_i, w_i, \sigma_i, T_s\}$ 后，进行如下操作对跨域消息进行验证。

首先，MEC 检查各个签名的新鲜度 T_s，若无效则将消息丢弃；否则，MEC 继续检查假名的有效期 T_{pub}，若都有效则从 MEC 区块链上获取相应的跨域认证信息 $\{C_j, \mathrm{PID}_i, \mathrm{pk}_i, P_j, T_i\}$，并对消息签名进行验证。

MEC 根据链上的跨域认证信息和接收的消息内容计算 $h_{i,1} = H_2(M_i, \mathrm{PID}_i, \mathrm{pk}_i, A_i, P_j, T_s)$，以及 $w_i = H_1(\mathrm{PID}_i, U_i, P_j)$，进而验证 $\mathrm{sig}_iP = A_i + h_{i,1}(K_i + w_iP_j)$ 是否成立，若成立则签名有效，接收该消息，否则丢弃该消息。

2) 批量验证。当 MEC 同时接收到 n 条来自不同信任域的消息签名对 $\{M_i, \mathrm{PID}_i, w_i, \sigma_i, T_s\}_{i=1}^n$ 时，可以将验证各信任域的域公钥参数 P_j 转换为验证主公钥参数 P_r，实现对不同信任域消息的批量验证。其中，签名的新鲜度 T_s 和假名的有效期 T_{pub} 的验证操作同单条消息验证过程一致，而对于多个消息签名验证操作如下。

MEC 除了计算各条消息相应的 $h_{i,1}$ 和 w_i 之外，还需要计算消息来源域的参数 $\mu_j = H_1(\mathrm{TA}_j, C_j, P_r)$，进而验证式(1)是否成立，若成立则接收消息，否则丢弃消息。

$$\sum_{i=1}^{n}\mathrm{sig}_iP = \sum_{i=1}^{n}A_i + \sum_{i=1}^{n}\left(h_{i,1}K_i\right) + \sum_{i=1}^{n}(h_{i,1}w_iC_j) + \sum_{i=1}^{n}(h_{i,1}w_i\mu_j)P_r \tag{1}$$

对于大量跨域消息签名的式(1)的正确性验证如下。

$$\begin{aligned}&\sum_{i=1}^{n}\mathrm{sig}_iP = \sum_{i=1}^{n}A_i + \sum_{i=1}^{n}(h_{i,1}K_i) + \\&\sum_{i=1}^{n}(h_{i,1}w_iC_j) + \sum_{i=1}^{n}(h_{i,1}w_i\mu_j)P_r = \\&\sum_{i=1}^{n}A_i + \sum_{i=1}^{n}(h_{i,1}K_i) + \sum_{i=1}^{n}h_{i,1}w_i((c_j + \mu_jr)P) = \\&\sum_{i=1}^{n}A_i + \sum_{i=1}^{n}h_{i,1}(K_i + w_iP_j)\end{aligned} \tag{2}$$

4 安全性分析

本节对方案的安全性进行分析。如表 1 所示，将所提方案与其他跨域消息认证方案进行对比，对比性能包括匿名性、不可伪造性、不可链接性、可追溯、抵抗常见攻击和跨域批量认证。

匿名性。所提方案中的车辆都使用 TA 生成的假名进行通信，其真实身份都隐藏在假名中，使除 TA 外的攻击者都无法从假名中获取车辆的真实身份。而 Chen 等方案[25]使用真实身份进行交互，用户身份信息容易被泄露。

不可伪造性。车辆假名由 TA 根据车辆真实身份和域私钥生成，其他任何实体都无法伪造车辆有效的假名。所提方案是基于 ECDLP 进行设计的，只有当车辆拥有完整的私钥时才能对消息进行签名，所以攻击者无法在解决 ECDLP 的概率多项式时间内伪造出有效的签名。

不可链接性。所提方案中车辆发送的每条消息都会使用不同的假名和相应的私钥进行签名，新假名和旧假名之间没有关系，攻击者无法通过 2 条消息链接到同一个车辆。而 Shen 等方案[21]和 Chen 等方案[25]每次通信都使用相同的身份标识。

可追溯。一旦发现恶意消息，注册域 TA 都可

表 1　　方案安全性分析

方案	匿名性	不可伪造性	不可链接性	可追溯	抵抗常见攻击	跨域批量认证
Shen 等方案[21]	√	√	×	√	√	×
Yang 等方案[23]	√	√	√	√	√	×
Chen 等方案[25]	×	√	×	√	√	√
所提方案	√	√	√	√	√	√

以根据车辆假名 $\mathrm{PID}_i=\{\mathrm{PID}_{i,2},T_{\mathrm{pub}}\}$，计算 $\mathrm{RID}_i=\mathrm{PID}_{i,2}H_0(s_j\mathrm{PID}_{i,1},P_j,T_i)$ 得到发送恶意消息的车辆真实身份。

抵抗常见攻击。所提方案通过引入数字签名以抵抗消息内容篡改攻击，只有拥有合法有效的假名和完整私钥的车辆才能生成有效的签名，从而抵抗了模仿攻击；为确保消息的新鲜度，设定签名时间戳以抵抗重放攻击。此外，车辆注册初始化和假名生成都是在 TA 的管理下实现的，避免了中间人攻击。

跨域批量认证。当接收到来自不同域的消息时，所提方案可以对这些消息进行批量处理，同时完成这些消息的验证过程，而 Shen 等方案[21]和 Yang 等方案[23]只能进行逐一验证。

5　性能分析

5.1　实验设置

为了评估分片在认证信息上链的处理性能，通过在 Intel Xeon Silver 4210 @ 2.20 GHz 处理器和 60 GB 内存的服务器上搭建和测试基于 Hyperledger Fabric 开发平台的未分片区块链和分片区块链。以 2021 年 1 月英国的米尔凯顿恩斯、德比和伯明翰 3 个城市的城区道路车流量数据作为基础数据集，并按各个城市城区的管理范围进行信任域的划分。在衡量作为分片节点的车流量检测点数量后，统一设定各域内各拥有 3 个分片，并以车流量表示节点内认证信息处理的工作负载。

为了更好地比较不同方案在跨域消息上的认证开销，相关测试在搭载 Inter(R) Core(TM) i5-10500 @ 3.10 GHz 处理器、16 GB 内存、Windows10 系统的计算机上进行，选择 BN-P156 和 SECG-K-160 参数并分别用于基于双线性配对的方案和基于椭圆曲线密码的方案，选择 p 和 q 分别为 256 bit 和 160 bit 的大素数，双线性配对记为 $e:\mathbb{G}_1\times\mathbb{G}_1\to\mathbb{G}_T$，$\mathbb{G}_1$ 为 q 阶素数的加法群，椭圆曲线加密记为 $E:y^2=(x^3+ax+b)\mathrm{mod}p$，并选择 SHA-256 为哈希函数。相关密码操作的执行时间如表 2 所示，通过调用 Miracl 密码库，计算出认证过程中所涉及的密码操作的执行开销，并忽略整数的加法和乘法操作、连接操作等执行开销极小的运算操作。

表 2　　相关密码操作的执行时间

操作标识	含义	执行时间/ms
T_{bm}	双线性配对的标量乘运算	0.624 0
T_{ba}	双线性配对的点加运算	0.001 4
T_{bp}	双线性配对	4.322 5
T_{ep}	模幂运算	3.342 7
T_{pm}	在 $\mathbb{G}_1$ 上的标量乘运算	0.356 2
T_{pa}	在 $\mathbb{G}_1$ 上的点加运算	0.002 6
T_{h}	哈希运算	0.000 6

5.2　跨域认证信息处理性能

为评估不同方案中认证信息上链的处理性能，本节实验将比较区块链的交易吞吐量和各分片的工作负载差异。其中，分片的工作负载差异反映了各分片能否有效发挥并行处理的能力。

5.2.1　交易吞吐量分析

区块链架构下交易吞吐量将直接影响区块链跨域信息上链的效率，实验中通过不断提高发送交易的速率来测试区块链的交易吞吐量。由于 Shen 等方案[21]和 Yang 等方案[23]都使用各信任域的 TA 作为区块链节点进行认证信息的跨域共享，因此，在信任域数量相同的情况下，所构成区块链的节点数量相同，故将其都标记为 Yang 等方案。

多域的交易吞吐量对比如图 4 所示。在 2 个、4 个和 6 个域的场景下，区块链的吞吐量随着发送交易速率的增加而变化。测试结果显示，所测试的区块链在达到最大吞吐量后，都将在最大吞吐量上下波动，波动区间为±45TPS，其中 Yang 等方案[23]的吞吐量比所提方案小。由于域数量增加使共识通信轮数的增加，Yang 等方案[23]的交易吞吐量随着域数量的增加而逐渐降低；而所提方案对区块链进行了分片，每个分片相当于规模较小的区块链，能够并行处理认证信息的上传，整个区块链的交易吞吐量也随着域数量的增加而线性增加。

在 2 个、4 个和 6 个域的场景下，所提方案分别比 Yang 等方案[23]的交易吞吐量提升了 207.6%、505.8%和 843.5%，并且车联网跨域认证信息上传中不存在跨分片交易的情况，因此分片区块链的交易吞吐量不会受该因素的影响。

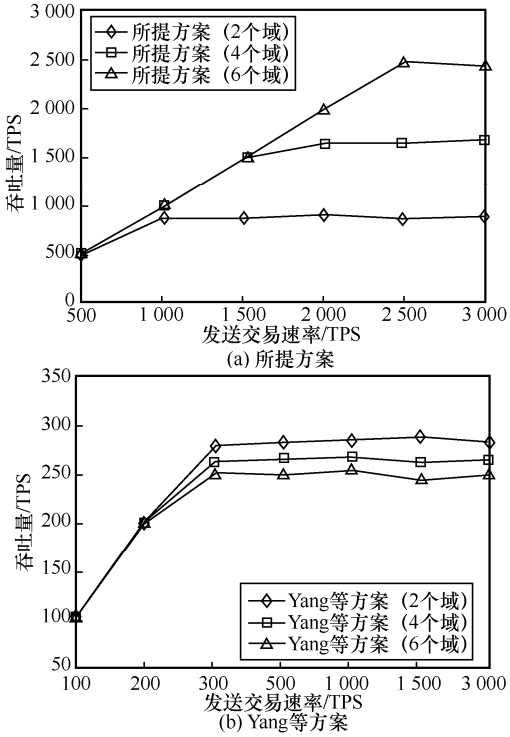

图 4　不同方案多域的交易吞吐量对比

多个域容易出现大量认证信息同时请求上传至区块链的情形，以完成认证信息的全域同步。实验表明，所提方案在多域场景下将具有更高的认证信息上链效率，更适用于大量的跨域认证信息处理需求。

5.2.2　分片区块链的负载分析

为了比较不同方案中各分片的工作负载差异，本节实验根据采集的车流量数据集设定了 3 种不同的车流量分布场景，将其分别标识为信任域 1、信任域 2 和信任域 3，通过给区块链内各分片添加相应的工作负载，即车流量数据，得出不同车流量分布场景下的各分片工作负载分布情况。

各分片工作负载分布如图 5 所示，横坐标 S31 表示 Singh 等方案[16]在信任域 3 的分片 1。在不同车流量分布场景中，所提方案中各分片的工作负载差异（即方差）都小于其他方案。其中，由于 Singh 等方案[16]的分片根据节点位置生成，容易出现高负载节点在同一个分片的情形；Wang 等方案[9]的分片则根据节点地址（即公钥）前几位分配生成，节点选择的随机性导致部分高负载分片的负载有所降低；而所提方案的分片区块链考虑了节点的位置及所需承担的工作负载，能够均衡各分片的工作负载。因此，如图 5(d)所示，在信任域 1、信任域 2 和信任域 3 这 3 种不同车流量分布场景中，所提方案相较于 Singh 等方案[16]和 Wang 等方

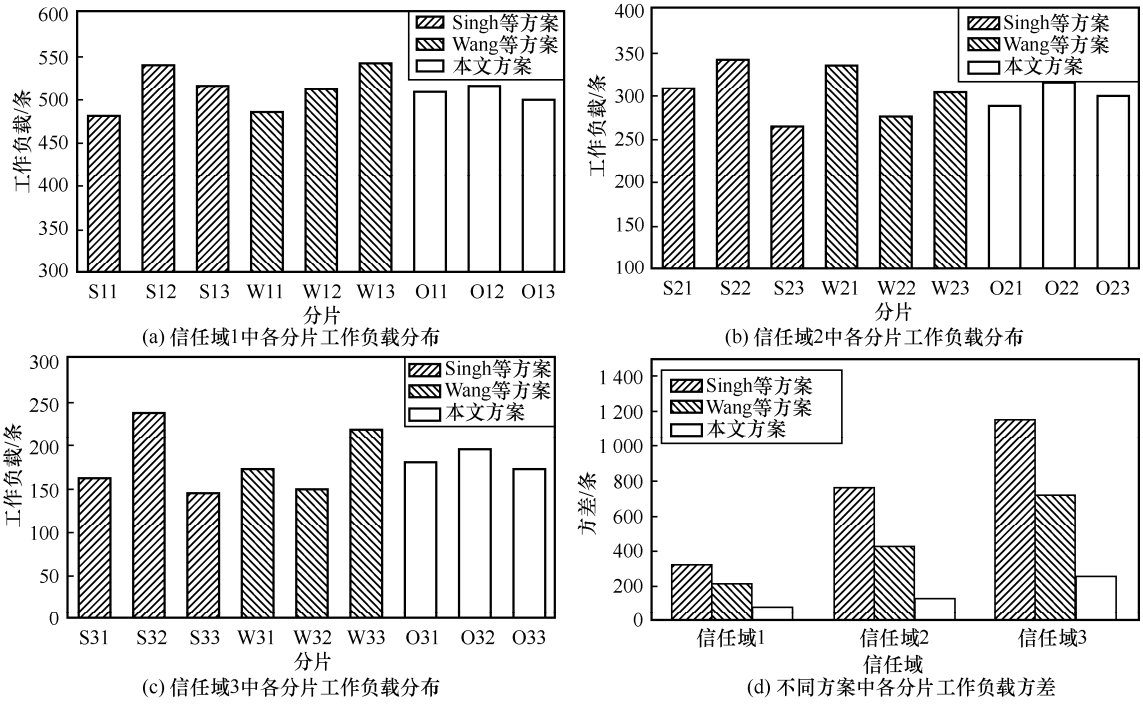

图 5　各分片工作负载分布

案[9]在分片工作负载差异上分别降低了 74.5%和 62.2%、80.3%和 64.1%、78.64%和 65.5%。实验结果表明，所提方案在不同车流量分布程度的场景中，都能有效地均衡各分片的工作负载，确保各分片发挥认证信息并行上链的处理能力，更适用于车流量分布不均的车联网场景。

5.3　跨域认证开销

为更好地评估方案中跨域消息的认证开销，本节实验将从计算开销和通信开销两部分进行分析。

5.3.1　计算开销

为更好地评估所提方案在认证过程中的计算开销，实验将与 Shen 等方案[21]、Yang 等方案[23]和 Chen 等方案[25]，分别在假名和部分密钥生成、跨域消息签名和跨域消息验证这 3 个认证阶段上进行比较。如表 3 所示，所提方案在认证过程中各个阶段的计算开销都小于其他方案。

表 3　　**计算开销比较**

方案	假名和部分密钥生成	离线签名	在线签名	跨域消息验证	批量验证(n 条消息)
Yang 等方案	$7T_{pm}+T_{pa}+6T_h$	0	T_h	$3T_{pm}+4T_{pa}+2T_h$	$3nT_{pm}+4nT_{pa}+2nT_h$
Shen 等方案	$3T_{ep}+4T_{bm}+T_{ba}+2T_{bp}+4T_h$	0	$T_{ep}+T_{bm}+T_{bp}+T_h$	$2T_{ep}+2T_{bm}+T_{ba}+T_{bp}+2T_h$	$2nT_{ep}+2nT_{bm}+nT_{ba}+nT_{bp}+2nT_h$
Chen 等方案	$2T_{bm}+3T_{ba}+T_{bp}+2T_h$	0	$2T_{bm}+T_{ba}+T_h$	$3T_{bm}+3T_{ba}+2T_{bp}+2T_h$	$(3n-1)T_{bm}+(5n-7)T_{ba}+2T_{bp}+(2n-1)T_h$
所提方案	$6T_{pm}+2T_{pa}+2T_h$	T_{pm}	T_h	$3T_{pm}+2T_{pa}+2T_h$	$(2n+2)T_{pm}+3nT_{pa}+3nT_h$

各方案中不同阶段的计算开销如图 6 所示。Shen 等方案[21]和 Chen 等方案[25]在假名和部分密钥生成、消息签名生成和签名验证阶段都涉及双线性配对和模幂运算等高计算开销操作，导致各部分开销都远高于所提方案。在假名和部分密钥生成阶段，所提方案相比于 Yang 等方案[23]的计算开销降低了 14.3%；在跨域消息签名阶段，Yang 等方案[23]直接将部分私钥作为签名的一部分省去了标量乘操作的执行开销，所提方案则采用离线签名的方式预先执行开销较大的标量乘操作，因此签名开销相同；在单个消息签名的验证阶段，所提方案的计算开销略小于 Yang 等方案[23]的计算开销。

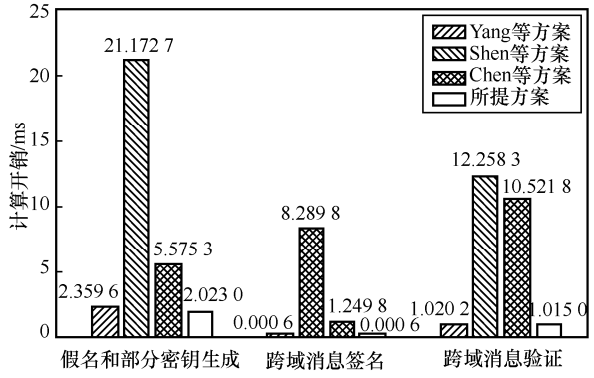

图 6　各方案中不同阶段的计算开销

如图 7 所示，在同时对大量跨域消息验证的计算开销上，所提方案的验证开销小于其他方案。具体来说，由于消息签名来自不同的信任域，Yang 等方案[23]和 Shen 等方案[21]只能对这些消息签名进行逐一验证。Chen 等方案[25]的跨信任域批量认证，只能以组内成员的形式进行批量验证。所提方案针对密钥和跨域消息签名的生成进行了改进，实现了对不同域消息的批量验证，因此，所提方案的验证开销将随着消息数量的增加而降低，并相较于 Yang 等方案[23]、Shen 等方案[21]和 Chen 等方案[25]的验证开销分别降低了 26.4%、94.7%和 67.3%。

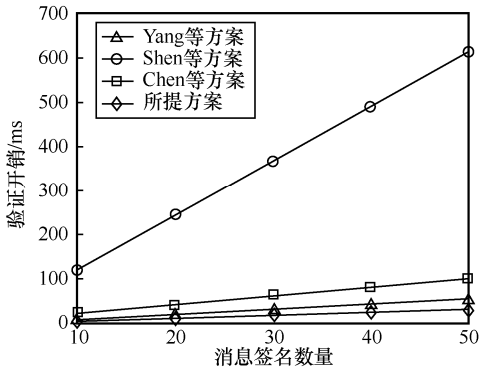

图 7　大量消息签名验证开销比较

由于全域大量消息的频繁跨域传输，导致接收方容易同时接收到大量来自不同信任域的消息。实验结果表明，所提方案在整个消息认证过程中的计算开销都低于其他方案的计算开销，并在大量消息认证的场景下，具有更高的跨域消息认证效率。

5.3.2 通信开销

为了评估跨域消息认证过程中的通信开销，实验将通信过程中所涉及的真实身份、假名和时间戳统一标识为 L_n，长度为 4 B；哈希标识为 L_h，长度为 32 B；$\mathbb{G}_1$ 群中元素标识为 L_G，长度为 64 B；跨域消息的标识为 L_m，以此进行认证过程中传输信息的数值化比较。

如表 4 所示，由于 Shen 等方案[21]需要将消息签名生成和验证过程都由接收方转交给可信的密钥生成中心（KGC, key generate center）完成，导致总通信开销都远大于所提方案。在假名和部分密钥生成中，由于 Yang 等方案[23]中车辆根据 RSU 的假名生成材料自行生成假名和密钥，使该部分的通信开销小于其他方案；而所提方案在密钥生成中车辆需要接收到 TA 生成的部分私钥后才能生成完整私钥，导致此阶段的通信开销略高于其他方案。在跨域消息签名中，所提方案比其他方案拥有更小的通信开销。

在跨域消息验证中，由于 Chen 等方案[25]由跨域组内的接收方根据本地信息直接进行验证，而所提方案中验证者直接通过查询链上的跨域认证信息进行验证，都不存在相应的通信开销，其他部分各方案的通信开销相近。因此，虽然所提方案在部分阶段的通信开销大于其他方案，但本文方案与 Yang 等方案[23]、Chen 等方案[25]的总通信开销相近，相较于 Shen 等方案[21]的总通信开销降低了约 51.5%。

6 结束语

本文提出了一种适用于大量跨域消息认证的车联网高效认证方案。具体而言，设计了车联网双层分片区块链架构，以维护不同域内实体之间的信任关系，确保全域信息的安全共享。通过设计一种适用于车联网实际应用场景的区块链分片方法，根据各路段的车流量来量化认证信息上链的数量，以此作为区块链中分片划分的关键依据，进而实现各分片间的负载均衡，提升跨域认证信息上链的效率。此外，提出了一种基于无证书公钥密码的车联网跨信任域批量认证方案，通过域密钥生成机制，将域公钥的验证转换为主公钥的验证，实现对不同信任域消息的批量验证，降低了认证开销。最后，通过安全性和性能分析证明，所提方案在保障安全性的同时，拥有更高的可拓展性和信息上链的处理能力，并有效地降低了跨域认证过程中的认证开销。

表 4 通信开销比较

方案	假名和部分密钥生成/B	跨域消息签名/B	跨域消息验证/B	总通信开销/B
Yang 等方案	$4L_n+2L_h+L_G\approx 144$	$L_m+3L_n+3L_h+2L_G\approx L_m+236$	$3L_n+3L_G\approx 204$	L_m+584
Shen 等方案	$3L_n+L_h+3L_G\approx 292$	$L_m+6L_n+5L_h+7L_G\approx 2L_m+612$	$L_m+4L_h+3L_G\approx L_m+300$	$3L_m+1204$
Chen 等方案	$L_n+2L_h+5L_G\approx 360$	$L_m+2L_n+4L_G\approx L_m+264$	0	L_m+624
所提方案	$8L_n+4L_h+4L_G\approx 416$	$L_m+2L_n+3L_h+L_G\approx L_m+168$	0	L_m+584

参考文献：

[1] TAN H W, XUAN S C, CHUNG I. HCDA: efficient pairing-free homographic key management for dynamic cross-domain authentication in VANETs[J]. Symmetry, 2020, 12(6): 1003.

[2] AGGARWAL S, KUMAR N, GOPE P. An efficient blockchain-based authentication scheme for energy-trading in V2G networks[J]. IEEE Transactions on Industrial Informatics, 2021, 17(10): 6971-6980.

[3] ALI I, CHEN Y, ULLAH N, et al. An efficient and provably secure ECC-based conditional privacy-preserving authentication for vehicle-to-vehicle communication in VANETs[J]. IEEE Transactions on Vehicular Technology, 2021, 70(2): 1278-1291.

[4] WANG P, LIU Y N. SEMA: secure and efficient message authentication protocol for VANETs[J]. IEEE Systems Journal, 2021, 15(1): 846-855.

[5] CHEN J, ZHAN Z Y, HE K, et al. XAuth: efficient privacy-preserving cross-domain authentication[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(5): 3301-3311.

[6] LIN C, HUANG X Y, HE D B. EBCPA: efficient blockchain-based conditional privacy-preserving authentication for VANETs[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 20(3): 1818-1832.

[7] 冯霞, 崔凯平, 谢晴晴, 等. VANET 中基于区块链的分布式匿名认证方案[J]. 通信学报, 2022, 43(9): 134-147.
FENG X, CUI K P, XIE Q Q, et al. Distributed anonymous authentication scheme based on blockchain in VANET[J]. Journal on Communications, 2022, 43(9): 134-147.

[8] XUE L Y, HUANG H P, XIAO F, et al. A cross-domain authentication scheme based on cooperative blockchains functioning with revocation for medical consortiums[J]. IEEE Transactions on Network and Service Management, 2022, 19(3): 2409-2420.

[9] WANG J, WANG H. Monoxide: scale out blockchains with asynchronous consensus zones[C]//Proceedings of the 16th USENIX symposium on networked systems design and implementation. Berkeley: USENIX Association, 2019: 95-112.

[10] HUANG H W, PENG X W, ZHAN J Z, et al. BrokerChain: a cross-shard blockchain protocol for account/balance-based state

sharding[C]//Proceedings of IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2022: 1968-1977.

[11] ZHENG P L, XU Q Q, LUO X P, et al. Aeolus: distributed execution of permissioned blockchain transactions via state sharding[J]. IEEE Transactions on Industrial Informatics, 2022, 18(12): 9227-9238.

[12] QI J Y, GAO T H. A privacy-preserving authentication and pseudonym revocation scheme for VANETs[J]. IEEE Access, 2020, 8: 177693-177707.

[13] ZHOU Y, LONG X, CHEN L, et al. Conditional privacy-preserving authentication and key agreement scheme for roaming services in VANETs[J]. Journal of Information Security and Applications, 2019, 47: 295-301.

[14] 张文波, 黄文华, 冯景瑜. 基于无证书签密的车联社会网络安全通信机制[J]. 通信学报, 2021, 42(7): 128-136.
ZHANG W B, HUANG W H, FENG J Y. Secure communication mechanism for VSN based on certificateless signcryption[J]. Journal on Communications, 2021, 42(7): 128-136.

[15] 黄冬艳, 李浪, 陈斌, 等. RBFT：基于 Raft 集群的拜占庭容错共识机制[J]. 通信学报, 2021, 42(3): 209-219.
HUANG D Y, LI L, CHEN B, et al. RBFT: a new Byzantine fault-tolerant consensus mechanism based on Raft cluster[J]. Journal on Communications, 2021, 42(3): 209-219.

[16] SINGH P K, SINGH R, NANDI S K, et al. Blockchain-based adaptive trust management in Internet of vehicles using smart contract[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(6): 3616-3630.

[17] ZHANG X, XIA W, CUI Q, et al. Efficient and trusted data sharing in a sharding-enabled vehicular blockchain[J]. IEEE Network, 2022: doi.org/10.1109/MNET.122.2100755.

[18] WANG J, HUANG J, KONG L, et al. A privacy-preserving vehicular data sharing framework atop multi-sharding blockchain[C]//Proceedings of 2021 IEEE Global Communications Conference. Piscataway: IEEE Press, 2021: 1-6.

[19] NARESH V S, ALLAVARPU V V L D, REDDI S. Blockchain IOTA sharding-based scalable secure group communication in large VANETs[J]. IEEE Internet of Things Journal, 2023, 10(6): 5205-5213.

[20] ZHANG Y, LI B, WU J X, et al. Efficient and privacy-preserving blockchain-based multifactor device authentication protocol for cross-domain IIoT[J]. IEEE Internet of Things Journal, 2022, 9(22): 22501-22515.

[21] SHEN M, LIU H S, ZHU L H, et al. Blockchain-assisted secure device authentication for cross-domain industrial IoT[J]. IEEE Journal on Selected Areas in Communications, 2020, 38(5): 942-954.

[22] TONG F, CHEN X, WANG K M, et al. CCAP: a complete cross-domain authentication based on blockchain for Internet of things[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 3789-3800.

[23] YANG Y H, WEI L J, WU J, et al. A blockchain -based multidomain authentication scheme for conditional privacy preserving in vehicular ad-hoc network[J]. IEEE Internet of Things Journal, 2022, 9(11): 8078-8090.

[24] SHEN J, LIU D Z, CHEN X F, et al. Secure real-time traffic data aggregation with batch verification for vehicular cloud in VANETs[J]. IEEE Transactions on Vehicular Technology, 2020, 69(1): 807-817.

[25] CHEN Q, WU T, HU C, et al. An identity-based cross-domain authenticated asymmetric group key agreement[J]. Information, 2021, 12(3): 112.

[26] KARYPIS G, KUMAR V. A fast and high quality multilevel scheme for partitioning irregular graphs[J]. SIAM Journal on scientific Computing, 1998, 20(1): 359-392.

[27] GALBRAITH S D, GAUDRY P. Recent progress on the elliptic curve discrete logarithm problem[J]. Designs, Codes and Cryptography, 2016, 78: 51-72.

[作者简介]

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

钟强（1998– ），男，江西赣州人，杭州师范大学硕士生，主要研究方向为网络安全、区块链和车联网安全认证。

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