基于新型可净化多重签名的车联网高效假名证书分发方案

刘召曼[1]，杨亚芳[1]，宁建廷[2]，赵运磊[3]
（1. 复旦大学计算机科学技术学院，上海 200082；2. 武汉大学国家网络安全学院，湖北 武汉 430000；
3. 密码科学技术国家重点实验室，北京 100036）

摘　要：现有假名证书方案未充分考虑多职能机构协同授予的需求。为此，提出了一种基于变色龙哈希（CH）和多重签名（MS）的可净化多重签名（SMS）方案。该方案引入净化功能，允许授权净化者在无须与原签名者交互的情况下更新签名数据，解决了车辆频繁更换假名时的快速响应问题。为防止滥用净化权限，SMS 通过验证多重签名来源，追踪恶意净化行为。进一步，所提方案将净化功能部署于路侧单元（RSU），提出了一种高效的假名证书分发方案。安全性分析表明，该方案能有效抵抗关联攻击和冒充攻击，且在认证过程中 RSU 与车辆的计算开销未显著增加，具有较好的效率和安全性。

关键词：车联网；位置隐私保护；匿名认证；假名证书；可净化多重签名
中图分类号：TN92
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024198

Efficient pseudonym certificate distribution scheme for Internet of vehicles based on novel sanitizable multi-signature

LIU Zhaoman[1], YANG Yafang[1], NING Jianting[2], ZHAO Yunlei[3]
1. College of Computer Science and Technology, Fudan University, Shanghai 200082, China
2. School of Cyber Science and Engineering, Wuhan University, Wuhan 430000, China
3. State Key Laboratory of Cryptography, Beijing 100036, China

Abstract: Existing pseudonym certificate schemes fail to adequately address the collaboration needs of multiple entities in the certificate issuance process. To address this, a sanitizable multi-signature (SMS) scheme based on chameleon Hash (CH) and multi-signature (MS) was proposed. By introducing a sanitizability function, SMS scheme allowed authorized sanitizers to update signature data without interacting with the original signers, resolving the issue of rapid response when vehicles frequently change pseudonyms. To prevent the abuse of sanitizability privileges, SMS verified the source of multi-signatures to trace malicious sanitizability actions. Furthermore, the proposed scheme deployed the sanitizability function on road-side units (RSU) and proposed an efficient pseudonym certificate distribution scheme. Security analysis shows that the scheme effectively resists correlation and impersonation attacks, with minimal computational overhead on RSU and vehicles, ensuring good efficiency and security during pseudonym certificate and anonymous authentication processes.

Keywords: Internet of vehicles, location privacy preservation, anonymous authentication, pseudonym certificate, sanitizable multi-signature

收稿日期：2024–07–31；**修回日期：**2024–11–05
通信作者：赵运磊，ylzhao@fudan.edu.cn
基金项目：国家重点研发计划基金资助项目（No.2022YFB2701601）；上海市协同创新基金资助项目（No.XTCX-KJ-2023-54）；上海市科委区块链关键技术攻关专项基金资助项目（No.23511100300）
Foundation Items: The National Key Research and Development Program of China (No.2022YFB2701601), Shanghai Collaborative Innovation Fund (No.XTCX-KJ-2023-54), Special Fund for Key Technologies in Blockchain of Shanghai Scientific and Technological Committee (No.23511100300)

0 引言

车载自组织网络（VANET, vehicular ad hoc network）是一种特殊的物联网（IoT, Internet of things）系统，旨在通过通信技术将车辆、道路基础设施和互联设备连接起来，改善道路交通的效率、安全性和环境友好性。VANET的主要组成部分包括车载单元（OBU, on-board unit）和路侧单元（RSU, road side unit），其中OBU被嵌入在车辆内，用于实现车辆之间和车辆到基础设施的通信。RSU则是安装在道路边缘、交通信号灯和高速公路收费站等地点的设备，用于提供网络连接和支持车辆之间的数据传输。随着通信技术的不断发展，车联万物（V2X, vehicle-to-everything）成为智能汽车和智慧交通的重要支撑技术之一[1]，其具体实现包括车辆间（V2V, vehicle-to-vehicle）、车辆与基础设施之间（V2I, vehicle-to-infrastructure）、车辆与行人之间（V2P, vehicle-to-person）和车辆与外部网络（V2N, vehicle-to-network）之间的通信[2-4]。

车联网的发展为道路交通系统带来了巨大的便利，但同时也引发了一系列安全和隐私问题。在车联网背景下，对安全的主要要求包括消息认证性、不可否认性和可追溯性，对隐私的主要要求包括匿名性和不可链接性。由于消息认证性、不可否认性等安全要求与隐私保护相矛盾，因此如何在保证通信安全的同时保护车辆隐私是目前车联网研究的热点之一[5]。

当前，V2X安全通信大多依赖于公钥基础设施（PKI, public key infrastructure）机制完成通信方身份的互相认证，在这一过程中证书包含的通信方的身份信息不可避免地会被泄露。基于此，匿名认证技术成为新的发展趋势。已被IEEE标准化[6]的安全证书管理系统（SCMS, security credential management system）[7]是基于PKI的目前最突出的证书管理系统之一。SCMS支持所有已知的V2X场景和V2X通信安全所必需的证书类型，其中，假名证书被用作车辆假名合法性的凭证。通过使用假名及其假名证书，车辆能够在V2X通信过程中实现匿名认证。

尽管车辆假名系统在保护车辆身份隐私方面发挥着关键作用，但由于假名与特定活动的关联，攻击者仍然可能通过分析与这些假名相关联的行为来推测车辆的运行轨迹。为了保护车辆的运行轨迹隐私，车辆假名和相应的假名证书需要被频繁更新。这一要求不仅增加了传统单一证书授权中心的工作负担，而且对那些对时延敏感的车联网服务构成了挑战。为了提升假名证书的分发效率，部分研究提出将认证假名即生成假名证书的功能委托给区域授权中心[8]或分布范围更广的RSU[9]。在这种情况下，如何安全地授予代理方假名认证功能并且使其高效地认证假名成为新的挑战。值得注意的是，这种方式仍然是单个可信权威中心（TAC, trusted authority center）的委托，而非多机构协作授予的模型。

本文考虑如下场景，车辆用户在首次连入车联网之前需经过车辆制造商、车管所、电信运营商等多个机构的实名认证，之后才能以合法身份与其他实体建立通信并享受车联网应用服务。为了保护通信安全和车辆隐私，车辆用户与通信方建立连接时利用假名和假名证书认证身份。考虑到连续的假名跟踪可能暴露车辆的运行轨迹，因此车辆必须频繁更新其假名和假名证书。

基于上述场景，本文构造了一个适用于车联网架构的高效假名证书分发方案，基于此方案车辆能够实现假名与假名证书的快速更新，进而提高匿名认证效率。具体而言，本文的主要贡献包括以下3个方面。

1) 本文构造了一个可净化多重签名（SMS, sanitizable multi-signature）方案作为理论构造块。与多重签名方案相比，SMS引入了一种独特的净化功能，允许授权的净化者在不需要与签名者群体交互的前提下对签名数据进行更新，并确保原始签名对新数据的有效性不受影响。这一设计逻辑能够实现车辆在频繁更换假名的场景中假名证书服务的快速响应。然而，这一净化功能也带来了潜在的安全隐患，如净化者可能滥用其权限，这成为本文工作面临的一项重要难点。为此，在SMS中引入了问责机制，通过验证多重签名的来源，能够有效追踪任何恶意净化行为，进一步增强假名证书服务的安全性和可靠性。

2) 基于上述构造的SMS方案，本文设计了一个假名证书分发方案。在该方案中，RSU充当净化者，代替本地认证中心负责为有假名需求的车辆颁发假名证书。与车辆直接向本地认证中心请求假名证书相比，本文提出的假名证书分发方案能够减轻本地认证中心的计算负担，并且能够减少假名证书的颁发时延。

3) 本文给出了SMS方案的安全性定义，并对其安全性进行了证明。此外，本文对假名证书分发方案的安全性和效率进行了分析。安全性分析表明，本文方案在实现匿名认证的同时具备不可否认性、可追溯性、通信内容的机密性和认证性，并且能够抵抗恶意车辆的冒充攻击。效率分析表明，与已有的单可信权威中心授予车辆假名证书相比，在不牺牲安全性和隐私性的前提下采用本文方案时，RSU和车辆负载的计算开销并没有显著增加。

1　相关工作

1.1　假名证书技术进展

近年来，研究者对车联网的匿名认证问题提出了多种解决方案，其中一种常见的解决方案是使用不包含车辆真实身份信息的假名证书。假名证书的生成方式包括基于PKI机制、基于身份基密码机制、基于群签名或环签名机制等。

主流的假名证书方案大多基于PKI机制[10-12]。在这种机制中，车辆的假名证书由可信权威中心颁发。为了避免关联攻击，每个假名证书只能被有限次地使用，这导致TAC需不定期地为车辆准备新的假名证书，给TAC和车辆带来了较大的存储负担。由于整个假名证书系统依赖于TAC的正常运作，当TAC遭受攻击时，容易使系统形成单点故障，整个系统的稳健性和可用性将受到直接威胁。此外，为了防止车辆在认证过程中接收到已被撤销的假名证书，车辆需要预先检查证书撤销列表（CRL, certificate revocation list），这又涉及CRL的更新问题，进一步增加了车辆的计算开销和通信时延。

为了克服基于PKI机制的假名证书方案中的证书管理问题，基于身份基密码机制的方案[13]被提出。在这种机制中，系统主密钥被存储在车辆的防篡改设备（TPD, tamper proof device）中，车辆利用系统主密钥可以自行生成任意数量的假名证书，从而避免了复杂的证书管理问题和单点故障问题。然而，该方案的安全性过度依赖TPD，一旦攻击者利用侧信道攻击从TPD中获得大量信息，系统中所有车辆的通信安全和隐私安全都将难以保障[14]。

文献[15-21]对上述方案进行了改进并提出了条件匿名认证方案。在这些方案中，RSU和车辆能够自行生成假名证书，而不需要TAC颁发或事先将系统主密钥存储在TPD中。但是，这些方案并不能完全抵御外部攻击，即攻击者能够通过窃听、注入新的操控数据或者重放之前发送的数据扰乱实体之间的通信。此外，上述方案还存在一个问题，即当车辆申请假名证书时需要提供真实的身份信息，这可能会导致用户被定位和跟踪，尤其是在车辆频繁申请假名证书的情况下。

采用群签名技术生成假名证书避免了车辆向TAC或RSU认证其身份的过程，进一步增强了使用假名证书的隐私性。在群签名技术中，一群车辆拥有群公钥，而群组中的每个车辆则拥有各自的私钥，假名证书可由其他车辆使用群公钥进行验证[22]。在Yue等[23]的研究中，车辆借助零知识协议向追踪管理器认证其是否可以加入群组，而群签名被看作车辆假名证书，用于认证通信消息的来源。此外，文献[24]使用环签名对交换信息进行匿名认证。尽管上述方案能增强通信方匿名认证的隐私性，但计算成本较高，并且对于移动车辆这类动态网络来说建立和维护群组相对比较困难。

为了提高假名证书分发的效率，部分方案提出使用层次式证书分发机制[9,24-27]，文献[24-25]的主要思路是由RSU为车辆提供临时假名证书，以避免复杂的证书撤销问题。不过，这些方案需要耗时的双线性对运算，并且要求车辆必须预先从TAC处获得一个固定假名、票据或令牌用于向RSU认证其身份。当车辆多次向同一个RSU发起身份认证时，RSU能够将固定假名、票据或令牌与车辆的临时假名进行关联，因此这类方案仍然无法抵御关联攻击。文献[9]提出了使用假名服务器和RSU减少RSU分配假名的开销。文献[27]提出了车辆可以匿名地向区域授权中心请求假名证书，其中区域授权中心是可信授权中心的下属分支。然而，RSU和区域授权中心的位置固定且只能被动地接受假名请求，当车辆不在RSU和区域授权中心的覆盖范围内时，假名证书的分发可能是低效的。之后，文献[28]提出了一种基于RSU和车辆的假名分发机制。然而，该系统仅给出了下载假名证书的步骤，并没有提出任何的数学模型。

不同假名证书生成方案的对比结果如表1所示。从表1中可以看出，亟须设计一个能够避免单点故障、密钥托管、抵抗外部攻击和关联攻击且能够实现简单动态管理的假名证书服务方案。

表1 不同假名证书生成方案的对比结果

类型	特点	不足
基于PKI机制[10-12]	证书由TAC生成	单点故障；证书管理复杂
基于身份基密码机制[13]	系统主密钥预先存于TPD中；证书可由车辆自主生成	存在密钥托管问题
条件匿名认证[15-21]	证书可由RSU生成或由车辆自主生成	不能抵抗外部攻击和关联攻击
基于群、环签名机制[22-24]	需要组建车辆群体；证书可由车辆自主生成；证书生成过程不会泄露隐私	签名长度长；动态管理困难

1.2 多重签名技术进展

多重签名（MS, multi-signature）技术[29]的研究近年来得到了广泛关注，尤其是在比特币及其他区块链应用的推动下[30]。多重签名允许一组签名者通过互动协议在同一消息上生成单个签名，每个签名者拥有独立的密钥对。这种机制不仅提高了交易的安全性，还有效减少了对单一信任中心的依赖。

在这一领域，Bellare等[31]提出的基于Schnorr的多重签名方案（简称BN方案）被广泛认可，并在plain公钥模型下被证明是安全的。在该模型中，签名者能够独立生成自己的密钥对，而不需要交互式密钥生成[32]或对私钥知识进行假设[32-33]，这为后续研究奠定了基础。

后续许多研究[34-36]努力将交互轮数减少至两轮，但Drijvers等[37]的研究指出，这些方案在面对任意数量的并发会话时无法在纯离散对数（DL, discrete logarithm）设置下保证安全性，并且容易受到亚指数复杂度攻击。为此，他们提出了改进的mBCJ方案[37]。虽然mBCJ方案成功地将交互轮数降至两轮，但由于其输出不具Schnorr特性，因此无法替代传统的Schnorr签名。尽管MuSig-DN[38]也只需两轮交互，但由于其强烈依赖于零知识协议，因此实现复杂度显著提高，导致其效率低于三轮交互的MuSig方案[29]。

MuSig2[39]作为第一个在并发签名会话下保持安全性的方案，其签名复杂度与传统Schnorr签名相当。此外，DWMS方案[40]作为一种基于多个随机数线性组合的两轮多重签名方案，与MuSig2在基本原理上有许多相似之处，但缺乏MuSig2的一些关键优化。这些优化包括聚合所有签名者的第一轮消息以节省带宽，以及通过设置常数系数来减少聚合过程中的指数运算。

综上所述，MuSig2在安全性和效率上表现出色，为本文的研究提供了强有力的技术支持。

2 基础知识

2.1 多重签名

多重签名方案MS由4种算法组成，分别为初始化（MS.Setup）、密钥生成（MS.KGen）、签名（MS.Sign）和验证（MS.Verify）算法。

1) $\mathrm{MS.Setup}(1^{\lambda}) \to \mathrm{pp}$。初始化算法输入安全参数$1^{\lambda}$，输出公共参数pp。

2) $\mathrm{MS.KGen}(\mathrm{pp}) \to (\mathrm{sk},\mathrm{pk})$。密钥生成算法由每个签名者独立运行，将公共参数pp作为输入，输出各自的签名密钥对(sk,pk)。

3) $\mathrm{MS.Sign} \to \hat{\sigma}$。签名算法是一个交互式协议，由$n$个签名者共同运行。经过几轮交互后，每个签名者$i \in \{1,\cdots,n\}$通过计算得到其对消息$m$的签名$\sigma_i$，并聚合$\sigma_1,\cdots,\sigma_n$，最终输出一个紧凑的签名$\hat{\sigma}$。

4) $\mathrm{MS.Verify}(L,m,\hat{\sigma}) \to \{0,1\}$。验证算法输入公钥集合$L=\{\mathrm{pk}_1,\cdots,\mathrm{pk}_n\}$、消息$m$和签名$\hat{\sigma}$，输出1或0表示$\hat{\sigma}$是一个在$L$下关于消息$m$的有效或无效的多重签名。

完备性要求对所有安全参数λ、所有$n \in \mathbb{Z}$、所有消息$m \in \mathcal{M}$、所有公共参数$\mathrm{pp} \leftarrow \mathrm{MS.Setup}(1^{\lambda})$以及所有签名密钥对$(\mathrm{sk}_i,\mathrm{pk}_i) \leftarrow \mathrm{MS.KGen}(\mathrm{pp})$，其中$i \in \{1,\cdots,n\}$，$\mathrm{MS.Verify}(L,m,\hat{\sigma})=1$的概率为1，其中$\hat{\sigma}$是由所有共同签名者$i \in \{1,\cdots,n\}$协作执行MS.Sign协议产生的多重签名。

安全性要求MS方案满足选择消息攻击下的存在性不可伪造性（EUF-CMA, existential unforgeability under chosen message attack），具体定义如下。

定义1 EUF-CMA安全。设$\mathrm{MS}=(\mathrm{MS.Setup},\mathrm{MS.KGen},\mathrm{MS.Sign},\mathrm{MS.Verify})$为多重签名方案。假设目标诚实签名者用1标识，且$(\mathrm{sk}_1,\mathrm{pk}_1) \leftarrow \mathrm{MS.KGen}(\mathrm{pp})$是目标诚实签名者的签名密钥对。考虑以下敌手$\mathcal{A}$和挑战者$\mathcal{C}$之间的EUF-CMA游戏。

初始化阶段。敌手$\mathcal{A}$被给予签名者1的公钥

pk_1，并且其可以扮演签名者 2,⋯,n 的角色，特别是它可以任意选择公钥 pk_2,⋯,pk_n。

查询阶段。敌手 $\mathcal{A}$ 可以访问签名预言机。它可以自适应地请求在任意公钥集合（其中至少包括一个 pk_1）下对任意消息的签名。

响应阶段。敌手 $\mathcal{A}$ 输出一个消息 m^*、一个公钥集合 L^* 和一个多重签名 $\hat{\sigma}^*$。

定义敌手 $\mathcal{A}$ 在上述游戏中的优势为 $\mathrm{Adv}_{\mathcal{A}}^{\text{EUF-CMA}}(1^\lambda)=\Pr[\mathrm{MS.Verify}(m^*,L^*,\hat{\sigma}^*)=1]$。为了使 EUF-CMA 安全定义更有意义，本文要求 $pk_1 \in L^*$ 且伪造者从未向签名预言机查询过 (m^*,L^*)。

以上概率取自 MS.KGen 算法和上述游戏过程中产生的随机性。如果在任意概率多项式时间（PPT, probabilistic polynomial time）敌手 $\mathcal{A}$ 对于上述游戏的优势可忽略不计，本文称多重签名方案是 EUF-CMA 安全的。

2.2　变色龙哈希

变色龙哈希（CH, chameleon Hash）由 4 个算法组成，分别为 CH.Setup、CH.KGen、CH.Hash 和 CH.Adapt。

1) $\mathrm{CH.Setup}(1^\lambda) \to pp_{CH}$。初始化算法以一个安全参数 1^λ 作为输入，输出公共参数 pp_{CH}，它决定了密钥空间 $\mathcal{K}$、陷门空间 $\mathcal{T}$ 和输入域 $\mathcal{M} \times \mathcal{R}$ 的大小。

2) $\mathrm{CH.KGen}(pp_{CH}) \to (td,hk)$。密钥生成算法以公共参数 pp_{CH} 为输入，输出一个陷门密钥 $td \in \mathcal{T}$ 和哈希公钥 $hk \in \mathcal{K}$。

3) $\mathrm{CH.Hash}(hk,m,r) \to h$。哈希算法以哈希公钥 hk、消息 $m \in \mathcal{M}$ 和随机数 $r \in \mathcal{R}$ 为输入，输出哈希值 h。

4) $\mathrm{CH.Adapt}(td,m,r,m') \to r'$。该算法输入陷门密钥 td、消息-随机数对 (m,r) 和新消息 m'，输出新随机数 r'，使得 CH.Hash(hk,m,r)=CH.Hash(hk,m',r')。

正确性。如果对所有安全参数 $\lambda \in \mathbb{N}$、所有公共参数 $pp_{CH} \leftarrow \mathrm{CH.Setup}(1^\lambda)$、所有哈希密钥对 $(td,hk) \leftarrow \mathrm{CH.KGen}(pp_{CH})$、所有消息 $m,m' \in \mathcal{M}$ 以及所有随机数 $r \in \mathcal{R}$，本文有对任意 $r' \leftarrow \mathrm{CH.Adapt}(td,m,r,m')$，CH.Hash(hk,$m$,$r$)= CH.Hash(hk,$m'$,$r'$)恒成立，则变色龙哈希被认为是正确的。

定义 2　抗碰撞性。在不知道陷门密钥 td 的情况下，任何敌手都不能有效地找到任意一对碰撞 (m,r) 和 (m',r')，使得 CH.Hash(hk,m,r)=CH.Hash(hk,m',r')成立。

3　可净化多重签名

可净化多重签名是一种特殊的多重签名方案，它允许半诚实的净化者对已签名的消息进行重编辑，并使初始签名对修改后的消息同样有效，而不需要再次与初始签名者群体交互。

3.1　可净化多重签名定义

关于消息空间为 $\mathcal{M}$ 的具有公开可问责的可净化多重签名方案 SMS 由以下 7 种算法组成。

1) $\mathrm{SMS.Setup}(1^\lambda) \to pp$。初始化算法输入一个安全参数 λ，并输出公共参数 pp。假设公共参数 pp 是所有其他算法的隐式输入。

2) $\mathrm{SMS.KGen}(pp) \to (sk,pk)$。密钥生成算法以公共参数 pp 为输入，对于任意签名用户，该算法输出签名密钥对 (sk,pk)，其中私钥 sk 被秘密保存，公钥 pk 被公开给系统中的所有用户。

3) SMS.Gen(pp)→(td,hk)。该算法为陷门密钥生成算法，输入公共参数 pp，该算法输出陷门密钥对(td,hk)，其中陷门密钥 td 被秘密保存，哈希公钥 hk 被公开给系统中的所有用户。

4) $\mathrm{SMS.Sign}(sk_i,hk,m,L) \to (hr,\hat{\sigma})$。签名算法是一个由所有签名者协作执行的协议。以签名者 $i \in \{1,\cdots,n\}$ 为例，算法输入签名者 i 的私钥 sk_i、哈希公钥 hk、待签名的消息 m 和公钥集合 $L=\{pk_1,\cdots,pk_n\}$。经过几轮交互后，与 L 对应的每个签名者 i 将生成一个签名 σ_i，并获得其余共同签名者的签名 σ_j $(j \in \{1,\cdots,n\} \setminus \{i\})$。该算法最终输出签名计算过程中使用的随机数 hr 以及与一般签名具有相同大小的多重签名 $\hat{\sigma}$。

5) $\mathrm{SMS.VerifyMS}(L,hk,m,hr,\hat{\sigma}) \to \{0,1\}$。给定共同签名者公钥集合 L、哈希公钥 hk、消息-随机数对 (m,hr) 和候选签名 $\hat{\sigma}$ 作为输入，如果 $\hat{\sigma}$ 是 L 下对 (m,hr) 的有效签名，该算法输出 1，否则输出 0。

6) $\mathrm{SMS.Sanitize}(sk_s,td,m,hr,\hat{\sigma},m') \to (hr',\hat{\sigma}')$。给定净化者的签名密钥 sk_s、陷门密钥 td、消息-签名对 $(m,hr,\hat{\sigma})$ 和一个新消息 m' 作为输入，净化算法输出一个针对新消息 (m',hr') 的有效签名 $\hat{\sigma}'$。

7) $\mathrm{SMS.VerifySS}(L,pk_s,hk,m',hr',\hat{\sigma}') \to \{0,1\}$。给定公钥集合 L、净化者公钥 pk_s、哈希公钥 hk、

消息-随机数对(m',hr')和候选签名$\hat{\sigma}'$作为输入，如果$\hat{\sigma}'$是L和pk_s下对(m,hr)的有效签名，该算法输出1，否则输出0。

正确性。正确性要求对所有安全参数λ、所有$n\in\mathbb{Z}$、所有消息$m\in\mathcal{M}$、所有公共参数$\mathrm{pp}\leftarrow\mathrm{SMS.Setup}(1^{\lambda})$、所有签名密钥对$(\mathrm{sk}_i,\mathrm{pk}_i)\leftarrow\mathrm{SMS.KGen}(\mathrm{pp})$以及所有陷门密钥对$(\mathrm{td},\mathrm{hk})\leftarrow\mathrm{SMS.Gen}(\mathrm{pp})$，$\mathrm{SMS.VerifyMS}(L,\mathrm{hk},m,\mathrm{hr},\hat{\sigma})=1$的概率为1，其中$L$为签名者的公钥集合列表，$(\mathrm{hr},\hat{\sigma})\leftarrow\mathrm{SMS.Sign}(\mathrm{sk}_i,\mathrm{hk},m,L)$由$L$中的所有共同签名者协作执行。本文还要求对所有$m'\in\mathcal{M}$、所有$(\mathrm{sk}_s,\mathrm{pk}_s)\leftarrow\mathrm{SMS.KGen}(\mathrm{pp})$以及所有$(\mathrm{hr}',\hat{\sigma}')\leftarrow\mathrm{SMS.Sanitize}(\mathrm{sk}_s,\mathrm{td},\mathrm{hk},m,\mathrm{hr},\hat{\sigma},m')$，有$\mathrm{SMS.VerifySS}(L,\mathrm{pk}_s,\mathrm{hk},m',\mathrm{hr}',\hat{\sigma}')=1$恒成立。

3.2 可净化多重签名安全模型

通过构造敌手$\mathcal{A}$和挑战者$\mathcal{C}$之间的安全实验$\mathrm{Exp}_{\mathcal{A},\mathrm{SMS}}^{\mathrm{EUF\text{-}CMA}}(\lambda)$和$\mathrm{Exp}_{\mathcal{A},\mathrm{SMS}}^{\mathrm{ACT}}(\lambda)$，本文分别给出了SMS所需的安全定义，包括不可伪造性和可问责性。安全实验中使用的预言机定义如算法1和算法2所示。

算法1 签名预言机算法$\mathcal{O}_{\mathrm{Sign}}(\mathrm{sk}_1,\cdot,\cdot,\cdot)$

输入 哈希公钥hk，消息m，公钥集合列表L

输出 多重签名$\hat{\sigma}$

1) if $\mathrm{pk}_1\notin L$

2) return $\perp$

3) $(\mathrm{hr},\hat{\sigma})\leftarrow\mathrm{SMS.Sign}(\mathrm{sk}_1,\mathrm{hk},m,L)$

4) $Q_1=Q_1\cup\{(m,\mathrm{hr},L)\}$

5) return $\mathrm{hr},\hat{\sigma}$

6) end if

算法2 净化预言机算法$\mathcal{O}_{\mathrm{Sanitize}}(\mathrm{sk}_s,\mathrm{td},\cdot,\cdot,\cdot,\cdot,\cdot,\cdot)$

输入 哈希公钥hk，消息m，随机数hr，多重签名$\hat{\sigma}$，新消息m'，公钥集合列表L

输出 新随机数hr′，新多重签名$\hat{\sigma}'$

1) if $\mathrm{SMS.VerifyMS}(L,\mathrm{hk},m,\mathrm{hr},\hat{\sigma})=0$

2) return $\perp$

3) $(\mathrm{hr}',\hat{\sigma}')\leftarrow\mathrm{SMS.Sanitize}(\mathrm{sk}_s,\mathrm{td},m,\mathrm{hr},\hat{\sigma},m')$

4) $Q_2=Q_2\cup\{(m',\mathrm{hr}')\}$

5) return $(\mathrm{hr}',\hat{\sigma}')$

6) end if

不可伪造性。不可伪造性要求敌手既不能伪造涉及至少一个诚实签名者的多重签名，也不能扮演净化者的角色伪造一个关于净化消息的有效签名。在不丧失一般性的情况下，本文假设存在一个用1标识的诚实签名者，并且敌手可以腐化所有其他共同签名者。被腐化的签名方的公钥可以由敌手任意选择，甚至可以是诚实签名者公钥的函数。这样，通过访问诚实签名者1的签名预言机，敌手能间接计算多重签名。

敌手$\mathcal{A}$和挑战者$\mathcal{C}$之间的不可伪造安全实验$\mathrm{Exp}_{\mathcal{A},\mathrm{SMS}}^{\mathrm{EUF\text{-}CMA}}(\lambda)$定义如图1所示。挑战者分别生成诚实签名者和净化者的密钥对$(\mathrm{sk}_1,\mathrm{pk}_1)$和$(\mathrm{sk}_s,\mathrm{pk}_s)$，其中$\mathrm{pk}_1$和$\mathrm{pk}_s$被给予敌手。安全实验允许敌手$\mathcal{A}$访问预言机$\mathcal{O}_{\mathrm{Sign}}$和$\mathcal{O}_{\mathrm{Sanitize}}$，其中$\mathcal{O}_{\mathrm{Sign}}$模拟诚实签名者的签名过程，$\mathcal{O}_{\mathrm{Sanitize}}$模拟净化者的净化过程。最终，敌手返回消息—随机数对(m^*,hr^*)、公钥集合L^*和签名σ^*。敌手的目标是输出一个多重签名或净化过的签名。敌手获胜的条件是以下2个事件之一成立。

1) $\mathrm{pk}_1\in L^*$，$(m^*,\mathrm{hr}^*,L^*)\notin Q_1$且伪造是有效的（即$\mathrm{SMS.VerifyMS}(L^*,\mathrm{hk},m^*,\mathrm{hr}^*,\sigma^*)=1$）。

2)$(m^*,\mathrm{hr}^*)\notin Q_2$且伪造是有效的（即$\mathrm{SMS.VerifySS}(L^*,\mathrm{pk}_s,\mathrm{hk},m^*,\mathrm{hr}^*,\sigma^*)=1$）。

$$\begin{aligned}&\text{Experiment } \mathrm{Exp}_{\mathcal{A},\mathrm{SMS}}^{\mathrm{EUF\text{-}CMA}}(\lambda)\\&\quad \mathrm{pp}\leftarrow\mathrm{Setup}(\lambda)\\&\quad \{(\mathrm{sk}_1,\mathrm{pk}_1),(\mathrm{sk}_s,\mathrm{pk}_s)\}\leftarrow\mathrm{KGen}(\mathrm{pp})\\&\quad (\mathrm{td},\mathrm{hk})\leftarrow\mathrm{Gen}(\mathrm{pp})\\&\quad Q_1,Q_2=\varnothing\\&\quad (m^*,\mathrm{hr}^*,L^*,\sigma^*)\leftarrow\mathcal{A}^{\mathrm{Sign,Sanitize}}(\mathrm{pk}_1,\mathrm{pk}_s,\mathrm{hk})\\&\quad \text{return } (\mathrm{pk}_1\in L^*\wedge(m^*,\mathrm{hr}^*,L^*)\notin Q_1\wedge\mathrm{VerifyMS}(L^*,\mathrm{hk},m^*,\mathrm{hr}^*,\sigma^*))\\&\qquad\qquad\vee\\&\qquad ((m^*,\mathrm{hr}^*)\notin Q_2\wedge\mathrm{VerifySS}(L^*,\mathrm{pk}_s,\mathrm{hk},m^*,\mathrm{hr}^*,\sigma^*))\end{aligned}$$

图1 $\mathrm{Exp}_{\mathcal{A},\mathrm{SMS}}^{\mathrm{EUF\text{-}CMA}}(\lambda)$安全实验

定义3 如果对任意PPT敌手$\mathcal{A}$，优势$\mathrm{Adv}_{\mathcal{A},\mathrm{SMS}}^{\mathrm{EUF\text{-}CMA}}(\lambda)=\Pr[\mathrm{Exp}_{\mathcal{A},\mathrm{SMS}}^{\mathrm{EUF\text{-}CMA}}(\lambda)=1]=\mathrm{negl}(\lambda)$，则可净化多重签名方案是EUF-CMA安全的。

可问责性。在本文方案中，可问责性是通过验证签名的来源来实现的。可问责性定义的核心是确保任何一方都无法伪造另一方的合法签名，从而追溯签名的真实来源，确保签名的真实性和责任归属。特别地，可问责性暗含了如果共同签名者（或净化者）没有对某个消息进行签名（净化），那么恶意净化者（或恶意共同签名者）不能指控共同签名者（或净化者）。正如不可伪造性的定义，本文

假设存在一个诚实签名者标识为1，并且敌手可以腐化所有其他共同签名者。通过访问诚实签名者1的签名预言机$\mathcal{O}_{\text{Sign}}$，敌手能间接计算多重签名。

敌手和挑战者$\mathcal{C}$之间的可问责安全实验$\text{Exp}^{\text{ACT}}_{\mathcal{A},\text{SMS}}(\lambda)$定义如图2所示，其中敌手拥有私钥$\text{sk}_s$（或$\text{sk}_1$）并且可以访问$\mathcal{O}_{\text{Sign}}$或$\mathcal{O}_{\text{Sanitize}}$。敌手的目标是输出一个消息-多重签名对（或一个净化消息-签名对）$(m^*,\text{hr}^*,L^*,\sigma^*)$。如果$\text{pk}_1 \in L^*$，$(m^*,\text{hr}^*,L^*) \notin Q_1$并且$\text{VerifyMS}(L^*,m^*,\text{hr}^*,\sigma^*)=1$（或者$(m^*,\text{hr}^*) \notin Q_2$且$\text{VerifySS}(L^*,\text{pk}_s,m^*,\text{hr}^*,\sigma^*)=1$），敌手将赢得游戏。

Experiment $\text{Exp}^{\text{ACT}}_{\mathcal{A},\text{SMS}}(\lambda)$
  $\text{pp} \leftarrow \text{Setup}(\lambda)$
  $\{(\text{sk}_1,\text{pk}_1),(\text{sk}_s,\text{pk}_s)\} \leftarrow \text{KGen}(\text{pp})$
  $(\text{td},\text{hk}) \leftarrow \text{Gen}(\text{pp})$
  $Q_1,Q_2=\varnothing$
  $\mathcal{A}$选择一个随机比特$b \in \{0,1\}$
  if $b==0$,
    $(m^*,\text{hr}^*,L^*,\sigma^*) \leftarrow \mathcal{A}^{\text{Sign}}(\text{pk}_1,\text{hk},\text{pk}_s,\text{sk}_s,\text{td})$
  return $(\text{pk}_1 \in L^* \wedge (m^*,\text{hr}^*,L^*) \notin Q_1 \wedge \text{VerifyMS}(L^*,\text{hk},m^*,\text{hr}^*,\sigma^*)$
  else if $b==1$,
    $(m^*,\text{hr}^*,L^*,\sigma^*) \leftarrow \mathcal{A}^{\text{Sanitize}}(\text{pk}_1,\text{hk},\text{pk}_s,\text{sk}_1)$
  return $(m^*,\text{hr}^*) \notin Q_2 \wedge \text{VerifySS}(L^*,\text{pk}_s,\text{hk},m^*,\text{hr}^*,\sigma^*)$

图2　$\text{Exp}^{\text{ACT}}_{\mathcal{A},\text{SMS}}(\lambda)$安全实验

定义4　如果对任意PPT敌手$\mathcal{A}$，优势$\text{Adv}^{\text{ACT}}_{\mathcal{A},\text{SMS}}(\lambda)=\Pr[\text{Exp}^{\text{ACT}}_{\mathcal{A},\text{SMS}}(\lambda)=1]=\text{negl}(\lambda)$，则可净化多重签名方案是可问责的。

3.3　可净化多重签名方案

本节给出基于多重签名方案Musig2[39]和变色龙哈希算法[41]构造的可净化多重签名方案。假设系统中存在n个共同签名者和一个净化者，并且在共同签名者中存在一个聚合者负责验证并聚合其他签名者的输出。值得注意的是，任意EUF-CMA安全的多重签名和抗碰撞的变色龙哈希可以构造一般的可净化多重签名。本文给出如下基于Musig2和CH的实例化是出于对性能的考虑。

1) $\text{SMS.Setup}(1^\lambda) \rightarrow \text{pp}$。输入安全参数$\lambda$，选择一个阶为素数$q$的群$\mathbb{G}$，其生成元用$g$表示。选择哈希函数$H_1:\{0,1\}^* \rightarrow \mathbb{Z}_q^*$和$H_3:\{0,1\}^* \rightarrow \mathbb{G}$，算法最终输出公共参数$\text{pp}=\{\mathbb{G},q,g,H_1,H_3\}$。

2) $\text{SMS.KGen}(\text{pp}) \rightarrow (\text{sk},\text{pk})$。输入公共参数，每个签名者$i \in \{1,\cdots,n\}$设置签名密钥为$\text{sk}_i=x_i$，其中$x_i \leftarrow Z_q^*$，计算$X_i=g^{x_i}$并公开公钥$\text{pk}_i=X_i$。同理，净化者获得签名密钥对$(\text{sk}_s,\text{pk}_s)=(x_s,X_s)$，公开公钥$\text{pk}_s$并秘密保存$\text{sk}_s$。

在Musig2[39]中，存在一个KeyAgg算法用于计算聚合公钥，其输入公钥集合$L=\{\text{pk}_1,\cdots,\text{pk}_n\}=\{X_1,\cdots,X_n\}$，对于$i \in \{1,\cdots,n\}$，计算$a_i=H_1(L,X_i)$，输出$X=\prod_{i=1}^{n} X_i^{a_i}$。聚合公钥的使用能进一步提高该方案的验证效率。

3) $\text{SMS.Gen}(\text{pp}) \rightarrow (\text{td},\text{hk})$。输入公共参数pp，选择$x_t \leftarrow Z_q^*$并设置陷门密钥为$\text{td}=x_t$，计算哈希公钥$\text{hk}=g^{x_t}$，公开hk并秘密保存td。值得注意的是，由哪一方生成陷门密钥对(td,hk)可以根据实际应用的需求来决定。

4) $\text{SMS.Sign}(\text{sk}_i,\text{hk},m,L) \rightarrow (\text{hr},\hat{\sigma})$。签名算法是一个由公钥集合$L$内的所有签名者协作执行的交互式协议。代替广播的方式，假设共同签名者中存在一个签名聚合者（SA, signature aggregator），其负责验证并聚合所有其他签名者的输出，以此减少签名者的计算开销和通信时延。具体来说，每个签名者$i \in \{1,\cdots,n\}$选择随机数$r_{i,1},r_{i,2},d_{i,1},d_{i,2} \xleftarrow{\$} \mathbb{Z}_q^*$，计算承诺值$R_{i,1}=g^{r_{i,1}}$、$R_{i,2}=g^{r_{i,2}}$、$D_{i,1}=g^{d_{i,1}}$和$D_{i,2}=g^{d_{i,2}}$并发送$(R_{i,1},R_{i,2},D_{i,1},D_{i,2})$给聚合者。聚合者一旦收到所有签名者的承诺值，SA将计算$R_1=\prod_{i=1}^{n} R_{i,1}$、$R_2=\prod_{i=1}^{n} R_{i,2}$、$D_1=\prod_{i=1}^{n} D_{i,1}$和$D_2=\prod_{i=1}^{n} D_{i,2}$并广播$(R_1,R_2,D_1,D_2)$。

当收到待签名的消息m后，SA选择$\alpha \xleftarrow{\$} \mathbb{Z}_q^*$，计算随机数元组$\text{hr}=(g^\alpha,\text{hk}^\alpha)$并广播$(m,\text{hr})$给系统中的其他签名者。

一旦收到承诺值(R_1,R_2,D_1,D_2)，每个签名者i将计算$b_1=H_1(X,R_1,R_2,m)$和$b_2=H_1(X,D_1,D_2,\text{hr})$，其中聚合公钥$X$可以由KeyAgg算法计算得到。之后，计算$h=g^\alpha H_3(\text{hk})^{H_1(m)}$、$R=\prod_{j=1}^{2} R_j^{b_1^{j-1}}=R_1R_2^{b_1}$、$D=\prod_{j=1}^{2} D_j^{b_2^{j-1}}=D_1D_2^{b_2}$、$c_1=H_1(X,R,h)$、$c_2=H_1(X,D,\text{hr}||m)$、$s_i=(r_{i,1}+r_{i,2}b_1+c_1a_ix_i) \bmod q$和$p_i=(d_{i,1}+d_{i,2}b_2+c_2a_ix_i) \bmod q$，其中$a_i=H_1(L,X_i)$，最后发送签名份额$\sigma_i=(s_i,p_i)$给聚合者。

当收到所有签名者$i \in \{1,\cdots,n\}$的签名份额σ_i后，SA首先验证每个签名份额的有效性，解析签

名 σ_i 为 (s_i,p_i)，计算 $\hat{s}=\sum_{i=1}^{n}s_i$ 和 $\hat{p}=\sum_{i=1}^{n}p_i$ 并输出元组 hr 和签名 $\hat{\sigma}=(\hat{\sigma}_1,\hat{\sigma}_2)=((R,\hat{s}),(D,\hat{p}))$。

5) SMS.VerifyMS$(X,\mathrm{hk},m,\mathrm{hr},\hat{\sigma})\rightarrow\{0,1\}$。输入聚合公钥 X、哈希公钥 hk、消息−随机数对 (m,hr) 以及签名 $\hat{\sigma}=(\hat{\sigma}_1,\hat{\sigma}_2)$ 后，验证者分解 hr 为 $(g^{\alpha},\mathrm{hk}^{\alpha})$，分解 $(\hat{\sigma}_1,\hat{\sigma}_2)$ 为 $((R,\hat{s}),(D,\hat{p}))$，计算 $h=g^{\alpha}H_3(\mathrm{hk})^{H_1(m)}$、$c_1=H_1(X,R,h)$ 和 $c_2=H_1(X,D,\mathrm{hr}\|m)$。如果 $g^{\hat{s}}=RX^{c_1}$ 且 $g^{\hat{p}}=DX^{c_2}$，验证者接受多重签名并且能够判定该签名产生自共同签名者群体，否则拒绝。

6) SMS.Sanitize$(\mathrm{sk}_s,\mathrm{td},\mathrm{hk},m,\mathrm{hr},\hat{\sigma},m')\rightarrow(\mathrm{hr}',\hat{\sigma}')$。输入净化者的签名密钥 sk_s、陷门密钥对 $(\mathrm{td},\mathrm{hk})$、消息−签名对 $(m,\mathrm{hr},\hat{\sigma})$ 以及新消息 m' 后，净化者分解随机数 hr 为 $(g^{\alpha},\mathrm{hk}^{\alpha})$，计算新随机数 $\mathrm{hr}'=(g^{\alpha'},\mathrm{hk}^{\alpha'})$，其中 $g^{\alpha'}=g^{\alpha}H_3(\mathrm{hk})^{H_1(m)-H_1(m')}$，$\mathrm{hk}^{\alpha'}=(g^{\alpha'})^{x_t}$。之后，净化者选择随机数 $d_s\xleftarrow{\$}\mathbb{Z}_q^*$，计算 $D_s=g^{d_s}$、$c_2=H_1(X_s,D_s,\mathrm{hr}'\|m')$ 和 $\hat{p}=d_s+c_2x_s$，并调整消息 m' 的签名为 $\hat{\sigma}=(\hat{\sigma}_1',\hat{\sigma}_2')=((R,\hat{s}),(D_s,\hat{p}))$，其中 $\hat{\sigma}_1'$ 是关于消息 m 的一个有效的多重签名，由于变色龙哈希的特性使其对消息 m' 同样有效。

7) SMS.VerifySS$(X,\mathrm{pk}_s,\mathrm{hk},m',\mathrm{hr}',\hat{\sigma}')\rightarrow\{0,1\}$。输入聚合公钥 X、净化者公钥 $\mathrm{pk}_s=X_s$、哈希公钥 hk、消息—随机数对 (m',hr') 和签名 $\hat{\sigma}'=(\hat{\sigma}_1',\hat{\sigma}_2')$，验证者解析 hr′ 为 $(g^{\alpha'},\mathrm{hk}^{\alpha'})$，解析 $(\hat{\sigma}_1',\hat{\sigma}_2')$ 为 $((R,\hat{s}),(D_s,\hat{p}))$，计算 $h=g^{\alpha'}H_3(\mathrm{hk})^{H_1(m')}$、$c_1=H_1(X,R,h)$ 和 $c_2=H_1(X_s,D_s,\mathrm{hr}'\|m')$。如果 $g^{\hat{s}}=RX^{c_1}$ 且 $g^{\hat{p}}=D_sX_s^{c_2}$，验证者接受签名并判定该签名为净化过的签名，否则拒绝。

4　系统架构和安全模型

4.1　系统架构设计

在现实场景中，首次入网的车辆必须经过多个机构如车辆制造商、车管所、电信运营商等的认证。这些机构在认证车辆时需要审核用户的真实身份和车辆的公钥，通过审查的车辆将获得相应的公钥证书。然而，当车辆的公钥证书被用于身份认证时，其中包含的用户身份信息将不可避免地被泄露。通过持续记录车辆公钥关联的活动，车辆的运行轨迹也容易被暴露。本文方案旨在解决实体认证过程中存在的身份泄露和轨迹泄露问题，系统架构如图 3 所示，系统中包括可信认证中心（TAC）、本地认证中心（LAC, local authority center）、路侧单元（RSU）和车辆等实体。

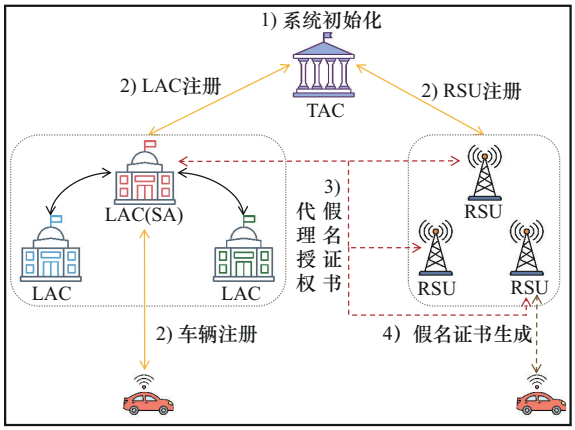

图 3　假名证书分发方案系统架构

TAC 是系统中具有最高信任度的权威机构，负责系统中所有 LAC 实体和 RSU 实体的注册和撤销。实体在首次加入车联网之前必须获得 TAC 对其身份和公钥的认证。LAC 包括一群职能不同的机构，共同负责为本地首次入网的车辆生成公钥证书，并且将生成假名证书的功能代理授权给 RSU。本文从 LAC 群体中选择一个 LAC 作为签名聚合者 SA，其负责接收外界请求，聚合 LAC 的认证结果并代表 LAC 群体对外界请求作出响应。RSU 负责为其管辖范围内有新假名需求的车辆生成假名证书，并对系统内发布虚假信息的车辆进行追踪。车辆内部有车载单元（OBU）模块，每个车辆通过 OBU 可以与其他实体（如人、车辆、基础设施、边缘网络）建立通信，车辆的私钥、假名、假名证书等隐私信息被存放在 OBU 中的防篡改模块中。

4.2　安全威胁

本文系统主要考虑来自内部和外部攻击者的威胁，其中内部攻击者主要指恶意车辆。恶意车辆可能会发送虚假的路况信息以破坏交通秩序或方便自己出行。此外，恶意车辆也会试图冒充诚实车辆的身份请求假名证书，并利用假名身份发布虚假消息，从而陷害诚实车辆。外部攻击者可能会窃听或篡改公开网络中传输的消息，从窃听到的消息中获取车辆的真实身份信息或推测车辆的行驶轨迹。

4.3　安全目标

为了抵御上述威胁，本文设计的假名证书分发方案需要实现以下安全目标。

1) 可追溯性。尽管假名能被用于保护隐私，但恶意攻击者可能滥用假名来发布虚假信息。本文

方案将车辆的假名和真实身份进行关联，关联信息由生成相应假名证书的代理方记录，当收到虚假信息报警后，由代理方追溯发布信息的车辆并告知LAC，接着由LAC更新车辆的恶意行为次数并决定是否撤销车辆的长期公钥证书。

2) 抗假冒攻击。攻击者可能尝试冒充合法车辆的身份申请假名证书并执行恶意活动。本文方案在假名证书请求阶段通过加密请求信息签名并实现对车辆真实身份的隐藏和车辆身份合法性的验证。

3) 通信内容的机密性和认证性。攻击者可能会通过窃听通信过程中的消息，以获取车辆的真实身份信息或推测车辆的行驶轨迹。此外，攻击者可能试图篡改通信过程中的消息，以破坏代理授权或假名证书生成过程。本文方案通过加密和签名实现对通信内容的保护和对消息来源以及通信过程中消息完整性的验证。

5　基于SMS的假名证书分发方案

针对车辆身份需要由多个授权机构认证的场景，本文基于可净化多重签名设计了一个假名证书分发方案，其将可信机构的认证权限委托给分布范围更广泛的RSU，从而进一步提升了假名更新效率。本文方案主要包括以下步骤。

1) 系统初始化。该步骤由TAC执行，其负责生成系统参数。

2) 实体注册。当收到实体的注册请求后，TAC审核实体的身份和公私钥信息，为通过审核的实体生成公钥证书。在本文的系统架构中，LAC和RSU在加入车联网系统之前必须先向TAC注册并获得公钥证书，车辆在加入车联网系统之前必须先向LAC注册并获得公钥证书。

3) 假名证书代理授权。RSU向LAC群体请求假名证书代理权限，LAC群体审查RSU身份后共同为合法RSU生成代理证书。获得代理证书的RSU负责为其管辖范围内有假名认证需求的车辆生成假名证书。

4) 假名证书生成。有新假名需求的车辆向其附近的RSU申请假名证书。当收到车辆的请求后，RSU审核车辆身份信息并为合法车辆生成假名证书。之后。RSU记录车辆身份信息及其假名证书用于对恶意行为的追溯。在以假名身份与其他车辆通信之前，车辆必须获得经LAC认证的假名。

5.1　系统初始化

该算法由TAC执行，输入安全参数λ，TAC调用SMS.Setup(1^{λ})算法和SMS.KGen(pp)算法分别生成系统公共参数$\mathrm{pp_{SMS}}=\{\mathbb{G},q,g,H_1,H_3\}$和公私钥对$(\mathrm{sk_{TAC}},\mathrm{pk_{TAC}})$。之后，选择安全的签名算法Sign(·)和公钥加密算法Enc(·)，最终TAC公开整个系统的公共参数$\mathrm{pp}=\{\mathrm{pp_{SMS}},\mathrm{pk_{TAC}},\mathrm{Sign}(\cdot),\mathrm{Enc}(\cdot)\}$。值得注意的是，以上签名算法和加密算法主要用于确保通信安全，其选择和应用可依据具体场景下的安全需求而定制，这里不特别指定。

5.2　实体注册

1) LAC注册和RSU注册

LAC和RSU等实体在加入车联网系统之前首先向TAC注册，注册过程可看作实体本身长期公钥证书的生成过程。以LAC为例，LAC调用SMS. KGen(pp)算法生成密钥对$(\mathrm{sk_{LAC}},\mathrm{pk_{LAC}})$，计算$S_{\mathrm{LAC}}=\mathrm{Sign}(\mathrm{sk_{LAC}},\mathrm{ID_{LAC}},\mathrm{pk_{LAC}})$，将身份信息$\mathrm{ID_{LAC}}$、公钥$\mathrm{pk_{LAC}}$以及签名$S_{\mathrm{LAC}}$通过安全信道发送给TAC。当收到LAC的注册请求后，TAC审核LAC的身份信息并验证签名的有效性。如果验证通过，则TAC生成LAC的证书$\mathrm{cert_{LAC}}$，并通过安全信道将证书$\mathrm{cert_{LAC}}$返回给LAC。

RSU注册过程与LAC注册类似，注册结束后，RSU将获得TAC授予的公钥证书$\mathrm{cert_{RSU}}$。

2) 车辆注册

本文方案要求车辆在加入车联网系统之前必须向多个LAC注册，这种考虑更贴合实际应用场景。车辆注册过程如图4所示，首先，车辆V生成签名密钥对$(\mathrm{sk}_V,\mathrm{pk}_V)$，并计算$S_V$=Sign$(\mathrm{sk}_V,\mathrm{ID}_V,\mathrm{pk}_V)$，将身份信息$\mathrm{ID}_V$、公钥$\mathrm{pk}_V$以及签名$S_V$通过安全信道发送给SA。SA调用SMS.Gen(pp)算法生成陷门密钥对(td, hk)，将哈希公钥hk、注册信息$m_{\mathrm{reg}}=\mathrm{ID}_V\|\mathrm{pk}_V$和随机数hr广播给其他LAC，并与其他LAC共同执行SMS.Sign$(\cdot,\mathrm{hk},m_{\mathrm{reg}},L)$得到多重签名$\hat{\sigma}$，其中“·”表示不同LAC各自的签名密钥，$L$包含LAC群体的公钥。这里本文限定SA生成陷门密钥是为了进一步提高LAC之间的通信效率。最后，SA通过安全信道将公钥证书$\mathrm{cert}_V=(\mathrm{ID}_V,\mathrm{pk}_V,\mathrm{hk},\mathrm{hr},\hat{\sigma})$发送给车辆$V$，并保存公钥证书$\mathrm{cert}_V$用于记录车辆恶意行为的次数。

完成注册的LAC、RSU和车辆获得相应的公钥证书，可进一步与其他实体建立安全通信。

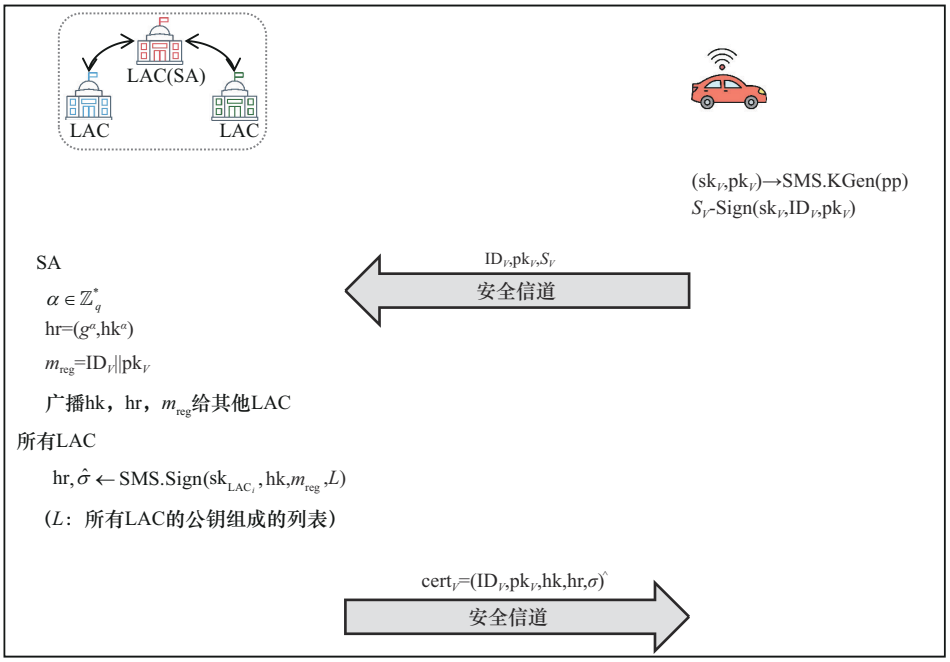

图4　车辆注册过程

5.3　假名证书代理授权

为了增强对车辆身份隐私和路径隐私的保护，采用假名方式与外界通信的车辆通常需要频繁更换假名和假名证书。类似于车辆公钥证书的授予方式，本文假设车辆假名由多个职能不同的LAC（如车辆服务商、车管所、电信运营商）共同认证。为了进一步减少假名证书请求的响应时延，本文将认证假名的功能代理授权给分布范围更广且距离车辆更近的RSU。

如图5所示，假名证书代理授权过程可细分为RSU代理请求和LAC代理授权2个过程。

1) RSU代理请求

RSU_i将其身份信息ID_i、空间位置Loc_i和时间戳ts保存为状态信息$state_i = ID_i||Loc_i||ts$，计算密文$CT_{i\to SA} = Enc(pk_{SA},state_i)$。之后，$RSU_i$计算关于$CT_{i\to SA}$的签名$S_i = Sign(sk_i,CT_{i\to SA})$。最后，$RSU_i$发送$cert_i||CT_{i\to SA}||S_i$给SA。

2) LAC代理授权

收到来自RSU_i的代理请求后，SA首先利用$cert_i$验证RSU_i的身份。之后，SA从$cert_i$中提取pk_i，并利用pk_i、$CT_{i\to SA}$和S_i验证密文的完整性，若验证通过，SA进一步用私钥sk_{SA}对密文$CT_{i\to SA}$进行解密获得$state_i'$。SA从$state_i'$中提取出时间戳ts′，如果当前时间在ts′范围内，则代表SA接受RSU_i的代理请求。

SA选择随机数$x_i,\alpha \in \mathbb{Z}_q^*$，将$x_i$作为分配给$RSU_i$的哈希陷门td，计算哈希公钥$hk = g^{x_i}$和随机数$hr = (g^\alpha,hk^\alpha)$。SA设置$m = state_i'||td$为待签名的消息，与其他LAC共同执行$SMS.Sign(\cdot,hk,m,L)$协议获得多重签名$\hat{\sigma}$，其中“·”表示不同LAC各自的签名密钥，$L$表示LAC群体的公钥集合。最后，SA计算密文$CT_{SA\to i} = Enc(pk_i,m||hr||\hat{\sigma})$，并将$CT_{SA\to i}$发送给$RSU_i$。

收到SA的响应后，RSU_i解密$CT_{SA\to i}$获得$m'||hr'||\hat{\sigma}'$，并从m'中提取哈希陷门td′。RSU_i计算$hk' = g^{td'}$，调用$SMS.VerifyMS(L,hk',m',hr',\hat{\sigma}')$，如果验证通过，$RSU_i$接受哈希陷门td并将其秘密保存在防篡改模块中。

5.4　假名证书生成

为提高假名证书申请效率，本文采用RSU_i周期性发布其代理身份信息，有需求的车辆通过接受代理信息并作出响应的方式来实现，具体生成过程如图6所示。

1) 假名证书申请

RSU_i周期性向其管辖范围内的车辆广播代理信息$M_{Agent} = cert_i||t_{stamp}||Sign(sk_i,t_{stamp})$，其中$t_{stamp}$表示代理信息有效的时间范围。当车辆$V$想要以新假名身份pid与外界通信时，车辆$V$接收代理信息并验证其有效性。如果验证通过，车辆$V$从$cert_i$中

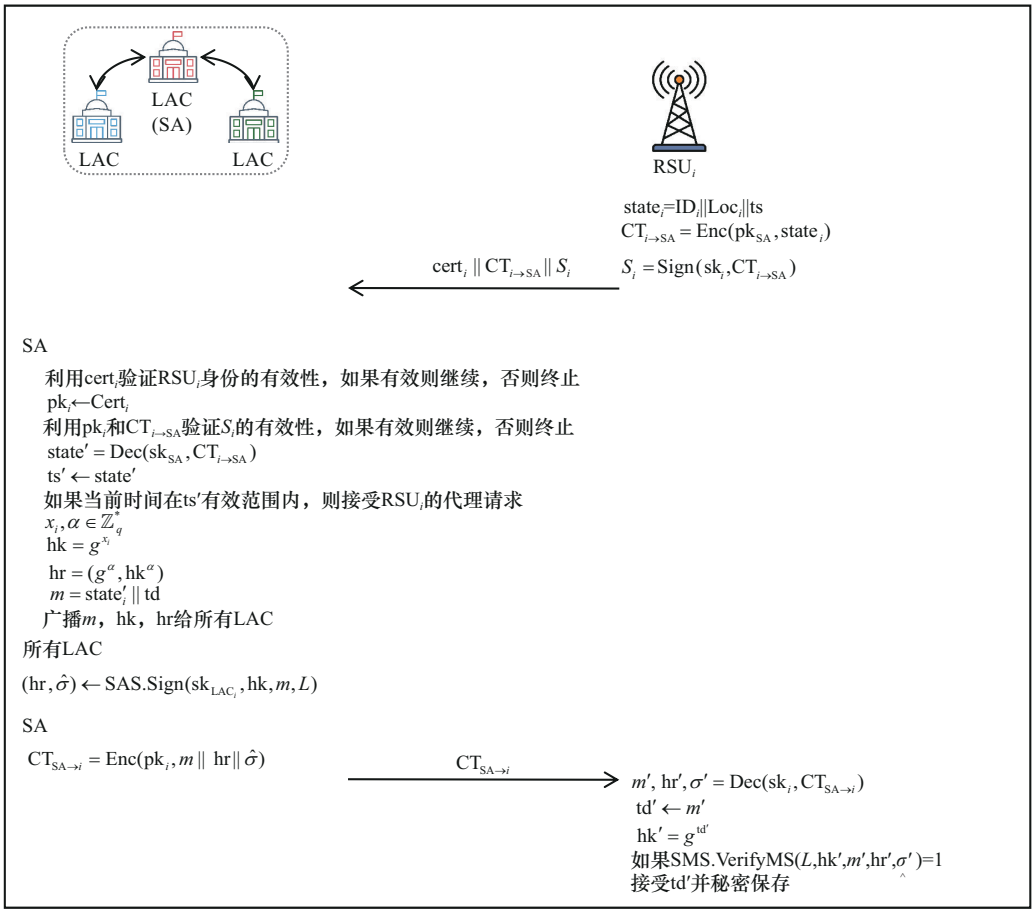

图5　假名证书代理授权过程

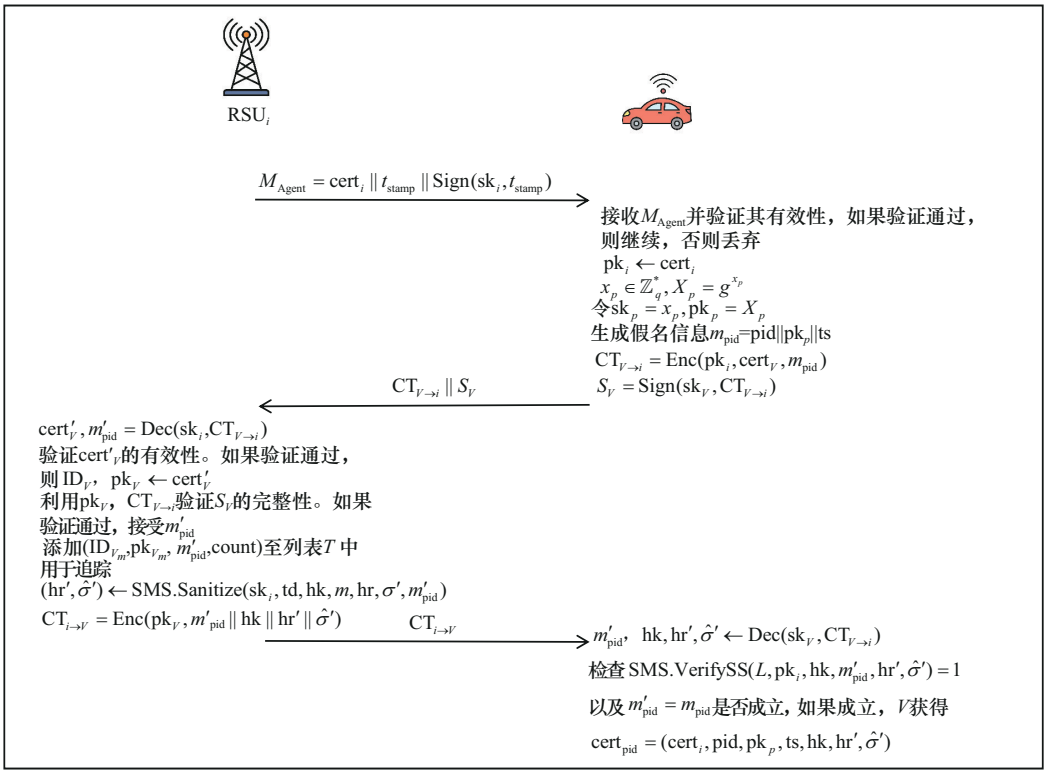

图6　假名证书生成过程

提取RSU_i的公钥pk_i，并为发起假名证书请求作准备。

具体来说，车辆V选择随机数$x_p \in \mathbb{Z}_q^*$作为假名密钥sk_p，计算$X_p = g^{x_p}$作为假名公钥pk_p，设置$m_{\mathrm{pid}} = \mathrm{pid}||\mathrm{pk}_p||\mathrm{ts}$作为请求消息，其中ts表示假名的有效期。之后，车辆V利用RSU_i的公钥pk_i加密cert_V和m_{pid}得到密文$\mathrm{CT}_{V\to i} = \mathrm{Enc}(\mathrm{pk}_i,\mathrm{cert}_V,m_{\mathrm{pid}})$，并利用长期私钥$\mathrm{sk}_V$对$\mathrm{CT}_{V\to i}$签名得到$S_V = \mathrm{Sign}(\mathrm{sk}_V,\mathrm{CT}_{V\to i})$。最终，车辆$V$发送$\mathrm{CT}_{V\to i}||S_V$给$\mathrm{RSU}_i$。

2) 假名证书响应

当收到车辆V的请求后，RSU_i解密密文$\mathrm{CT}_{V\to i}$获得cert'_V和m'_{pid}，之后，RSU_i利用cert'_V验证车辆V的身份。验证通过后，RSU_i从cert'_V中提取ID_V和pk_V，并利用pk_V、$\mathrm{CT}_{V\to i}$和S_V验证密文的完整性。若验证通过，RSU_i添加记录$(\mathrm{ID}_V,\mathrm{pk}_V,m'_{\mathrm{pid}},\mathrm{count})$至列表$T$中用于恶意行为追踪，其中count用于记录车辆$V$恶意行为的次数。

RSU_i将自身签名私钥sk_i、陷门密钥对(td,hk)、消息-签名对$(m,\mathrm{hr},\hat{\sigma})$以及$m'_{\mathrm{pid}}$作为输入，执行$\mathrm{SMS.Sanitize}(\mathrm{sk}_i,\mathrm{td},\mathrm{hk},m,\mathrm{hr},\hat{\sigma},m'_{\mathrm{pid}})$算法得到输出值$(\mathrm{hr}',\hat{\sigma}')$。最终，$\mathrm{RSU}_i$利用$\mathrm{pk}_V$对$m'_{\mathrm{pid}}||\mathrm{hk}||\mathrm{hr}'||\hat{\sigma}'$加密，并将结果密文$\mathrm{CT}_{i\to V}$返回给$V$，其中$\mathrm{CT}_{i\to V} = \mathrm{Enc}(\mathrm{pk}_V,m'_{\mathrm{pid}}||\mathrm{hk}||\mathrm{hr}'||\hat{\sigma}')$。

车辆V解密$\mathrm{CT}_{i\to V}$获得$m'_{\mathrm{pid}}||\mathrm{hk}||\mathrm{hr}'||\hat{\sigma}'$后，检查$\mathrm{SMS.VerifySS}(L,\mathrm{pk}_i,\mathrm{hk},m'_{\mathrm{pid}},\mathrm{hr}',\hat{\sigma}') = 1$以及$m'_{\mathrm{pid}}=m_{\mathrm{pid}}$是否成立。如果上述2个条件成立，$V$获得在ts时间内与假名信息$(\mathrm{pid},\mathrm{pk}_p)$相对应的假名证书$\mathrm{cert}_{\mathrm{pid}} = (\mathrm{cert}_i,\mathrm{pid},\mathrm{pk}_p,\mathrm{ts},\mathrm{hk},\mathrm{hr}',\hat{\sigma}')$。否则，车辆$V$将重新申请假名证书。

5.5 匿名身份认证

当车辆从RSU处获得假名证书后，可以用假名身份与外界建立安全通信。

为了方便说明，本文以单向认证为例展开介绍。假设车辆V_m在行驶过程中想要向周边车辆V_n匿名发送求助信息，双方先通过传输层安全（TLS, transport layer security）协议进行密钥交换。经过第一轮握手之后，V_n获得V_m支持的密码套件和V_m选择的随机数$k_1 \in \mathbb{Z}_q^*$，V_m获得V_n支持的密码套件和V_n选择的随机数$k_2 \in \mathbb{Z}_q^*$。之后，V_m将$\mathrm{cert}_{\mathrm{pid}}$发送给车辆$V_n$。

车辆V_n提取$\mathrm{cert}_{\mathrm{pid}}$中的时间戳ts，检查$\mathrm{cert}_{\mathrm{pid}}$是否在有效期内。如果在有效期内，$V_n$从$\mathrm{cert}_i$中提取RSU公钥$\mathrm{pk}_i$，从$\mathrm{cert}_{\mathrm{pid}}$中提取假名pid、公钥$\mathrm{pk}_p$和时间戳ts作为验证消息$m' = \mathrm{pid}||\mathrm{pk}_p||\mathrm{ts}$并执行$\mathrm{SMS.VerifySS}(L,\mathrm{pk}_i,\mathrm{hk},m',\mathrm{hr}',\hat{\sigma}')$算法。如果验证通过，$V_n$则认为$V_m$具备假名pid和公钥$\mathrm{pk}_p$对应的私钥。

之后，车辆V_n选择随机数$k_3 \in \mathbb{Z}_q^*$并用公钥pk_p对其加密，将加密随机数$\mathrm{prekey} = \mathrm{Enc}(\mathrm{pk}_p,k_3)$发送给$V_m$。收到加密消息后，$V_m$用私钥$\mathrm{sk}_p$解密获得随机数$k_3$。

最后，双方使用随机数(k_1,k_2,k_3)通过Diffie-Hellman密钥协商算法获得会话密钥k_{DH}。

5.6 恶意车辆追溯

当握手阶段结束后，车辆V_m可以利用共享密钥k_{DH}与车辆V_n秘密通话。具体来说，V_m将发送$M_{\mathrm{req}} = \mathrm{CT}_{\mathrm{pid}\to n}||S_{\mathrm{pid}}$，其中$\mathrm{CT}_{\mathrm{pid}\to n} = E(k_{\mathrm{DH}},m_{\mathrm{req}})$，$m_{\mathrm{req}}$为明文消息，$S_{\mathrm{pid}} = \mathrm{Sign}(\mathrm{sk}_{\mathrm{pid}},\mathrm{CT}_{\mathrm{pid}\to n})$。

当收到M_{req}后，车辆V_n利用握手阶段得到的假名公钥$\mathrm{pk}_{\mathrm{pid}}$验证密文的完整性，验证通过后，$V_n$通过解密密文得到明文消息$m_{\mathrm{req}}$。

如果V_n察觉到m_{req}为虚假信息时，V_n将收集证据并请求相关RSU对恶意车辆追溯。

车辆V_n从$\mathrm{cert}_{\mathrm{pid}}$中提取$\mathrm{cert}_i$以获取$\mathrm{RSU}_i$的相关信息。之后，$V_n$与$\mathrm{RSU}_i$建立安全通信，将追溯请求$M_{\mathrm{trace}} = k_{\mathrm{DH}}||\mathrm{cert}_{\mathrm{pid}}||\mathrm{CT}_{\mathrm{pid}\to n}||S_{\mathrm{pid}}$秘密发送给$\mathrm{RSU}_i$。收到请求后，$\mathrm{RSU}_i$检查报告的真实性。如果检查通过，$\mathrm{RSU}_i$根据$\mathrm{cert}_{\mathrm{pid}}$中的$(\mathrm{pid},\mathrm{pk}_p,\mathrm{ts})$检索列表$T$，得到车辆$V_m$的真实信息，并修改$V_m$对应记录中的count=count+1。$\mathrm{RSU}_i$进一步将虚假报告$M_{\mathrm{trace}}$和车辆假名记录$(\mathrm{ID}_{V_m},\mathrm{pk}_{V_m},m'_{\mathrm{pid}},\mathrm{count})$发送给LAC，LAC从数据库中检索$V_m$，并调整对应记录的count=count+1。如果count超过系统设置的阈值，LAC则吊销V_m的长期公钥证书。值得注意的是，在本文的设置中，采用阈值机制而不是对每个单独的指控或异常立即采取行动，这允许系统容忍一定程度的异常或误报，以防因误判而错误地惩罚良好用户。

6 安全性证明

本文首先构造了基于Musig2(v=2)和变色龙哈希的可净化多重签名方案，其中Musig2(v=2)旨在签名处理阶段使用2个nonce的Musig2版本。然后设计了基于可净化多重签名的假名证书分发方案。

在方案执行过程中额外采用加密和签名方式实现通信方身份认证，通信内容的机密性和认证性。本节首先证明了可净化多重签名方案安全性，然后对假名证书分发方案的安全性进行分析。

6.1　SMS 安全性证明

定理 1　如果 Musig2 是 EUF-CMA 安全的并且 CH 是抗碰撞（CR, collision-resistant）安全的，则 SMS 方案是 EUF-CMA 安全的。具体地说，对于任意具有优势 $\mathrm{Adv}_{\mathcal{A}}^{\text{EUF-CMA}}(1^{\lambda})$ 的 PPT 敌手 $\mathcal{A}$，存在 PPT 敌手 $\mathcal{B}_{\mathrm{MS}}$ 和敌手 $\mathcal{B}_{\mathrm{CH}}$，使得 $\mathrm{Adv}_{\mathcal{A},\mathrm{SMS}}^{\text{EUF-CMA}}(1^{\lambda})\leqslant \mathrm{Adv}_{\mathcal{B},\mathrm{MS}}^{\text{EUF-CMA}}(1^{\lambda})+\mathrm{Adv}_{\mathcal{B},\mathrm{CH}}^{\mathrm{CR}}(1^{\lambda})$ 其中，$\mathrm{Adv}_{\mathcal{B},\mathrm{MS}}^{\text{EUF-CMA}}(1^{\lambda})$ 表示敌手 $\mathcal{B}_{\mathrm{MS}}$ 攻破底层 Musig2(v=2)方案的优势，$\mathrm{Adv}_{\mathcal{B},\mathrm{CH}}^{\mathrm{CR}}(1^{\lambda})$ 表示敌手 $\mathcal{B}_{\mathrm{CH}}$ 攻破底层 CH 方案的优势。

证明　考虑敌手 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 之间的 EUF-CMA 安全实验。对于来自敌手 $\mathcal{A}$ 的每一个针对诚实签名者 1 的签名查询 m，设 $(\sigma_h,\sigma_{\mathrm{hr}})$ 是返回的签名，其中 $h=\mathrm{CH}(\mathrm{hk},m,\mathrm{hr})$ 并且 hr 是计算签名时使用的随机数。用 Q_1 表示由请求签名查询时的输入集合 (m,hr,L)。设 $(m^*,\mathrm{hr}^*,\sigma^*=(\sigma_h^*,\sigma_{\mathrm{hr}}^*))$ 是敌手 $\mathcal{A}$ 输出的多重签名且 Win 表示敌手 $\mathcal{A}$ 获胜的事件。如果 $\mathrm{pk}_1\in L^*$，$\mathrm{VerifyMS}(L^*,\mathrm{hk},m^*,\mathrm{hr}^*,\sigma^*)=1$ 且 $(m^*,\mathrm{hr}^*,L^*)\notin Q_1$，则敌手 $\mathcal{A}$ 获胜。本文划分 Win 事件为 2 种情况。

情况 1。存在 $(m,\mathrm{hr},\cdot)\in Q_1$，使得 $\mathrm{CH}(\mathrm{hk},m,\mathrm{hr})=\mathrm{CH}(\mathrm{hk},m^*,\mathrm{hr}^*)$ 且 $(m,\mathrm{hr})\neq(m^*,\mathrm{hr}^*)$。

情况 2。对于任意 $(m,\mathrm{hr},\cdot)\in Q_1$，$\mathrm{CH}(\mathrm{hk},m,\mathrm{hr})\neq\mathrm{CH}(\mathrm{hk},m^*,\mathrm{hr}^*)$。

情况 1 暗含了一个 CH 的碰撞，为了证明它，构造了一个针对 CH 的 PPT 敌手 $\mathcal{B}_{\mathrm{CH}}$。首先，$\mathcal{B}_{\mathrm{CH}}$ 生成 n+1 对签名公私钥 $(\mathrm{pk}_1,\mathrm{sk}_1),\cdots,(\mathrm{pk}_n,\mathrm{sk}_n)$ 和 $(\mathrm{pk}_s,\mathrm{sk}_s)$，基于此，敌手 $\mathcal{B}_{\mathrm{CH}}$ 可以完美地模拟签名者 $1,\cdots,n$ 的签名过程以及净化者的签名过程。之后，敌手 $\mathcal{B}_{\mathrm{CH}}$ 均匀随机地选择哈希密钥 hk，并传递 $\mathrm{pk}_1,\cdots,\mathrm{pk}_n$, pk_s 和 hk 给敌手 $\mathcal{A}$。为了回答敌手 $\mathcal{A}$ 的净化查询，$\mathcal{B}_{\mathrm{CH}}$ 需进一步向其挑战者求助碰撞发现预言机。因为 $\mathcal{B}_{\mathrm{CH}}$ 拥有净化者的签名密钥 sk_s，它能够对挑战者返回的碰撞进行签名。综上所述，$\mathcal{B}_{\mathrm{CH}}$ 能够完成来自敌手 $\mathcal{A}$ 的签名问询和净化问询。

当敌手 $\mathcal{A}$ 输出多重签名 $(m^*,\mathrm{hr}^*,\sigma^*)$ 后，$\mathcal{B}_{\mathrm{CH}}$ 计算 $h^*=\mathrm{CH}(\mathrm{hk},m^*,\mathrm{hr}^*)$ 并检索 Q_1。因为是情况 1，所以至少有一个记录 $(m,\mathrm{hr},\cdot)\in Q_1$ 满足 $\mathrm{CH}(\mathrm{hk},m,\mathrm{hr})=\mathrm{CH}(\mathrm{hk},m^*,\mathrm{hr}^*)$ 且 $(m,\mathrm{hr})\neq(m^*,\mathrm{hr}^*)$。最终，$\mathcal{B}_{\mathrm{CH}}$ 输出 $((m,\mathrm{hr}),(m^*,\mathrm{hr}^*))$ 作为其找到的 CH 碰撞。因此，无论何时敌手 $\mathcal{A}$ 成功并且敌手 $\mathcal{A}$ 执行的是情况 1，$\mathcal{B}_{\mathrm{CH}}$ 也会成功。

情况 2 暗含了敌手 $\mathcal{A}$ 伪造了一个针对 $h^*=\mathrm{CH}(\mathrm{hk},m^*,\mathrm{hr}^*)$ 的有效的签名 σ_h^* 且对任意 $(m,\mathrm{hr},\cdot)\in Q_1$，$\mathrm{CH}(\mathrm{hk},m,\mathrm{hr})\neq h^*$。因此能够构造一个针对 Musig2($v$=2)的 EUF-CMA 安全的 PPT 敌手 $\mathcal{B}_{\mathrm{MS}}$。假设目标诚实签名者用 1 标识。首先，敌手 $\mathcal{B}_{\mathrm{MS}}$ 生成一对 CH 的公私钥 $(\mathrm{hk},\mathrm{td})$ 和净化者的签名密钥对 $(\mathrm{pk}_s,\mathrm{sk}_s)$，用于模拟预言机 $\mathcal{O}_{\mathrm{Sanitize}}$ 并响应敌手 $\mathcal{A}$ 的净化查询。其次，$\mathcal{B}_{\mathrm{MS}}$ 生成签名者 $2,\cdots,n$ 的公私钥 $(\mathrm{pk}_2,\mathrm{sk}_2),\cdots,(\mathrm{pk}_n,\mathrm{sk}_n)$，以模拟签名者 $2,\cdots,n$ 的独立签名过程。然后，$\mathcal{B}_{\mathrm{MS}}$ 均匀随机地选择一个群元素记为 pk_1 作为签名者 1 的公钥，将公钥 $\mathrm{pk}_1,\cdots,\mathrm{pk}_n,\mathrm{pk}_s$ 发送给敌手 $\mathcal{A}$。为了完成敌手 $\mathcal{A}$ 对预言机 $\mathcal{O}_{\mathrm{Sign}}$ 的问询，$\mathcal{B}_{\mathrm{MS}}$ 进而向其挑战者请求敌手 $\mathcal{A}$ 的签名问询，并把签名结果转发给敌手 $\mathcal{A}$。

当敌手 $\mathcal{A}$ 最终输出针对 (m^*,hr^*) 的签名 $\sigma^*=(\sigma_h^*,\sigma_{\mathrm{hr}}^*)$ 后，$\mathcal{B}_{\mathrm{MS}}$ 计算 $h^*=\mathrm{CH}(\mathrm{hk},m^*,\mathrm{hr}^*)$，并输出 (h^*,σ_h^*) 或 $(\mathrm{hr}^*\|m^*,\sigma_{\mathrm{hr}}^*)$ 作为其伪造。无论什么时候敌手 $\mathcal{A}$ 成功且执行的是情况 2，整个游戏都能成功地终止。

综上所述，假设 $\mathrm{Adv}_{\mathcal{B},\mathrm{CH}}^{\mathrm{CR}}(1^{\lambda})$ 表示敌手 $\mathcal{B}_{\mathrm{CH}}$ 找到哈希碰撞的优势，$\mathrm{Adv}_{\mathcal{B},\mathrm{MS}}^{\text{EUF-CMA}}(1^{\lambda})$ 表示敌手 $\mathcal{B}_{\mathrm{MS}}$ 伪造有效多重签名的优势，则敌手 $\mathcal{A}$ 攻破 SMS 方案的优势 $\mathrm{Adv}_{\mathcal{A}}^{\text{EUF-CMA}}(1^{\lambda})\leqslant\mathrm{Adv}_{\mathcal{B},\mathrm{MS}}^{\text{EUF-CMA}}(1^{\lambda})+\mathrm{Adv}_{\mathcal{B},\mathrm{CH}}^{\mathrm{CR}}(1^{\lambda})$。证毕。

定理 2　如果 Musig2(v=2)是 EUF-CMA 安全的，并且变色龙哈希方案 CH 是 CR 安全的，则 SMS 方案实现了可问责性。

证明　考虑敌手 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 之间的游戏 $\mathrm{Exp}_{\mathcal{A},\mathrm{SMS}}^{\mathrm{ACT}}(1^{\lambda})$。设目标诚实签名者用 1 标识，请求签名查询时的输入 (m,hr,L) 构成的集合用 Q_1 表示，请求净化查询时的输入 (m',hr') 构成的集合用 Q_2 表示。设 $(L^*,m^*,\mathrm{hr}^*,\sigma^*=(\sigma_h^*,\sigma_{\mathrm{hr}}^*))$ 是敌手 $\mathcal{A}$ 输出的消息−签名对，Win 是敌手 $\mathcal{A}$ 获胜的事件。可问责性有 2 个方面：一是共同签名者伪造了一个净化者的签名，并且能成功地指控净化者；二是净化者伪造了一个共同签名者的签名，且能成功地指控聚合签名者。其中任意一种情况的发生均看作 Win 事件发

生（也称作敌手$\mathcal{A}$获胜）。具体来说，Win事件发生涉及以下2种情况之一。

情况1。在不知道净化者s的密钥的情况下，$\text{VerifySS}(L^*,\text{pk}_s,\text{hk},m^*,\text{hr}^*,\sigma^*)=1$且$(m^*,\text{hr}^*)\notin Q_2$。情况1暗含了敌手$\mathcal{A}$伪造了一个净化者的有效签名。进一步地，情况1又可以分为以下2种情况。

1) 存在$(m,\text{hr})\in Q_2$，使得$\text{CH}(m,\text{hr})=\text{CH}(m^*,\text{hr}^*)$且$(m,\text{hr})\neq(m^*,\text{hr}^*)$。

2) 对于任意$(m,\text{hr})\in Q_2$，$\text{CH}(m,\text{hr})\neq\text{CH}(m^*,\text{hr}^*)$。

为此，本文构造了一个敌手$\mathcal{B}_s$。首先，$\mathcal{B}_s$生成n个签名公私钥对$(\text{pk}_1,\text{sk}_1),\cdots,(\text{pk}_n,\text{sk}_n)$，均匀随机地选择2个群元素记为$\text{pk}_s$和hk，将$\text{pk}_s$、$(\text{pk}_1,\text{sk}_1),\cdots,(\text{pk}_n,\text{sk}_n)$和hk发送给$n$个共同签名者。因此，敌手$\mathcal{A}$能扮演共同签名者的角色完成多重签名的计算过程。针对敌手$\mathcal{A}$发起的净化问询，敌手$\mathcal{B}_s$进一步问询其挑战者，并将问询结果转发给敌手$\mathcal{A}$，这意味着敌手$\mathcal{B}_s$能完美地模拟净化过程。

如果敌手$\mathcal{A}$的伪造属于1)的情况，那么在Q_2中至少存在一项记录(m,hr)，满足$\text{CH}(m,\text{hr})=\text{CH}(m^*,\text{hr}^*)$且$(m,\text{hr})\neq(m^*,\text{hr}^*)$。此时，敌手$\mathcal{B}_s$输出$(m,\text{hr},m^*,\text{hr}^*)$作为其找到的CH碰撞。

如果敌手$\mathcal{A}$的伪造属于2)的情况，这意味着$(m^*,\text{hr}^*)\notin Q_2$且$\text{Verify}(\text{pk}_s,\text{hr}^*\|m^*,\sigma^*_{\text{hr}})=1$。也就是说针对敌手$\mathcal{A}$的任意净化查询，$\text{hr}^*$从未作为问询结果的一部分被返回，并且$(\text{hr}^*,\sigma^*_{\text{hr}})$是一个有效的消息签名对。此时，敌手$\mathcal{B}_s$输出$(\text{hr}^*\|m^*,\sigma^*_{\text{hr}})$作为其伪造。因此，无论何时敌手$\mathcal{A}$成功并且敌手$\mathcal{A}$执行的是2)的情况，$\mathcal{B}_s$也会成功。

情况2。在不知道签名者1的密钥的情况下，$\text{VerifyMS}(L^*,\text{hk},m^*,\text{hr}^*,\sigma^*)=1$，$\text{pk}_1\in L^*$并且$(m^*,\text{hr}^*,L^*)\notin Q_1$，这暗含了敌手$\mathcal{A}$伪造了一个有效的多重签名。情况2的证明与定理1的证明类似，这里不再赘述。

综上所述，假设$\text{Adv}_{\mathcal{B}_s}(1^\lambda)$表示敌手$\mathcal{B}_s$找到哈希碰撞以及伪造有效签名的优势，$\text{Adv}_{\mathcal{B}_1}(1^\lambda)$表示敌手$\mathcal{B}_1$找到哈希碰撞以及伪造有效多重签名的优势，则敌手$\mathcal{A}$攻破SMS方案的优势$\text{Adv}_{\mathcal{A}}^{\text{EUF-CMA}}(1^\lambda)\leqslant\text{Adv}_{\mathcal{B}_s}(1^\lambda)+\text{Adv}_{\mathcal{B}_1}(1^\lambda)$。证毕。

6.2 安全性分析

本节将分析假名证书分发方案如何抵抗冒充攻击，保证消息的完整性和可追溯性。

1) 抵抗冒充攻击

系统中的RSU作为LAC代理为车辆生成假名证书，在这一过程中可能存在以下几种冒充攻击。

① 如果攻击者冒充RSU_i为车辆授予假名证书，则攻击者首先需要广播有关RSU_i的代理信息，尽管这可以从网络中监听并截取RSU_i的代理信息来实现。但攻击者还需要知道车辆的假名信息并产生一个针对假名的净化签名，否则将无法通过车辆的验证。由于假名信息已经用RSU_i的公钥pk_i加密，且生成净化签名需要使用RSU_i的私钥，如果攻击成功，这将违背底层加密算法的密文不可区分性以及SMS方案的不可伪造性，因此，攻击者无法冒充RSU_i。

② 如果恶意车辆V_n冒充V_m向RSU请求假名证书，则V_n必须产生一个公钥pk_{V_m}验证通过的假名签名，并且能解密RSU用公钥pk_{V_m}加密的假名证书。如果V_n攻击成功，这将违背底层签名算法的不可伪造性以及底层加密算法的密文不可区分性，因此，车辆V_n无法冒充V_m。

2) 恶意行为的可追溯性

当车辆以假名身份pid发送虚假信息时，授予该假名证书的RSU将联合LAC揭露车辆的真实身份并记录车辆的恶意行为次数。根据假名证书中的假名信息$(\text{pid},\text{pk}_p,\text{ts})$，RSU可以在授予假名证书的列表$T$中查找车辆的真实身份信息$(\text{ID}_V,\text{pk}_V)$，并将这些车辆真实身份信息发送给LAC，由LAC查找移动边缘计算（MEC, mobile edge computing）云服务器更新车辆恶意行为的次数，如果恶意行为的次数超过设定阈值，LAC将吊销车辆长期公钥证书。因此，本文方案能够实现对恶意行为的追溯。

3) 通信内容的机密性和认证性

在RSU向LAC申请假名证书代理权限的过程中，RSU的代理请求采用加密并签名的方式被传输，并且代理信息（包括RSU状态信息、哈希陷门、随机数和多重签名等）以加密的方式被返回给RSU。如果代理请求信息被篡改后仍能通过验证，这将打破底层签名算法的不可伪造性；如果攻击者能从LAC返回的密文中获取到关于假名证书的代理信息，这将打破底层加密算法的密文不可区分性；如果加密的假名证书代理信息被篡改后仍能通过验证，这将打破底层SMS方案的不可伪造性。在车辆向RSU申请假名证书的交互过程中，信息

同样采用加密并签名的方式被传输。因此，本文方案在假名证书授权和假名证书生成时满足通信内容的机密性和认证性要求。

7　性能分析

本文选择了一些具有代表性的匿名认证方案进行对比分析。这些方案的安全需求与假名证书分发方案存在一定的相似性。通过这种比较能够全面评估本文方案在车联网隐私保护和通信安全方面的实际贡献。为此，表 2 详细展示了假名证书分发方案与现有先进方案在各项安全性需求上的性能对比。

表 2　不同方案基于安全性需求的性能对比

方案	冒充攻击	可追溯性	匿名性	机密性和认证性
文献[18]	×	√	√	√
文献[19]	×	√	√	√
文献[20]	√	√	√	×
文献[21]	√	×	×	×
本文方案	√	√	√	√

然后，从理论角度分析了 SMS 方案的计算复杂度和通信复杂度，分析结果如表 3 所示，其中，E 为群 $|\mathbb{G}|$ 上的单个指数运算，M 为群 $|\mathbb{G}|$ 上的单个乘法运算，$|\mathbb{G}|$ 为乘法循环群，$|\mathbb{Z}_q|$ 为 q 阶加法循环群，计算复杂度主要关注指数运算、乘法运算等开销大的操作。接着使用 Python 在具有 2.3 GHz AMD R5-5600U 内核，6 GB RAM，型号为 XiaoxinAir 14+的 PC 上实现了 SMS 方案。在实现过程中，本文选择具有 256 bit 安全级别的 secp256k1 曲线作为循环群，并且选择 Sha256 实例化 CH 中的哈希函数。SMS 方案的平均计算开销和通信开销如表 4 所示，其中，$T_{\mathrm{ECC.Enc}}$ 为执行一次 ECC 加密算法的时间开销；$T_{\mathrm{ECC.Dec}}$ 为执行一次 ECC 解密算法的时间开销；T_{Sign} 为执行一次 Schnorr 签名算法的时间开销；T_{Verify} 为执行一次 Schnorr 验证算法的时间开销；$T_{\mathrm{SMS.Sign}}$ 为 n=3 时执行一次 SMS 签名算法的时间开销；$T_{\mathrm{SMS.Sanitize}}$ 为 n=3 时执行一次 SMS 净化算法的时间开销；$T_{\mathrm{SMS.Verify}}$ 为 n=3 时执行一次 SMS 验证算法的时间开销。公钥和聚合公钥以压缩形式存储（即由 1 B 的前缀和 32 B 的 x 坐标组成）。值得注意的是，表中 KeyAgg 算法和 Sign 算法的计算开销指的是当共同签名者的数量 n=3 时的情况。从表 3 可以看出，SMS 方案具有常数阶验证开销以及恒定的签名尺寸。为了更直观地反映 SMS 方案的性能优势，本文将 SMS 方案、可批量验证的 Schnorr 方案[42]以及 ECDSA 方案[43]分别应用于多方 LAC 认证车辆的场景中，并统计采用上述不同方案将产生的车辆公钥证书尺寸以及验证车辆证书所需的时间。已知车辆公钥证书包括车辆信息、车辆公钥和认证中心的签名等信息，其中本文方案假设车辆身份信息占 20 B，车辆公钥占 33 B。如图 7 所示，当 n=1 时，采用 SMS 方案产生的车辆证书尺寸要比采用 Schnorr 方案和 ECDSA 方案时分别多 65 B 和 66 B。而随着 TAC 数量增多，采用 SMS 方案的优势逐渐显现，特别地，当 n=10 时，与采用 Schnorr 方案和 ECDSA 方案相比，采用 SMS 方案产生的车辆证书尺寸可分别减少约 53.7% 和 73.6%。在车辆证书验证开销方面，如图 8 所示，当 n=1 时，采用 SMS 方案的证书验证开销较 Schnorr 方案和 ECDSA 方案增加了近一倍。当 n=10 时，与采用 Schnorr 方案和 ECDSA 方案相比，采用 SMS 方案时的证书验证开销可分别减少约 65.2% 和 80%。SMS 方案的性能优势会随着 TAC 数量的增多而进一

表 3　SMS 方案的计算复杂度和通信复杂度

计算复杂度							通信复杂度			
KeyGen		KeyAgg	Sign		Verify	Sanitize	pk		X	$\hat{\sigma}$
$1E$（签名者）	$2E$（净化者）	$nE+(n-1)M$	$7E+3M$（签名者）	$9E+(4n-1)M$（签名聚合者）	$5E+3M$	$3E+2M$	$\|\mathbb{G}\|$（签名者）	$2\|\mathbb{G}\|$（净化者）	$\|\mathbb{G}\|$	$2\|\| + 2\|\mathbb{Z}_q\|$

表 4　SMS 方案的平均计算开销和通信开销

KeyGen							KeyAgg		
KeyGen		KeyAgg	Sign		Verify	Sanitize	pk	X	$\hat{\sigma}$
0.41（签名者）	0.80（净化者）	2.72	4.25	11.34	3.53	3.89	33	33	130

步扩大，这使得采用SMS方案的假名证书分发方案也更加具备扩展性。

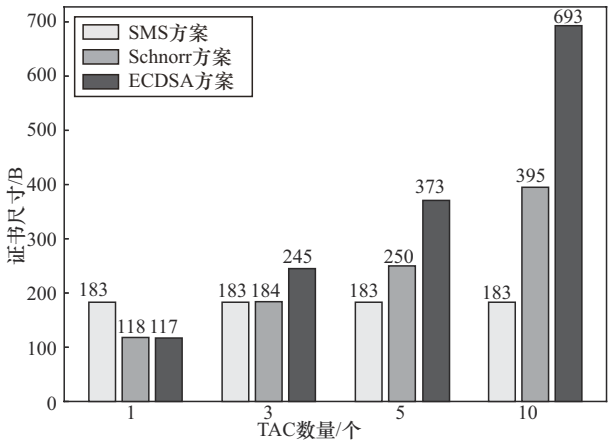

图7　不同签名方案下的证书尺寸对比

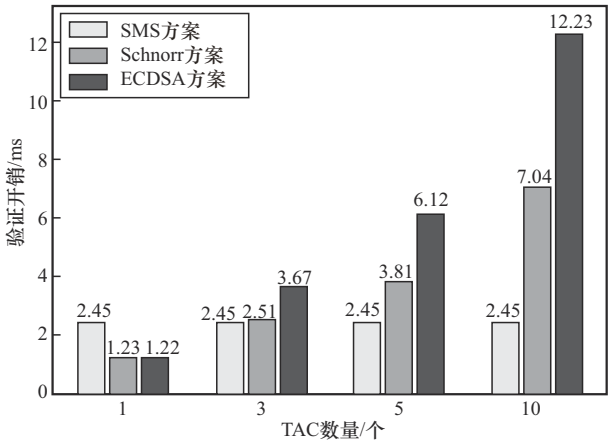

图8　不同签名方案下的车辆证书验证开销

最后，本文评估了假名证书分发方案在假名证书生成过程和消息匿名认证过程中参与实体的计算开销（如表5所示）和通信开销（如表6所示），并与已有的匿名认证方案文献[15]、文献[16]和文献[23]进行了比较。假设公钥证书由身份、公钥和签名组成，因此，LAC和RSU的公钥证书占118 B，车辆的公钥证书占183 B。值得注意的是，本文方案考虑由多方LAC共同生成假名证书，而文献[15]、文献[16]和文献[23]仅仅考虑单个LAC生成假名证书的情形。基于此事实，如图9所示，采用本文方案时RSU的计算开销相比文献[15]仅增加了5.36 ms。尽管采用文献[16]时RSU的计算开销最低，但是它不能抵御冒充攻击。这是因为在该方案中，车辆申请假名证书时会公开其身份信息，因此恶意车辆可以冒充诚实车辆申请假名证书。在假名证书生成阶段，采用本文方案和文献[16]时车辆具有接近最低的计算开销，但文献[16]要求车辆向TAC申请假名证书，当假名需要被频繁更新时，这将产生更大的通信时延。在消息匿名认证阶段，如图10所示，采用文献[15]、文献[16]和本文方案时车辆之间具有近似的计算开销，而文献[23]需要大量的配对和指数运算，因此其计算性能最差。

综上分析，本文方案在考虑由多方LAC认证车辆假名的背景下，与仅考虑单个LAC认证车辆假名的匿名认证方案文献[15]、文献[16]和文献[23]相比，在假名证书生成和匿名认证阶段具有可比较的计算开销，特别是在假名证书生成过程中由车辆

表5　　**假名证书分发方案参与实体的计算开销**

阶段	LAC/ms	RSU/ms	V/ms
代理请求（RSU→LAC）	0	$T_{\text{ECC.Enc}}+T_{\text{Sign}}=1.20$	0
代理授权（LAC→RSU）	$2T_{\text{Verify}}+T_{\text{ECC.Dec}}+T_{\text{SMS.Sign}}+T_{\text{ECC.Enc}}=15.46$	$T_{\text{ECC.Dec}}+T_{\text{SMS.Verify}}=3.56$	0
假名证书请求（V→RSU）	0	$2T_{\text{Verify}}+T_{\text{ECC.Dec}}=3.87$	$T_{\text{ECC.Enc}}+T_{\text{Sign}}=1.23$
假名证书响应（RSU→V）	0	$T_{\text{SMS.Sanitize}}+T_{\text{ECC.Enc}}=4.07$	$T_{\text{ECC.Dec}}+T_{\text{SMS.Verify}}=3.56$
总计	15.46	12.70	4.79

表6　　**假名证书分发方案参与实体的通信开销**

阶段	LAC/B	RSU/B	V/B
代理请求（RSU→LAC）	$\perp$	$\lvert\text{Cert}_i\rvert + \lvert\text{CT}_{i\to\text{SA}}\rvert + \lvert\sigma\rvert = 227$	0
代理授权（LAC→RSU）	$\lvert\text{CT}_{\text{SA}\to i}\rvert = 272$	0	0
假名证书请求（V→RSU）	0	0	$\lvert\text{Cert}_V\rvert + \lvert\text{CT}_{V\to i}\rvert + \lvert\sigma\rvert = 305$
假名证书响应（RSU→V）	0	$\lvert\text{CT}_{i\to V}\rvert = 286$	0

负载的部分甚至优于对比方案，这使本文方案更适用于对实时性要求高的车联网通信场景。

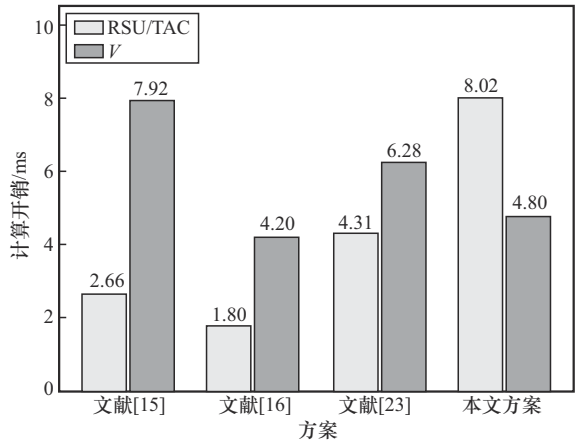

图9　假名证书生成阶段的计算开销对比

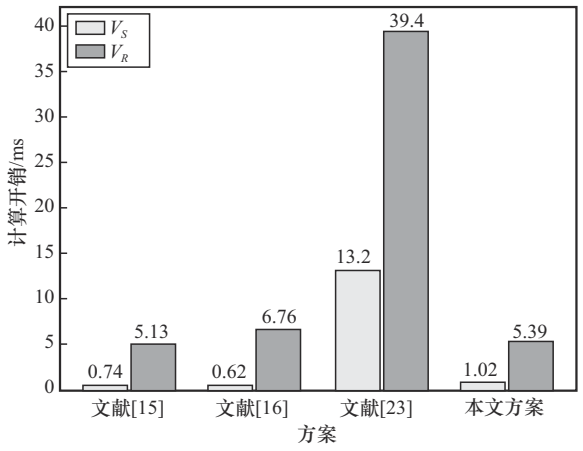

图10　匿名认证阶段的计算开销对比

8　结束语

本文探讨了由多个可信权威中心共同生成车辆假名证书的匿名认证场景，并构建了一个SMS方案作为理论支持，该方案授予净化者在不需要与原始签名者交互的情况下更新签名数据的能力，并确保一组签名者产生的多重签名对更新后的数据依然有效。这一特性特别适用于支持车辆在频繁更换假名的环境中实现假名证书服务的快速响应。此外，SMS方案通过其内置的问责机制增强了系统对潜在滥用行为的防御能力。之后，本文基于SMS方案设计了一种假名证书分发机制。在该机制中，原本由多个可信权威中心承担的生成假名证书的职责被委托给了地理分布更广泛且更接近车辆的路侧单元。这一策略不仅减少了车辆获取假名证书的时延，而且间接提升了车辆假名更新的整体效率。本文方案能够实现通信内容的机密性、认证性以及对恶意行为的可追溯性。基于本文方案，车辆能在匿名认证过程中抵抗冒充攻击和关联攻击。与现有的匿名认证方案相比，本文方案首次考虑到由多方可信权威中心生成车辆假名证书，并且车辆在获得假名证书和匿名认证的过程中并没有额外增加过多的计算开销。值得注意的是，本文并没有关注假名证书如何撤销以及如何在车联网系统范围内更新已撤销的假名证书列表。因此，在未来的工作中，将考虑以有效的方式解决假名证书的撤销问题。

参考文献：

[1] NOOR-A-RAHIM M, LIU Z L, LEE H, et al. 6G for vehicle-to-everything (V2X) communications: enabling technologies, challenges, and opportunities[J]. Proceedings of the IEEE, 2022, 110(6): 712-734.

[2] AMEEN H A, MAHAMAD A K, ZAIDAN B B, et al. A deep review and analysis of data exchange in vehicle-to-vehicle communications systems: coherent taxonomy, challenges, motivations, recommendations, substantial analysis and future directions[J]. IEEE Access, 2019, 7: 158349-158378.

[3] ZORKANY M E, YASSER A, GALAL A I. Vehicle to vehicle“V2V” communication: scope, importance, challenges, research directions and future[J]. The Open Transportation Journal, 2020, 14(1): 86-98.

[4] GUPTA M, BENSON J, PATWA F, et al. Secure V2V and V2I communication in intelligent transportation using cloudlets[J]. IEEE Transactions on Services Computing, 2022, 15(4): 1912-1925.

[5] ERCAN S, AYAIDA M, MESSAI N. An enhanced pseudonym certificates distribution mechanism for connected vehicles[J]. International Journal of Communication Systems, 2022, 35(7): e5100.

[6] IEEE.1609.2.1-2022. IEEE standard for wireless access in vehicular environments (WAVE)-certificate management interfaces for end entities[S]. 2022.

[7] BRECHT B, THERRIAULT D, WEIMERSKIRCH A, et al. A security credential management system for V2X communications[J]. IEEE Transactions on Intelligent Transportation Systems, 2018, 19(12): 3850-3871.

[8] MANVI S S, TANGADE S. A survey on authentication schemes in VANETs for secured communication[J]. Vehicular Communications, 2017, 9: 19-30.

[9] BELLIKAR G, BHATIA A, HANSDAH R C, et al. 3TAAV: a three-tier architecture for pseudonym-based anonymous authentication in VANETs[C]//Proceedings of the 2018 International Conference on Information Networking (ICOIN). Piscataway: IEEE Press, 2018: 420-425.

[10] LI S Z, WANG N, DU X H, et al. Supervisable anonymous management of digital certificates for blockchain PKI[C]//Proceedings of the 6th International Conference of Pioneering Computer Scientists, Engineers and Educators. Berlin: Springer, 2020: 130-144.

[11] RAYA M, HUBAUX J P. Securing vehicular ad hoc networks[J]. Journal of Computer Security, 2007, 15(1): 39-68.

[12] STUDER A, SHI E, BAI F, et al. TACKing together efficient authentication, revocation, and privacy in VANETs[C]//Proceedings of the 2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks. Piscataway: IEEE Press, 2009: 1-9.

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

[14] KILTZ E, PIETRZAK K. Leakage resilient ElGamal encryption[C]// Proceedings of the 16th International Conference on the Theory and Application of Cryptology and Information Security, Berlin: Springer, 2010: 595-612.

[15] MAURYA C, CHAURASIYA V K. Efficient anonymous batch authentication scheme with conditional privacy in the Internet of vehicles (IoV) applications[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(9): 9670-9683.

[16] AZEES M, VIJAYAKUMAR P, DEBOARH L J. EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(9): 2467-2476.

[17] WANG Q L, OU M, YANG Y, et al. Conditional privacy-preserving anonymous authentication scheme with forward security in vehicle-to-grid networks[J]. IEEE Access, 2020, 8: 217592-217602.

[18] 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.

[19] ZHANG J, ZHONG H, CUI J, et al. An extensible and effective anonymous batch authentication scheme for smart vehicular networks[J]. IEEE Internet of Things Journal, 2020, 7(4): 3462-3473.

[20] FENG X, SHI Q C, XIE Q Q, et al. P2BA: a privacy-preserving protocol with batch authentication against semi-trusted RSUs in vehicular ad hoc networks[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 3888-3899.

[21] BAGGA P, SUTRALA A K, DAS A K, et al. Blockchain-based batch authentication protocol for Internet of vehicles[J]. Journal of Systems Architecture, 2021, 113: 101877.

[22] QU F Z, WU Z H, WANG F Y, et al. A security and privacy review of VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2015, 16(6): 2985-2996.

[23] YUE X H, CHEN B, WANG X B, et al. An efficient and secure anonymous authentication scheme for VANETs based on the framework of group signatures[J]. IEEE Access, 2018, 6: 62584-62600.

[24] GAO T H, DENG X Y. A pseudonym ring building scheme for anonymous authentication in VANETs[C]//International Conference on Broadband and Wireless Computing, Communication and Applications. Berlin: Springer, 2018: 481-489.

[25] LU R, LIN X, ZHU H, et al. ECPP: efficient conditional privacy preservation protocol for secure vehicular communications[C]//Proceedings of the IEEE INFOCOM 2008-The 27th Conference on Computer Communications. Piscataway: IEEE Press, 2008: 1229-1237.

[26] HUANG D J, MISRA S, VERMA M, et al. PACP: an efficient pseudonymous authentication-based conditional privacy protocol for VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2011, 12(3): 736-746.

[27] BENAROUS L, KADRI B, BITAM S, et al. Privacy-preserving authentication scheme for on-road on-demand refilling of pseudonym in VANET[J]. International Journal of Communication Systems, 2020, 33(10): e4087.

[28] BOUALOUACHE A, SENOUCI S M, MOUSSAOUI S. HPDM: a hybrid pseudonym distribution method for vehicular ad-hoc networks[J]. Procedia Computer Science, 2016, 83: 377-384.

[29] MAXWELL G, POELSTRA A, SEURIN Y, et al. Simple Schnorr multi-signatures with applications to Bitcoin[J]. Designs, Codes and Cryptography, 2019, 87(9): 2139-2164.

[30] WULLG P, NICK J, PUFFING T. Schnorr signatures for secp256k1, January 2020[R]. 2020.

[31] BELLARE M, NEVEN G. Multi-signatures in the plain public-key model and a general forking lemma[C]//Proceedings of the 13th ACM Conference on Computer and Communications Security. New York: ACM Press, 2006: 390-399.

[32] MICALI S, OHTA K, REYZIN L. Accountable-subgroup multisignatures: extended abstract[C]//Proceedings of the 8th ACM Conference on Computer and Communications Security. New York: ACM Press, 2001: 245-254.

[33] BOLDYREVA A. Threshold signatures, multisignatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme[C]// International Workshop on Public Key Cryptography. Berlin: Springer, 2002: 31-46.

[34] LU S, OSTROVSKY R, SAHAI A, et al. Sequential aggregate signatures and multisignatures without random oracles[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2006: 465-485.

[35] BAGHERZANDI A, CHEON J H, JARECKI S. Multisignatures secure under the discrete logarithm assumption and a generalized forking lemma[C]//Proceedings of the 15th ACM Conference on Computer and Communications Security. New York: ACM Press, 2008: 449-458.

[36] SYTA E, TAMAS I, VISHER D, et al. Keeping authorities“honest or bust”with decentralized witness cosigning[C]//Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2016: 526-545.

[37] DRIJVERS M, EDALATNEJAD K, FORD B, et al. On the security of two-round multi-signatures[C]//Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2019: 1084-1101.

[38] NICK J, RUFFING T, SEURIN Y, et al. MuSig-DN: schnorr multi-signatures with verifiably deterministic nonces[C]//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2020: 1717-1731.

[39] NICK J, RUFFING T, SEURIN Y. MuSig2: simple two-round Schnorr

multi-signatures[C]//Annual International Cryptology Conference. Berlin: Springer, 2021: 189-221.

[40] ALPER H K, BURDGES J. Two-round trip schnorr multi-signatures via delinearized witnesses[C]//Annual International Cryptology Conference. Berlin: Springer, 2021: 157-188.

[41] CHEN X F, ZHANG F G, TIAN H B, et al. Discrete logarithm based chameleon hashing and signatures without key exposure[J]. Computers & Electrical Engineering, 2011, 37(4): 614-623.

[42] SCHNORR C P. Efficient signature generation by smart cards[J]. Journal of Cryptology, 1991, 4(3): 161-174.

[43] JOHNSON D, MENEZES A, VANSTONE S. The elliptic curve digital signature algorithm (ECDSA)[J]. International Journal of Information Security, 2001, 1(1): 36-63.

[作者简介]

刘召曼（1995– ），女，山东济南人，复旦大学博士生，主要研究方向为车联网安全、匿名认证、数字签名、可编辑区块链。

杨亚芳（1994– ），女，河南濮阳人，博士，复旦大学在站博士后，主要研究方向为公钥密码学、车联网安全。

宁建廷（1988– ），男，浙江衢州人，博士，武汉大学教授，主要研究方向为公钥密码学、数据安全、区块链安全等。

赵运磊（1974– ），男，山东阳谷人，博士，复旦大学特聘教授，主要研究方向为后量子密码、密码协议和计算理论。