车联网环境下无证书匿名认证方案

刘雪艳*① 王 力① 邸丽娟① 杜小妮① 牛淑芬②

①(西北师范大学数学与统计学院 兰州 730070)

②(西北师范大学计算机科学与工程学院 兰州 730070)

摘 要：通过信息共享，车联网(IoV)为车辆提供各种应用，以提高道路安全和交通效率。然而，车辆之间的公开通信导致了车辆隐私泄露和各种攻击。因而，安全且保护隐私的信息共享方法是非常必要的，并且对车辆间通信的安全性和保密性提出了更高的要求，所以该文提出了一种支持批量验证的非线性对的无证书匿名认证方案。在该方案中，首先，采用无证书签名机制避免了证书管理和密钥托管问题；其次结合区域管理局生成的长期伪身份和自己生成的短期伪身份保证车辆的强匿名性和签名的新鲜性，避免路侧单元计算伪身份造成的身份泄露和时延；再次，采用无对的聚合签名提供批验证，减少车联网环境中路侧单元的计算量；最后，当发生恶意事件时，区域管理局可以追踪车辆的真实身份并由可信中心撤销该用户。安全性证明和分析表明，该方案具有高的安全性，并满足完整性、可追踪性、匿名性、可撤销性等安全要求。将该方案与现有的方案进行了比较，效率分析表明该方案更有效。

关键词：车联网；非线性对；无证书；椭圆曲线离散对数问题；匿名性；批验证

中图分类号：TP309; TP915 **文献标识码**：A **文章编号**：1009-5896(2022)01-0295-10

DOI: 10.11999/JEIT201069

Certificateless Anonymous Authentication Scheme for Internet of Vehicles

LIU Xueyan① WANG Li① HUAN Lijuan① DU Xiaoni① NIU Shufen②

①(*School of Mathematics and Statistics*, *Northwest Normal University*, *Lanzhou* 730070, *China*)

②(*School of Computer Science and Engineering*, *Northwest Normal University*, *Lanzhou* 730070, *China*)

Abstract: Through information sharing, the Internet of Vehicles (IoV) provides various applications for vehicles to improve road safety and traffic efficiency. However, the open communication between vehicles lead to vehicle privacy leakage and various attacks. Therefore, information sharing methods with security and privacy protection are very necessary, so a pairing-free and certificateless anonymous authentication scheme supporting batch authentication is proposed. In this scheme, firstly, the problem of certificate management and key escrow can be avoided by using the certificateless signature; Secondly, the combination of the long-term pseudo-identity generated by the regional authority and the short-term pseudo-identity generated by itself, the strong anonymity of vehicle and the freshness of signature are guaranteed, and the identity disclosure and the communication delay caused by Road-side-unit computing pseudo identity are avoided; Thirdly, the aggregating signature without pairing is used to provide batch verification, which reduces greatly the computational burden of RSUs in vehicle network environment; Finally, when a malicious event occurs, the Regional Trusted Authority (RTA) can track the real identity of the vehicle. Security proof and analysis show that, the scheme has high security, and meets the security requirements.

Key words: Internet of Vehicles (IoV); Certificateless; Pairing-free; Elliptic curve discrete logarithm problem; Anonymous; Batch verification

收稿日期：2020-12-18；改回日期：2021-05-30；网络出版：2021-08-26

*通信作者： 刘雪艳 liuxy@nwnu.edu.cn

基金项目：国家自然科学基金(61662071, 61772022,71764025)

Foundation Items: The National Natural Science Foundation of China (61662071,61772022,71764025)

1 引言

车联网(Internet of Vehicles, IoV)是物联网在交通领域中的一种应用。其通过车辆自带的传感器收集车辆和道路交通数据，并将这些数据通过无线通信传输给智能终端。车联网中每个节点利用相邻节点的信息提供交通管理、车辆定位、速度控制等服务。因为其中的节点具有移动性，导致频繁的拓扑变化，所以它是一种根据车辆需求智能提供服务的动态网络[1]。

车联网主要利用传感器数据采集、无线射频识别以及短距离通信等技术，实现车辆与车辆 (Vehicle-to-Vehicle, V2V)、车辆与路边基础设施(Vehicle-to-Infrastructure, V2I)进行互相通信和信息交换，从而实现对车辆和道路的完全控制。在车联网系统中，车载单元(On-Board-Unit, OBU)的工作原理是在专用短程通信系统的帮助下，集成和利用诸如全球定位系统、微型传感器和嵌入式系统，使得车辆可以和周围其他车辆或路侧单元(Road-Side-Units, RSUs)进行消息传递。RSUs通过有线信道和无线信道与可信中心(Trusted Authority, TA)或OBU进行信息传递，它可以接受来自OBU信息并传递给TA，同时也可以接受TA发送的信息并传递给OBU。

车联网系统具有车辆节点规模大，行驶速度快，通信信道开放等特点，所以车联网环境下各节点之间的通信面临着巨大挑战。恶意攻击者可能会窃听消息，注入虚假消息或修改消息来造成流量中断，或者跟踪车辆节点获取车辆隐私信息如车主的身份隐私、位置隐私信息等[2]。所以，在车联网中需要关注3个重要问题，首先，对于消息来源的可靠性需要高效认证；其次，车辆信息应该得到很好的隐私保护；最后对于恶意用户，他们的身份应该是可追踪的。

因此，在IoV中共享的信息必须满足可验证性、完整性、隐私性、不可否认性、可追溯性、匿名性等安全要求。

(1)动机与工作。虽然一些研究工作提出了用于IoV部署的消息认证方案[3–7]，但它们不能提供必要的安全特性，而且易受到各种已知攻击，此外，这些方案需要大量的计算和通信开销，使得它们无法适应实时场景。针对这些问题，本文在IoV环境下，提出了一种基于椭圆曲线密码(Elliptic Curve Cipher, ECC)无对的无证书匿名认证方案。主要工作如下：

(a) 密钥生成中心(Key Generation Center, KGC)生成车辆的部分私钥，车辆联合部分私钥和自己的秘密值共同产生实际私钥，以此解决密钥托管问题；

(b) 在注册阶段区域管理局(Regional Trusted Authority, RTA)为车辆生成一个长期的伪身份用于后续的部分密钥生成，而在和其他车辆或RSUs通信时车辆自身生成一个短期的伪身份。长期-短期伪身份的联合使用保证了强匿名性和签名的新鲜性，并且避免了RSUs生成临时伪身份造成的身份泄露和时延问题；

(c) 采用无双线性对的同态签名和批量验证，提高了RSUs验证消息的效率；

(d) 当有恶意事件发生时，RTA可以通过长-短期伪身份追踪车辆真实身份，并由TA撤销该用户。

在上述工作中，该方案达到了车联网中消息的可认证性，消息发送者的匿名性，身份的可追踪性，消息的不可抵赖性，不可链接性，前向安全性和后向安全性以及消息认证的高效性等。

(2)相关工作。在安全和隐私的背景下，一些针对车联网的公钥基础设施(Public Key Infrastructure, PKI)的方案[3,4]已经被提出，但是该方案存在车辆很难管理和存储数量丰富的公私钥对和相关证书问题。此外，TA需要维护一个证书撤销列表(Certificate Revocation List, CRL)，其中存储被吊销车辆的证书，这通常是庞大的。Raya和Hubaux[5]通过使用匿名证书来隐藏用户的真实身份，为车联网引入了一种匿名认证方案。他们建议每辆车都存储一些匿名证书，这样车辆就可以在每个认证过程中使用不同的公私钥对避免可追溯性。但是，这会造成车辆不得不存储大量的对。因此，密钥的安全分发、密钥管理和存储变得非常复杂。

为了解决传统PKI认证方案的问题，出现了许多基于身份的认证方案。文献[6]把车辆的身份属性作为公共密钥，因此不需要系统为其生成公钥证书。基于身份的认证方案不仅能够保护车辆的隐私信息还能够保护消息的完整性，但是其存在密钥托管问题。文献[7]使用于ECC设计了一种新的基于身份的条件隐私保护认证方案，该方案传输签名消息所需的通信带宽更小。为了提高系统效率，文献[8]提出了一种高效匿名认证协议。文献[9]提出了一种可扩展的、满足批量验证的条件隐私保护认证方案。在该方案中，伪身份和相应的私钥由PKG单独生成。然后，文献[10]提出了一种高效的基于身份的批量验证方案，并指出了一些安全风险。文献[11]通过改进文献[10]的方案，提出了一种不需要双线性对的基于身份的批验证安全方案。文献[12]采用了一种基于身份加密的环签名方案，对环签名方案进行了修改，实现了签名者的模糊性，提高了车载网络的隐私要求。然而，环签名方案在车联网

中并不适用，不能实现有条件的隐私。文献[13]提出了一种高效匿名批处理认证方案，该方案利用哈希链和消息认证码为通信提供批处理验证。仿真结果表明，当消息数大于23条时，文献[13]比其他批处理验证方案效率更高。文献[14]提出了一种新的基于身份验证的框架，通过使用假名和基于门限的分布式控制分别实现匿名性与不可否认性。在车联网中采用签密技术的方案[15]也被提出，由于车联网节点不受计算能力限制，因此比签名和加密方法具有相当大的优势。然而，在所有这些基于身份的方案中，主要的障碍是KGC利用自己的主密钥生成一个车载实体的密钥。它不能确保不可否认性，因为KGC滥用车辆的访问能力可以签署和解密任何消息，从而导致密钥托管问题。

为了克服证书管理和密钥托管问题，文献[16]在2003年引入了基于无证书的机制。2011 年，文献[17]提出了一种车联网环境下的无证书认证方案，方案中车辆的假名由车辆自身和可信中心TA共同生成，车辆的私钥由车辆自身和KGC共同生成，保护了车辆隐私信息，并且解决了密钥托管问题。2014 年，文献[18]提出了一种车联网环境下更加安全的无证书认证方案，主要用于实现V2I之间的安全通信。同时，无证书认证方案也能够实现可追踪性，一旦有车辆传播不合法的消息，TA能够通过自己的主私钥追踪车辆的真实身份[19]。2018年，文献[20]提出了车载网中可证安全的无证书聚合签名算法，但文献[21]认为文献[20]是不安全的，并进一步提出了一个改进的无证书聚合签名方案。

此外，上述部分文献利用了椭圆曲线加密技术，椭圆曲线密码学主要是将椭圆曲线应用到密码学中，利用椭圆曲线离散对数问题(Elliptic Curve Discrete Logarithm Problem, ECDLP)构成椭圆曲线密码学(ECC)。由于其占用内存小不易破解等优点广泛应用于一些安全领域，如加密、解密、数字签名和安全协议等。

当今社会人们的隐私意识越来越强，为了进一步加强安全，提高效率，需要一个避免密钥托管的强匿名认证方案来保护隐私。因此，本文提出了一个有效且高效的无证书匿名认证方案，该方案没有涉及 PKI 证书，减少了系统车辆的存储负担，并且采用无对的聚合方法以减少RSUs验证的时间。

2　准备工作

2.1　无证书密码学

(1) 公钥加密(PKC)。在PKC中，每个用户都有一个公钥和一个私钥。私钥是保密的，而公钥是公开的。用户的公钥通过证书(即受信任的证书颁发机构在公钥上的签名)与用户相关联。这使得接收方确保它们拥有的公钥是发送方的正确公钥。想要使用公钥的接收者必须验证相应的证书以确保密钥的有效性。因此，需要一个公钥基础设施(PKI)——一系列可信赖的第三方，可以依赖他们来担保身份与特定公钥之间的联系。但是该特性会导致证书颁发机构需要大量的存储和计算能力来管理证书。

(2) 基于身份的加密(ID-PKC)。为了避免证书管理问题，引入了ID-PKC的概念。基于身份的方案将实体的公钥设置为其数字身份，从而消除了对公钥基础设施的需要，而且KGC使用主密钥生成实体的私钥。因此，ID-PKC的一个固有问题是“密钥托管”。

(3) 无证书密码学。文献[17]引入了无证书公钥加密(CL-PKC)的概念，它消除了在PKC中使用证书，并解决了ID-PKC中的密钥托管问题。CL-PKC的基本思想是：KGC为用户产生一个部分私钥，用户选取一个秘密值，并与部分私钥结合生成用户的私钥，用户私钥由KGC和用户联合产生。KGC不知道用户的完整私钥，从而避免了密钥托管问题。和基于证书的公钥密码体制相比，无证书的公钥密码学不需要证书的管理，所需负载更小，因此更适用于低宽带需求和低能量消耗的移动应用环境。

2.2　椭圆曲线

设F_p表示阶为p的有限域，其中p是大素数。通常定义一个标准椭圆曲线E为：$y^2=x^3+ax+b \bmod p$，其中$a,b\in F_p$，且$\Delta=4a^3+27b^2\neq 0$。E上的点和无穷远处的点O构成一个循环加法椭圆曲线群

$$G=\{(x,y):x,y\in F_p,E(x,y)=0\}\cup\{O\}$$

G有以下性质：

(1) 加法(+/–)：设P与Q为G上的两个点，若$P\neq Q$则有$R=P+Q$, R是E与连接P, Q两点直线的交点。若$P=Q$，则有$R=P+Q$，R是E与$P(Q)$点切线的交点。若$Q=-P$，则有$P+Q=P-P=O$；

(2) 标量乘法$(\cdot)$：设$P\in G$,$m\in Z_q^*$，则在G上的标量乘法为$m\cdot P=P+P+\cdots+P$(共m次)。

2.3　椭圆曲线离散对数问题(ECDLP)

已知E/F_p上的点P，给定点对(P,mP)，求整数$m\in Z_p$，这个问题称为椭圆曲线离散对数问题，简写为ECDLP。当点P有大的素数阶时，认为求解ECDLP是计算上不可行的。

3 系统模型

本节介绍了本文方案的体系结构、安全模型和安全性要求。

3.1 体系结构

IoV结构由5个实体组成：可信中心(TA)、区域管理局(RTA)、密钥生成中心(KGC)、路侧单元(RSUs)和车载单元(OBU)。IoV网络模型如图1所示。

(1) 可信中心(TA)：它是完全可信赖的权威，具有足够的计算和通信资源，并且拥有车辆的真实身份列表，并且为系统生成公私钥对和系统参数。TA通常为交通管理部门。

(2) 区域管理局(RTA)：即区域TA，负责注册车辆和RSUs。RTA为注册的车辆分配一个防篡改设备(Tamper-Proof Device, TPD)，其具有高强度的安全特性，可以阻止各类环境下的信息泄露攻击。

(3) 密钥生成中心(KGC)：在IoV系统中KGC是另一个丰富了计算和通信资源的可信实体。KGC负责为IoV中的车辆生成部分私钥。

(4) 路侧单元(RSUs)：RSUs部署在路边，是TA, KGC和OBU之间的桥梁。RSUs与RTA和KGC通过有线连接，与OBU通过无线信道连接。其主要负责验证车辆广播的消息。

(5) 车载单元(OBU)：车载单元嵌入到车辆中，并广播与交通有关的信息、位置标识和驾驶状态等。该设备有自己的时钟，用于生成正确的时间戳，为此，所有TA, RTA, KGC, RSUs和OBU都有大致同步的时钟。其负责将敏感信息存储在车辆的防篡改设备(TPD)中，并向车辆和附近的RSUs广播消息。

3.2 安全模型

本文的安全模型是在文献[1]安全模型基础上提出的，其中的敌手可以不受限制地访问公共信道，并且可以在公共信道上读取、拦截、重放、修改、制造和删除传输的分组。假设TA, RTA, KGC和RSUs是IoV环境中的可信实体。在IoV环境中的车辆配备了防篡改设备TPD，故敌手不能读取、写入或删除TPD的内容。由于本方案利用了无证书密码学的思想，故用户的公钥没有得到认证，所以在敌手模型中，必须允许敌手有权利用他自己选择的不合法公钥代替用户的公钥，而且由于KGC知道系统主密钥，从而能够计算所有用户的部分私钥，但他不能替换用户的公钥。所以本文将敌手类型分为两类，类型I的敌手模拟一个外部攻击者，充当恶意的第三方，并且能够请求和替换系统中的公钥。类型II的敌手是一个内部攻击者，可以访问KGC的主密钥，充当恶意但被动的KGC，但不能替换用户的公钥。如果两类敌手均能在多项式时间内以不可忽略的概率赢得其与挑战者之间的游戏，则一定分别存在一个多项式时间内的挑战者解决ECDLP问题，但这与ECDLP为困难性问题矛盾。

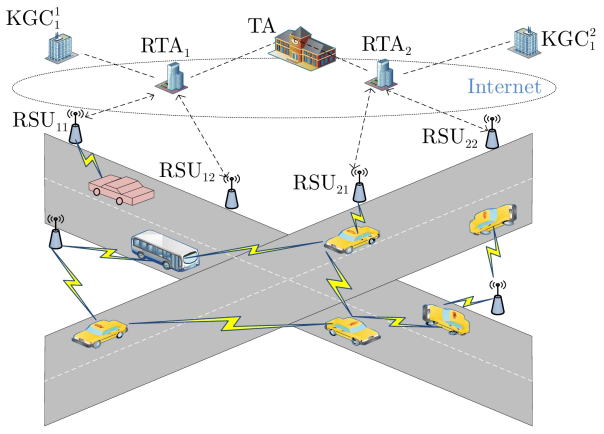

图 1 IoV网络模型

3.3 安全性要求

(1) 可认证性：消息的真实性确保接收到的消息确实是由声称这样做的车辆发送的。

(2) 完整性：它确保消息在从发送方传递到接收方时没有被修改、伪造或丢弃。

(3) 匿名性：IoV中的其他车辆和敌手无法通过分析同一车辆发送的多条消息或其伪身份来识别发送者的真实身份。

(4) 可追溯性：仅RTA就可以通过获取发送者的伪身份来识别发送者的真实身份，并且可以识别车辆发送的恶意消息。

(5) 不可链接性：敌手不能在同一发送者发送的消息中找到任何共同的知识，所有的假名不应该透露他们之间的任何联系。

(6) 前向安全性与后向安全性：敌手无法通过当前的签名消息推断出之前或之后的签名消息。

4 本文方案

4.1 本文方案总览

图2给出了本文方案的总览，当车辆发起注册请求时，TA将车辆的真实身份列表UL从其数据库转发给RTA，然后车辆通过安全信道向RTA发送注册请求，完成注册后的车辆便可向车辆配备一个TPD设备，并且同时给车辆生成一个长期伪身份；接着，车辆结合KGC产生的部分密钥、RTA分配的长期伪身份，生成自己的公私钥；当车辆在进入RSUs区域时先生成一个短期伪身份，然后把签名消息发送给RSUs；当RSUs收到车辆发来的消息时，进行验证。

4.2 具体方案

(1) 系统初始化

G是一个椭圆曲线上的循环加法群，生成元为

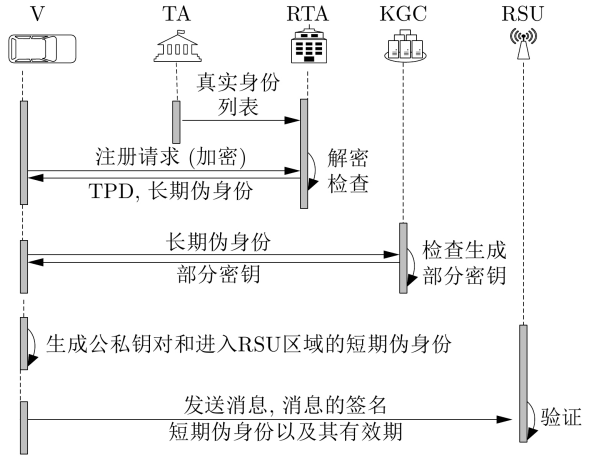

图 2 方案总览图

P，阶为q，TA随机选取$r_1 \in Z_q^*$为其主密钥，计算$T_{\text{pub}} = r_1 P$, KGC随机选取$r_2 \in Z_q^*$为主密钥，计算$K_{\text{pub}} = r_2 P$，TA选取以下哈希函数$h_1 : \{0,1\}^* \to Z_q^*$，$h_2 : \{0,1\}^* \to G$，$h_3 : \{0,1\}^* \times Z_q^* \times G \times G \times \{0,1\}^* \to Z_q^*$。TA和KGC公布参数为：$\{G, P, T_{\text{pub}}, K_{\text{pub}}, h_1(\cdot), h_2(\cdot), h_3(\cdot)\}$。

(2) 车辆注册

(a) TA事先将车辆真实身份列表UL从其数据库转发给RTA。车辆通过使用RTA的公钥对真实身份RID_i和PWD_i进行加密，其中PWD_i为用户的口令，然后RTA用其私钥解密。

(b) RTA检查真实数据列表UL。如果该RID_i存在，则RTA为该车辆装备一个TPD，其中存储了RID_i和PWD_i，以及系统私钥与参数。同时随机选取$t \in Z_q^*$，计算长期伪身份$\text{QID}_i = th_1(\text{RID}_i) \bmod q$并存储于TPD中，用于网络实体之间的通信，帮助隐藏车辆的实际身份RID_i，并将长期伪身份QID_i上传至UL。只有在发生冲突时，RTA才能向执法部门透露车辆的实际身份。

(3) 部分密钥生成

当车辆V_i发送QID_i给KGC请求部分私钥时，KGC执行以下操作：

KGC将检查TA通过安全通道发送的撤销列表，以确认车辆V_i是否被撤销。如果找到匹配项，KGC将停止生成部分密钥。否则，KGC继续为V_i生成部分密钥，且部分私钥为$\text{SK}_1^i = r_2 \text{QID}_i \bmod q$。

(4) 用户密钥生成

从KGC接收到部分密钥后，V_i按照给定的步骤继续生成其公钥和私钥对：

V_i随机选择$x_i \in Z_q^*$，计算$V_{\text{pub}_i} = x_i P$，私钥为$\text{SK}^i = \left(x_i, \text{SK}_1^i\right)$，并且在进入新RTA区域时公私钥需更新。$V_i$将$\text{SK}^i$存储在防篡改设备TPD中作为其密钥，并将$V_{\text{pub}_i}$作为其公钥发布。

(5) 短期伪身份的生成

当车辆V_i进入RSUs区域时，车辆V_i需生成短期伪身份：

(a) V_i在TPD_i中输入QID_i和PWD_i，然后TPD_i验证，通过则启动短期伪身份生成过程。

(b) TPD_i验证RID_i和PWD_i，如果正确，则TPD_i选择一个随机数s。计算短期伪身份$\text{FID}^i = \left\{\text{FID}_1^i, \text{FID}_2^i, T_i\right\}$，其中$\text{FID}_1^i = sP$，$\text{FID}_2^i = \text{RID}_i \oplus h_2\left(\{sT_{\text{pub}}\}_x || \text{QID}_i || T_i\right)$，$T_i$为短期伪身份的有效期。$\{A\}_x$指椭圆曲线点$A$的$x$坐标。

(6) 签名

为了确保认证和消息的完整性，每个消息$m_i \in (0,1)^*$必须由车辆V_i签名。车辆V_i使用其长期伪身份、短期伪身份、私钥来生成如下签名。

输入$\left\{m_i, \text{QID}_i, \text{FID}^i, T_j\right\}$，$T_j$为当前时间戳。$V_i$随机选取$b_i \in Z_q^*$，计算$U_i = b_i P$，$h_i = h_3\left(m_i || \text{FID}_1^i || V_{\text{pub}_i} || U_i || T_j\right)$，$V_i = \text{SK}_1^i \text{FID}_2^i + b_i \text{QID}_i + h_i(x_i + b_i)$，签名为$\sigma_i = (U_i, V_i)$。$V_i$广播$\{m_i, \sigma_i, \text{QID}_i, \text{FID}^i, T_j\}$给RSUs。

(7) 验证

该阶段由RSUs执行。给定消息m_i上的签名σ_i，对应的车辆短期伪身份FID^i及其公钥V_{pub_i}，则任何验证者都可以验证签名。如果T_j不新鲜，伪身份的有效期T_i过期均丢弃信息并且停止操作。否则，计算$h_i = h_3\left(m_i || \text{FID}_1^i || V_{\text{pub}_i} || U_i || T_j\right)$和$W_i = \text{QID}_i \text{FID}_2^i K_{\text{pub}} + h_i V_{\text{pub}_i}$，如果式(1)成立，则RSUs接收$\left\{m_i, \sigma_i, \text{QID}_i, \text{FID}^i, T_j\right\}$

$$V_i P - (\text{QID}_i + h_i) U_i = W_i \tag{1}$$

正确性证明如下：

$$\begin{aligned}
&V_i P - (\text{QID}_i + h_i) U_i \\
&\quad = \left[\text{SK}_1^i \text{FID}_2^i + b_i \text{QID}_i + h_i(x_i + b_i)\right] \\
&\qquad \cdot P - (\text{QID}_i + h_i) U_i \\
&\quad = r_2 \text{QID}_i \text{FID}_2^i P + b_i \text{QID}_i P + h_i x_i P \\
&\qquad + h_i b_i P - (\text{QID}_i + h_i) U_i \\
&\quad = \text{QID}_i \text{FID}_2^i K_{\text{pub}} + U_i \text{QID}_i + h_i V_{\text{pub}_i} \\
&\qquad + h_i U_i - U_i \text{QID}_i - U_i h_i \\
&\quad = \text{QID}_i \text{FID}_2^i K_{\text{pub}} + h_i V_{\text{pub}_i} \\
&\quad = W_i
\end{aligned}$$

证毕

(8) 批量验证

RSUs 1次性验证1组签名，以降低每次验证1个签名时的计算复杂度。在IoV环境中，RSUs接收到来自不同载体的n个签名$(\sigma_i)\, i = 1, 2, \cdots, n$批量消息签名验证的步骤为：

首先判断每个签名的时间戳是否新鲜以及短期

伪身份的有效期是否失效，若两个条件有1个满足则终止验证。然后生成新鲜且有效的签名列表(σ_i) $i=1,2,\cdots,n'$。其次计算h_i=$h_3\left(m_i||\mathrm{FID}_1^i||V_{\mathrm{pub}_i}||U_i||T_j\right)$和$W_i=\mathrm{QID}_i\mathrm{FID}_2^iK_{\mathrm{pub}}+h_iV_{\mathrm{pub}_i}, i=1,2,\cdots,n'$，再判断式(2)是或否成立，若成立，则RSUs接收这组签名。

$$\sum_{i=1}^{n'}\left[V_iP-\left(\mathrm{QID}_i+h_i\right)U_i\right]=\sum_{i=1}^{n'}W_i \tag{2}$$

正确性证明如下：

$$\begin{aligned}
&\sum_{i=1}^{n'}\left[V_iP-\left(\mathrm{QID}_i+h_i\right)U_i\right]\\
&=\sum_{i=1}^{n'}\left[\mathrm{SK}_1^i\mathrm{FID}_2^i+b_i\mathrm{QID}_i+h_i\left(x_i+b_i\right)\right]P\\
&\quad-\sum_{i=1}^{n'}\left(\mathrm{QID}_i+h_i\right)U_i\\
&=\sum_{i=1}^{n'}r_2\mathrm{QID}_i\mathrm{FID}_2^iP+\sum_{i=1}^{n'}b_i\mathrm{QID}_iP+\sum_{i=1}^{n'}h_ix_iP\\
&\quad+\sum_{i=1}^{n'}h_ib_iP-\sum_{i=1}^{n'}\mathrm{QID}_iU_i-\sum_{i=1}^{n'}h_iU_i\\
&=\sum_{i=1}^{n'}\mathrm{QID}_i\mathrm{FID}_2^iK_{\mathrm{pub}}+\sum_{i=1}^{n'}U_i\mathrm{QID}_i+\sum_{i=1}^{n'}h_iV_{\mathrm{pub}_i}\\
&\quad+\sum_{i=1}^{n'}h_iU_i-\sum_{i=1}^{n'}\mathrm{QID}_iU_i-\sum_{i=1}^{n'}h_iU_i\\
&=\sum_{i=1}^{n'}\left[\mathrm{QID}_i\mathrm{FID}_2^iK_{\mathrm{pub}}+h_iV_{\mathrm{pub}_i}\right]\\
&=\sum_{i=1}^{n'}W_i
\end{aligned}$$

证毕

(9) 追踪与撤销

当发生恶意事件时，RTA通过计算

$$\mathrm{RID}_i=\mathrm{FID}_2^i\oplus h_2\left(\left\{r_1\mathrm{FID}_1^i\right\}_x||\mathrm{QID}_i||T_i\right) \tag{3}$$

来跟踪V_i的真实身份，并上报TA，当TA收到恶意车辆的真实身份时，将该身份从车辆的真实身份列表UL中删除，从而更新UL，并将更新后的UL发送给RTA与KGC。

正确性证明如下：

$$\begin{aligned}
\mathrm{RID}_i=&\mathrm{FID}_2^i\oplus h_2\left(\left\{r_1\mathrm{FID}_1^i\right\}_x||\mathrm{QID}_i||T_i\right)\\
=&\mathrm{RID}_i\oplus h_2\left(\left\{sT_{\mathrm{pub}}\right\}_x||\mathrm{QID}_i||T_i\right)\\
&\oplus h_2\left(\left\{r_1\mathrm{FID}_1^i\right\}_x||\mathrm{QID}_i||T_i\right)\\
=&\mathrm{RID}_i\oplus h_2\left(\left\{sr_1P\right\}_x||\mathrm{QID}_i||T_i\right)\\
&\oplus h_2\left(\left\{r_1sP\right\}_x||\mathrm{QID}_i||T_i\right)\\
=&\mathrm{RID}_i
\end{aligned}$$

证毕

5 安全性证明与分析

5.1 安全性证明

定理1 在基于椭圆曲线离散对数安全性假设(ECDLP)前提下，所提方案针对类型I的攻击者A1是存在性、不可伪造性以防止适应性选择消息攻击。

引理1 如果在随机预言机模型中存在一个类型I的敌手A1，他能够进行至多Q_{PPK}次部分私钥提取询问，Q_{PK}次公钥询问，$Q_i\,(i=1\sim3)$次哈希询问以及Q_σ次签名询问后伪造一个合法的签名，则ECDLP是可解的。

证明 挑战者算法C首先与敌手A1交互生成ECDLP问题的一个实例，给定$P,Q=aP$，其中$a\in Z_q^*,P\in G$。挑战者C的目标是求出a。

初始化阶段：挑战者C初始化系统参数$\{G,P,T_{\mathrm{pub}},K_{\mathrm{pub}}=Q,h_1(.),h_2(.),h_3(.)\}$，将系统参数发送给A1，C随机选取ID*作为游戏的挑战身份。敌手A1做以下询问。

询问阶段：敌手A1适应性地进行多项式有界的以下预言机询问。

h_1询问：当A1以(ID_i)向此预言机进行询问时，C通过列表$L_1=(\mathrm{ID}_i,h_1(I\mathrm{D}_i))$对A1与C之间的问答进行记录。如果C在$L_1$中查询到对应的$(\mathrm{ID}_i,h_1(\mathrm{ID}_i))$，C将$h_1(\mathrm{ID}_i)$返回给A1，否则C随机选取$h_1(\mathrm{ID}_i)\in Z_q^*$发送给A1，然后将$(\mathrm{ID}_i,h_1(\mathrm{ID}_i))$添加到列表$L_1$中。

h_2询问：当A1以$\left(\left\{sT_{\mathrm{pub}}\right\}_x,\mathrm{QID}_i,T_i\right)$向此预言机进行询问时，C通过列表$L_2=\left(\left\{sT_{\mathrm{pub}}\right\}_x,\mathrm{QID}_i,T_i,u_i\right)$对A1与C之间的问答进行记录。如果C在$L_2$中查询到对应的$\left(\left\{sT_{\mathrm{pub}}\right\}_x,\mathrm{QID}_i,T_i,u_i\right)$，C将$u_i$返回给A1，否则C随机选取$u_i\in Z_q^*$发送给A1，然后将$\left(\left\{sT_{\mathrm{pub}}\right\}_x,\mathrm{QID}_i,T_i,u_i\right)$添加到列表$L_2$中。

h_3询问：当A1以$\left(m_i,\mathrm{FID}_1^i,V_{\mathrm{pub}_i},U_i,T_j,\right)$向此预言机进行询问时，C通过列表$L_3=\left(m_i,\mathrm{FID}_1^i,V_{\mathrm{pub}_i},U_i,T_j,v_i\right)$对A1与C之间的问答进行记录。这里假定A1已经进行了公钥提取查询得到了V_{pub_i}，因此如果C在L_3中查询到对应的$\left(m_i,\mathrm{FID}_1^i,V_{\mathrm{pub}_i},U_i,T_j,v_i\right)$，C将$v_i$返回给A1，否则C随机选取$v_i\in Z_q^*$发送给A1，然后将$\left(m_i,\mathrm{FID}_1^i,V_{\mathrm{pub}_i},U_i,T_j,v_i\right)$添加到列表$L_3$中。

部分钥提取询问：当A1以QID_i向此预言机进行询问时，C通过列表$L_{\mathrm{par}}=\left(\mathrm{QID}_i,\mathrm{SK}_1^i\right)$对A1与C之间的问答进行记录。如果C在$L_{\mathrm{par}}$中查询到对应的$\left(\mathrm{QID}_i,\mathrm{SK}_1^i\right)$，C将$\mathrm{SK}_1^i$返回给A1，否则，如果$\mathrm{QID}_i\neq\mathrm{QID}^*$，C随机选取$\mathrm{SK}_1^i\in Z_q^*$，并将$\mathrm{SK}_1^i$发送给A1，然后将$\left(\mathrm{QID}_i,\mathrm{SK}_1^i\right)$保存到列表$L_{\mathrm{par}}$中。

公钥提取询问：当A1以QID_i向此预言机进行询问时，C通过列表$L_{\mathrm{pub}}=(\mathrm{QID}_i,x_i,V_{\mathrm{pub}_i})$对A1与C之间的问答进行记录。如果C在$L_{\mathrm{pub}}$中查询到对应的$(\mathrm{QID}_i,x_i,V_{\mathrm{pub}_i})$，C将$V_{\mathrm{pub}_i}$返回给A1，否则，如果$\mathrm{QID}_i\neq\mathrm{QID}^*$，C随机选取$x_i,b_i,s\in Z_q^*$，令$V_{\mathrm{pub}_i}=x_iP$，$U_i=b_iP$，$\mathrm{FID}_1^i=sP$，$h_3\left(m_i||\mathrm{FID}_1^i||V_{\mathrm{pub}_i}||U_i||T_j\right)$，并将$V_{\mathrm{pub}_i}$发送给A1，并将$(m_i,\mathrm{FID}_1^i,V_{\mathrm{pub}_i},U_i,T_j,)$和$(\mathrm{QID}_i,x_i,V_{\mathrm{pub}_i})$分别添加到$L_3$列表和$L_{\mathrm{pub}}$列表中。

秘密值提取询问：当A1以QID_i向此预言机进行询问时，如果$\mathrm{QID}_i=\mathrm{QID}^*$，C放弃并终止操作；否则C查找列表$L_{\mathrm{pub}}$，如果存在记录$(\mathrm{QID}_i,x_i,V_{\mathrm{pub}_i})$, C返回$x_i$给A1，如果不存在，C执行公钥询问生成元组$(x_i,V_{\mathrm{pub}_i})$，返回$x_i$给A1，并将$(x_i,V_{\mathrm{pub}_i})$添加到$L_{\mathrm{pub}}$列表中。

公钥替换询问：当A1以$(\mathrm{QID}_i,V_{\mathrm{pub}_i}')$向此预言机进行询问时，C首先从$L_{\mathrm{pub}}$中找到相应的记录$(\mathrm{QID}_i,x_i,V_{\mathrm{pub}_i})$，如果不存在，则对$\mathrm{QID}_i$进行公钥询问，将$V_{\mathrm{pub}_i}$替换成A1自由选取的$V_{\mathrm{pub}_i}'$，并令$x_i=\perp$。

签名询问：A1以(QID_i,m_i)向此预言机进行询问，C分别从列表$L_1,L_2,L_3,L_{\mathrm{par}},L_{\mathrm{pub}}$中恢复$h_1\left(\mathrm{QID}_i\right)$, $h_2\left(\{sT_{\mathrm{pub}}\}_x||\mathrm{QID}_i||T_i\right)$, $h_3\left(m_i||\mathrm{FID}_1^i||V_{\mathrm{pub}_i}||U_i||T_j\right)$，若$\mathrm{QID}_i\neq\mathrm{QID}^*$，则C输出消息$m_i$对应的签名$\sigma_i$，并将$\sigma_i$传给A1；否则，C随机选取$b_i\in Z_q^*$并计算$U_i=b_iP$，$h_i=h_3\left(m_i||\mathrm{FID}_1^i||V_{\mathrm{pub}_i}||U_i||T_j\right)$，$V_i=\mathrm{SK}_1^i\mathrm{FID}_2^i+b_i\mathrm{QID}_i+h_i\left(x_i+b_i\right)$。$\sigma_i=(U_i,V_i)$表示签名者对消息$m_i$的一个正确的签名。最后C将$\sigma_i$返回给A1。

伪造：最后A1输出一个伪造签名。若$\mathrm{QID}_i\neq\mathrm{QID}^*$，C停止模拟，否则C从预言机查询列表中找到相应的签名信息$\{m_i,\sigma_i,\mathrm{QID}_i,\mathrm{FID}^i,T_j\}$，若敌手A1赢得该游戏，则有：$V_iP-\left(\mathrm{QID}_i+h_i\right)U_i=\mathrm{QID}_i\mathrm{FID}_2^iK_{\mathrm{pub}}+h_iV_{\mathrm{pub}_i}$。再利用分叉引理[22]在多项式时间内得到另外2组有效的签名$\sigma_i{}^{(\ell)},(\ell=2,3)$，并且这3个签名都要满足$V_i{}^{(\ell)}P-\left(\mathrm{QID}_i+h_i\right)U_i{}^{(\ell)}=W_i$。又因为$V_{\mathrm{pub}_i}=x_iP$, $U_i=b_iP$, $K_{\mathrm{pub}}=aP$，所以有以下3个线性无关的方程组：

$$V_i{}^{(\ell)}-\left(\mathrm{QID}_i+h_i\right)b_i{}^{(\ell)}=\mathrm{QID}_i\mathrm{FID}_2^ia+h_ix_i,\ell=1,2,3。$$

挑战者C求解这3个方程的解，并将a输出作为ECDLP问题的解。　　证毕

定理2　在基于椭圆曲线离散对数安全性假设(ECDLP)前提下，所提方案针对类型II的攻击者A2是存在性、不可伪造性以防止适应性选择消息攻击。

证明思路与方法同定理1，但与定理1的证明不同的是A2仅有哈希值询问、公钥提取询问、秘密值询问、私钥提取询问、签名询问的能力，不具有公钥替换的能力，所以证明过程这里不再赘述。

5.2 安全性分析证明

(1) 消息认证性：RSUs或RSUs领域内的任何车辆都可以通过验证车辆的伪身份FID^i，并使用其签名σ_i来验证消息m_i。另外，该方案在ECDLP是困难的情况下，没有多项式时间的对手可以伪造有效的签名。

(2) 匿名性：在IoV环境中的车辆V_i使用其伪身份$\mathrm{FID}^i=\left(\mathrm{FID}_1^i,\mathrm{FID}_2^i,T_i\right)$发送消息$\{m_i,\sigma_i,\mathrm{QID}_i,\mathrm{FID}^i,T_j\}$，其中$\mathrm{FID}_1^i=sP$，$\mathrm{FID}_2^i=\mathrm{RID}_i\oplus h_2\left(\{sT_{\mathrm{pub}}\}_x||\mathrm{QID}_i||T_i\right)$，$T_i$为$\mathrm{FID}^i$的有效期。为了提取真实身份$\mathrm{RID}_i$，敌手应计算$\mathrm{FID}_2^i\oplus h_2\left(\{sT_{\mathrm{pub}}\}_x||\mathrm{QID}_i||T_i\right)$。显然，敌方不可能从$\mathrm{FID}_2^i$中计算车辆$V_i$的真实身份$\mathrm{RID}_i$。因此，该方案保证了车辆的隐私性。

(3) 可追踪性与可撤销性：当接收到来自车辆V_i的可疑消息$\{m_i,\sigma_i,\mathrm{QID}_i,\mathrm{FID}^i,T_j\}$时，RSUs验证伪身份并通过安全信道向TA发送$\{\mathrm{FID}^i,s\}$。TA通过式(3)$\mathrm{RID}_i=\mathrm{FID}_2^i\oplus h_2\left(\{sT_{\mathrm{pub}}\}_x||\mathrm{QID}_i||T_i\right)$来检索车辆的真实身份。因此，该方案实现了可追溯性与可撤销性。

(4) 不可链接性：在所提出的方案中，车辆V_i和RSUs随机选择t, s，以产生QID_i, FID^i。考虑到t，s的随机性，任何一个敌手不可能链接任何两类伪身份QID_i和FID^i。

(5) 前向安全性与后向安全性：在本文方案中，如果敌手获得了签名消息$\sigma_i=(U_i,V_i)$，其中$U_i=b_iP$, $V_i=\mathrm{SK}_1^i\mathrm{FID}_2^i+b_i\mathrm{QID}_i+h_i\left(x_i+b_i\right)$，因为$b_i$具有随机性，所以每次签名所选择的$b_i$是不同的，故地方无法通过当前的签名消息推断出之前或之后的签名消息。

(6) 抗各种类型攻击

(a) 重放攻击保护：车辆V_i发送的消息$\{m_i,\sigma_i,\mathrm{QID}_i,\mathrm{FID}^i,T_j\}$带有发送方的时间戳$T_j$。任何邻近车辆或RSUs可以通过检查$T_j$来验证消息的新鲜度。它防止在RSUs域中重复广播消息$\{m_i,\sigma_i,\mathrm{QID}_i,\mathrm{FID}^i,T_j\}$。因此，该方案可以防止重放攻击。

(b) 模拟攻击防护：为了实现模拟，敌方需要生成$\{m_i,\sigma_i,\mathrm{QID}_i,\mathrm{FID}^i,T_j\}$对消息$m_i$进行有效签名。然而，此操作在ECDLP假设下是不可能的。

(c) 中间人攻击保护：从ECDLP问题中，敌手显然不可能模拟一辆车，并生成$\{m_i,\sigma_i,\mathrm{QID}_i,\mathrm{FID}^i,T_j\}$，因此，该方案不易受到中间人攻击。

(d) 密钥托管弹性：在所提出的方案中，车辆V_i的私钥$\mathrm{SK}^i=\left(x_i,\mathrm{SK}_1^i\right)$包括由KGC计算的部分私钥$\mathrm{SK}_1^i$以及车辆$V_i$随机选择的$x_i$，因此，恶意的KGC在不知道$x_i$的情况下无法生成有效的签名。因此，所提出的方案不受密钥托管问题的影响。

6 性能分析

由于车辆间通信具有瞬时性特征，所以IoV系统对计算开销与通信开销的要求更为苛刻，因而本节对本文方案与文献[23–25]在计算开销、通信开销、功能与安全性方面进行了对比分析，主要涉及了签名阶段与验证阶段，其中，$T_{\mathrm{SM-G1}}$表示双线性变换后群上的点乘运算，$T_{\mathrm{SM-G}}$表示椭圆曲线上的点乘运算，T_{MTPH}表示映射到点的哈希运算，$T_{\mathrm{PA-G1}}$表示双线性群上的加法运算，T_{BP}表示对运算，T_{MM}表示模乘运算。

6.1 计算复杂度

在文献[23]中，用户在签名阶段需要执行4个双线性变换后群上的点乘运算、1个哈希T_{MTPH}和2个经双线性变换后群上的加法运算，即用户共需要$4T_{\mathrm{SM-G1}}+T_{\mathrm{MTPH}}+2T_{\mathrm{PA-G1}}$；RSUs在验证时需要执行3个经双线性变换后的群上的点乘运算、4个双线性对运算和2个映射到点的哈希函数，即RSUs共需要$4T_{\mathrm{BP}}+3T_{\mathrm{SM-G1}}+2T_{\mathrm{MTPH}}$。用同样的方法可以计算出文献[24,25]的计算开销，如表1所示。本文方案在签名过程中只需1个椭圆曲线上的点乘运算和两个模乘运算，即$T_{\mathrm{SM-G}}+2T_{\mathrm{MM}}$，在验证过程中需要执行3个椭圆曲线上的点乘运算，即$3T_{\mathrm{SM}}$。

表 1 计算运行时间对比

方案	签名	验证
文献[23]	$4T_{\mathrm{SM-G_1}}+T_{\mathrm{MTPH}}+2T_{\mathrm{PA-G_1}}$	$4T_{\mathrm{BP}}+3T_{\mathrm{SM-G_1}}+2T_{\mathrm{MTPH}}$
文献[24]	$4T_{\mathrm{SM-G_1}}$	$4T_{\mathrm{SM-G_1}}+2T_{\mathrm{BP}}$
文献[25]	$2T_{\mathrm{SM-G}}$	$5T_{\mathrm{SM-G}}+3T_{\mathrm{PA-G}}$
本文方案	$T_{\mathrm{SM-G}}+2T_{\mathrm{MM}}$	$3T_{\mathrm{SM-G}}$

由表1可知，本文方案中签名阶段不存在计算复杂度较大的双线性对运算，仅用到计算复杂度较小的点乘运算。方案建立在计算开销较小的椭圆曲线的基础上，与文献[23–25]在验证阶段均有一定的效率优势。本文仿真实验的环境为：Win10的操作系统、CPU主频为2.3 GHz、内存为4 GB的环境，采用Miracl库。图3和图4显示了本文方案与对比方案在签名和认证过程中批量认证的消息个数与所消耗时间(实验中取100 次的平均值)的关系，可以直观看到，随着n的增大，相比其他方案，本文方案更加高效。

6.2 通信复杂度

本文方案与文献[23–25]在部分私钥、公钥、伪身份的生成以及签名的通信量比较如表2所示。在Miracl库中循环群G上的元素占据32 Bytes，经过双线性变换后的群(G_1)的元素占据64 Bytes。假设椭圆曲线群G中的元素大小为40 Bytes，经过双线性变换后的群G_1中的元素大小为128 Bytes，整数域Z_q^*中的元素大小为20 Bytes。通过比较分析可以发现，本文方案在通信复杂度方面也存在一定的优势。

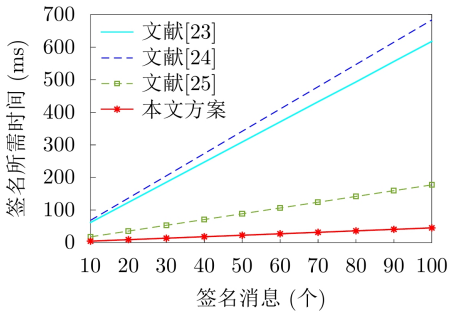

图 3 签名阶段计算复杂度比较

6.3 功能性

本文方案与文献[23–25]主要在消息的真实性、身份的可追踪性、匿名性、隐私性、不可链接性、

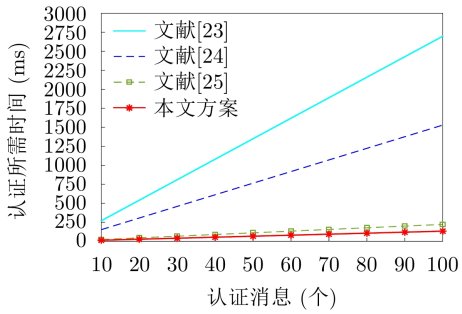

图 4 验证阶段计算复杂度比较

表 2 通信复杂度比较(Bytes)

方案	通信复杂度
文献[23]	532
文献[24]	208
文献[25]	244
本文方案	164

不可伪造性以及批验证和密钥托管弹性进行比较。如表3所示，本文方案与文献[23–25]相比提供了更好的安全性和功能性。

综合分析，本文在签名和验证阶段的计算复杂度均比其他3个方案小，虽然图3和图4表明文献[25]与本文方案相差不大，但文献[25]的通信开销相比较大，所以本文方案更适用于低时延和计算量低的车联网。

表 3　功能与安全性比较

方案	消息真实性	可追踪性	匿名性	身份隐私	不可链接性	不可伪造性	批验证	密钥托管弹性
文献[23]	√	√	√	×	√	√	×	×
文献[24]	√	√	√	√	√	√	×	×
文献[25]	√	√	√	√	√	√	√	√
本文方案	√	√	√	√	√	√	√	√

7　结论

为提高网络的可扩展性，本文提出了一种有效的不使用双线性对的无证书聚合签名方案。从而解决了以往传统认证方案中的密钥托管问题。RTA生成的长期伪身份和车辆自己生成的短期伪身份的相结合保证了车辆的强匿名性和签名的新鲜新；采用聚合无双线性对的方式进行签名和验证，随着节点数量的增加，大大减少了RSUs的验证时间，提高了网络的可扩展性；并且在发生恶意事件时，RTA可以追踪到车辆的真实身份并由TA撤销该用户。该方案具有完整性、隐私性、不可否认性、可追踪性、匿名性和撤销性等安全性。效率分析表明，本文方案的认证效率最高提升了95.06%，故该认证方案实现了计算效率高、速度快的车辆认证。因此，本文提出的方案对于动态可扩展网络中的车辆通信更加有效。车联网是一种使万物通信成为可能的自组织网络，因而接下来的工作是研究车联网环境下的跨域匿名认证方案。

参 考 文 献

[1] SUTRALA A K, BAGGA P, DAS A. K, *et al*. On the design of conditional privacy preserving batch verification-based authentication scheme for Internet of Vehicles deployment[J]. *IEEE Transactions on Vehicular Technology*, 2020, 69(5): 5535–5548. doi: 10.1109/TVT.2020.2981934.

[2] 谭富元. 车联网环境下高效安全认证方案的研究[D]. [硕士论文], 重庆邮电大学, 2018.
TAN Fuyuan. Research on efficient and secure authentication scheme in vehicular Ad-Hoc network[D]. [Master dissertation], Chongqing University of Posts and Telecommunications, 2018.

[3] LIN Xiaodong, SUN Xiaoting, HO P H, *et al*. GSIS: A secure and privacy-preserving protocol for vehicular communications[J]. *IEEE Transactions on Vehicular Technology*, 2007, 56(6): 3442–3456. doi: 10.1109/tvt.2007.906878.

[4] SUN Yipin, LU Rongxing, LIN Xiaodong, *et al*. An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications[J]. *IEEE Transactions on Vehicular Technology*, 2010, 59(7): 3589–3603. doi: 10.1109/tvt.2010.2051468.

[5] RAYA M and HUBAUX J P. Securing vehicular ad hoc networks[J]. *Journal of Computer Security*, 2007, 15(1): 39–68. doi: 10.3233/jcs-2007-15103.

[6] ZHANG Chenxi, LU Rongxing, LIN Xiongdong, *et al*. An efficient Identity-Based batch verification scheme for vehicular sensor networks[C]. IEEE INFOCOM 2008-The 27th Conference on Computer Communications, Phoenix, USA, 2008: 246–250.

[7] LO N W and TSAI J L. An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2016, 17(5): 1319–1328. doi: 10.1109/tits.2015.2502322.

[8] LIU Yawei, HE Zongjian, ZHAO Shengjie, *et al*. An efficient anonymous authentication protocol using batch operations for VANETs[J]. *Multimedia Tools and Applications*, 2016, 75(24): 17689–17709. doi: 10.1007/s11042-016-3614-9.

[9] WANG Yimin, ZHONG Hong, XU Yan, *et al*. Efficient extensible conditional privacy-preserving authentication scheme supporting batch verification for VANETs[J]. *Security and Communication Networks*, 2016, 9(18): 5460–5471. doi: 10.1002/sec.1710.

[10] TZENG S F, HORNG S J, LI Tianrui, *et al*. Enhancing security and privacy for identity-based batch verification scheme in VANETs[J]. *IEEE Transactions on Vehicular Technology*, 2017, 66(4): 3235–3248. doi: 10.1109/tvt.2015.2406877.

[11] HU Xiaoming, WANG Jian, XU Huajie, *et al*. Secure and Pairing-free Identity-based Batch Verification Scheme in

Vehicle Ad-hoc Networks[M]. HUANG Deshuang, HAN K, and HUSSAIN A. Intelligent Computing Methodologies. Cham: Springer, 2016: 11–20.

[12] GAMAGE C, GRAS B, CRISPO B, *et al*. An identity-based ring signature scheme with enhanced privacy[C]. 2006 Securecomm and Workshops, Baltimore, USA, 2006: 1–5. doi: 10.1109/seccomw.2006.359554.

[13] JIANG Shunrong, ZHU Xiaoyan, and WANG Liangmin. An efficient anonymous batch authentication scheme based on HMAC for VANETs[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2016, 17(8): 2193–2204. doi: 10.1109/tits.2016.2517603.

[14] SUN Jinyuan, ZHANG Chi, and FANG Yuguang. An ID-based framework achieving privacy and non-repudiation in vehicular ad hoc networks[C]. Proceedings of IEEE Military Communications Conference, Orlando, USA, 2007: 1–7. doi: 10.1109/milcom.2007.4454834.

[15] BAEK J, STEINFELD R, and ZHENG Yuliang. Formal proofs for the security of Signcryption[J]. *Journal of Cryptology*, 2007, 20(2): 203–235. doi: 10.1007/s00145-007-0211-0.

[16] AL-RIYAM S S and PATERSON K G. Certificateless public key cryptography[C]. The 9th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, China, 2003: 452–473.

[17] SONG Jun, ZHUANG Yanyan, PAN Jianping, *et al*. Certificateless secure upload for drive-thru internet[C]. 2011 IEEE International Conference on Communications (ICC), Kyoto, Japan, 2011: 1–6. doi: 10.1109/icc.2011.5962528.

[18] SONG Jun, HE Chunjiao, ZHANG Lei, *et al*. Toward an RSU-unavailable lightweight certificateless key agreement scheme for VANETs[J]. *China Communications*, 2014, 11(9): 93–103. doi: 10.1109/cc.2014.6969774.

[19] HORNG S J, TZENG S F, HUANG P H, *et al*. An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks[J]. *Information Sciences*, 2015, 317: 48–66. doi: 10.1016/j.ins.2015.04.033.

[20] 王大星, 滕济凯. 车载网中可证安全的无证书聚合签名算法[J]. 电子与信息学报, 2018, 40(1): 11–17. doi: 10.11999/JEIT170340.

WANG Daxing and TENG Jikai. Probably secure certificateless aggregate signature algorithm for vehicular Ad Hoc network[J]. *Journal of Electronics & Information Technology*, 2018, 40(1): 11–17. doi: 10.11999/JEIT170340.

[21] 杨小东, 麻婷春, 陈春霖, 等. 面向车载自组网的无证书聚合签名方案的安全性分析与改进[J]. 电子与信息学报, 2019, 41(5): 1265–1270. doi: 10.11999/JEIT180571.

YANG Xiaodong, MA Tingchun, CHEN Chunlin, *et al*. Security analysis and improvement of certificateless aggregate signature scheme for vehicular Ad Hoc network[J]. *Journal of Electronics & Information Technology*, 2019, 41(5): 1265–1270. doi: 10.11999/JEIT180571.

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

[23] KUMAR P, KUMARI S, SHARMA V, *et al*. Secure CLS and CL-AS schemes designed for VANETs[J]. *The Journal of Supercomputing*, 2019, 75(6): 3076–3098. doi: 10.1007/s11227-018-2312-y.

[24] JIANG Haobin, HUA Lei, and WAHAB L. SAES: A self-checking authentication scheme with higher efficiency and security for VANET[J]. *Peer-to-Peer Networking and Applications*, 2021, 14(2): 528–540. doi: 10.1007/s12083-020-00997-0.

[25] GAYATHRI N B, THUMBUR G, REDDY P V, *et al*. Efficient pairing-free certificateless authentication scheme with batch verification for vehicular Ad-hoc networks[J]. *IEEE Access*, 2018, 6: 31808–31819. doi: 10.1109/ACCESS.2018.2845464.

刘雪艳：女，1978年生，副教授，硕士生导师，研究方向为密码学与云计算中数据隐私保护.

王 力：女，1995年生，硕士生，研究方向为密码学与信息安全.

郇丽娟：女，1997年生，硕士生，研究方向为密码学与信息安全.

杜小妮：女，1972年生，教授，博士生导师，研究方向为密码学与信息安全.

牛淑芬：女，1976年生，副教授，硕士生导师，研究方向为密码学与信息安全.

责任编辑：马秀强