计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.200500116

车联网环境下基于区块链技术的条件隐私消息认证方案

熊　玲[1,2]　李发根[1]　刘志才[2]
1 电子科技大学计算机科学与工程学院(网络空间安全学院)　成都 611731
2 西华大学计算机与软件工程学院　成都 610039
(xiongling.swjtu@aliyun.com)

摘　要　随着网络与信息技术的飞速发展,车联网作为实现自动驾驶乃至无人驾驶的重要组成部分,是未来智能交通系统的核心模块。因此,车联网环境中的安全和条件隐私问题成为亟待解决的研究热点问题。然而,当前车联网环境中的大多数条件隐私消息认证方案不能很好地解决数据跨域通信问题。区块链技术的去中心化和不可伪造性等优良特性为车联网环境中的跨域通信问题提供了一个可行的解决方案,但是目前车联网环境中基于区块链技术的消息认证方案还存在不可链接性问题。为了解决这一问题,文中基于物理不可克隆函数和区块链技术设计了一个适用于车联网环境的具有条件隐私的轻量级消息认证方案。该方案能够提供消息认证、消息完整性、匿名、不可链接性以及可追踪性等安全属性。

关键词:车联网;条件隐私;认证;区块链;物理不可克隆函数
中图法分类号　TP391

Conditional Privacy-preserving Authentication Scheme Based on Blockchain for Vehicular Ad Hoc Networks

XIONG Ling[1,2],LI Fa-gen[1] and LIU Zhi-cai[2]
1 School of Computer Science and Engineering(School of Cyberspace Security),University of Electronic Science and Technology of China,Chengdu 611731,China
2 School of Computer and Software Engineering,Xihua University,Chengdu 610039,China

Abstract　With the rapid development of network and information techniques,as an important part of automatic driving,the vehicular ad hoc networks are the core module of the future intelligent transportation system. As a result,the security and conditional privacy of the vehicular ad hoc networks (VANET) has become an urgent research hotspot. However,most of the current conditional privacy-preserving authentication schemes for VANET environment suffer from the problem of cross-datacenter authentication. To the best of our knowledge,blockchain technology has lots of advantages like decentralized and unforgeability bringing a promising solution to this problem compared with the traditional cryptography technologies. However,the current message authentication schemes based on blockchain technology for VANET environment cannot provide unlinkability. To address this issue,this paper designs a lightweight conditional privacy-preserving authentication scheme for VANET environment using physically unclonable function and blockchain technology,which can provide message authentication,integrity,identity privacy preserving,unlinkability and traceability.

Keywords　Vehicular ad hoc networks,Conditional privacy,Authentication,Blockchain,Physically unclonable function

1　引言

1.1　研究背景

车联网通过人、车、路的和谐密切配合来提高交通运输效率,缓解交通阻塞,提高路网通过能力,减少交通事故。车联网系统一般包括车辆管理中心、道路基础设施以及车辆设备。为了保障车辆的行驶安全,车辆在行驶过程中,车载设备需要将交通信息实时地广播给附近的车辆或道路基础设施,如交通拥堵和交通信号等信息[1]。

由于车联网系统通常是在无线网络环境下运行,恶意攻击者很容易截获、插入、删除和修改传输的信息。为了确保车辆或道路基础设施收到的消息是合法的,需要对车联网中的消息进行认证和完整性保护。此外,如果车辆的标识信息在通信过程中泄露,车辆的位置、运行轨迹等隐私信息就可能会暴露,从而被攻击者利用并进行破坏。因此需要对车辆的标识信息进行保护,防止攻击者识别和追踪该车辆。同时,若恶意的车辆为了自己的利益而发送一个伪造的交通信息,车辆管理中心应能迅速地追踪到恶意车辆[1-3]。我们把这种在车

到稿日期:2020-05-25　返修日期:2020-08-15　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:中国博士后面上基金(2019M663475);四川省科技厅项目(2020JDRC0100)
This work was supported by the China Postdoctoral Science Foundation (2019M663475) and Science and Technology Fund of Sichuan Province (2020JDRC0100).
通信作者:李发根(fagenli@uestc.edu.cn)

辆通信过程中保护车辆的隐私，同时在车辆违法时追踪车辆的安全属性称为条件隐私。因此，安全和条件隐私问题成为车联网中最重要和棘手的课题，受到了各国政府、高校和研究机构的高度重视。

为了解决车联网中的安全和条件隐私问题，学者们设计了一系列适用于车联网环境中的条件隐私认证方案(如文献[1-3])。这些方案有效地解决了车联网环境中的各种安全和隐私问题，但是对于车辆的跨数据中心的问题并没有给出有效的解决方法。然而，传统的跨域技术并不适用于高度移动的车联网系统，区块链技术与生俱来的去中心化和不可伪造性等优良特性为车联网上跨域管理提供了一个可行的解决方案。最近，Yao 等[4]基于区块链技术设计了一个适用于车联网环境的轻量级匿名认证方案，该方案可以有效地解决车辆的跨数据中心问题。但是该方案没有考虑车辆通信消息的不可链接性，当车辆进入不同的边缘设备管理区域时，使用的是静态的假名，攻击者可以根据静态的假名追踪车辆，从而导致用户的隐私泄露。为了解决这个问题，我们利用物理不可克隆函数和区块链技术设计了一个适用于车联网环境的轻量级的条件隐私消息认证方案。

1.2 研究现状

当前，车联网环境下的隐私保护方案按照采用的密码技术主要分为 5 类：基于伪随机证书技术、基于群签名技术、基于身份的签名技术、基于对称密码技术以及混合密码技术(如伪随机证书和对称技术混合使用)。目前，已有一系列适用于车联网环境的具有隐私保护特性的认证方案。例如，2015 年，He 等[1]基于双线性对设计了具有隐私保护特性的认证方案，该方案能够进行批验证，其安全性在车辆中的通信设备(Tamper-Proof Device，TPD)是安全的情况下成立，需要保证存储在 TPD 中的密钥不会泄露。接着，Lo 等[2]设计的新方案没有强依赖 TPD，但该方案需要存储大量的秘密参数。Zhang 等[3]基于一次性的聚合签名技术提出了认证方案，该方案是 He 等[1]和 Lo 等[2]方案的折中，然而其在通信时需要一个可信的第三方参与认证，由于车联网环境中车辆较多，这给可信第三方增加了大量的计算和通信代价。最近，Liu 等[5]在 Zhang 等[3]方案的基础上设计了新的条件隐私方案，该方案避免了每次认证消息时都需要可信第三方参与。以上方案有效地解决了车联网环境中的各种安全问题，但是它们在解决车辆跨数据中心的问题时并没有太大优势。文献[3]的方案甚至在每次车辆通信时都需要与注册的车辆管理中心通信，若车辆进入其他车辆管理中心的管理区域，还需要两个区域的车辆管理中心进行额外的通信。显然，传统的集中式认证方式已经不能满足日益增长的跨域通信需求。

区块链技术为上述问题提供了可行的解决方法。目前已经有多个方案利用区块链技术来解决车联网环境中的安全问题。例如，Kang 等[6]利用联盟链解决了车联网数据的安全存储和共享；Li 等[7]基于区块链技术设计了一个保护乘客隐私的拼车方案。但这两个方案并没有考虑车辆的跨域通信问题。2019 年，Yao 等[4]基于区块链技术设计了一个解决车联网环境中跨域问题的匿名认证方案，该方案可以达到用户匿名、消息认证、消息完整性等安全需求。由于该方案利用区块链存放车辆的临时公钥、假名和身份标识等信息，车辆再次发送消息时，接收者通过假名访问区块链获得该车辆的临时公钥，由于认证过后车辆每次与边缘设备通信时都使用该假名，而假名是静态的，使得该方案不能达到不可链接性。最近，Wazid 等[8]利用雾计算设计了一个适用于车联网环境的轻量级认证密钥协商协议，但是该方案并不能解决轻量级密码协议存在的一些安全问题[9-10]，如去同步攻击。

1.3 本文贡献

为了解决上述问题，本文基于物理不可克隆函数和区块链技术，设计了适用于车联网环境的具有条件隐私的消息认证方案。本文的具体贡献如下：

(1)结合物理不可克隆函数和区块链技术的优势，设计了具有条件隐私的消息认证方案。新方案能够抵抗车辆设备秘密信息的泄露攻击，即使攻击者获取了车辆设备中的秘密信息，仍然无法假冒合法的车辆发送信息。

(2)所提方案能够有效地解决车辆跨域通信问题，车辆进入另一个车辆管理中心的管理区域时，不需要车辆管理中心之间进行额外的通信。此外，车辆在每次消息认证过程中不需要与车辆管理中心通信。

(3)所提方案能够提供消息认证、消息完整性、匿名等安全属性。此外，该方案在注册时预存了一系列假名，每次发送消息使用未用的假名，从而解决了 Yao 等[4]方案中存在的不可链接性问题。

2 预备知识

2.1 区块链技术

区块链是一组数据区块按照时间顺序排列的数据结构，以密码学方式保证的不可篡改和不可伪造的去中心化共享账本[11]。本文以车联网环境中的各个边缘设备和车辆管理中心为区块链网络的节点，建立一个去中心化的联盟链。如表 1 所列，联盟链维护两个列表，一个是未使用列表，该表在车辆注册时由车辆管理中心发送到区块链网络中；另一个是已使用列表，该表由消息验证过程中车辆所在区域的边缘设备发送到区块链网络中。联盟链中的各个网络节点可以访问并读取这两个表。该区块链的共识算法采用广泛使用的 PoS 共识算法[12]。

表 1 区块链的两个列表

Table 1 Two lists of blockchain

未使用列表	已使用列表
AID_1, R_1	AID_1
AID_2, R_2	AID_2
AID_3, R_3	
AID_4, R_4	⋮
⋮	

2.2 物理不可克隆函数

物理不可克隆函数(Physically Unclonable Function，PUF)利用每颗芯片制造时的偏差产生不可预知的、独一无二的、且无法克隆的电子指纹[13-14]。PUF 采用挑战应答模式，假设 PUF 的挑战为 C，响应为 R，则 $R=PUF_D(C)$。一个理想的 PUF 函数具有以下属性：

(1)响应值不可预测，其取决于芯片的制造差异。

(2)不可能产生两个完全相同的芯片电子指纹。

(3)对于相同的挑战，不同芯片的 PUF 的响应是不一致的。

(4)对于同一个芯片的 PUF，由于存在噪声，相同的挑战

产生的响应并不完全相同。

2.3　模糊提取技术

模糊提取由两个算法组成：密钥生成 FE. Gen()和密钥恢复 FE. Rep()[15-16]。FE. Gen()是概率性的密钥生成算法，在本文方案中，FE. Gen()的输入为车辆设备中 PUF 的响应值 R，输出为密钥 key 和辅助数据 hd，即 $(key, hd) = FE.Gen(R)$。$FE.Rep()$是确定性的密钥恢复算法，其输入是具有噪声的 R'和辅助数据 hd，即 $key' = FE.Rep(R', hd)$。在 R 和 R'的汉明距离足够小的情况下，key 和 key'是相等的，辅助数据可以不用加密，而响应值 R 和 R'必须保密[8-9]。

3　系统模型与假设

3.1　系统模型

如图 1 所示，本文的车联网系统由车载设备(On-board-units，OBUs)、道路交通基础设施(Road-side-units，RSUs)、边缘设备(Edge Devices，EDs)和车辆管理中心(Trust Authority，TRA)组成。TRA 是一个可信的管理中心，负责车辆和 RSUs 的管理。OBUs 是安装在车辆上负责处理车辆终端的感知、计算和通信任务的设备，其上安装有 PUF 的芯片，具有不可克隆性。RSUs 是固定在路边的公共基础设施，负责连接车辆和 TRA。EDs 为车辆提供即时快速的处理。各个区域的边缘设备和 TRA 作为区块链的节点，共同组成区块链网络，参与车辆和道路交通基础设施之间的通信。

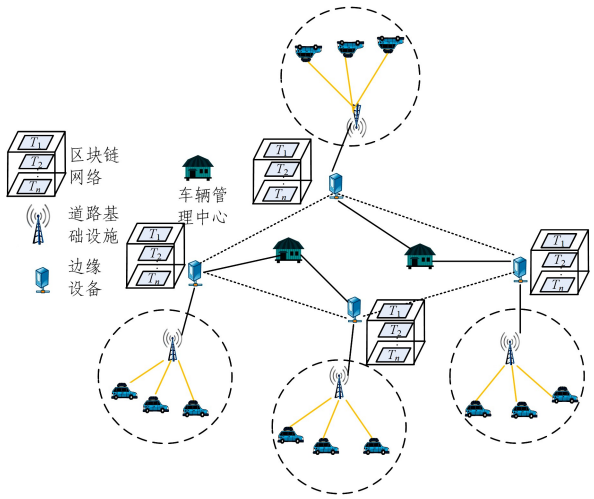


图 1　车联网系统框图

Fig. 1　System framework for Vehicular ad hoc networks

3.2　攻击能力

假设 A 是一个概率多项式时间攻击者，A 的攻击目标为成功伪造车辆 OBU_i 发送消息。A 的攻击能力如下：

(1)A 能够控制信道中传输的消息，并能截获、删除、插入该消息，同时攻击者具有伪造消息攻击、重放攻击、窃听攻击、车辆追踪、消息否认、篡改攻击、拒绝服务攻击等能力。

(2)A 可以是车联网系统中一辆合法的车辆。

3.3　安全需求

由于车联网运行在无线网络环境中，车联网环境需要更高的安全要求，具体如下。

(1)消息认证：消息接收者能够验证收到消息的合法性。

(2)消息完整性：接收者收到消息后能确认消息是否被篡改过。

(3)车辆匿名：攻击者 A 不能从信道中传输的消息确定车辆的标识信息。

(4)不可链接性：攻击者 A 不能确定多条消息是否是由同一车辆发出的。

(5)可追踪性：车辆发出违法的消息后，车辆管理中心应能追踪到。

4　本文方案

在介绍本文方案之前，首先对本文方案所使用的符号进行定义，具体如表 2 所列。

表 2　符号定义

Table 2　Definition of notations

符号	定义
OBU_i	安装在车辆上负责处理消息的设备
Ed_i	边缘设备
PUF_{Vi}	安装在 OBU_i 上的 PUF 函数
ID_{Vi}	车辆的唯一的标识
$h_{key}(x)$	对消息 x 进行带密钥的 hash 运算
‖	连接符号

4.1　车辆注册阶段

当车辆 OBU_i 想要与边缘设备 EDs 通信时，必须先向 TRA 申请注册，具体注册过程如下：

(1)TRA 选择 n 个随机数 $C_1, C_2, \cdots, C_n$，构成挑战集合 $C = \{C_1, C_2, \cdots, C_n\}$，将 C 发送给 OBU_i。

(2)收到 C 后，OBU_i 计算 $R_i = PUF_{Vi}(C_i)$，得到 $R = \{R_1, R_2, \cdots, R_n\}$，将 R 通过安全信道发送给 TRA。

(3)TRA 收到 R 后，为 $R_i(1 \leqslant i \leqslant n)$生成一个假名 AID_i，得到 $AID = \{AID_1, AID_2, \cdots, AID_n\}$。将$\{ID_{Vi}, AID, R\}$存储于安全存储区，然后将$\{AID, R\}$发送到区块链网络，由 Pos 共识算法写入未使用列表，最后发送 AID 给 OBU_i。

(4)OBU_i 收到 AID 后，将其与对应的 C 存储于安全存储区。

4.2　消息签名阶段

当车辆进入某个 Ed_i 的管理区域时，需要发送消息 M 给 Ed_i，具体的消息签名过程如下：

(1)OBU_i 选择一个未使用过的 AID_i 和对应的 C_i，计算 $R_i' = PUF_{Vi}(C_i)$，$(key, hd) = FE.Gen(R_i')$，$\sigma = h_{key}(M \| AID_i)$。

(2)OBU_i 将$\{AID_i, M, hd, \sigma\}$发送给 Ed_i。

4.3　消息验证阶段

当 Ed_i 收到签名消息后，需要验证 M 的合法性，具体验证过程如下：

(1)Ed_i 检查 AID_i 是否在区块链的已使用列表里，若在，则终止协议；否则继续以下步骤。

(2)Ed_i 根据 AID_i 在区块链的未使用列表里搜索得到 R_i，计算 $key = FE.Rep(hd, R_i)$，$\sigma' = h_{key}(M \| AID_i)$。判断 σ'与收到的 σ 是否相等，如果相等，则验证成功，Ed_i 将 AID_i 发送到区块链网络，区块链网络由 Pos 共识算法将其写入已使用列表；否则，消息验证失败。

5　安全性分析

5.1　形式化分析

5.1.1　攻击模型

本节在文献[15-16]的基础上建立新方案的安全模型。

假定车辆 OBU_i 和边缘设备 Ed_i 之间有概率多项式时间攻击者 A，该模型定义为 A 和挑战者 ζ 的游戏，$OBU_i \in V$，$Ed_i \in E$，V 为车辆集合，E 为边缘设备集合，$\Pi_{V,s}$ 为车辆预言机，用于会话 s 中与边缘设备交互，$\Pi_{E,s}$ 为边缘设备预言机，用于会话 s 中与车辆交互，则 A 可以进行如下询问：

Execute(V,E)：该询问模拟 A 的被动攻击能力，即 A 能够截获车辆和边缘设备之间的通信消息。

Send(P,s,V′,M)：该询问模拟 A 的主动攻击，A 假冒 V′发送消息 M 给预言机 $\Pi_{P,s}$，$\Pi_{P,s}$ 按照协议的规定将结果返回给 A。如 P′和 M 为空，则表示车辆发起一个新的会话。

Reveal(Sid)：该询问模拟合法的恶意的车辆攻击。

需要注意的是，可以多次询问 *Execute* 和 *Send* 预言机，但只能询问一次 *Reveal* 预言机。

5.1.2 安全假设

(1)不可克隆假设：记不可克隆函数 PUF：$\{0,1\}^{l_1} \rightarrow \{0,1\}^{l_2}$，其中 l_1 是输入挑战值的比特长度，l_2 是输出响应值的比特长。若没有物理设备已知挑战值，则计算响应值是非常困难的。PUF 的安全性可以定义为下面的挑战响应游戏：

阶段 1 A 随机选择一个挑战值 C_i，并且收到其响应值 $R_i = PUF(C_i)$。

挑战：A 选择一个没有被询问过的挑战值 C_x。

阶段 2 A 能够继续询问 PUF 获得更多的挑战响应值(注：不包括要挑战的挑战值)。

响应：A 在不知道物理设备的情况下，输出响应值 $R_i' = PUF(C_i)$。

如果 A 赢得游戏，则 A 可以成功伪造一个 R_i'，使得 $R_i' = R_i$。

(2)消息认证函数假设：一个消息认证函数定义为 $h:\{0,1\}^k \times \{0,1\}^* \rightarrow \{0,1\}^{k'}$，输入为长度 k 比特的密钥 $key \in \{0,1\}^k$ 和任意长度的消息 $M \in \{0,1\}^*$，输出为固定长度的比特串 σ，记作 $\sigma = h_{key}(M)$。在训练阶段，攻击者 A 可以多次询问 h 函数，并得到其输出值 σ。然后，挑战者随意选择一个消息认证输出值 σ 或随机数，A 要成功区分该值是消息输出值还是随机数是非常困难的，即 A 猜测的概率大约为 $1/2+\varepsilon$，ε 是可以忽略的，则称该消息认证函数是理想的。

5.1.3 安全性分析

引理 1 本文方案中，即使攻击者 A 询问了 Reveal 预言机，车辆设备中的秘密值也不会被泄露。

证明：本文方案中，合法车辆的秘密值 key 是由 $R_i' = PUF_{Vi}(C_i)$，$(key,hd) = FE.Gen(R_i')$ 计算得到的。显然，没有秘密信息 R_i'，无法计算得到 key，而 R_i' 值是 C_i 经过 PUF 计算得到的。A 询问了 Reveal 预言机后，可以得到 $AID = \{AID_1, AID_2, \cdots, AID_n\}$ 和 $C = \{C_1, C_2, \cdots, C_n\}$，由不可克隆函数的假设可以得到，即使 A 已经获得了不可克隆函数的响应值 C_i，在没有物理设备 PUF_{Vi} 的情况下，A 计算响应值 R_i' 是非常困难的。

引理 2 在没有询问 Reveal 预言机的条件下，本文方案的假名具有不可链接性。

证明：本文方案利用假名替代车辆的真实标识在信道中传输。由于假名是随机选择的独立的随机数，每个假名之间是不可关联的。这一系列假名预存于车辆设备的存储区，且每个假名只用一次，每次通信时使用一个，使用后记录在区块链的已使用列表中，下次不再使用。因此攻击者 A 不询问 Reveal 预言机是无法链接每个假名的。

定理 1 假设 PUF 函数是不可克隆的，消息认证函数值是理想的，则本文方案可提供消息认证。

证明：攻击者 A 试图伪造一个合法车辆消息的认证，可以将该攻击定义为下列的挑战者 ζ 和 A 之间的游戏：

(1)ζ 选择一个合法的车辆 OBU_i。

(2)A 可以多次询问 Execute 和 Send 预言机，询问完后，A 通知 ζ。

(3)A 发起 Send，预言机伪造 OBU_i。

(4)如果 ζ 认证成功，则 A 赢得了游戏。

为了成功认证，A 必须获得有效的 AID_i 和对应的 R_i'，然而根据引理 1 可知，即使 A 询问了 Reveal 预言机，仍然无法推算出 R_i'，因此不能计算出有效的 $(key,hd) = FE.Gen(R_i')$ 使得 $\sigma = h_{key}(M||AID_i)$。综上所述，本文方案中，只有合法的车辆才能够计算出消息 M 的合法消息认证值。

定理 2 本文方案中的车辆发送的消息是不可链接的。

证明：在车联网系统中，为了保护用户的隐私，通常需要车辆发送的信息是不可链接的。如果攻击者 A 能够确定多条消息是从某一车辆发出的，则认为 A 能成功追踪车辆。该攻击可以定义为下列的挑战者 ζ 和 A 之间的游戏：

(1)ζ 选择两个合法的车辆 OBU_0 和 OBU_1。

(2)A 可以多次询问 Execute 和 Send 预言机，询问完后，A 通知 ζ。

(3)A 随机地选择一个车辆 OBU_i，$i \in \{0,1\}$。

(4)A 可再次询问 Execute 和 Send 预言机。

(5)A 猜测 i 的值为 b，如果 $b=i$，则 A 赢得游戏。

记 A 猜测成功概率为 $Pr[b=i]$，则猜测成功的优势为 $\varepsilon = Pr[b=i] - 1/2$。由引理 2 可知，$A$ 在没有询问 Reveal 预言机的条件下，本文方案的假名具有不可链接性，因此，A 猜测正确的优势 ε 是可以忽略的。

5.2 非形式化分析

5.2.1 消息认证

本文方案利用带密钥的 hash 函数实现消息认证，hash 函数的密钥 key 由 PUF 的响应值 R_i' 确定，与响应值 R_i' 的汉明距离足够小的响应值 R_i 存于区块链的未使用列表中，边缘设备收到消息后，可以通过访问区块链获取到 R_i，从而恢复密钥 key。由于仅车辆设备和区块链拥有 R_i，任何第三方无法获取密钥，因此验证者验证消息成功后，消息一定是合法的消息。

5.2.2 完整性

本文方案利用带密钥的 hash 函数实现消息的完整性，若消息 M 在信道中被修改，则响应的带密钥的 hash 值也需要相应地改变。由于任何第三方没有正确的 R_i，无法获取密钥，因此其无法获得消息的带密钥的 hash 值。

5.2.3 车辆匿名

本文方案使用假名替代车辆的真实标来实现车辆匿名，每个假名是随机生成的随机数，与车辆的真实标识信息是独

立的、不相关的，因此攻击者获得假名后，无法由其推算出车辆的真实标识，从而实现车辆匿名。

5.2.4　不可链接性

本文方案使用假名来解决车辆信息不可链接性问题，车辆每次发送消息时都使用一个未使用过的合法的假名，边缘设备验证成功后，将该假名存储于区块链上已经使用的表中。由定理 2 可得，本文方案能够提供不可链接性。

5.2.5　可追踪性

当车辆发送违法信息后，可以在区块链上找出该消息对应的假名，由于车辆在注册时，TRA 存储了用户假名和真实用户信息，当需要追踪时，TRA 可根据数据库中存储的假名搜索到车辆的真实信息。

5.3　安全功能对比

表 3 将本文方案与 Yao 等[4]的方案进行安全功能对比，结果表明本文方案可抵抗上述所有攻击。

表 3　安全功能对比结果

Table 3　Comparison results of security features

安全特征	Yao 等[4]	本文方案
消息认证	是	是
完整性	是	是
匿名	是	是
不可链接性	否	是
可追踪性	是	是

本文首先总结了当前车联网环境中的消息通信协议所面临的跨域问题，区块链为解决该问题提供了可行的方法。然而 Yao 等[4]基于区块链技术设计的方案不能达到不可链接性，从而不能实现真正的条件隐私。为了解决该问题，本文基于不可克隆函数和区块链技术，设计了一个适用于车联网环境的具有条件隐私的消息认证方案。该方案能够满足车联网环境下的多种安全需求，同时能抵抗多种现有的攻击。目前，本文方案采用假名技术实现不可链接性，这需要车辆设备预先存储一个假名集合和对应的挑战值集合，如果假名使用完毕，车辆需要重新申请注册。我们下一步将研究不需要预先存储假名，同时又可实现不可链接性的轻量级条件隐私消息认证方案。

参 考 文 献

[1] HE D, ZEADALLY S, XU B, et al. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks[J]. IEEE Trans. Inf. Forensics Security, 2015, 10(12): 2681-2691.

[2] LO N, TSAI J. An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings[J]. IEEE Trans. Intell. Transp. Syst., 2016, 17(5): 1319-1328.

[3] ZHANG L, WU Q, DOMINGO J, et al. Distributed aggregate privacy-preserving authentication in VANETs[J]. IEEE Trans. Intell. Transp. Syst., 2017, 18(3): 516-526.

[4] YAO Y, CHANG X, MISIC J, et al. BLA: Blockchain-Assisted Lightweight Anonymous Authentication for Distributed Vehicular Fog Services[J]. IEEE Internet of Things Journal, 2019, 6(2): 3775-3784.

[5] LIU Z, XIONG L, PENG T, et al. A Realistic Distributed Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks[J]. IEEE Access, 2018, 6: 26307-26317.

[6] KANG J, YU R, HUANG X, et al. Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks[J]. IEEE Internet of Things Journal, 2019, 6(3): 4660-4670.

[7] LI M, ZHU L, LIN X. Efficient and Privacy-Preserving Carpooling Using Blockchain-Assisted Vehicular Fog Computing[J]. IEEE Internet of Things Journal, 2019, 6(3): 4573-4584.

[8] WAZID M, BAGGA P, DAS A, et al. AKM-IoV: Authenticated Key Management Protocol in Fog Computing-Based Internet of Vehicles Deployment[J]. IEEE Internet of Things Journal, 2019, 6(5): 8804-8817.

[9] WANG D, WANG P. Two Birds with One Stone: Two-Factor Authentication with Security Beyond Conventional Bound[J]. IEEE Trans. Dependable Secur. Comput., 2018, 15(4): 708-722.

[10] WANG D, WANG N, WANG P, et al. Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity[J]. Information Sciences, 2015, 321: 162-178.

[11] ZHOU C, LU H, XIANG Y, et al. Survey on Application of Block chain in VANET[J]. Computer Science, 2020, 47(2): 213-220.

[12] KIAYIAS A, RUSSELL A, DAVID B, et al. Ouroboros: A provably secure proof-of-stake blockchain protocol[C]// Annual International Cryptology Conference. 2017: 357-388.

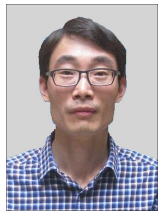
[13] AYSU A, GULCAN E, MORIYAMA D, et al. End-to-end Design of a PUF-based Privacy Preserving Authentication Protocol [C]// The annual Conference on Cryptographic Hardware and Embedded Systems. 2015: 556-576.

[14] DELVAUX J, GU D, VERBAUWHEDE I, et al. Efficient Fuzzy Extraction of PUF-Induced Secrets: Theory and Applications [C]// The annual Conference on Cryptographic Hardware and Embedded Systems. 2016: 412-431.

[15] GOPE P, LEE J, QUEK T. Lightweight and Practical Anonymous Authentication Protocol for RFID Systems Using Physically Unclonable Functions[J]. IEEE Trans. Information Forensics and Security, 2018, 3(11): 2831-2843.

[16] GOPE P, SIKDAR B. Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices[J]. IEEE Internet of Things Journal, 2019, 6(1): 580-589.

XIONG Ling, born in 1983, Ph.D, is a member of China Computer Federation. Her main research interests include authentication protocol and blockchain.



LI Fa-gen, born in 1979, Ph.D, professor, Ph.D supervisor, is a member of IEEE. His main research interests include cryptography and network security.