基于物理不可克隆函数的轻量级可证明安全车联网认证协议

夏卓群[①] 苏 潮[①] 徐梓桑*[①] 龙科军[②]
[①](长沙理工大学计算机与通信工程学院 长沙 4100150)
[②](智能道路与车路协同湖南省重点实验室 长沙 410015)

摘 要：车联网(IoVs)广泛用于获取车辆和道路状况等信息，但是这些信息都是在公共信道中进行传输，所以最重要和关键的要求之一就是在严格延迟要求下的数据安全。其中，认证是解决数据安全最常用的方法，但是由于车联网的资源受限和对延迟敏感等特点，车辆认证需要在一定的消耗和延迟内完成。然而，现有方案容易遭受物理、伪造和共谋等攻击，同时也产生了昂贵的通信和计算成本。该文提出一种基于物理不可克隆函数(PUF)的车路云协同轻量级安全认证方案。所提议方案采用轻量级的物理不可克隆函数作为车联网实体的信任保证，抵御攻击者对实体的物理和共谋等攻击；采用车路云协同的架构，在经过可信机构(TA)认证的路边单元(RSU)上完成认证运算，大大减轻了TA的计算压力，并将挑战响应对(CRPs)的更新应用到假名的构造更新中，保护身份和轨迹隐私的同时也能在身份追踪阶段披露恶意车辆身份。在实际场景的模拟实验中，通过与其它方案进行比较，表明该方案更加安全和高效。

关键词：车联网；认证协议；隐私保护；物理不可克隆函数；车路云协同
中图分类号：TN915.08; TN918.4 **文献标识码**：A **文章编号**：1009-5896(2024)09-3788-09
DOI: 10.11999/JEIT240141

A Lightweight and Provably Secure Authentication Protocol for Internet of Vehicles Using Physical Unclonable Function

XIA Zhuoqun[①] SU Chao[①] XU Zisang[①] LONG Kejun[②]
[①](*School of Computer and Communication Engineering, Changsha University of Science and Technology Changsha, Changsha* 410015, *China*)
[②](*Hunan Key Laboratory of Smart Roadway and Cooperative Vehicle-Infrastructure Systems, Changsha* 410014, *China*)

Abstract: The Internet of Vehicles (IoVs) is widely used to obtain information about vehicles and road conditions, which is transmitted in public channels. Hence, the most important requirement is the data security. Because of characters of IoVs, we need to make it keep in a strict delay. Authentication is a common method to solve it. Due to limited resources and delay sensitivity of IoVs, vehicles must complete authentication within appropriate resources cost and delay. However, existing schemes are prone to physical, forgery and collusion attacks, and moreover, they are computationally heavy. Therefore, a lightweight security identity authentication scheme for vehicle-road collaboration is proposed in this paper, which utilizes lightweight Physical Unclonable Function (PUF) as the trust root of entities to resist physical and collusion attacks; Besides, most of computations are offloaded to Road Side Units (RSUs) certified by Trusted Authority (TA) through the vehicle-road-cloud collaboration architecture; In addition, vehicular pseudonym construction and update include Challenge-Response Pairs (CRPs), which are utilized to protect identity and trajectory privacy and expose malicious vehicular identities in identity tracking phase. Furthermore, there are formal and informal security analyses to prove our scheme is secure. Finally, the simulation experiment shows our scheme is more secure and efficient than other schemes in real scenarios.

收稿日期：2024-03-06；改回日期：2024-08-22；网络出版：2024-08-30
*通信作者： 徐梓桑 xzsszx111@csust.edu.cn
基金项目：国家自然科学基金(52172313)，湖南省自然科学基金(2023JJ30033)，新疆维吾尔自治区重点研发计划(2023B03004-3)，湖南省自然科学基金(2024JJ6066)，湖南省教育厅科学研究项目(23B0288)
Foundation Items: The National Natural Science Foundation of China(52172313), Hunan Natural Science Foundation (2023JJ30033), Xinjiang Uygur Autonomous Region Key Research and Development Program (2023B03004-3), The Natural Science Foundation of Hunan Province of China (2024JJ6066), The Research Foundation of Education Bureau of Hunan Province of China (23B0288)

Key words: Internet of Vehicles(IoVs); Authentication protocol; Privacy protection; Physical Unclonable Function (PUF); Vehicle-road-cloud collaboration

1　引言

车联网(Internet of Vehicles)技术是一种提高道路交通安全和便利性的新兴技术，车联网环境中一般包含3种实体，分别是配备车载单元(On Board Unit, OBUs)的车辆、分布广泛的RSU，以及拥有巨大计算能力的可信机构(Trusted Authority, TA)[1]。然而，资源受限、高移动性和网络异构等车联网特性使得车辆通信面临安全和隐私保护方面的巨大挑战[2,3]。

在车联网场景中，攻击者可以通过攻击获取实体和公共信道中的隐私信息，除了常见的攻击外，实体更加可能遭受到物理攻击[4,5]。因此，车辆和路边单元(Road Side Unit, RSU)中保存的秘密信息可能会被攻击者通过物理攻击的方式获取。然而目前大部分身份认证方案都假设车辆和RSU是物理安全的，这与实际情况并不符合[6]。所以，研究者将物理不可克隆函数(Physical Unclonable Function, PUF)应用到车联网的身份认证中，从而实现在条件隐私保护的情况下完成身份认证[7]。现有方案虽然能够实现条件隐私保护，但是基于云中心的方案有集中计算的弊端，并不能满足日益复杂的车联网环境对延迟敏感的特性[8]。所以，研究者们将基于分布式的方案引入到车联网中，有效地减少了云服务器的压力和传输消耗，避免了云方案的缺点[9,10]。

基于上述存在的问题，本文提出一种车路云协同的轻量级安全认证方案，抵御认证过程中可能面临的物理和共谋等攻击，保护认证车辆的身份和轨迹隐私信息，并且在RSU上实现批量认证，降低认证延迟，提高认证效率。

本文的贡献总结如下：

(1)本文设计了一种轻量级车路云协同认证方案，使用PUF保护车辆和RSU的物理安全。车辆利用挑战响应对存储车辆秘密信息和构造车辆假名，并且通过挑战响应对(Challenge-Response Pairs, CRPs)更新推动假名更新，保护车辆的身份隐私。

(2)本文方案将认证计算卸载到经过TA验证授权的RSU上进行，而无需将车辆假名上传到TA，保护车辆的轨迹隐私。

(3)使用椭圆曲线加密(Elliptic Curve enCryption, ECC)保护认证过程公共信道中的参数信息安全，能够抵抗常见的主被动攻击，减少通信消耗。

2　相关工作

为了在车联网认证场景中实现有效的隐私保护，Xi等人[11]提出一种基于零知识证明和椭圆曲线加密的车联网匿名认证方案，实现了用户的匿名性和真实性。Liu等人[12]提出了一种基于分层假名的条件隐私保护认证方案，通过层次化的假名方案保护用户的隐私，并且可以通过恢复假名实现条件隐私。但是两种方案都需要维护一个巨大的车辆撤销列表。Wei等人[13]提出一种基于智能终端的多模态隐式认证方案，但是需要搜集用户的行为数据进行训练，且存在泄露用户行为模型的风险。

由于车联网中实体的特性，其遭受物理攻击的风险大大增加[14]。Aman等人[6]提出应用物理不可克隆函数来提供认证过程所需要的安全保证。该方案通过PUF的挑战响应对来进行认证以及生成会话密钥。Umar等人[8]提出一种车联网轻量级隐私保护认证方案。但是两种方案都没有充分利用RSU的计算和存储资源。另外，此类方案会增加TA单点故障的风险，同时也增加了通信消耗和延迟。Xie等人[7]提出一种基于椭圆曲线加密和PUF的认证方案，但是该方案不能抵抗共谋攻击。

为减轻云辅助认证方案中可能面临的单点故障风险，车路云协同被引入到车联网认证中[15]。通过近端通信响应车辆请求，车路云协同方案将云中心的计算任务卸载到边缘环境中进行，降低延迟和消耗，以及云中心的计算压力。Wazid等人[16]提出了一种基于雾计算的认证方案。每个注册车辆和RSU可以使用其身份信息来构建会话密钥。由于每个RSU都拥有完整的车辆真实身份，而半信任的RSU可能会泄露合法车辆的身份隐私。因此，想要充分利用RSU的资源，就必须保证其在认证过程中是未被破坏的可信实体。

综上所述，现有方案不能很好地平衡隐私保护和成本之间的关系。为了解决以上问题，本文提出一种轻量级车路云协同车联网认证方案，在保证认证过程中RSU实体物理安全的情况下，充分利用其资源，有效减轻了TA的资源压力，并且减少了认证过程中延迟和消耗。

3　相关知识

3.1　物理不可克隆函数

PUF本质上是使用芯片内部结构来提供不可复制的单向输出功能，它将随机的物理变化引入芯片的微观结构中，其利用设备的内在物理构造将一组挑战输出为唯一对应的响应，任意挑战都会输出一个不可预测的响应。PUF具有物理安全、高吞吐量、不可克隆性和结构简单等特点，且任何篡改

PUF的行为都会改变其物理结构，从而导致PUF不可用。此外，本文使用模糊提取器来获得足够稳定的PUF响应，从而避免诸如温度和电压之类的环境因素影响PUF对相同输入产生的输出[17]。

3.2 椭圆曲线加密

椭圆曲线加密的安全性来源于椭圆曲线离散对数问题(Elliptic Curve Discrete Logarithm Problem, ECDLP)的困难性，相比传统的RSA算法，ECC在相同长度的密钥下能够提供更高的安全性。其原理为设F_p是一个有限域，阶为大素数p，定义椭圆曲线E为：$y^2 = x^2 + ax + b \bmod p$，$a, b \in Z_p^*$。设$P$, Q为E上的两个随机点，若$x \in Z_p^*$，且满足$Q = x \cdot P$，攻击者难以在多项式时间内计算出x。

4 系统模型和安全需求

4.1 系统模型

本文提出一种安全高效的车联网隐私保护认证方案，系统模型如图1所示，其中一共包含3种实体：TA, RSU和车辆。本文使用PUF的特性来保证车联网的物理安全，充分利用RSU的资源，从而提供安全高效的认证服务。

(1)可信机构：TA是完全可信的，它拥有强大的计算和通信能力，负责注册车辆和RSU，以及保存其他实体的挑战响应对(Challenge-Response Pairs, CRP)等秘密信息，并为验证车辆身份的RSU提供信任的保证。

(2)路边单元：RSU是半可信的，每个RSU都配备了PUF，且相互独立。RSU负责TA和车辆之间的通信，以及在认证过程中负责验证车辆身份，其通信和计算能力强于车辆，但是弱于TA。

(3)车辆：车辆是车联网中分布最广泛的实体，但是被普遍认为是不可信的，且每辆车都配备了OBU和PUF。

4.2 攻击者模型

攻击者可以窃听、拦截、修改或删除公开传输的信息。

攻击者可能是注册的车辆或内部攻击者，这表示攻击者可能会发送恶意消息或发起内部攻击。

攻击者可以对OBUs和RSU发起侧信道攻击获取信息，但难以破解PUF和ECC。

5 车路云协同的轻量级认证方案

本文认证方案分为4个部分：初始化，RSU注册、车辆注册和验证过程。其中初始化、RSU注册和车辆注册都在安全信道中进行，且只进行1次，而验证过程在公共信道中进行。在注册阶段将设备的挑战响应对存储到TA中；在验证阶段，车辆选择同一个挑战，将通过PUF输出的响应返回可信中心，如果两个响应一致，则通过认证。此外，PUF参与车辆假名的构造与更新。详细参数如表1所示。

5.1 初始化

TA负责初始化系统参数，包括选择单向Hash函数$h(\cdot)$，椭圆曲线E(GF)和基点P，以及选择随机数n_t作为TA的私钥x_{TA}，并计算公钥$X_{\mathrm{TA}} = x_{\mathrm{TA}} \cdot P$。与已有方案使用的双线性映射相比，Hash函数和椭圆曲线更加轻量级，适合资源受限的车联网场景。

5.2 RSU注册

RSU利用PUF和ECC完成自身秘密信息的生成和加密存储。如图2所示，RSU将自身PUF作为

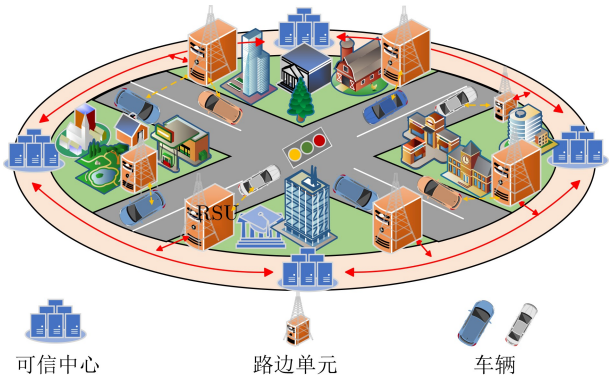

图 1 车路云协同的车联网认证模型

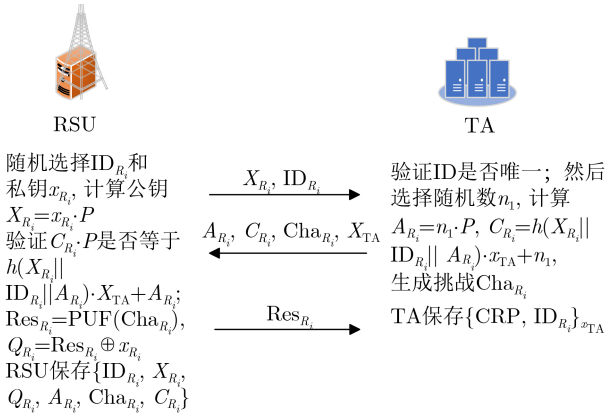

图 2 RSU注册

表 1 参数含义对照表

符号	描述
TA	可信中心
V_i	第i个车辆
ID	实体身份
X, x	实体的公钥和私钥
CRP	PUF的挑战响应对
T	时间戳
SK	会话密钥

信任根和加密存储私钥的工具，利用ECC保证公共信道中的信息不会被泄露，RSU中CRP的正确与否，决定了RSU是否合法，这能够抵御针对RSU的物理和伪造攻击。

(1) RSU随机选择自身ID_{R_i}和自身私钥x_{R_i}，计算$X_{R_i}=x_{R_i}\cdot P$，然后将X_{R_i}和ID_{R_i}发送给TA。

(2) TA验证ID的唯一性和合法性。若不符合，重新选取。TA选择随机数n_1，计算$A_{R_i}=n_1\cdot P$，$C_{R_i}=h(X_{R_i}||\mathrm{ID}_{R_i}||A_{R_i})x_{\mathrm{TA}}+n_1$。然后随机生成挑战$\mathrm{Cha}_{R_i}$，将$\{A_{R_i},X_{\mathrm{TA}},C_{R_i},\mathrm{Cha}_{R_i}\}$发送到RSU上。

(3) RSU验证$C_{R_i}\cdot P$是否等于$h(X_{R_i}||\mathrm{ID}_{R_i}||A_{R_i})X_{\mathrm{TA}}+A_{R_i}$?如果通过验证，则使用$\mathrm{Cha}_{R_i}$生成响应$\mathrm{Res}_{R_i}=\mathrm{PUF}(\mathrm{Cha}_{R_i})$。将$x_{R_i}$进行加密，即$Q_{R_i}=\mathrm{Res}_{R_i}\oplus x_{R_i}$，RSU保存$\{\mathrm{ID}_{R_i},X_{R_i},Q_{R_i},A_{R_i},C_{R_i},\mathrm{Cha}_{R_i}\}$；然后将$\mathrm{Res}_{R_i}$发送到TA使用$x_{\mathrm{TA}}$加密存储$\{\mathrm{Cha}_{R_i},\mathrm{Res}_{R_i},\mathrm{ID}_{R_i}\}$。

5.3 车辆注册

车辆中PUF的CRP决定了车辆是否合法，在保持轻量级的同时，能够使车辆抵御可能面临的物理攻击和伪造攻击，详细过程如图3所示。

(1) 车辆首先随机选择身份ID_{Vi}和私钥x_{V_i}，并计算公钥$X_{V_i}=x_{V_i}\cdot P$，将$\{\mathrm{ID}_{V_i},X_{V_i}\}$发送到TA。

(2) TA检查ID_{V_i}是否唯一和合法，然后选择随机数n_2，生成挑战Cha_{V_i}，并计算$A_{V_i}=n_2\cdot P$，$K_1=h(\mathrm{ID}_{V_i}||A_{V_i})$，$C_{V_i}=K_1\cdot x_{\mathrm{TA}}+n_2$，，$W_1=n_3\cdot P, L_1=n_3\cdot X_{\mathrm{TA}}$，然后将$\{\mathrm{Cha}_{V_i},X_{\mathrm{TA}},C_{V_i},A_{V_i}\}$通过安全信道发送给$V_i$。

(3) V_i根据收到的Cha_{V_i}生成响应$\mathrm{Res}_{V_i}=\mathrm{PUF}(\mathrm{Cha}_{V_i})$，然后计算验证$C_{V_i}\cdot P$是否等于$h(\mathrm{ID}_{V_i}||A_{V_i})X_{\mathrm{TA}}+A_{V_i}$?若等于，则计算$Q_{V_i}=\mathrm{Res}_{V_i}\oplus\mathrm{ID}_{V_i}$，$\mathrm{PID}_{V_i}=h(\mathrm{ID}_{V_i}||\mathrm{Cha}_{V_i}||\mathrm{Res}_{V_i})$，$S_{V_i}=(h(\mathrm{ID}_{V_i}||W_1))^{-1}h(\mathrm{PID}_{V_i})$，车辆中保存$\{\mathrm{Cha}_{V_i},Q_{V_i},W_1,L_1,\mathrm{PID}_{V_i},X_{V_i},C_{V_i}\}$。

(4) TA加密保存$\{\mathrm{ID}_{V_i},(h(\mathrm{ID}_{V_i}))^{-1}A_{V_i},\mathrm{CRP}_{V_i}\}$。

5.4 验证阶段

车辆进入RSU范围内接收其ID_{V_i}和X_{R_i}，然后将验证参数使用CRP加密后传送给RSU。RSU使用自己的CRP加密后传送给TA。若TA使用实体相应的CRP解密后获得结果，若验证后与U_1和U_2符合，则表示车辆通过了TA的验证，TA认为车辆和RSU都是合法的，在保持轻量级的同时提供了足够高的安全性。之后，RSU和车辆相互验证后构建会话密钥，详细过程如图4所示。

(1)车辆进入RSU范围时，车辆选取当前时间戳T_1，计算$U_1=h(W_1||L_1||T_1)$，并使用Res_{V_i}加密$M_2=\{W_1\}_{\mathrm{Res}_{V_i}}$，然后将$\{T_1,M_2,U_1,\mathrm{PID}_{V_i},C_{V_i},L_1,K_1\}$发送到RSU。

(2)RSU生成T_2和n_4，然后使用Res_{R_i}加密M_2，并计算$U_2=h(M_3||T_2||\mathrm{Res}_{R_i})$，然后将$\{M_3,U_1,U_2,\mathrm{ID}_{R_i},T_2\}$发送到TA。

(3)TA使用相应RSU和车辆的CRP解密获得W_1，然后验证参数U_1。若等于，说明车辆和RSU所采用的CRP是正确的，RSU和车辆未被破坏和伪造，即它们是可信的。

(4)TA生成T_3，将$M_4=\{\mathrm{ID}_{R_i},T_3\}$使用$\mathrm{Res}_{V_i}$加密后，使用$\mathrm{Res}_{R_i}$加密$M_5=\{M_4,\mathrm{ID}_{R_i},T_3\}_{\mathrm{Res}_{R_i}}$，计算$U_3=h(\mathrm{ID}_{R_i}||M_5||T_3)$，将$\{M_5,U_3\}$发送给RSU, RSU验证参数是否有效；然后计算验证$C_{V_i}\cdot P$是否等于$K_1\cdot X_{\mathrm{TA}}+W_1$。若一致，RSU生成会话密钥$\mathrm{SK}_{R_iV_i}=h(W_1\cdot x_{R_i}||T_3||\mathrm{ID}_{R_i}||\mathrm{PID}_{V_i})$，并且计算参数$U_4=h(\mathrm{SK}_{R_iV_i}||T_3||\mathrm{ID}_{R_i}||\mathrm{PID}_{V_i})$，然后将$\{M_4,\mathrm{SK}_{R_iV_i},U_4\}$发送给车辆。

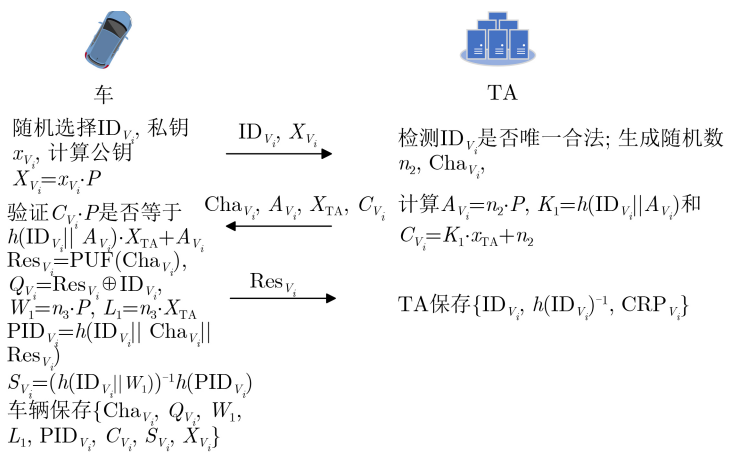

图 3 车辆注册

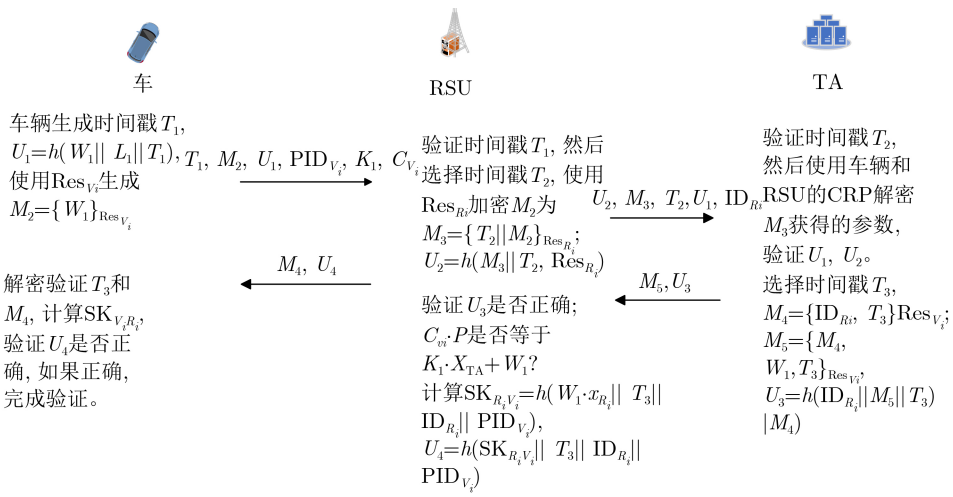

图 4 车辆验证

(5)车辆解密M_4后验证T_3是否在有效期间，生成会话密钥$\mathrm{SK}_{V_iR_i}=h(n_3\cdot W_2||T_3||x_{V_i}\cdot X_{R_i}||\mathrm{PID}_{V_i})$判断是否等于$\mathrm{SK}_{R_iV_i}$，以及$U_4$是否相等。若一致，完成认证；若不一致，则丢弃请求。

(6)当有多个车辆同时向一个RSU请求认证时，使用车辆的CRP向TA验证当前RSU是否可信；当验证通过后，RSU计算$\sum C_{Vi}\cdot P$是否等于$\sum(K_1\cdot X_{\mathrm{TA}})+\sum W_1$。若等于，则表示当前车辆都通过了验证，然后构建会话密钥。

5.5 假名更新

车辆假名更新无需第三方参与，当需要车辆更新假名时，执行$\mathrm{PID}_{\mathrm{new}}^{V_i}=h(Q_{V_i}||\mathrm{Cha}_{V_i}||\mathrm{Res}_{V_i})$，同时，车辆中的$S_{Vi}$也进行相应的更新，从而使TA不会丧失对恶意车辆的追踪能力。此外，车辆上传CRP到TA，保持TA中的信息正确。

5.6 恶意身份追踪

当发现车辆有恶意行为时，TA令RSU计算$\mathrm{MV}=(h(\mathrm{PID}_{V_i}))^{-1}S_{V_i}$，将MV发送给TA，TA通过存储的信息可以披露恶意车辆的身份信息。

6 安全性分析

6.1 形式化安全分析

本节使用随机预言模型(Random Oracle Model, ROM)对所提方案进行形式化安全分析[18]。

引理1 攻击者无法预测PUF的响应。

证明 本文将PUF建模为$\{0,1\}^{l_1}$->$\{0,1\}^{l_2}$，即输入一个l_1长度的挑战，PUF输出一个长度为l_2的响应。本文在挑战者C和攻击者A之间基于博弈进行建模，用来论证PUF的安全性。

(1) A发送C_i给C, C返回R_i给A。

(2) C随机选取与C_i不同的C_x，并生成R_x。

(3) A可以向C进行查询，获得对应的响应R_x。

(4) A输出C_x的猜测R_x'，若$R_x'=R_x$，则A获胜。

攻击者A在此轮博弈中的获胜优势定义为$\alpha_{\mathrm{A}}^{\mathrm{PUF}}=\Pr[R_x'=R_x]$，PUF会对挑战产生唯一且不可预测的响应[19]。因此，攻击者A只能通过猜测获得响应R_x，所以$\alpha_{\mathrm{A}}^{\mathrm{PUF}}=1/2^{l_2}$。

引理2 方案的秘密信息是安全的

证明 攻击者从车辆和RSU获取秘密信息的途径有两种，一种是使用物理攻击获取秘密信息，但是车辆和RSU中的秘密信息是使用R_x进行加密存储，破解加密信息必须获取R_x，但是根据引理1知道这是不可能的；第2种途径是通过存储的C_x生成R_x，但是任何篡改和分离PUF的行为都会使其失效。

所提方案一共有3种参与者，彼此之间可以运行多种协议，实体之间运行的一个协议被认为是一个实例。任何一个参与者都可以有多个不同的实例。本文将实体V_i的实例a定义为Φ_V^a。接收状态是指当实体接收到了想要的消息时，进入接收状态。

预言查询：攻击者可以对通信的消息进行窃听、修改和拦截，通过对下列多种查询进行建模模拟攻击者的攻击。

Execute(Φ_V^a, Φ_{RSU}^b, Φ_{TA}^c)：攻击者执行此查询就是对所提出的方案发起了被动攻击。攻击者能够通过这种查询窃听公共信道中的信息，从而获得实体在执行协议期间产生的各种消息。

Send(Φ_V^a, Φ_{RSU}^{ab}, M)：这个查询是模拟攻击者发起针对实体的主动攻击。如果参与方认为信息M是合法的，那么接收者会向攻击者做出响应。

Reveal(Φ_V^a)：攻击者可以通过这个查询获得Φ_V^a与它的合作者完成验证后共享的会话密钥SK。

Corrupt(Φ_V^a)：这个查询模拟了测信道攻击，攻击者使用这个查询可以用来腐化破坏车辆。

Corrupt($\Phi^b_{\rm RSU}$)：攻击者使用这个查询可以用来腐化破坏RSU，返回存储在RSU中的信息。

Test(Φ^a_V, $\Phi^b_{\rm RSU}$, b)：如果车辆和RSU之间可以计算出会话密钥SK，并且在接收Test查询后，生成一个随即位b，如果b=1，将SK返回；若b=0，则返回一个随机值。这个查询最多只能执行1次。

定理3　定义$\mathrm{Adv}^{\rm T}_{\rm A}$为攻击者破坏方案安全性的成功概率，攻击者所具有的优势为

$$\mathrm{Adv}^{\rm T}_{\rm A} \le \frac{\mathrm{q}^2_{\rm HA}}{2^{l_{\rm Hash}+1}} + \frac{(\mathrm{q}_{\rm SE}+\mathrm{q}_{\rm EX})^2}{2n} + \mathrm{q}_{\rm SE}\cdot\left(2\cdot\mathrm{Adv}^{\rm PUF}_{\rm A}\right) + \mathrm{Adv}^{\rm ECDLP}_{\rm A} \tag{1}$$

其中，$q_{\rm HA}$代表Hash执行的次数，$q_{\rm SE}$代表Send执行的次数，$q_{\rm EX}$代表Execute执行的次数。$l_{\rm Hash}$代表Hash函数返回消息的长度，n表示椭圆曲线加密后的消息长度。攻击者破坏PUF和ECDLP的优势分别表示为$\mathrm{Adv}^{\rm PUF}_{\rm A}$，$\mathrm{Adv}^{\rm ECDLP}_{\rm A}$。

证明_假设攻击者能够破坏方案的安全性，那么存在一个攻击者A能在多项式时间破解哈希函数$h(\cdot)$的安全性。在经过多次博弈后，计算攻击者累加的获胜优势。

Game_0：这个博弈模拟了攻击者的初始化攻击。在这个博弈中，可以得到

$$\mathrm{Adv}^{\rm T}_{\rm A} = \left|\Pr[\mathrm{Win}_0] - \frac{1}{2}\right| \tag{2}$$

Game_1：这个博弈模拟了窃听攻击，攻击者能够获得公共信道的所有消息，但是由于ECDLP，攻击者不能通过窃听攻击增加博弈1获胜的概率。所以，博弈1和博弈0的概率相等

$$\Pr[\mathrm{Win}_1] = \Pr[\mathrm{Win}_0] \tag{3}$$

Game_2：这个博弈模拟了攻击者的主动攻击。这个博弈维护了一个哈希列表H_m，当收到攻击者的$h(m)$查询时，若H=$h(m)\in H_m$，输出H；反之，随机选取一个值，并记录在H_m中。Game_2模拟了Hash结果和哈希列表H_m之间的碰撞攻击。

根据生日悖论，哈希碰撞的概率为$\frac{q_{\rm HA}}{2^{l_{\rm Hash}+1}}$，产生与原消息一致的消息的概率为$\frac{(q_{\rm SE}+q_{\rm EX})^2}{2n}$。于是

$$\Pr[\mathrm{Win}_2] - \Pr[\mathrm{Win}_1] \le \frac{(\mathrm{q}_{\rm SE}+\mathrm{q}_{\rm EX})^2}{2n} + \frac{\mathrm{q}^2_{\rm HA}}{2^{l_{\rm Hash}+1}} \tag{4}$$

Game_3：这个博弈模拟了攻击者执行Corrupt(Φ^a_V)和Corrupt($\Phi^b_{\rm RSU}$)来获得存储在RSU和车辆中的信息。攻击者如果想要获取RSU和车辆中的信息，就需要突破PUF的保护。因此，可以得到

$$\Pr[\mathrm{Win}_3] - \Pr[\mathrm{Win}_2] \le \mathrm{q}_{\rm SE}\cdot(2\cdot\mathrm{Adv}^{\rm PUF}_{\rm A}) \tag{5}$$

Game_4：攻击者能从公共信道中获取实体用来构造会话密钥的信息，但是这部分信息已经经过了椭圆曲线加密。这个博弈模拟了通过这些信息构造会话密钥，所以

$$\Pr[\mathrm{Win}_4] - \Pr[\mathrm{Win}_3] \le \mathrm{Adv}^{\rm ECDLP}_{\rm A} \tag{6}$$

因为会话密钥中包含随机数，产生过程是独立和随机的，所以，可以得到

$$\Pr[\mathrm{Win}_4] = \frac{1}{2} \tag{7}$$

综合以上式子，可以得到

$$\mathrm{Adv}_{\rm A} = \left|\Pr\left[\mathrm{Win}_0 - \frac{1}{2}\right]\right| \le \frac{\mathrm{q}^2_{\rm HA}}{2^{l_{\rm Hash}+1}} + \frac{(\mathrm{q}_{\rm SE}+\mathrm{q}_{\rm EX})^2}{2n} + \mathrm{q}_{\rm SE}\cdot\left(2\cdot\mathrm{Adv}^{\rm PUF}_{\rm A}\right) + \mathrm{Adv}^{\rm ECDLP}_{\rm A} \tag{8}$$

6.2 非形式化分析

(1) 抵抗重放攻击：在本方案中，两个实体之间的交互会伴随着时间戳的传递，如果超出时间范围的消息将被丢弃，所以可以抵抗重放攻击。

(2) 抵抗TA伪造攻击：若攻击者想要伪造成TA向车辆或者RSU发送消息，他需要知道车辆和RSU的挑战响应对。因为车辆和RSU向TA传输的消息是使用CRP加密的。

(3) 抵抗物理克隆攻击：当攻击者试图破坏车辆的OBU和RSU上的存储设备时，都将会从物理层面上改变PUF的构造，从而使得它的响应发生不可恢复的变化，所以攻击者对车辆和RSU的物理攻击是无效的。

(4) 抵抗车辆伪造攻击：因为攻击者不可能知道TA的私钥$x_{\rm TA}$，所以不能构造出正确的C_{V_i}，即$C_{V_i} = h(\mathrm{ID}_{V_i}||A_{V_i})\cdot x_{\rm TA} + n_2$，也就不能通过RSU对车辆的认证，即$C_{V_i}\cdot P$不等于$h(\mathrm{PID}_{V_i})\cdot X_{\rm TA}+Y_{V_i}+W_1$。所以，攻击者不能将恶意车辆伪造为合法车辆。

(5) 抵抗中间人攻击：本方案的消息都经过了加密操作，若没有相应秘密信息并不能解密消息，也不能通过车辆对于接收信息的验证。

(6) 抵抗共谋攻击：如果攻击者企图为恶意车辆进行认证时， RSU和车辆在进行验证的时候需要TA对于它们的CRP进行确认，不能通过的实体不能参与认证。

(7) 匿名性和不可链接性：由于每次构造参数时会选取随机数以及CRP，而这些随机数并没有在信道中公开进行传输，所以即使攻击者知道了密钥也不能恢复以前的会话密钥。

(8) 前后向保密：由于车辆在每次会话后都会生成新的假名，并且在生成过程中会添加随机数，所以车辆能够保持匿名性，并且假名之间是不可链接的。

7 性能分析

为了评估了各个方案的计算性能，本文使用Intel I5 9300H(2.4 GHz)处理器，16 GB内存和Windows 11操作系统上通过The ONE(Opportunistic Network Environment simulator)模拟器进行模拟实验。图5展示了实验所用的新加坡市真实场景地图。

7.1 计算消耗

本文设定$T_{\rm ECC}$, $T_{\rm Hash}$, $T_{\rm SE}$分别为ECC, Hash和对称加密所需要的时间，且分别为20 ms, 0.002 ms和20.2 ms。对比已有方案，本文方案有效减少了延迟，平衡了实体的计算负载，达到了总体最小的计算开销。表2显示了相关方案的计算开销。

7.2 通信消耗

通信消耗主要是验证阶段实体间的信息交换，为了计算信息的大小，本文设定Hash、对称加密、ECC、随机数、CRP、身份和时间戳的大小分别为256 bit, 128 bit, 160 bit, 256 bit, 128 bit, 32 bit和32 bit。

本文方案的通信开销优于文献[6,11,20]方案，只比文献[7]方案稍多，但是方案[7]在共谋攻击方面存在明显的缺陷。表3展示了与相关方案之间的通信开销对比。

7.3 安全性能

由6.2节的非形式化分析可以得知，本方案在安全性能方面具有良好的性能，能够抵御常见的各种攻击和安全风险，并且本方案也具有追溯恶意用户的能力。表4展示了与相关方案的安全属性对比，其中“√”表示提供该安全属性，“–”表示不提供该安全属性。

图 5 仿真实验实际场景地图

表 2 实体的计算开销(ms)

文献	V	RSU	TA	合计
[7]	120.21	121.06	/	241.27
[6]	20.76	41.52	141.41	203.70
[20]	40.00	100.01	120.01	260.02
[11]	80.20	100.02	20.00	200.22
本文	40.20	60.20	60.60	161.00

7.4 模拟实验

为了评估了各个方案的性能表现，本文选取了平均延迟、平均跳数、传送率和路由开销四个性能指标，分别对各个方案的仿真实验结果进行性能分析对比。从图6–图9可以得到：

(1)本方案的延迟远远小于文献[6]、文献[11]和文献[20]，只有文献[7]与本文的方案处在同一量级，平均延迟保持在30 ms以下，能够对车辆的认证服务请求做出快速响应。

表 3 实体的通信开销(bit)

文献	V	RSU	TA	合计
[7]	864	576	/	1440
[6]	288	1408	1152	2848
[20]	960	2048	768	3776
[11]	1760	768	1380	3908
本文	768	704	384	1856

表 4 安全属性

安全属性	文献[7]	文献[6]	文献[20]	文献[11]	本文
A_1	√	√	√	√	√
A_2	–	–	–	–	√
A_3	√	√	–	–	√
A_4	–	√	√	–	√
A_5	√	–	–	√	√
A_6	–	√	–	√	√
A_7	√	√	√	√	√
A_8	√	–	√	√	√
A_9	√	–	√	√	√
A_{10}	√	√	√	√	√

A_1：重放攻击；A_2：TA伪造攻击；A_3：物理克隆攻击；A_4：车辆伪造攻击；A_5：中间人攻击；A_6：共谋攻击；A_7：匿名性；A_8：不可链接性；A_9：前后向保密；A_{10}：身份追踪

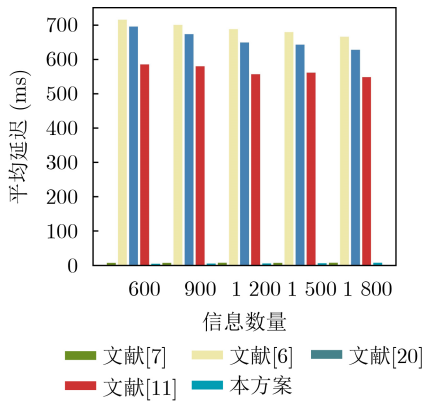

图 6 平均延迟

(2)本文方案比文献[6]、文献[7]、文献[11]和文献[20]有更低的信息平均跳数，不会因为服务请求的增多对网络产生大的压力，具有更加优越的性能表现，体现了良好的鲁棒性，性能表现优于其它现有方案。

(3)本方案的传送率为99.88%，而文献[7]的传送率为99.83%，两者接近且都表现出较高的可靠性水平，这两个方案在传送率方面表现出色，性能表现优于其他现有文献中提出的方案。

(4)在开销比方面，本方案仅仅比文献[7]稍高，但是优于文献[6]、文献[11]和文献[20]，并且本文方案的安全性能要比文献[7]更加完善。

8　结论

本文提出一种车路云协同的轻量级安全认证方案，采用物理不可克隆函数作为实体的信任保证，抵御攻击者对车联网实体的物理和共谋等攻击；采用车路云协同的架构，将计算过程卸载到经过TA验证授权的RSU上进行，实现对车辆身份的快速认证，并有效降低了通信和计算成本以及云中心的计算压力。通过与相关方案进行对比分析，证明了本方案在安全和效率方面都具有一定的优势。

参 考 文 献

[1] XIE Qi and HUANG Juanjuan. Improvement of a conditional privacy-preserving and desynchronization-resistant authentication protocol for IoV[J]. *Applied Sciences*, 2024, 14(6): 2451. doi: 10.3390/app14062451.

[2] JAVAID U, AMAN M N, and SIKDAR B. A scalable protocol for driving trust management in internet of vehicles with blockchain[J]. *IEEE Internet of Things Journal*, 2020, 7(12): 11815–11829. doi: 10.1109/JIOT.2020.3002711.

[3] ELHALAWANY B M, EL-BANNA A A A, and WU Kaishun. Physical-layer security and privacy for vehicle-to-everything[J]. *IEEE Communications Magazine*, 2019, 57(10): 84–90. doi: 10.1109/MCOM.001.1900141.

[4] KUMAR V, AHMAD M, MISHRA D, *et al.* RSEAP: RFID based secure and efficient authentication protocol for vehicular cloud computing[J]. *Vehicular Communications*, 2020, 22: 100213. doi: 10.1016/j.vehcom.2019.100213.

[5] XIONG Jinbo, MA Rong, CHEN Lei, *et al.* A personalized privacy protection framework for mobile crowdsensing in IIoT[J]. *IEEE Transactions on Industrial Informatics*, 2020, 16(6): 4231–4241. doi: 10.1109/tii.2019.2948068.

[6] AMAN M N, JAVAID U, and SIKDAR B. A privacy-preserving and scalable authentication protocol for the internet of vehicles[J]. *IEEE Internet of Things Journal*, 2021, 8(2): 1123–1139. doi: 10.1109/jiot.2020.3010893.

[7] XIE Qi, DING Zixuan, and ZHENG Panpan. Provably secure and anonymous V2I and V2V authentication protocol for VANETs[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2023, 24(7): 7318–7327. doi: 10.1109/TITS.2023.3253710.

[8] UMAR M, ISLAM S K H, MAHMOOD K, *et al.* Provable secure identity-based anonymous and privacy-preserving inter-vehicular authentication protocol for VANETS using PUF[J]. *IEEE Transactions on Vehicular Technology*, 2021, 70(11): 12158–12167. doi: 10.1109/TVT.2021.3118892.

[9] WU Anmulin, GUO Yajun, and GUO Yimin. A decentralized lightweight blockchain-based authentication mechanism for Internet of Vehicles[J]. *Peer-to-Peer Networking and Applications*, 2023, 16(3): 1340–1353. doi: 10.1007/s12083-022-01442-0.

[10] LI Jie, LIN Yuanyuan, LI Yibing, *et al*. BPA: A novel blockchain-based privacy-preserving authentication scheme for the internet of vehicles[J]. *Electronics*, 2024, 13(10): 1901. doi: 10.3390/electronics13101901.

[11] XI Ning, LI Weihui, JING Lv, *et al*. ZAMA: A ZKP-based anonymous mutual authentication scheme for the IoV[J]. *IEEE Internet of Things Journal*, 2022, 9(22): 22903–22913. doi: 10.1109/JIOT.2022.3186921.

[12] LIU Jingwei, PENG Chuntian, SUN Rong, *et al*. CPAHP: Conditional privacy-preserving authentication scheme with hierarchical pseudonym for 5G-enabled IoV[J]. *IEEE Transactions on Vehicular Technology*, 2023, 72(7): 8929–8940. doi: 10.1109/TVT.2023.3246466.

[13] WEI Fushan, ZEADALLY S, VIJAYAKUMAR P, *et al*. An intelligent terminal based privacy-preserving multi-modal implicit authentication protocol for internet of connected vehicles[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2021, 22(7): 3939–3951. doi: 10.1109/TITS.2020.2998775.

[14] LIANG Yangfan, LUO Entao, and LIU Yining. Physically secure and conditional-privacy authenticated key agreement for VANETs[J]. *IEEE Transactions on Vehicular Technology*, 2023, 72(6): 7914–7925. doi: 10.1109/TVT.2023.3241882.

[15] WANG Denghui, YI Yuping, YAN Shan, *et al*. A node trust evaluation method of vehicle-road-cloud collaborative system based on federated learning[J]. *Ad Hoc Networks*, 2023, 138: 103013. doi: 10.1016/j.adhoc.2022.103013.

[16] WAZID M, BAGGA P, DAS A K, *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. doi: 10.1109/JIOT.2019.2923611.

[17] GOPE P, DAS A K, KUMAR N, *et al*. Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks[J]. *IEEE Transactions on Industrial Informatics*, 2019, 15(9): 4957–4968. doi: 10.1109/TII.2019.2895030.

[18] BELLARE M and ROGAWAY P. Random oracles are practical: A paradigm for designing efficient protocols[C]. Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, USA, 1993: 62–73. doi: 10.1145/168588.168596.

[19] NURKIFLI E H and HWANG T. Provably secure authentication for the internet of vehicles[J]. *Journal of King Saud University-Computer and Information Sciences*, 2023, 35(8): 101721. doi: 10.1016/j.jksuci.2023.101721.

[20] YADAV K A and VIJAYAKUMAR P. LPPSA: An efficient Lightweight Privacy-Preserving Signature-based Authentication protocol for a vehicular ad hoc network[J]. *Annals of Telecommunications*, 2022, 77(7/8): 473–489. doi: 10.1007/s12243-021-00897-1.

夏卓群：男，教授，研究方向为社交网络、移动网络、VANET以及网络和信息安全.

苏　潮：男，硕士生，研究方向为隐私保护和网络安全.

徐梓桑：男，讲师，研究方向为嵌入式系统、信息安全和密码.

龙科军：男，教授，研究方向为交通控制、交通信息技术和智能交通系统.

责任编辑：余　蓉