

基于国密SM2的车联网高效匿名认证协议

苏彬庭^{1,2}, 方禾¹, 许力^{1,2,3}

(1. 福建师范大学, 福建 福州 350117; 2. 网络安全与教育信息化福建省高校工程研究中心, 福建 福州 350117;
3. 福建省网络安全与密码技术重点实验室, 福建 福州 350117)

摘要: 身份认证是车联网安全防护的关键, 然而, 现有的很多认证方案效率低且不兼容国产密码算法。为进一步提升认证效率, 丰富国产密码算法在车联网领域的应用, 提出了一种基于国密SM2的匿名切换认证协议。该协议结合伪身份认证机制, 强化了车辆隐私信息保护, 有效隐藏车辆的真实身份和行驶数据。该协议不仅融合了国产密码算法, 在认证效率上也表现良好, 特别在密集车辆环境下, 该协议设计了一种巧妙的批量认证算法。为了验证协议性能, 基于Fedora系统的QT平台, 对协议的批量认证算法进行测试, 测试认证车辆数为10, 20, 40, ..., 320的批量认证效率。随着认证车辆数的增加, 批量认证算法展示出的效率优势越发明显, 当认证车辆数达到320辆时, 路侧单元(road side unit, RSU)认证效率提升了约65%, 极大地减轻了RSU并发认证压力。理论和AVISPA工具实验分析证明, 所设计的协议在车联网安全的自主可控性方面更有优势, 不仅能够有效抵抗重放攻击和中间人攻击等攻击行为, 并且在认证效率上也有显著提升, 为车联网系统的身份认证提供了更为安全有效的解决方案。

关键词: 车联网; 认证协议; SM2; 批量认证; AVISPA

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2025030

Efficient anonymous authentication protocol for internet of vehicles based on Chinese cryptographic SM2

SU Binting^{1,2}, FANG He¹, XU Li^{1,2,3}

1. Fujian Normal University, Fuzhou 350117, China
2. Engineering Research Center of Cyber Security and Education Informatization, Fuzhou 350117, China
3. Fujian Provincial Key Laboratory of Network Security and Cryptology, Fuzhou 350117, China

Abstract: A critical component of cybersecurity protection in the internet of vehicles (IoV) was identity authentication.

收稿日期: 2024-10-16; 修回日期: 2025-02-26

通信作者: 许力, xuli@fjnu.edu.cn

基金项目: 国家自然科学基金(62471139); 国家科技项目备案-中央引导地方科技发展专项(2023L3007); 福建省中青年教师教育科研项目(JAT220813)

Foundation Items: The National Natural Science Foundation of China(62471139), The National Science and Technology Project Record-Centralized Guided Local Science and Technology Development Special Project(2023L3007), Educational Research Projects of Young and Middle-aged Teachers in Fujian Province(JAT220813)

引用格式: 苏彬庭, 方禾, 许力. 基于国密SM2的车联网高效匿名认证协议[J]. 网络与信息安全学报, 2025, 11(3): 98-108.

Citation Format: SU B T, FANG H, XU L. Efficient anonymous authentication protocol for internet of vehicles based on Chinese cryptographic SM2[J]. Chinese Journal of Network and Information Security, 2025, 11(3): 98-108.

* 第二十七届中国科协年会“AI时代网络技术创新”专题

tion. However, many existing authentication schemes were plagued by low efficiency and incompatibility with domestic cryptographic algorithms. To further enhance authentication efficiency and expand the application of domestic cryptographic algorithms in the IoV domain, an anonymous handover authentication protocol was designed based on the Chinese national cryptographic SM2 algorithm. A pseudo-identity authentication mechanism was integrated into the protocol to strengthen the protection of vehicle privacy information, effectively concealing vehicles' real identities and operational data. Domestic cryptographic algorithms were incorporated into the protocol, which also demonstrated superior performance in authentication efficiency. In densely vehicle environments, an innovative batch authentication algorithm was employed by the protocol. To validate the protocol's performance, tests of the batch authentication algorithm were conducted on a QT platform based on the Fedora system, with the batch authentication efficiency for 10, 20, 40, ..., 320 vehicles being evaluated. As the number of authenticated vehicles increased, the efficiency advantages of the batch authentication algorithm became more pronounced. When authenticating 320 vehicles, the road side unit (RSU) verification efficiency improved by approximately 65%, significantly alleviating the concurrent authentication pressure on RSUs. Both theoretical analyses and experiments using the AVISPA tool confirm that the proposed protocol offers enhanced advantages in the autonomous controllability of IoV security. It not only effectively resists replay attacks and man-in-the-middle attacks but also achieves significant improvements in authentication efficiency, thus providing a more secure and effective identity authentication solution for IoV systems.

Keywords: internet of vehicles, authentication protocol, SM2, batch authentication, AVISPA

0 引言

随着智能交通的飞速发展,车联网作为其核心组成部分,通过强大的网络连接能力,实现了车到车、车到基础设施、车到智能设备等多元实体间的无缝通信^[1]。作为汽车联网服务的前沿形式,车联网展现出极为广泛且多元化的应用场景,深度渗透至车辆安全、交通管理、信息服务、智慧城市构建及智能交通系统等众多领域。它的诞生不仅极大地提升了交通系统的智能化水平,还显著增强了道路安全性,并为乘客带来了更加舒适、便捷的出行体验^[2-3]。一个典型的车联网设施架构主要由信任机构(trusted authority, TA)、路侧单元(road side unit, RSU)、车辆组成^[4-6]。在这一架构中,车辆扮演着至关重要的角色,它通过与RSU的连接,无缝融入车联网中,进而获得与周边车辆、基础设施乃至整个互联网进行高效通信的能力。然而,这种高度互联的环境也带来如恶意攻击、窃取敏感数据、数据篡改等^[6-10]安全挑战。

身份认证是车联网安全体系的重要组成部分,其高度安全性和可靠性直接关系车辆的通信安全、道路交通安全和车辆隐私等方面。近几年,车联网领域的身份认证技术迅速崛起,该技术成为众多学者竞相探索与研究的热点。Sikarwar等^[7]提出

了一种基于MAC(medium access control)的认证方案,以解决车辆认证过程中容易受到密钥泄露以及分布式拒绝服务等安全攻击。针对当前车联网环境中普遍存在的单点故障难题,何业锋等^[11]提出了一种基于阈值的边缘辅助身份认证方案。该方案在车辆初始认证阶段构建并分发认证令牌,这种机制不仅显著降低了认证过程中的时延,提高了车联网系统的响应速度和可靠性,还有效降低了单点故障对系统稳定性的影响,为车联网的安全高效运行提供了强有力的技术支撑。张应辉等^[12]针对5G-V2X场景中大量车辆执行切换认证的效率问题,提出了一种基于轨迹预测的安全高效群组切换认证协议。首先,通过预测车辆轨迹,提前完成密钥协商协议。其次,通过用户分组算法将具有移动相关性的车辆视为同一群组,再采用无证书聚合签名技术批量认证群组内所有车辆,从而提高群组切换认证协议的效率。

然而,上述的方案在保护车辆隐私信息方面存在局限性,无法有效保护车辆的身份、运动轨迹等隐私信息。为了克服这一挑战,研究者基于伪身份、群签名以及区块链等技术提出了一系列的安全隐私保护认证方案^[3-4,10,13-20]。Qiao等^[4]设计了一种基于证书的高效匿名身份认证协议,旨在解决车辆自组织网络中的安全性和隐私保护问

题。该协议具有动态匿名性、身份认证、不可伪造性等特性,确保了车辆间通信的匿名性,同时满足了车联网中数据传输的实时性需求。Azec等^[16]提出了一种高效的匿名认证方案,可以有效防止恶意车辆进入车联网。然而这种方案需要进行复杂的双线性对运算,导致认证效率偏低。Zhu等^[18]为了确保认证过程交换数据的真实性和完整性,且能保护用户隐私,提出了一种具有条件隐私保护的无证书聚合签名方案。方案不仅具备出色的安全特性,在计算效率和通信效率方面也有较高的性能。为了应对 Vasudev-Das 协议容易遭受密码猜测攻击的缺陷,Liu等^[19]提出了一种增强的安全隐私保护可追踪认证协议。该协议不仅能够有效抵御冒充、篡改、重放以及内部攻击等多种安全威胁,还显著提升了车辆身份和位置隐私信息的保护能力,确保了数据传输与认证过程中的高度安全性和隐私性。

国密算法的应用领域主要涵盖身份认证、访问控制、账户管理以及数据安全等多个方面,涉及通信协议、认证协议、电子签名等关键技术^[21-26]。然而,尽管国密算法在这些领域取得了显著进展,但在车联网领域中的应用却相对有限。为了保障车联网安全的自主可控,本文基于国密 SM2 的标识密码算法^[27-28]提出了一种高效且匿名的车联网认证协议。该协议不仅提升了认证效率,更在车辆完成初始接入认证后,通过伪身份机制和批量认证算法,极大地优化了车辆切换认证流程。相较于国内外同类研究,本文的主要贡献体现在以下 3 个方面。

1) 国产密码算法的深度适配与优化:为强化车联网身份认证技术对国产密码算法的兼容性,本文基于 SM2 数字签名算法,构建了一种高效匿名认证协议。该协议不仅显著提升了车辆在认证过程中对国产密码算法的适配能力,还确保了身份认证过程的安全性、与现有研究相比,该协议在保障安全自主可控方面展现出了更为突出的优势。

2) 密集车辆场景下认证效率的提升:针对密集车辆场景下多车同时切换认证时面临的效率低难题,本文在切换认证协议中设计了一种高效的批量认证算法。该算法通过精简认证流程、实现多车请

求的并行处理,大幅提升了路侧单元的认证效率。相较于逐个认证的方法,本文所设计的算法认证效率提升约 65%,有效缓解了并发认证带来的巨大压力,为车联网的高效运行提供了有力保障。

3) 强化车辆安全性和隐私保护。本文引入了伪身份认证机制,该机制不仅能够有效隐藏车辆的真实身份及行驶轨迹,而且即使数据被截获,攻击者也难以追踪到真实车辆,为车辆提供了更为严密的隐私保护屏障。基于安全协议认证工具 AVISPA,对所设计的协议进行仿真分析,结果表明,所设计的协议是安全的,能够有效抵抗中间人攻击和重放攻击。

1 预备知识

SM2 是国家密码管理局发布的椭圆曲线公钥密码算法,主要用于数据加密、数字签名、密钥交换等。在 SM2 数字签名中,每个签名者有一对公私钥对,其中私钥用于产生签名,认证者用签名者公钥认证签名。SM2 数字签名主要包含下面 4 个步骤。

1) 系统参数生成:输入安全参数 λ ,输出系统参数 $\{E, a, b, q, G, n, P, H_v\}$ 。其中 E 是有限域上由 a 和 b 定义的一条椭圆曲线。在包含无穷远点和 E 的所有点中选取素数 n 阶循环群 G 和生成元 $P \in G$, H_v 是安全哈希函数。

2) 密钥生成:输入系统参数,随机选取 $d \in \mathbb{Z}_n^*$ 作为签名者私钥 SK,计算签名者公钥 $PK = dP$ 。

3) 签名:输入系统参数、签名者私钥 SK 和签名消息 m 。随后选取 $k \in \mathbb{Z}_n^*$,计算 $K = kP = (x_K, y_K)$, $e = H_v(m)$, $r = (e + x_K) \bmod n$ 。若 $r = 0$ 或 $r + k = 0$,则重新选取 k 并重新计算其他参数;否则计算 $s = (1 + d)^{-1}(k - rd) \bmod n$ 。若 $s = 0$,则重新选取 k 并重新计算其他参数;否则输出签名 $\sigma = (r, s)$ 。

4) 认证:输入系统参数、签名者公钥 PK、签名消息 m 和待认证的签名 σ ,若 $r, s \notin \mathbb{Z}_n^*$,则输出 0;否则计算 $t = (r + s) \bmod n$ 。若 $t = 0$,则输出 0;否则计算 $K' = sG + tPK = (x'_K, y'_K)$, $e' = H_v(m)$, $r' = (e' + x'_K) \bmod n$ 。若 $r' = r$,则输出 1,否则输出 0。其中输出 1 表示认证通过,输出 0 表示认证不通过。

2 系统模型和安全性要求

2.1 系统模型

如图1所示,传统的车联网系统由信任机构、路侧单元和车辆组成。

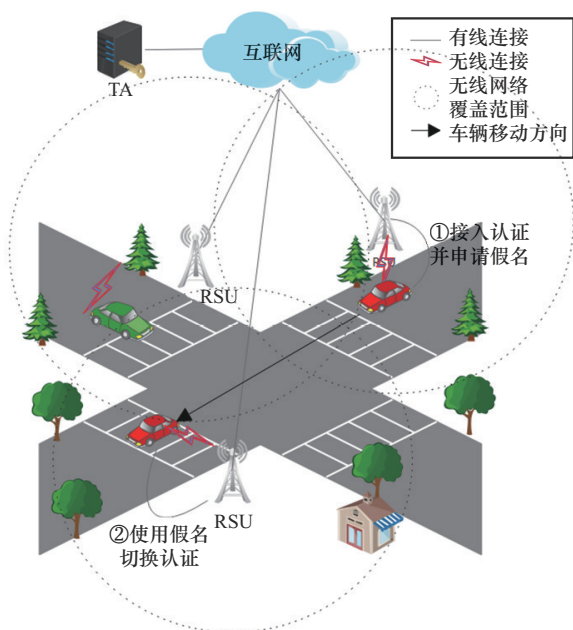


图1 系统模型
Figure 1 System model

1) TA: 扮演着完全可信的角色。在系统初始化的关键阶段,TA负责生成并分发系统运行所必需的各项参数,确保整个车联网系统的安全稳定运行。此外,TA还承担着为RSU和车辆提供注册服务的重任,通过严格的身份认证流程,确保只有合法的实体能够接入车联网系统。

2) RSU: 车联网系统中不可或缺的无线通信设备,主要职责是为过往车辆提供接入车联网的便捷服务,通常被安装在道路沿线。RSU不仅具备与TA进行安全通信的能力,还能够与周边其他RSU建立稳定的连接,共同构建一个广泛覆盖的通信网络。

3) 车辆: 每辆车都配备了先进的车载单元,这不仅使车辆能够融入车联网生态系统,还赋予了它们唯一的身份编号,如车辆识别码。

2.2 安全性要求

在复杂多变的车联网中,一个支持匿名的安全切换认证协议,需要满足以下安全性要求。

1) 用户匿名性: 任何没有主密钥的敌手,都

无法根据截获的消息来推测车辆的真实身份或者追踪车辆的行为。

2) 双向认证: 为确保加入网络节点的安全性,车辆和路侧单元之间必须完成严格的双向认证过程。这一过程要求车辆和路侧单元相互认证对方的身份和凭据,以确保通信双方的真实性。

3) 条件可追踪性: 在出现争议或需要追踪车辆行为时,系统能够在一定条件下追踪到车辆的真实身份。

4) 安全密钥建立: 在完成切换认证阶段后,认证双方将建立起临时会话密钥,确保通话内容私密性。

5) 前向安全性: 过去的会话密钥与当前的会话密钥没有关联性,不会因为信息泄露而影响彼此。

6) 抵抗各类攻击: 认证协议需要能够抵抗包括重放攻击、中间人攻击等在内的各类安全攻击。

3 协议设计

本节主要对方案的算法进行描述,算法共包含5个部分:系统初始化、注册阶段、接入认证、切换认证和批量认证。首先,阐述系统初始化流程,车辆完成注册后,采用基于国密SM2的标识数字签名技术设计所接入认证协议。随后,在车辆行驶过程中,为确保通信的持续性和安全,车辆会利用预先获取的假名及密钥信息,执行高效的匿名切换认证。此外,考虑到车辆拥堵场景下对认证效率的特殊要求,本文创新性地设计了批量认证算法。在车辆密集区域,路侧单元能够迅速执行批量认证操作,显著提升整体认证效率。

3.1 系统初始化

TA产生并发布系统参数,见表1,具体步骤如下。

TA输入安全参数 λ ,随机选取大素数 q ,确定椭圆曲线 $E: y^2 = x^3 + ax + b \pmod{q}$ ($a, b \in \mathbb{Z}_q^*$),在包含无穷远点和 E 的所有点中选取素数 n 阶循环群 G 和生成元 $P \in G$,其中 P 的坐标为 (x_P, y_P) 。随机选取 $x \in \mathbb{Z}_n^*$,计算 $P_{pub} = xP$,同时选取3个安全哈希函数: $H_1: \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^n$, $H_2: \{0,1\}^* \rightarrow \{0,1\}^{256}$ 和 $H_3: \{0,1\}^* \times \{0,1\}^* \rightarrow \mathbb{Z}_n^*$ 。选择 x 作为系统主私钥 msk ,并公开系统参数 $\{E, a, b, q, G, n, P, P_{pub}, H_1, H_2, H_3\}$ 。

表 1 系统参数
Table 1 System parameters

参数	含义
RID_i, VID_i	第 i 个路侧单元和第 i 辆车身份 ID
E	有限域上的一条椭圆曲线
G	n 阶循环群
P	群 G 的一个生成元
msk	系统主私钥
PID_j	车辆的伪身份 ID
ts	时间戳
exp	密钥和身份信息的有效期
H_1, H_2, H_3	安全哈希函数
PTK	路侧单元和车辆协商的会话密钥
$\parallel$	级联运算符

3.2 注册阶段

3.2.1 路侧单元 RSU_i

TA 选择 $RID_i \in \mathbb{Z}_n^*$ 作为路侧单元 RSU_i 的身份 ID, 选取随机数 $u_R \in [1, n-2]$, 并计算 $Q_R = u_R P = (x_{Q_R}, y_{Q_R})$, $w_R = H_3(RID_i \parallel Q_R)$ 和 $d_R = u_R + x_{w_R} \pmod{n}$, 并将 (RID_i, d_R, Q_R) 通过安全通道发送给 RSU_i 秘密保存。

3.2.2 车辆 V_i

TA 选择 $VID_i \in \mathbb{Z}_n^*$ 作为车辆 V_i 的身份 ID, 选取随机数 $u_v \in [1, n-2]$, 并计算 $Q_v = u_v P = (x_{Q_v}, y_{Q_v})$, $w_v = H_3(VID_i \parallel Q_v \parallel \exp)$, $d_v = u_v + x_{w_v} \pmod{n}$, 其中 $\exp$ 是该车辆身份及相关密钥的有效期, 将 $(VID_i, d_v, Q_v, \exp)$ 通过安全通道发送给车辆 V_i 秘密保存。当 V_i 获得注册信息后, 可预计算认证过程密钥信息, 以减少认证过程所产生的计算时延。 V_i 根据注册阶段所获得的密钥和系统公开参数, 计算 $Z_v = H_2(ENTL_v \parallel VID_i \parallel a \parallel b \parallel x_P \parallel y_P \parallel x_{Q_v} \parallel y_{Q_v})$ 和 $e_v = H_1(Z_v \parallel ts)$, 其中 $ENTL_v$ 是 VID_i 的比特长度, ts 是时间戳。选取随机数 $k_v \in \mathbb{Z}_n^*$, 计算 $K_v = k_v P = (x_{K_v}, y_{K_v})$, $r_v = (e_v + x_{K_v}) \pmod{n}$, 如果 $r_v = 0$ 或 $r_v + k_v = 0$, 则重新选取 k_v 并计算其他参数; 否则计算 $\sigma_v = (1 + d_v)^{-1} (k_v - r_v d_v) \pmod{n}$, 若 $\sigma_v = 0$, 则重新选取 k_v 并计算其他参数。

3.3 接入认证

接入认证过程如图 2 所示, 具体步骤如下。

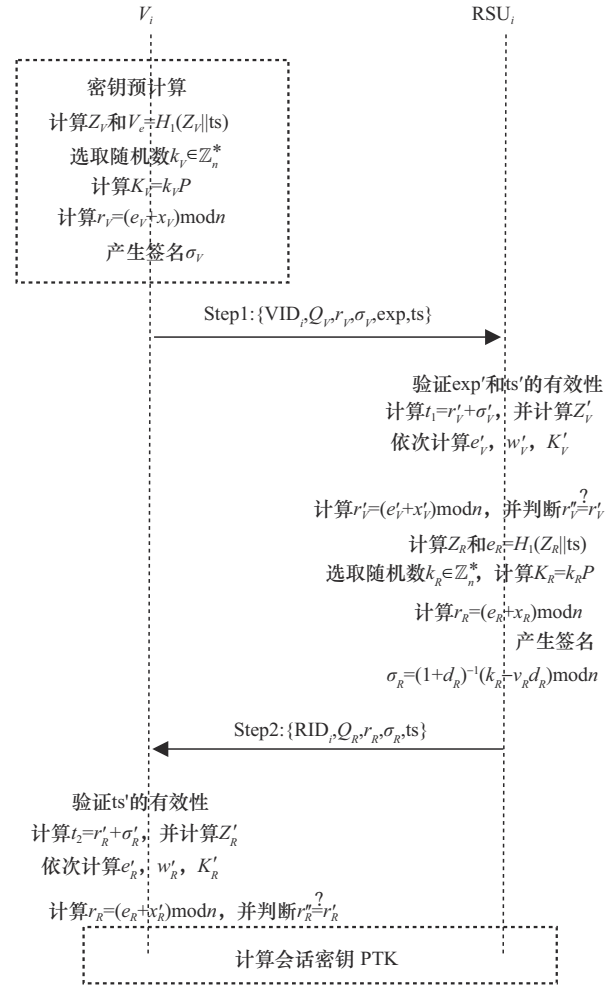


图 2 接入认证过程

Figure 2 Access authentication process

Step1 V_i 将预计算得到的签名信息和相关参数 $\{VID_i, Q_v, r_v, \sigma_v, \exp, ts\}$ 发送给 RSU_i 请求接入认证。

Step2 当收到 V_i 的认证请求消息 $\{VID_i, Q_v, r'_v, \sigma'_v, \exp, ts'\}$ 后, RSU_i 首先通过 $\exp'$ 认证该车辆密钥信息是否有效, 并认证时间戳 ts' 是否过期。如果有效且没过期, 计算 $t_1 = r'_v + \sigma'_v$, 若 $t_1 = 0$, 则认证不通过; 否则, 依次计算 $Z'_v = H_2(ENTL_v \parallel VID_i \parallel a \parallel b \parallel x_P \parallel y_P \parallel x'_{Q_v} \parallel y'_{Q_v})$, $e'_v = H_1(Z'_v \parallel ts')$, $w'_v = H_3(VID_i \parallel Q'_v \parallel \exp')$, $K'_v = \sigma'_v P + t_1 (Q'_v + w'_v P_{pub}) = (x'_{K_v}, y'_{K_v})$ 和 $r''_v = (e'_v + x'_{K_v}) \pmod{n}$ 。如果 $r''_v \neq r'_v$, 则证明该车辆不合法, 拒绝接入请求; 否则, 计算 $Z_R = H_2(ENTL_R \parallel RID_i \parallel a \parallel b \parallel x_P \parallel y_P \parallel x_{Q_R} \parallel y_{Q_R})$ 和 $e_R = H_1(Z_R \parallel ts)$, 其中 $ENTL_R$ 是 RID_i 的比特长度, ts 是时间戳。选取随

机数 $k_R \in \mathbb{Z}_n^*$, 计算 $K_R = k_R P = (x_R, y_R)$ 和 $r_R = (e_R + x_R) \bmod n$, 如果 $r_R = 0$ 或 $r_R + k_R = 0$, 则重新选取 k_R 并计算其他参数; 否则计算 $\sigma_R = (1 + d_R)^{-1}(k_R - r_R d_R) \bmod n$ 。若 $\sigma_R = 0$, 则重新选取 k_R 并计算其他参数; 否则, 将 $\{ \text{RID}_i, Q_R, r_R, \sigma_R, \text{ts} \}$ 发送给 V_i 认证, 并计算与 V_i 的临时会话密钥 $\text{PTK}_R = k_R x'_{V'}$ 。

Step3 当收到 RSU_i 的返回的消息 $\{ \text{RID}'_i, Q'_R, r'_R, \sigma'_R, \text{ts}' \}$ 后, V_i 首先认证时间戳 ts' 是否过期, 如果没过期, 则计算 $t_2 = r'_R + \sigma'_R$, 若 $t_2 = 0$ 则认证不通过; 否则依次计算 $Z'_R = H_2(\text{ENTL}_R \| \text{RID}'_i \| a \| b \| x_P \| y_P \| x'_{Q_R} \| y'_{Q_R})$ 、 $e'_R = H_1(Z'_R \| \text{ts}')$ 、 $w'_R = H_3(\text{RID}'_i \| Q'_R)$ 、 $K'_R = \sigma'_R P + t_2(Q'_R + w'_R P_{\text{pub}}) = (x'_R, y'_R)$ 和 $r''_R = (e'_R + x'_R) \bmod n$ 。如果 $r''_R \neq r'_R$, 则证明该路侧单元不合法, 拒绝接入; 否则计算临时会话密钥 $\text{PTK}_V = k_V x'_R$, 并开始通信。

当 V_i 完成接入认证后, V_i 将通过 RSU_i 向 TA 发送获取假名请求。具体步骤如下: ①TA 选取 l 个不相关联的随机数 $\text{PID}_j \in \mathbb{Z}_n^*, j \in [1, l]$ 作为 V_i 的假名身份 ID。②对于 PID_j , TA 选取随机数 $r_j \in \mathbb{Z}_n^*$, 计算 $R_j = r_j P$, $w_j = H_3(\text{PID}_j \| R_j \| \text{exp}_j)$ 和 $s_j = r_j + x w_j$, 其中 exp_j 是假名 PID_j 及其相关密钥的有效期。③TA 将每个假名和其对应的密钥信息进行封装 $(\text{PID}_j, s_j, R_j, \text{exp}_j)$, 然后加密发送给 V_i 保存。

3.4 切换认证

Step1 V_i 选取随机数 $k_V \in \mathbb{Z}_n^*$, 计算 $K_V = k_V P = (x_V, y_V)$, 生成消息 $m = \{ \text{PID}_j, R_j, K_V, \text{exp}_j, \text{ts} \}$, 并产生签名 $\sigma_V = k_V + s_j H_2(m)$, 并将消息 $\{ m, \sigma_V \}$ 发送给 RSU_i 请求切换认证。

Step2 当收到 V_i 的切换认证请求消息 $\{ m', \sigma'_V \}$ 后, 其中 $m' = \{ \text{PID}'_j, R'_j, K'_V, \text{exp}'_j, \text{ts}' \}$, RSU_i 首先通过 exp'_j 认证身份密钥信息是否有效, 并认证时间戳 ts' 是否过期, 如果有效且没过期, 则计算 $P_V = H_3(\text{PID}'_j \| R'_j \| \text{exp}'_j) P_{\text{pub}} + R'_j$ 。如果 $\sigma'_V P$ 和 $K'_V + H_2(m') P_V$ 相等, 则证明该车辆合法, 允许其接入。计算 $e_R = H_1(Z_R \| \text{ts})$, 其中 ts 是时间戳。选取随机数 $k_R \in \mathbb{Z}_n^*$, 计算 $K_R = k_R P = (x_R, y_R)$ 和 $r_R = (e_R + x_R) \bmod n$, 如果 $r_R = 0$ 或 $r_R + k_R = 0$, 则重新选取 k_R 并计算其他参数; 否则计算 $\sigma_R =$

$(1 + d_R)^{-1}(k_R - r_R d_R) \bmod n$ 。若 $\sigma_R = 0$, 则重新选取 k_R 并计算其他参数; 否则, 将 $\{ \text{RID}_j, Q_R, r_R, \sigma_R, \text{ts} \}$ 发送给 V_i 认证, 并计算与 V_i 的临时会话密钥 $\text{PTK}_R = k_R x'_{V'}$ 。

Step3 当收到 RSU_i 的返回的消息 $\{ \text{RID}'_j, Q'_R, r'_R, \sigma'_R, \text{ts}' \}$ 后, V_i 首先认证时间戳 ts 是否过期, 如果没过期, 计算 $t_2 = r'_R + \sigma'_R$, 若 $t_2 = 0$, 则认证不通过; 否则依次计算 $Z'_R = H_2(\text{ENTL}_R \| \text{RID}'_j \| a \| b \| x_P \| y_P \| x'_{Q_R} \| y'_{Q_R})$ 、 $e'_R = H_1(Z'_R \| \text{ts}')$ 、 $w'_R = H_3(\text{RID}'_j \| Q'_R)$ 、 $K'_R = \sigma'_R P + t_2(Q'_R + w'_R P_{\text{pub}}) = (x'_R, y'_R)$ 、 $r''_R = (e'_R + x'_R) \bmod n$ 。如果 $r''_R \neq r'_R$, 则证明该路侧单元不合法, 拒绝接入; 否则计算临时会话密钥 $\text{PTK}_V = k_V x'_R$, 并开始通信。

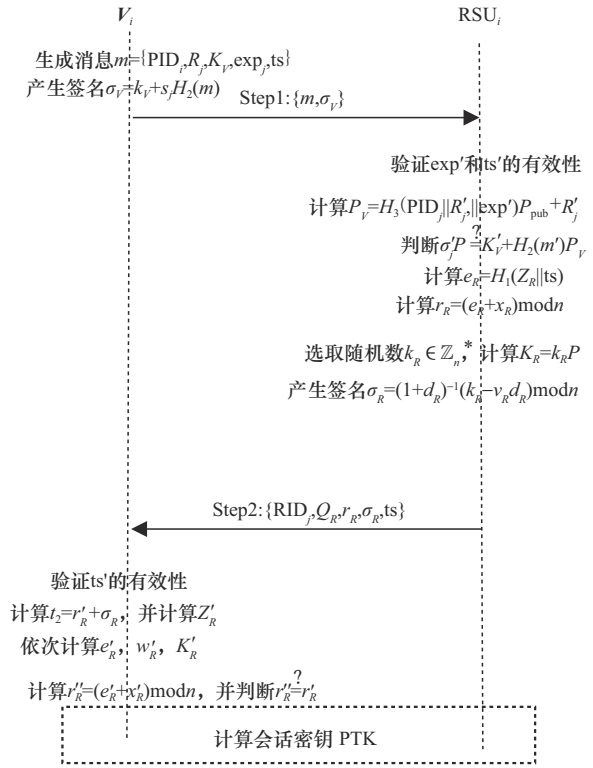


图3 切换认证过程

Figure 3 Handover authentication process

3.5 批量认证

在拥堵的交通环境中, 当多辆汽车竞相进行切换认证时, 路侧单元面临着并行处理的挑战, 这往往导致部分车辆无法正常完成认证过程。针对这一难题, 本文所设计的协议引入了批量认证算法, 显著增强了RSU的并发处理能力, 从而

实现了多部车辆的无缝、高效同步认证。具体方案分为两种场景。

(1) 两辆车场景

假设身份为 PID_1 和 PID_2 的两辆车同时请求认证, 其发送给 RSU 的认证消息分别为 $\{m_1, \sigma_1\}$ 和 $\{m_2, \sigma_2\}$, 其中 $m_1 = \{PID_1, R_1, K_1, \exp_1, ts_1\}$, $m_2 = \{PID_2, R_2, K_2, \exp_2, ts_2\}$ 。

Step1 两辆车各自将认证消息 $\{m_1, \sigma_1\}$ 和 $\{m_2, \sigma_2\}$ 发送给 RSU 请求切换认证。

$$\begin{aligned} (\sigma_1 + \sigma_2)P &= K_1 + H_2(m_1)P_{v1} + K_2 + \\ &H_2(m_2)P_{v2} = K_1 + K_2 + \\ &H_2(m_1)[H_3(PID_1||R_1||\exp_1)P_{pub} + R_1] + \\ &H_2(m_2)[H_3(PID_2||R_2||\exp_2)P_{pub} + R_2] = \\ &K_1 + K_2 + H_2(m_1)H_3(PID_1||R_1||\exp_1)P_{pub} + \\ &H_2(m_1)R_1 + H_2(m_2)H_3(PID_2||R_2||\exp_2)P_{pub} + (1) \\ &H_2(m_2)R_2 = (K_1 + K_2) + \\ &[H_2(m_1)R_1 + H_2(m_2)R_2] + \\ &[H_2(m_1)H_3(PID_1||R_1||\exp_1) + \\ &H_2(m_2)H_3(PID_2||R_2||\exp_2)]P_{pub} \end{aligned}$$

Step2 当 RSU 收到切换请求消息后, 首先认证车辆 PID_1 和 PID_2 身份信息有效期和时间戳是否过期, 如果认证通过, 则依据式(1)进一步确认车辆的合法性, 确认车辆是合法的, RSU 才会允许车辆接入网络。

(2) n 辆车场景

假设 n 辆车同时发起切换认证请求, 它们的身份分别为 $PID_1, PID_2, \dots, PID_n$, 每辆车发送的请求认证消息分别为 $\{m_1, \sigma_1\}, \{m_2, \sigma_2\}, \dots, \{m_n, \sigma_n\}$, 其中 $m_i = \{PID_i, R_i, K_i, \exp_i, ts_i\}$ 。

Step1 n 辆车各自将认证消息 $\{m_1, \sigma_1\}, \{m_2, \sigma_2\}, \dots, \{m_n, \sigma_n\}$ 发送给 RSU 请求切换认证。

Step2 当 RSU 收到切换请求消息后, 首先认证车辆 $PID_1, PID_2, \dots, PID_n$ 身份信息有效期和时间戳是否过期, 如果认证通过, 则依据式(2)进一步确认车辆的合法性, 车辆是合法的, RSU 才会允许车辆接入网络。

$$\begin{aligned} \left(\sum_{i=1}^n \sigma_i \right) P &= \sum_{i=1}^n [K_i + H_2(m_i)R_i] + \\ &\left[\sum_{i=1}^n H_2(m_i)H_3(PID_i||R_i||\exp_i) \right] P_{pub} \end{aligned} \quad (2)$$

4 性能分析

4.1 切换认证协议性能分析

本文所设计的协议性能分析设定的安全参数 λ 为 32 byte。设定 T_M 、 T_A 、 T_e 和 T_p 分别表示椭圆曲线上点乘运算、椭圆曲线上加法运算、模指数运算和双线性对运算。为获得精准的性能分析数据, 本文在搭载不同处理器的 Windows7 系统上, 通过运行 Miracl 库对各类型运算进行 10 000 次测试, 并取平均计算耗时。表 2 给出各类运算计算耗时。后文如无特殊说明, 将以 2.0 GHz 处理器进行分析计算。

表 2 各类运算计算耗时

Table 2 Execution time of various operations

运算方式	单次计算耗时/ms		
	1.2 GHz 处理器	1.8 GHz 处理器	2.0 GHz 处理器
T_M	4.152	2.765	2.466
T_A	0.143	0.092	0.081
T_e	23.206	15.336	13.701
T_p	13.281	8.738	7.834

如表 3 所示, 忽略简单运算的时间, 将本文方案与文献[8,15-17]方案进行比较。文献[8,15]方案需要复杂的双线性对运算, 因此认证效率较低; 本文方案与文献[16-17]方案认证效率相当, 单次认证共涉及 5 次 T_M 和 4 次 T_A 计算, 预计耗时 12.65 ms。本文对不同方案在不同处理器上的认证效率进行了对比分析。从图 4 中可以看出, 相较于其他方案, 本文方案展现出了更高的认证效率。

表 3 认证效率比较分析

Table 3 Comparative analysis of authentication efficiency

方案	逐个认证	批量认证 n 次
文献[8]	$6T_p + 22T_M$	$4nT_p + (6n - 1)T_M$
文献[15]	$6T_p + 6T_M$	$(3n + 1)T_p + (n + 2)T_M$
文献[16]	$2T_p + 5T_e$	$(1 + n)T_p + (4 + n)T_e$
文献[17]	$8T_M$	$5nT_M$
本文方案	$5T_M + 4T_A$	$(3n + 2)T_M + 4nT_A$

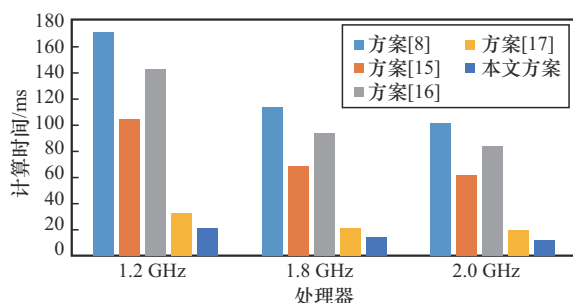


图4 认证效率比较

Figure 4 Comparison results of authentication efficiency

4.2 批量认证

忽略简单的运算, RSU对两辆车逐个认证需要产生6次 T_M 和4次 T_A , 预计耗时15.12 ms; 而批量认证两辆车共产生4次 T_M 和4次 T_A , 预计耗时10.19 ms。假设 n 辆车同时请求认证, RSU在逐辆认证下需要产生 T_M 共 $3n$ 次, T_A 共 $2n$ 次, 预计耗时 $7.56n$ ms; 而批量认证需要产生 T_M 共 $n+2$ 次, T_A 共 $2n$ 次, 预计耗时 $2.63n+4.93$ ms, 随着认证车辆数量的增加, RSU的认证效率提升约65%。

如图5所示, 本文依托Fedora release 9系统环境, 在QT Creator 2.4.1开发平台上, 设计了多线程模拟路侧单元和车辆, 通过Socket技术模拟汽车向路侧单元发起切换认证请求的场景。将本文方案与文献[8,15-17]方案进行模拟测试, 测试10, 20, 40, ..., 320辆车在10 000次批量认证过程后的单次批量认证平均时间以及RSU的每次认证平均时间, 批量认证模拟测试结果见表4。当认证车辆数量达到320辆时, RSU的认证效率较传统方法提升了约65%, 与理论分析提升的效率一致。如图6所示, 相较于传统的逐个认证, 在认证车辆数量增多的情况下, 本文设计的批量认

证方案所展现出的效率优势越发明显, 且优于其他批量认证方案, 具有良好的应用价值。



图5 切换认证协议测试系统

Figure 5 Handover authentication protocol testing system

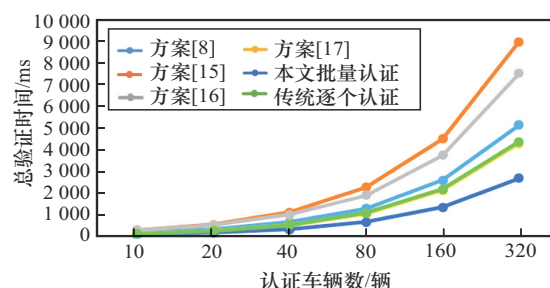


图6 批量认证效率分析

Figure 6 Analysis of batch authentication efficiency

5 安全性分析

5.1 AVISPA工具可视化仿真分析

AVISPA是一种网络安全协议的分析工具, 它不仅可以发现协议攻击和漏洞, 还可以对有限和无限数量会话的协议进行认证^[29-30]。AVISPA分析工具集成了OFMC、CL-AtSe、SATMC和TA4SP这4款认证工具, 均以HLPSP (high level protocol specification language)为输入, 自动转化为IF (intermediate format)语言之后, 用

表4 批量认证模拟测试结果

Table 4 Test results of batch authentication simulation

车辆数	方案[8]	方案[15]	方案[16]	方案[17]	RSU认证时间/总认证时间/ms		RSU认证效率提升比例
					本文批量认证	传统逐个认证	
10	192	295	315	137	32/94	79/139	59.3%
20	367	577	547	282	60/181	159/278	61.9%
40	681	1157	1027	5434	116/349	317/557	63.6%
80	1323	2316	1925	1077	226/691	635/1117	64.4%
160	2637	4583	3819	2179	447/1376	1270/2229	64.8%
320	5245	9125	7659	4365	887/2736	2540/4451	65.1%

户选择后台认证器进行分析。

使用 HLPSSL 对系统角色进行定义, V、R 和 TA 分别表示车辆、路侧单元和可信机构。选取 Dolev-Yao 作为攻击模型, 该模型给予入侵者极为强大的能力, 其不仅能够拦截、解析并篡改消息内容, 还能发送伪造的新消息, 借此伪装成其他通信实体。设定安全目标如图 7 所示, 涵盖车辆和路侧单元之间的强认证, 具体涉及两个强认证目标 rsu_vic_kr 和 vic_rsu_kv , 以及两者之间协商会话密钥的保密性 kh 。后端运用 OFMC 和 CL-AtSe 两款认证工具进行仿真分析, 仿真结果如图 8 和图 9 所示。结果显示“SAFE”, 表明该协议是安全的, 能够达到预先设定的强认证和密钥机密性的目标。在车辆和路侧单元角色建立及通信过程中, 通过引入随机数, 确保消息的唯一性, 有效抵御攻击者利用截获的消息实施重放攻击。同时, 采用加密算法和强认证, 保障数据完整性和双方身份的真实性, 有力防止攻击者冒充用户进行通信的行为。

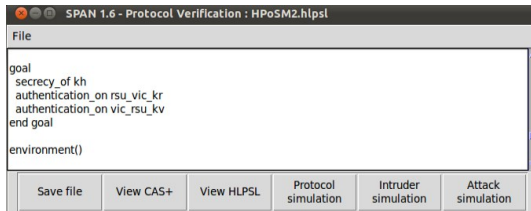


图 7 设定安全目标
Figure 7 Set safety goals

假设攻击者掌握了一定的通信数据, 并企图利用这些数据突破密钥保密性。攻击者通过分析截获的消息, 结合已知的部分密钥信息, 试图破解会话密钥。在针对强认证目标 rsu_vic_kr 和 vic_rsu_kv 的攻击中, 攻击者利用 Dolev-Yao 模型赋予的能力, 伪装成合法车辆 V, 向路侧单元 R 发送伪造的消息, 试图绕过强认证机制, 建立与路侧单元的通信连接, 进而获取敏感信息。针对攻击者对密钥保密性的攻击, 系统采用了复杂的加密算法以及密钥协商机制。在会话密钥协商过程中, 利用非对称加密和哈希函数等技术, 确保即使攻击者获取部分信息, 也无法推算出完整的会话密钥。对于攻击者针对强认证目标的攻击, 路侧单元 R 在接收到消息后, 依据预设的强认证机制, 对消息中的认证信息进行多维度认证, 一旦发现认证信

息异常, 路侧单元 R 立即拒绝与攻击者进行通信, 从而保障了系统的安全性。

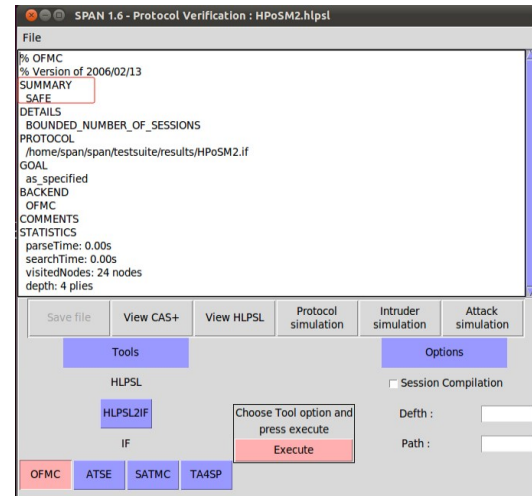


图 8 OFMC 工具仿真结果
Figure 8 OFMC tool simulation results

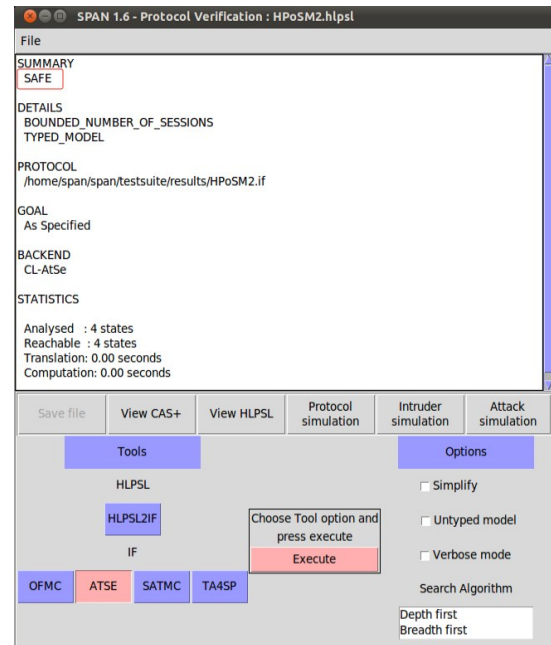


图 9 CL-AtSe 工具仿真结果
Figure 9 CL-AtSe tool simulation results

5.2 协议安全特性分析

1) 用户匿名性: 在切换认证过程中, 车辆使用互不关联的假名 $PID_j \in \mathbb{Z}_n^*, j \in [1, l]$ 请求认证, 确保每次认证过程所使用的假名均不相同。因此, 任何未掌握主密钥的潜在威胁者, 仅凭截获的信息既无法识别出车辆的真实身份, 也无法追踪车辆的活动轨迹。

2) 双向认证：RSU可以通过认证车辆签名的有效性来确认车辆身份的合法性，认证方法见式(3)。在消息没有被篡改的条件下 $\sigma'_V P$ 和 $K'_V + H_2(m')P_V$ 是相等的。车辆通过判断 r''_R 和 r'_R 是否一致，从而确定RSU是否合法，而判断 r''_R 和 r'_R 是否一致，只需要判断 K_R 和 K'_R 是否一致即可，判断方法见式(4)。在消息没有被篡改的条件下， K_R 和 K'_R 是相等的。

$$\begin{aligned}\sigma'_V P &= K'_V + H_2(m')P_V = \\ k_V P + H_2(m)s_j P &= \\ (k_V + s_j H_2(m))P &= \sigma_V P\end{aligned}\quad (3)$$

$$\begin{aligned}K'_R &= \sigma_R P + t_2(Q_R + w_R P_{\text{pub}}) = \\ \sigma_R P + (r_R + \sigma_R)(u_R P + w_R xP) &= \\ \sigma_R P + (r_R + \sigma_R)d_R P &= \\ (\sigma_R + r_R d_R + \sigma_R d_R)P &= \\ [(1 + d_R)\sigma_R + r_R d_R]P &= \\ (k_R - r_R d_R + r_R d_R)k_R &= k_R P = K_R\end{aligned}\quad (4)$$

3) 条件可追踪性：在检测到潜在的安全威胁或确认系统内部存在攻击行为时，TA能够利用其掌握的所有假名及其密钥信息，通过分析传输的消息内容，来追溯并确认攻击者的真实身份。

4) 安全密钥建立：当车辆与路侧单元成功完成双向身份认证后，双方会根据相互交换的参数以及各自持有的密钥信息，由式(5)共同生成一个安全会话密钥。

$$\text{PMK}_R = k_R x'_V = k_R k_V P = k_V x'_R = \text{PMK}_V \quad (5)$$

5) 前向安全性：在车辆每次进行切换认证的过程中，为了保障通信的机密性和不可预测性，车辆会采用全新的、不与其他会话相关联的假名进行身份隐藏，并且会为每次会话生成独特的会话密钥。因此，即使攻击者能够窃听到当前的通信信息，包括假名和会话密钥的交换过程，他们也无法利用这些信息来推导出之前的会话密钥。

6) 抵抗各类攻击：为了确保消息传输的安全性，在每次传送的消息中都嵌入了时间戳和随机数。时间戳的加入确保了消息的时效性，使得攻击者难以通过截获消息来发起重放攻击。同时，随机数的引入增加了消息的唯一性，进一步降低了重放攻击的成功率。此外，每次消息的签名过程都严格依赖于签名者的私密信息以及一组公开参数，这种机制确保了签名的不可伪造性。攻击

者即使截获了消息和签名，也无法在没有获得签名者密钥的情况下伪造有效的签名，因此能够有效地抵御中间人攻击。

6 结束语

本文基于国密SM2设计了一种匿名切换认证协议，该协议通过融合国产密码算法、提升切换认证效率以及增强匿名性和隐私保护，为车联网系统提供了更为高效、安全的解决方案。特别是在密集车辆环境下，该协议引入了批量认证算法，RSU认证效率较传统方法提升约65%，极大地缓解了RSU认证压力。通过理论与AVISPA工具实验分析证明，该方案在保障系统安全性的同时，大幅提高了认证效率，为车辆间的高效、安全通信及数据交换提供了强有力的支持。

未来工作将重点关注该协议在车联网中的实际应用，通过试验来进一步认证和优化认证协议的安全性和性能。

参考文献：

- [1] SON S, LEE J, PARK Y, et al. Design of blockchain-based light-weight V2I handover authentication protocol for VANET[J]. IEEE Transactions on Network Science and Engineering, 2022, 9(3): 1346-1358.
- [2] LI X C, YIN X C. Blockchain-based group key agreement protocol for vehicular ad hoc networks[J]. Computer Communications, 2022, 183: 107-120.
- [3] CUI J, TAO X F, ZHANG J, et al. HCPA-GKA: A hash function-based conditional privacy-preserving authentication and group-key agreement scheme for VANETs[J]. Vehicular communications, 2018, 14: 15-25.
- [4] QIAO Z R, MA K, ZHOU Y W, et al. An anonymous and efficient certificate-based identity authentication protocol for VANET[J]. IEEE Internet of Things Journal, 2023.
- [5] 张海波, 余艺, 王冬宇, 等. 面向车联网通勤的双阶段认证密钥协商协议[J]. 通信学报, 2024, 45(5): 128-139.
ZHANG H B, Y Y, WANG D Y, et al. Two-stage authentication and key agreement protocol for commuting in Internet of vehicles[J]. Journal on Communications, 2024, 45(5): 128-139.
- [6] TAN H W, ZHENG W Y, VIJAYAKUMAR P. Secure and efficient authenticated key management scheme for UAV-assisted infrastructure-less IoVs[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(6): 6389-6400.
- [7] SIKARWAR H, DAS D. A novel MAC-based authentication scheme (NoMAS) for internet of vehicles (IoV)[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(5): 4904-4916.
- [8] 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.
- [9] XU Z Y, HE D B, KUMAR N, et al. Efficient certificateless aggregate signature scheme for performing secure routing in VANETs[J]. Security and Communication Networks, 2020, 2020(1): 5276813.
- [10] LI X, LIU T, OBADAT M S, et al. A lightweight privacy-preserving authentication protocol for VANETs[J]. IEEE Systems Journal, 2020, 14(3): 3547-3557.
- [11] 何业锋, 张茜, 陈鸣欣, 等. 车联网中基于阈值的边缘辅助身份认证方案[J]. 计算机应用研究, 2024, 41(10): 3155-3159.
- HE Y F, ZHANG X, CHEN M X, et al. Threshold-based edge-assisted identity authentication scheme in VANET[J]. Application Research of Computers, 2024, 41(10): 3155-3159.
- [12] 张应辉, 钱佳乐, 曹进, 等. 5G-V2X 中基于轨迹预测的安全高效群组切换认证协议[J]. 通信学报, 2023, 44(8): 144-154.
- ZHANG Y H, QIAN J L, CAO J, et al. Secure and efficient group handover authentication protocol based on trajectory prediction in 5G-V2X[J]. Journal on Communications, 2023, 44(8): 144-154.
- [13] MUHAMMAD A S, XIONG L, KHALID M, et al. A cost-efficient anonymous authenticated and key agreement scheme for v2i-based vehicular ad-hoc networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2024, 25(9): 12621-12630.
- [14] ZHAO C, GUO N, GAO T H, et al. PEPA: Paillier cryptosystem-based efficient privacy-preserving authentication scheme for VANETs[J]. Journal of Systems Architecture, 2023, 138: 102855.
- [15] YANG A J, WENG J, YANG K, et al. Delegating authentication to edge: A decentralized authentication architecture for vehicular networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2020, 23(2): 1284-1298.
- [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] LI S L, YANG R L, CHEN J G. A privacy-preserving authentication scheme for VANETs with exculpability[J]. Security and Communication Networks, 2023, 2023(1): 8676929.
- [18] ZHU F, YI X, ABUADDBA A, et al. A security-enhanced certificateless conditional privacy-preserving authentication scheme for vehicular ad hoc networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(10): 10456-10466.
- [19] LIU X X, WANG Y C, LI Y P, et al. PTAP: A novel secure privacy-preserving & traceable authentication protocol in VANETs[J]. Computer Networks, 2023, 226: 109643.
- [20] SU H D, DONG S, WANG N, et al. An efficient privacy-preserving authentication scheme that mitigates TA dependency in VANETs[J]. Vehicular Communications, 2024, 45: 100727.
- [21] SHEN S Y, YANG Y, LIU X M. Toward data privacy preservation with ciphertext update and key rotation for IoT[J]. Concurrency and Computation: Practice and Experience, 2023, 35(20): e6729.
- [22] HU X H, ZHENG X, ZHANG S S, et al. A high-performance elliptic curve cryptographic processor of SM2 over GF(p)[J]. Electronics, 2019, 8(4): 431.
- [23] 郭辉, 罗勇, 郭晓璐. 基于国密算法的车载以太网控制器身份认证方法[J]. 网络与信息安全学报, 2022, 8(6): 20-28.
- GUO H, LUO Y, GUO X L. Automotive ethernet controller authentication method based on national cryptographic algorithms[J]. Chinese Journal of Network and Information Security, 2022, 8(6): 20-28.
- [24] WU K H, CHENG R, CUI W C, et al. A lightweight SM2-based security authentication scheme for smart grids[J]. Alexandria Engineering Journal, 2021, 60(1): 435-446.
- [25] 胡小明, 陈海婵. 可证明安全的 SM2 盲适配器签名方案[J]. 网络与信息安全学报, 2024, 10(2): 59-68.
- HU X M, CHEN H C. Proven secure blind adaptor signature scheme based on the SM2[J]. Chinese Journal of Network and Information Security, 2024, 10(2): 59-68.
- [26] JI H H, ZHANG H J, SHAO L S, et al. An efficient attribute-based encryption scheme based on SM9 encryption algorithm for dispatching and control cloud[J]. Connection Science, 2021, 33(4): 1094-1115.
- [27] GB/T 32918.2-2016, 信息安全技术 SM2 椭圆曲线公钥密码算法 第 2 部分: 数字签名算法[S]. 2016.
- GB/T 32918.2-2016, Information security technology - SM2 elliptic curve public key cryptographic algorithm - Part 2: Digital signature algorithm [S]. 2016.
- [28] 何德彪, 张佳妮, 陈泌文, 等. 一种基于 SM2 的身份基的数字签名方法与系统: CN108809658A[P]. 2018-11-13.
- HE D B, ZHANG J N, CHEN B W, et al. An identity-based digital signature method and system based on SM2: CN108809658A[P]. 2018-11-13.
- [29] 陆思奇, 程庆丰, 赵进华. 安全协议形式化分析工具比较研究[J]. 密码学报, 2014, 1(6): 568-577.
- LU S Q, CHENG Q F, ZHAO J H. Comparison study of formal verification tools for security protocols[J]. Journal of Cryptologic Research, 2014, 1(6): 568-577.
- [30] TEAM T A. HLPSSL tutorial—the AVISPA project[EB]. 2005.

[作者简介]



苏彬庭 (1990-), 男, 福建泉州人, 福建师范大学实验师, 主要研究方向为网络与信息安全。



方禾 (1991-), 女, 福建莆田人, 福建师范大学教授, 主要研究方向为无线网络安全、智能认证、信任管理。



许力 (1970-), 男, 福建福州人, 福建师范大学教授, 主要研究方向为网络与数据安全、计算机通信网络、大数据与信息化、复杂系统分析。