车联网场景下轻量级 RFID 认证协议的设计与安全分析

路玉君 [1]
LU Yujun

摘 要 目前车联网场景下的射频识别技术认证协议难以兼顾轻量级部署与安全防护，为了解决这一问题，文章研究设计了一种基于哈希函数结合异或运算的轻量级射频识别技术认证协议。利用异或运算完成车辆 Tag 与路侧单元在信任中心的注册，并引入动态临时身份以解决车联网设备隐私泄露问题。结果显示，研究协议在认证总时长上的表现优于对比协议，其在训练集和测试集中的认证总时长增长幅度远远小于对比协议。当标签总数为 400 时，研究协议在训练集和测试集中的认证总时长分别为 0.89log(*t*) 和 0.75log(*t*)。当运算次数为 3 000 时，研究协议的运算时间仅仅为 2.89 ms，而此时基于异或运算的射频识别认证协议和基于椭圆曲线密码的射频识别认证协议的运算时间分别达到了 8.13 ms 和 13.09 ms。以上结果说明研究协议能够有效适配车联网资源受限与安全防护的双重需求。

关键词 车联网场景；轻量级；RFID 认证协议；哈希函数；XOR

doi：10.3969/j.issn.1672-9528.2026.04.021

0 引言

随着车联网向智能交通范式的演进，车辆身份快速核验与动态轨迹追溯等需求在车联网场景下日益迫切 [1-2]。射频识别技术（radio frequency identification, RFID）因其低成本部署、抗干扰性能强等优点逐渐成为车载终端与路侧单元（road side unit, RSU）快速交互的核心支撑 [3-4]。而车联网具有开放性的通信环境，同时 RFID 标签的资源受限使得认证协议面临着轻量级部署与高安全防护的双重挑战 [5]。部分轻量级协议的运算实现身份混淆，通常因缺乏完整校验机制使得其难以抵御消息篡改与窃听攻击 [6-7]。而异或运算（exclusive OR, XOR）具有运算可逆和硬件友好的优势，不需要复杂的解密算法和计算资源即可实现高效运算过程。李喜艳等人面向图像加密与信息隐藏问题创新性地提出了一种加密域可逆隐藏方法，利用 XOR 提取出秘密信息。结果表明该方法能够通过 XOR 和误差控制确保安全性 [8]。另外，哈希函数能够保证签名的唯一性和消息的完整性，具有出色的抗碰撞性。邹光南小组针对车联网中资源受限车辆的安全认证难题提出一种基于变色龙哈希函数的连续轻量级身份认证协议，结果显示该方法可通过简化密码操作实现低开销认证 [9]。因此研究选择结合 XOR 与哈希函数构建一种轻量级 RFID 认证协议，通过 SHA-128 截断版哈希函数完成消息完整性校验，并利用 XOR 降低标签计算负担。研究的创新性在于设计了场景适配的轻量级架构，通过动态临时身份（provisional identity, PID）生成机制、密钥与身份联动更新机制适应车辆快速切换 RSU 的动态拓扑。研究旨在通过该方法为车联网提供有效的 RFID 认证解决方案，促进智能交通系统的规模化安全落地。

1 面向车联网场景的轻量级 RFID 认证协议设计

1.1 基于 XOR 的 RFID 认证协议构建

XOR 作为一种针对二进制位的逻辑运算，相较于传统加密算法具有更简单的运算规则和更快的计算速度。车联网场景下，RFID 认证协议中标签与写读器、信任中心之间的传输数据需要保护，且通常需要应用于资源受限的标签设备上 [10-11]。XOR 可对数据进行加密混淆使得截获者难以直接获取原始数据信息，可作为车联网场景下低成本标签方案的探索方向。在密钥管理方面，XOR 运算在每次认证过程中可利用其结合新生成的随机数对原有密钥进行更新。标签和信任中心（trust authority, TA）无需复杂的密钥协商协议，均可按照 XOR 运算得到新密钥并实现密钥的同步更新。根据此过程保证了每次认证的密钥新鲜度，在提升系统安全性的同时降低了密钥管理的复杂度。因此研究将 XOR 用于车联网场景下 RFID 认证协议的构建中，过程如图 1 所示。

1. 山西铁道职业技术学院 山西太原 030013

[基金项目] 山西省教育科学“十四五”规划 2022 年度规划课题“数字教育资源智慧化应用提升高职教育高质量发展研究”（GH-220002）

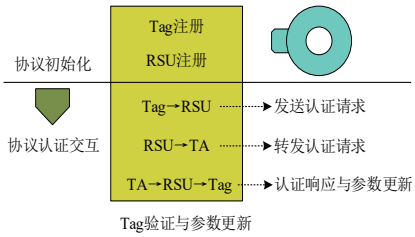

图 1 基于 XOR 的 RFID 认证协议

图 1 中，协议的初始化阶段作为协议安全的基础，负责完成车辆 Tag 与 RSU 在 TA 的注册并存储核心交互参数。TA 在车载 RFID Tag 注册部分为每个标签分配标签唯一标识（tag identification, TID）与初始共享密钥（K_0，4 字节）。将 TID 与 K_0 写入 Tag 后利用 TA 在本地数据库中存储“TID-K_0”的映射关系。RSU 注册部分利用 TA 为每个 RSU 分配路侧单元标识（road side unit identification, RID）（4 字节）、RSU 与 TA 的共享密钥（K_{RSU}，4 字节）。将 RID 与 K_{RSU} 存储至 RSU 中，TA 本地存储 RID、K_{RSU} 映射用于验证 RSU 身份的合法性。协议认证交互流程基于 XOR 的认证流程进行 3 轮消息交互，并通过随机数动态混淆数据以避免固定密钥泄露。为了避免重放攻击，首先利用 Tag 生成 16 位随机数 R_1，将自身 TID 通过与 K_0、R_1 的 XOR 运算混淆生成认证消息 M_1，其计算公式 [12] 为：

$$M_1 = \mathrm{TID} \oplus K_0 \oplus R_1 \tag{1}$$

式中：R_1 用于后续 TA 与 Tag 的参数同步。利用 Tag 将“M_1+R_1”发送至 RSU 后生成 16 位随机数 R_2，并将接收的 M_1、R_1 和 RID 整合为消息 M_2。M_2 的计算公式为：

$$M_2 = M_1 \oplus R_1 \oplus \mathrm{RID} \oplus R_2 \tag{2}$$

同时 RSU 通过 K_{RSU} 结合 XOR 运算生成校验值 M_3 以确保自身身份的可验证性。M_3 的计算公式为：

$$M_3 = R_2 \oplus K_{RSU} \tag{3}$$

RSU 将“M_2+M_3+R_1+R_2”发送至 TA 后首先验证 RSU 身份，通过本地存储的 K_{RSU} 计算后与 M_3 进行对比，显示一致则确认 RSU 合法。其次反向推导 M_1 并结合 R_1 与本地“TID-K_0”映射计算得到 TID，确认 Tag 已注册后通过 TA 生成新共享密钥 K_1，采用 XOR 运算生成响应消息 M_4，其计算公式 [13] 为：

$$M_4 = K_1 \oplus R_1 \oplus R_2 \tag{4}$$

最后将加密的“M_4+K_1”发送至 RSU 解密，由 Tag 接收后通过本地 R_1、R_2 计算，根据车辆认证情况向车辆发送认证结果。结果为有效密钥格式则确认 TA 与 RSU 合法，同时更新本地密钥为 K_1 完成一次认证。

1.2 引入 Hash 函数的轻量级 RFID 认证协议优化

虽然基于 XOR 的 RFID 认证协议能够在有限的时间内快速完成数据处理和身份验证，但是此阶段的协议并不能检测消息传输过程中是否存在篡改行为，固定密钥在车辆快速切换 RSU 覆盖区域时容易被截获复用。而 Hash 函数具备较好的单向性与抗碰撞性，在数字签名中能够保障其唯一性与消息完整性。在车辆高速切换 RSU 时无需频繁与云端 TA 交互即可完成密钥更新，能够有效降低 5G 网络切换时的认证中断风险 [14]。因此研究引入 Hash 函数对提出的轻量级 RFID 认证协议进行优化，优化后的认证协议如图 2 所示。

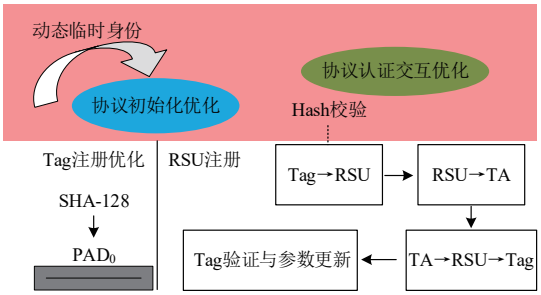

图 2 基于哈希函数与 XOR 的 RFID 认证协议

图 2 中，在协议初始化阶段引入 PID 以解决固定 PID 导致的车联网设备隐私泄露问题。当 TA 生成 PID 后通过 SHA-128 截断版对 PID 与初始密钥 K_0 的 Hash 值进行计算，得到初始临时身份 PID_0，其计算公式为：

$$\mathrm{PID}_0 = \mathrm{SHA\text{-}128\text{-}Trunc}(\mathrm{TID} \| K_0) \tag{5}$$

为确保与前一阶段协议的兼容性，协议保持 PID 与 K_{RSU} 的存储与映射关系不变。协议认证交互流程的优化中，在 XOR 的基础上新增 Hash 运算，利用车辆 Tag 生成 16 位随机数 R_1 后通过 SHA-128 截断版计算 PID_0 与 K_0 的 Hash 值，并生成消息校验值 M_1_Check。PID_0 与 K_0 的 Hash 值计算公式为 [15]：

$$\begin{cases} \mathrm{Hash\_PID} = \mathrm{SHA\text{-}128\text{-}Trunc}(\mathrm{PID}_0 \| K_0) \\ M_1 = \mathrm{PID}_0 \times \mathrm{Hash\_PID} \times \mathrm{R}_1\mathrm{M}_1\mathrm{\_Check} \\ \quad = \mathrm{SHA\text{-}128\text{-}Trunc}(M_1 \| R_1) \end{cases} \tag{6}$$

Tag 将“M_1+M_1_Check+R_1”发送至 RSU 后计算 M_1，显示与 M_1_Check 一致则确认 M_1 未被篡改。随后通过 RSU 生成 16 位随机数 R_2，计算自身 PID_0、K_{RSU} 与接收参数的 Hash 值后生成 RSU 身份校验值 M_2_Check，通过 XOR 运算整合消息 M_2 的计算公式为：

$$\begin{aligned} M_2 &= M_1 \oplus R_2 \oplus \mathrm{RID} M_2\mathrm{\_Check} \\ &= \mathrm{SHA\text{-}128\text{-}Trunc}(M_2 \| R_2 \| K_{RSU}) \end{aligned} \tag{7}$$

随后 RSU 将“M_2+M_2_Check+R_1+R_2+RID”发送至 TA 后通过本地映射计算与 M_2_Check 对比，结果一致则确认 RSU 合法。认证响应与动态更新部分通过 TA 解析 Tag 的身份，并由 TA 生成新密钥 K_1 与新临时身份 PID_1，其计算公式为：

$$PID_1=SHA\text{-}128\text{-}Trunc(TID_0 \| K_1) \quad (8)$$

最终经 Tag 比对 M_3 后更新本地 PID 为 PID_1、K 为 K_1 并完成认证。标签和 TA 在每次认证完成后均依据上述规则更新密钥与 PID，形成“一次一密”的动态安全链以确保车联网高移动性场景下每次认证的安全性与隐私保护。同时通过密钥与身份更新阶段有效适应车辆快速切换 RSU 的动态拓扑。

2 RFID 认证协议的性能验证

为了验证所提出的 RFID 认证协议，研究选择将其与基于异或运算的射频识别认证协议（XOR-based radio frequency identification authentication protocol, XOR-RFID）、基于椭圆曲线密码的射频识别认证协议（elliptic curve cryptography-based radio frequency identification authentication protocol, ECC-RFID）协议进行对比。实验环境设置中，Tag 为 ATmega 16（8 位 AVR 单片机），RSU 选择树莓派 4B（R2000 模块），TA 为普通 PC 机，处理器选择 Intel i5。内存大小为 8 GB，操作系统为 Linux，协议基于 C 语言实现，仿真与测试工具为 NS-3 网络、OpenSSL 库。研究将通信频率设置为 915 MHz，通信速率 27 kbit/s，车辆移动速度和 RSU 间距分别设置为 60 km/h 和 500 m。选择 SHA-128 截断版作为协议的哈希函数，输出长度的共享密钥长度均为 128 位，随机数长度为 64 位。研究利用 NS-3 网络仿真工具对车联网中车辆的移动轨迹、RSU 分布、RFID 标签与 RSU 的通信过程进行模拟，生成包含认证请求和响应消息等认证交互数据。并通过设置不同的攻击场景生成带攻击标签的数据集以测试协议的安全性，将生成的数据按照 7:3 的比例划分为训练集和测试集。首先得到不同协议在车联网特定仿真场景下的认证总时长对比结果，如图 3 所示。

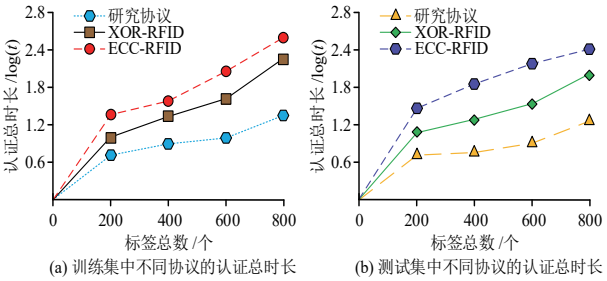

图 3 不同协议的认证总时长对比结果

综合图 3 可以看出，当标签总数为 400 时，研究协议在训练集和测试集中的认证总时长分别为 0.89log(*t*) 和 0.75log(*t*)。而训练集中，XOR-RFID 协议和 ECC-RFID 协议在标签总数为 400 时的认证总时长分别为 1.34log(*t*) 和 1.58log(*t*)。由此可知，研究协议面对车联网场景下标签数量增多时能够快速完成协议认证。为了验证研究协议在实际场景下的应用效果，研究选择在校园内搭建小型车联网测试环境并部署实际 RFID 标签与 RSU 设备。实验车辆在车辆时速 120 km/h 场景下行驶，通过与 RSU 认证交互记录下各协议的性能数据。随后研究测试了三种协议在不同运算次数下的运算时长和认证延迟，结果如图 4 所示。

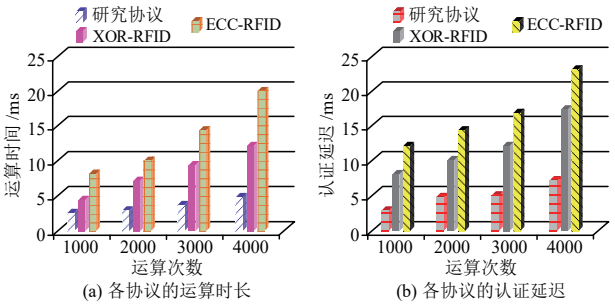

图 4 三种协议的运算时长与认证延迟

图 4（a）中，研究协议的运算时间随运算次数的增加而缓慢上升。当运算次数为 3 000 时，研究协议的运算时间仅仅为 2.89 ms，而此时 XOR-RFID 协议和 ECC-RFID 协议的运算时间分别达到了 8.13 ms 和 13.09 ms。图 4（b）中显示，研究协议的认证延迟远远低于对比协议，在相同运算次数下研究协议的认证延迟更低。上述结果说明，研究协议在车联网场景下的运算效率更高、认证响应更快。随后研究对三种协议的安全性能进行了对比，结果如表 1 所示。

表 1 安全性能对比结果

可抵御攻击类型	协议类型		
	研究协议	XOR-RFID 协议	ECC-RFID 协议
标签跟踪	√	×	√
物理攻击	√	√	√
篡改攻击	√	√	√
重放攻击	√	√	×
去同步攻击	√	√	×
窃听攻击	√	×	√
假冒攻击	√	√	×

从表 1 中可以看出，研究协议能够抵御标签跟踪、物理攻击和篡改攻击等所有测试的攻击类型。XOR-RFID 虽然能够抵御物理攻击和篡改攻击等，但该协议因缺乏有效隐私保护使得其无法抵御标签跟踪和窃听攻击，而 ECC-RFID 协议的安全性能更差。以上结果表明，研究协议能够满足车联网场景下 RFID 协议认证的安全需求。最后为了测试研究协议的轻量级性能，研究基于 8 位 AVR 单片机（1 MHz 主频）模拟车规级 RFID 标签算力，采用 ISO 18000-7 标准测试协议的单次认证能耗，利用 RSU 射频为被动标签供电。通信数据量的测试环境为 915 MHz 信道，测试结果如表 2 所示。

表 2 各协议的轻量级性能对比

指标	标签计算开销（指令周期）	标签存储开销 /Byte	单次认证能耗 /μJ	通信数据量 /bit	协议代码量 /Byte
研究协议	386	8	1.8	128	480
XOR-RFID 协议	579	32	4.2	256	1 024
ECC-RFID 协议	1 790	64	15.6	512	2 860

从表 2 中可以看出，研究协议的标签存储开销仅仅为 8 byte，单次认证能耗 1.8 μJ，通信数据量和协议代码量均显示最低。说明研究协议更适配于车联网中标签低算力的特点，具有明显的计算效率优势。而 XOR-RFID 协议和 ECC-RFID 协议的单次认证能耗分别达到了 4.2 μJ 和 15.6 μJ，其协议代码量和标签计算开销也显著高于研究协议。由此可知，研究协议能够减少车联网无线信道的传输负担并提升通信效率。在满足车联网 RFID 认证功能的同时更好地适配车联网场景下标签的资源约束。

3 结论

研究针对目前车联网场景下 RFID 认证协议动态拓扑适配能力薄弱的缺点设计了一种基于 XOR 结合哈希函数的认证协议，基于 XOR 认证流程进行 3 轮消息交互，并通过随机数动态混淆数据以避免固定密钥泄露。实验结果显示，研究协议能够抵御标签跟踪、物理攻击和篡改攻击等所有测试的攻击类型，其标签存储开销仅仅为 8 byte，单次认证能耗 1.8 μJ，通信数据量和协议代码量均显示最低。而 XOR-RFID 协议和 ECC-RFID 协议的单次认证能耗分别达到了 4.2 μJ 和 15.6 μJ。训练集中，XOR-RFID 协议和 ECC-RFID 协议在标签总数为 400 时的认证总时长分别为 1.34log(t) 和 1.58log(t)。XOR-RFID 协议无法抵御标签跟踪和窃听攻击，ECC-RFID 协议无法抵御重放攻击、去同步攻击和假冒攻击。综合来看，研究协议能够为车联网环境下路侧协同交互等场景提供一种安全高效的解决方案，但是其密钥更新与身份验证依赖单一信任中心的集中式管理，大量跨域认证请求会进一步延长响应延迟。

参考文献：

[1] 潘涛 , 左开中 , 王涛春 , 等 . 移动 RFID 高效率认证协议设计 [J]. 计算机应用研究 , 2023, 40(2):595-600.

[2] 贾昊洲 , 徐鹏 , 王丹琛 , 等 . 一种基于新型混淆操作的 RFID 双向认证协议 [J]. 计算机工程与科学 , 2025, 47(2): 247-255.

[3] 范文兵 , 常正泰 , 艾璐琳 , 等 . 基于 PUF 的高安全性轻量级 RFID 三方认证协议 [J]. 郑州大学学报 : 工学版 , 2023, 44(2): 46-52.

[4] 寇广岳 , 魏国珩 , 平源 , 等 .RFID 安全认证协议综述 [J]. 计算机工程与科学 , 2023, 45(1):77-84.

[5] 徐鹤 , 戴嫚嫚 , 李鹏 , 等 . 基于反射信号特征的 RFID 标签和移动终端跨域互联方法 [J]. 南京邮电大学学报 : 自然科学版 , 2023, 43(2):63-75.

[6]WU A M L, GUO Y J, GUO Y M. A decentralized lightweight blockchain-based authentication mechanism for internet of vehicles[J]. Peer-to-peer networking and applications, 2023, 16: 1340-1353.

[7] 王云峰 , 赵梓旭 . 基于预约机制的 RFID 防碰撞安全认证协议 [J]. 火力与指挥控制 , 2024, 49(9):173-179.

[8] 李喜艳 , 周清雷 , 刘征 . 信息预处理的加密域大容量可逆图像信息隐藏 [J]. 计算机应用与软件 , 2023, 40(3):343-349.

[9] 邹光南 , 尤启迪 , 金星虎 , 等 . 面向车联网车辆的轻量级持续身份认证协议 [J]. 电子学报 , 2024, 52(6):1903-1910.

[10] 刘长庚 , 刘亚丽 , 陆琪鹏 , 等 . 抵抗物理克隆攻击的车载遥控门锁双因子认证协议 [J]. 计算机应用 , 2023, 43(11): 3375-3384.

[11] 蒋诚智 , 徐浩 , 黄传峰 . 抗穷举攻击改进 RFID 双向认证协议舰船网络安全研究 [J]. 舰船科学技术 , 2023, 45(14): 172-175.

[12] 贺嘉琦 , 彭长根 , 付章杰 , 等 . 面向 RFID 的轻量级双向认证协议 [J]. 计算机工程与应用 , 2023, 59(18):268-277.

[13]KHAN M N, RAHMAN H U, HUSSAIN T, et al. Enabling trust in automotive IoT: lightweight mutual authentication scheme for electronic connected devices in internet of things[J]. IEEE transactions on consumer electronics, 2024, 70(3): 5065-5078.

[14]KUMAR S, BANKA H, KAUSHIK B, et al. An ultra-lightweight secure RFID authentication protocol for low-cost tags[J]. Journal of computer virology and hacking techniques, 2024, 20: 803-818.

[15] 乔子芮 , 杨启良 , 周彦伟 , 等 . 可证明安全的高效车联网认证密钥协商协议 [J]. 计算机学报 , 2023, 46(5):929-944.

【作者简介】

路玉君（1991—），女，山西长治人，硕士，讲师，研究方向：人工智能、物联网。

（收稿日期：2025-09-26 修回日期：2026-04-14）