面向车联网的轻量级认证密钥协商协议

刘亚丽[1,2,3]，庞小辉[1,2,3]，陈东东[1,2,3]，王鹏超[1,2,3,4]，周毅[1,2,3]

（1.江苏师范大学计算机科学与技术学院，江苏 徐州 221116；2.南京大学计算机软件新技术全国重点实验室，江苏 南京 210023；
3.桂林电子科技大学广西密码学与信息安全重点实验室，广西 桂林 541004；4.东南大学网络空间安全学院，江苏 南京 211189）

摘　要：针对张等提出的面向车联网通勤的双阶段认证密钥协商协议进行分析，发现其不能抵抗秘密泄露攻击、中间人攻击等多种攻击。为解决协议面临的安全隐患问题，提出一种面向车联网的轻量级认证密钥协商（LAKA）协议。首先，通过异或和对称加密算法对私密值加密，保证私密值的隐私性；其次，利用车辆和路边单元的私密值生成认证请求，确保协议的安全性；再次，性能分析表明，与同类方案相比，在计算代价上具有明显优势；最后，利用BAN逻辑和ProVerif工具进行形式化分析与验证，证明其具有更强的安全性和隐私保护性。

关键词：车联网；轻量级；认证协议；密钥协商；隐私保护

中图分类号：TN915.08

文献标志码：A

DOI：10.11959/j.issn.1000–436x.2025143

Lightweight authentication key agreement protocol for Internet of vehicles

LIU Yali[1,2,3], PANG Xiaohui[1,2,3], CHEN Dongdong[1,2,3], WANG Pengchao[1,2,3,4], ZHOU Yi[1,2,3]

1. College of Computer Science and Technology, Jiangsu Normal University, Xuzhou 221116, China
2. State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210023, China
3. Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin 541004, China
4. School of Cyber Science and Engineering, Southeast University, Nanjing 211189, China

Abstract: An analysis of the two-stage authentication and key agreement protocol for commuting in Internet of vehicles proposed by Zhang et al. revealed its vulnerability to various malicious attacks, which included secret leakage attack and man-in-the-middle attack. To address security risks faced by the protocol, a lightweight authentication key agreement (LAKA) protocol for Internet of vehicles was proposed. Firstly, private values were encrypted by XOR and symmetric encryption algorithm, which ensured the privacy of private value. Secondly, authentication requests were generated by the private values of vehicles and roadside unit, which guaranteed the security of the protocol. Thirdly, performance analysis shows that it has a significant advantage in terms of computational cost compared with the similar protocols. Finally, formal analysis and verification by BAN logic and ProVerif tool confirm that it enhances security and privacy preservation.

Keywords: Internet of vehicles, lightweight, authentication protocol, key agreement, privacy preservation

---

收稿日期：2025–05–29；**修回日期：**2025–08–13

通信作者：庞小辉，pangxiaohui@jsnu.edu.cn

基金项目：国家自然科学基金资助项目（No.61702237）；南京大学计算机软件新技术全国重点实验室资助项目（No.KFKT2025B54）；徐州市科技计划基金资助项目（No.KC22052）；广西密码学与信息安全重点实验室（桂林电子科技大学）研究课题基金资助项目（No.GCIS202114）；江苏师范大学研究生科研与实践创新计划基金资助项目（No.2025XKT1439, No.2025XKT1441）；教育部产学合作协同育人基金资助项目（No.202101374001）

Foundation Items： The National Natural Science Foundation of China (No.61702237), Opening Foundation of State Key Laboratory for Novel Software Technology, Nanjing University (No.KFKT2025B54), Science and Technology Planning Foundation of Xuzhou City (No.KC22052), Opening Foundation of Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology(No.GCIS202114), Postgraduate Research & Practice Innovation Program of Jiangsu Normal University (No.2025XKT1439, No.2025XKT1441), University-Industry Collaborative Education Program of China (No.202101374001)

0　引言

近年来，车联网（IoV, Internet of vehicles）技术在日常生活中得到广泛应用[1-2]。每辆车通过车载单元（OBU, on-board unit）进行车对车（V2V, vehicle-to-vehicle）通信[3]，通过路边单元（RSU, road side unit）进行车对RSU（V2R, vehicle-to-RSU）通信[4]。攻击者易于通过V2V和V2R公开信道获取信息，导致用户隐私泄露和信息篡改等安全隐患[5-6]。

为了解决车联网中各实体通信的安全隐患问题，Ali等[7]提出一种可证明安全、高效的基于短签名的有条件隐私保护认证方案，使用哈希函数代替映射到点的哈希函数，支持批量签名验证方法，但没有考虑不可链接性。Wang等[8]提出一种用于车对车通信的基于无证书的匿名可撤销身份认证协议，将身份认证与流量信息认证分离开，避免了频繁身份撤销列表检查的问题，然而不能保证匿名性和隐私性。Feng等[9]提出一种双线性群中的新型隐私保护认证协议，通过发送签名与盲证书给RSU完成认证，但双线性配对导致计算代价增加。Liang等[10]提出一种适用于IoV的物理安全和条件隐私密钥协商方案，利用物理不可克隆函数（PUF, physical unclonable function）防止攻击者从车辆和RSU中物理提取秘密信息，认证过程不需要可信机构（TA, trusted authority）参与，然而其计算和通信开销较大。Wei等[11]提出一种安全认证密钥协商方案，通过设计的基于树的密钥协商算法实现认证车辆的加入和撤出，但认证效率低下。Xie等[12]提出一种基于椭圆曲线的轻量级匿名身份认证协议，使用PUF和生物特征避免RSU捕获攻击和OBU入侵攻击，但存在密钥托管问题。Awais等[13]提出一种可证明安全的轻量级认证密钥协商协议，利用RSU、雾节点和云服务器实现轻量级的认证密钥协商，但存在实时数据处理时延较高的问题。Tomar等[14]提出一种基于切比雪夫多项式和区块链的雾环境车联网认证方案，将区块链集成到雾环境的车辆自组织网络中，但不能保证车辆的匿名性。Zhu等[15]提出一种基于无证书聚合签名的车联网认证方案，支持签名的批量验证和用户的条件隐私保护，但无法抵抗冒充攻击。Li等[16]提出一种抗恶意密钥生成中心（KGC, key generation center）的无证书聚合签名协议，以抵御外部攻击者和内部恶意KGC，然而不能抵抗冒充攻击。张海波等[17]提出一种面向车联网通勤的双阶段认证密钥协商（TSAKA）协议，在初始认证阶段利用车辆、RSU和TA间协商的独立会话密钥，声称实现了任意2个实体间传输信息的安全性，但经过分析发现，该协议[17]无法抵抗秘密泄露攻击、中间人攻击、冒充攻击、拒绝服务（DoS, denial-of-service）攻击等多种恶意攻击。

为了增强车联网认证的安全性和隐私性，本文对文献[17]进行详细的安全性分析，指出其存在的安全隐患，并提出改进的轻量级认证密钥协商（LAKA）协议。LAKA协议通过异或和对称加密算法对各实体的私密值和随机值进行加密，保证私密值和随机值的安全性，有效抵抗秘密泄露攻击、中间人攻击等多种恶意攻击，使用BAN逻辑和ProVerif工具进行形式化分析与验证，并进行安全性和性能对比分析。

1　TSAKA协议

本节对文献[17]的初始认证阶段进行介绍，快速认证阶段详见文献[17]。

1.1　TSAKA中车辆与RSU生成认证请求阶段

文献[17]中车辆与RSU生成认证请求时实体间的信息交互步骤如下。

1) 车辆选择$r_{\mathrm{V}} \in Z_q^*$，计算$P_{\mathrm{V}} = r_{\mathrm{V}}G$。

2) 车辆计算$\mathrm{RE_V} = H(T_{\mathrm{SVR_1}} \| \mathrm{VID_1} \| S_{\mathrm{V}})$。

3) 车辆把$M_1 = \{T_{\mathrm{SVR_1}}, \mathrm{VID_1}, P_{\mathrm{V}}, \mathrm{RE_V}\}$给$\mathrm{RSU_1}$。

4) 若$T_{\mathrm{RVR_1}} - T_{\mathrm{SVR_1}} < \Delta t$成立，则$\mathrm{RSU_1}$接收$M_1$，并选择$r_{\mathrm{R_1}} \in Z_q^*$，计算$P_{\mathrm{R_1}} = r_{\mathrm{R_1}}G$。

5) $\mathrm{RSU_1}$计算$\mathrm{RE_R} = H(T_{\mathrm{SR_1T}} \| \mathrm{RID} \| S_{\mathrm{R_1}})$。

6) $\mathrm{RSU_1}$发送消息M_2给TA，其中$M_2 = \{T_{\mathrm{SVR_1}}, \mathrm{VID_1}, P_{\mathrm{V}}, \mathrm{RE_V}, T_{\mathrm{SR_1T}}, \mathrm{RID}, P_{\mathrm{R_1}}, \mathrm{RE_R}\}$。

1.2　TSAKA中TA验证并生成会话密钥阶段

文献[17]中TA验证并生成会话密钥时实体间的信息交互步骤如下。

1) 若$T_{\mathrm{RR_1T}} - T_{\mathrm{SR_1T}} < \Delta t$成立，则TA接收$M_2$。

2) 若TA验证$\mathrm{RE_R}$、$\mathrm{RE_V}$成立，则计算$A_{\mathrm{R}} = H(\mathrm{RE_R} \| S_{\mathrm{R_1}})$和$A_{\mathrm{V}} = H(\mathrm{RE_V} \| S_{\mathrm{V}})$。

3) TA选择$r_{\mathrm{T}} \in Z_q^*$，计算$P_{\mathrm{T}} = r_{\mathrm{T}}G$，并计算$P_{\mathrm{R_1T}} = S_{\mathrm{R_1}} \oplus P_{\mathrm{T}}$、$P_{\mathrm{VT}} = S_{\mathrm{V}} \oplus P_{\mathrm{T}}$和$P_{\mathrm{VR_1}} = S_{\mathrm{V}} \oplus P_{\mathrm{R_1}}$。

4) TA记录对车辆旅行表的访问时间$\mathrm{Time_1}$，计算$\mathrm{TKS_1} = H(\mathrm{Time_1})$，作为车辆与$\mathrm{RSU_2}$认证参数。

5) TA 计算 $SK_{VT} = r_T P_V$、$SK_{R_1T} = r_T P_{R_1}$。

6) TA 选择时间戳 T_{STR_1}，把消息 M_3 发给 RSU_1，其中 $M_3 = \{T_{STR_1}, A_R, A_V, P_{R_1T}, P_{VT}, P_{VR_1}, TKS_1\}$。

1.3 TSAKA 中 RSU 与车辆生成会话密钥阶段

文献[17]中车辆与 RSU 生成会话密钥时实体间的信息交互步骤如下。

1) 若 $T_{RTR_1} - T_{STR_1} < \Delta t$ 成立，则 RSU_1 接收 M_3。

2) 若 RSU_1 验证 A_R 成立，则计算 $P_T = P_{R_1T} \oplus S_{R_1}$，以及 $SK_{VR_1} = r_{R_1} P_V$、$SK_{R_1T} = r_{R_1} P_T$。

3) RSU_1 发送消息 M_4 给车辆，其中 $M_4 = \{T_{SR_1V}, A_V, P_{VT}, P_{VR_1}, TKS_1\}$。

4) 若 $T_{RR_1V} - T_{SR_1V} < \Delta t$ 成立，则车辆接收 M_4。

5) 若车辆验证 A_V 成立，则计算 $P_{R_1} = P_{VR_1} \oplus S_V$、$P_T = P_{VT} \oplus S_V$。

6) 车辆计算 $SK_{VR_1} = r_V P_{R_1}$、$SK_{VT} = r_V P_T$。

2 对 TSAKA 协议的安全性分析

在文献[17]中，作者声称私密值无法被攻击者 A 所拥有，并无法伪造合法的认证请求通过 TA 的认证。通过安全性分析发现，A 成功发起秘密泄露攻击、中间人攻击、冒充攻击、DoS 攻击等多种恶意攻击，证明文献[17]初始认证阶段存在安全隐患。

2.1 秘密泄露攻击

攻击者截取信息并计算私密值时实体间的信息交互如图 1 所示，具体步骤如下。

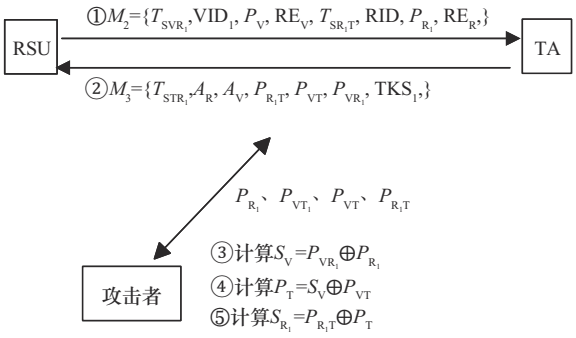


图 1 攻击者截取信息并计算私密值时实体间的信息交互

1) A 截获消息 M_2 中的 P_{R_1}。

2) A 截获消息 M_3 中的 P_{VR_1}、P_{VT} 和 P_{R_1T}。

3) A 计算得到车辆私密值 $S_V = P_{VR_1} \oplus P_{R_1}$。

4) A 计算得到 TA 公钥 $P_T = S_V \oplus P_{VT}$。

5) A 计算得到 RSU_1 私密值 $S_{R_1} = P_{R_1T} \oplus P_T$。

因此，A 获得车辆与 RSU_1 的私密值 S_V、S_{R_1}。

利用形式化分析工具 ProVerif[18]对文献[17]进行秘密泄露攻击，验证结果如图 2 所示。其中，event(acc1)表示 TA 验证 RSU 成功，event(acc2)表示 TA 验证车辆成功，event(acc3)表示 TA 端会话密钥建立成功，event(acc4)表示 RSU 验证 TA 成功，event(acc5)表示 RSU 端会话密钥建立成功，event(acc6)表示车辆验证 TA 成功，event(acc7)表示车辆端会话密钥建立成功。图 2 验证结果表明，文献[17]的初始认证阶段存在安全隐患，车辆私密值 S_V 和 RSU_1 私密值 S_{R_1} 均易被 A 窃取。

图 2 利用 ProVerif 工具对文献[17]进行秘密泄露攻击的验证结果

2.2 中间人攻击

A 得到车辆私密值 S_V 和 RSU_1 私密值 S_{R_1} 后发起中间人攻击，具体步骤如下。

1) A 截获 $M_1 = \{T_{SVR_1}, VID_1, P_V, RE_V\}$。

2) A 篡改时间戳为 T'_{SVR_1}，并利用 S_V 伪造新的认证请求 $RE'_V = H(T'_{SVR_1} \| VID_1 \| S_V)$。

3) A 发送 $M_1' = \{T'_{\mathrm{SVR}_1}, \mathrm{VID}_1, P_{\mathrm{V}}, \mathrm{RE}'_{\mathrm{V}}\}$ 给 RSU_1。

4) A 截获消息 M_2，并篡改时间戳 $T'_{\mathrm{SR}_1\mathrm{T}}$，利用 S_{R_1} 伪造新的认证请求 $\mathrm{RE}'_{\mathrm{R}} = H(T'_{\mathrm{SR}_1\mathrm{T}} \| \mathrm{RID} \| S_{\mathrm{R}_1})$。

5) A 将篡改后的消息 M_2' 发送给 TA，其中 $M_2' = \{T'_{\mathrm{SVR}_1}, \mathrm{VID}_1, P_{\mathrm{V}}, \mathrm{RE}'_{\mathrm{V}}, T'_{\mathrm{SR}_1\mathrm{T}}, \mathrm{RID}, P_{\mathrm{R}_1}, \mathrm{RE}'_{\mathrm{R}}\}$。

6) 由于 A 使用真实的私密值 S_{V} 和 S_{R_1} 生成认证请求，TA 均能验证通过。

因此，A 完成了中间人攻击。

2.3　冒充攻击

A 得到车辆私密值 S_{V} 和 RSU_1 私密值 S_{R_1} 后发起冒充攻击，具体步骤如下。

1) A 选择 $r'_{\mathrm{V}} \in Z_q^*$，计算 $P'_{\mathrm{V}} = r'_{\mathrm{V}} G$。

2) A 篡改时间戳 T'_{SVR_1}，利用 S_{V} 伪造新的认证请求 $\mathrm{RE}'_{\mathrm{V}} = H(T'_{\mathrm{SVR}_1} \| \mathrm{VID}_1 \| S_{\mathrm{V}})$。

3) A 发送 $M_1' = \{T'_{\mathrm{SVR}_1}, \mathrm{VID}_1, P'_{\mathrm{V}}, \mathrm{RE}'_{\mathrm{V}}\}$ 给 RSU_1。

4) A 截获消息 M_2，并篡改时间戳 $T'_{\mathrm{SR}_1\mathrm{T}}$，利用 S_{R_1} 伪造新的认证请求 $\mathrm{RE}'_{\mathrm{R}} = H(T'_{\mathrm{SR}_1\mathrm{T}} \| \mathrm{RID} \| S_{\mathrm{R}_1})$。

5) A 将篡改后的消息 M_2' 发送给 TA，其中 $M_2' = \{T'_{\mathrm{SVR}_1}, \mathrm{VID}_1, P'_{\mathrm{V}}, \mathrm{RE}'_{\mathrm{V}}, T'_{\mathrm{SR}_1\mathrm{T}}, \mathrm{RID}, P_{\mathrm{R}_1}, \mathrm{RE}'_{\mathrm{R}}\}$。

6) 由于 A 使用真实的私密值 S_{V} 和 S_{R_1} 生成认证请求，TA 均能验证通过。

7) TA 计算 $\mathrm{SK}'_{\mathrm{VT}} = r_{\mathrm{T}} P'_{\mathrm{V}}$ 和 $\mathrm{SK}'_{\mathrm{R}_1\mathrm{T}} = r_{\mathrm{T}} P_{\mathrm{R}_1}$。

8) RSU_1 计算 $\mathrm{SK}'_{\mathrm{VR}_1} = r_{\mathrm{R}_1} P'_{\mathrm{V}}$ 和 $\mathrm{SK}'_{\mathrm{R}_1\mathrm{T}} = r_{\mathrm{R}} P_{\mathrm{T}_1}$。

9) A 计算 $\mathrm{SK}'_{\mathrm{VR}_1} = r'_{\mathrm{V}} P_{\mathrm{R}_1}$ 和 $\mathrm{SK}'_{\mathrm{VT}} = r'_{\mathrm{V}} P_{\mathrm{T}}$。

因此，A 完成了冒充攻击。

2.4　DoS 攻击

A 得到车辆私密值 S_{V} 和 RSU_1 私密值 S_{R_1} 后发起 DoS 攻击，具体步骤如下。

1) A 截获消息 M_2，其中 $M_2 = \{T_{\mathrm{SVR}_1}, \mathrm{VID}_1, P_{\mathrm{V}}, \mathrm{RE}_{\mathrm{V}}, T_{\mathrm{SR}_1\mathrm{T}}, \mathrm{RID}, P_{\mathrm{R}_1}, \mathrm{RE}_{\mathrm{R}}\}$。

2) A 伪造大量 $\mathrm{RE}_{\mathrm{V}} = H(T_{\mathrm{SVR}_1} \| \mathrm{VID}_1 \| S_{\mathrm{V}})$。

3) A 伪造大量 $\mathrm{RE}_{\mathrm{R}} = H(T_{\mathrm{SR}_1\mathrm{T}} \| \mathrm{RID} \| S_{\mathrm{R}_1})$。

4) A 将大量伪造的车辆和 RSU 认证请求 RE_{V}、RE_{R} 发送给 TA。

5) 由于 A 使用真实的私密值 S_{V} 和 S_{R_1} 生成认证请求，TA 均能验证通过，因此占用大量的系统资源进而引发 DoS 攻击。

因此，A 完成了 DoS 攻击。

综上所述，文献[17]的初始认证阶段生成车辆、RSU、TA 之间的会话密钥和车辆旅行时间表，是后续快速认证阶段的基础，初始认证阶段存在的安全隐患直接导致文献[17]无法抵抗秘密泄露攻击、中间人攻击、冒充攻击、DoS 攻击等恶意攻击。

3　LAKA 协议

为抵抗文献[17]遭受的多种恶意攻击，本文提出了 LAKA 协议。

3.1　注册阶段

本阶段主要完成车辆、RSU 通过安全信道向 TA 注册。

3.1.1　车辆注册阶段

1) 车辆选择随机数 $c_i \in Z_q^*$，计算 $r_i = \mathrm{PUF}(c_i)$。

2) 车辆计算其私密值 $S_{\mathrm{V}_i} = r_i G$，并将其与服务标识码（SID）发送给 TA。

3) 若 TA 检查 SID 存在且未绑定车辆，则接收注册请求，并为车辆生成假名 VID_i，随后将其与私密值 S_{T} 发送给车辆。

4) 车辆收到 VID_i 和 S_{T} 后，将其保存到本地。

3.1.2　RSU 注册阶段

1) RSU_j 选择随机数 $c_j \in Z_q^*$，计算 $r_j = \mathrm{PUF}(c_j)$。

2) RSU_j 计算其私密值 $S_{\mathrm{R}_j} = r_j G$，并将其与设备标识码（RID）发送给 TA。

3) 若 TA 检查 RID 存在，则接收注册请求，并将其私密值 S_{T} 发送给 RSU_j。

4) RSU_j 收到 S_{T} 后，将其保存到本地。

3.2　初始认证阶段

本阶段主要完成车辆、RSU 和 TA 之间的会话密钥协商。

3.2.1　车辆与 RSU 生成认证请求阶段

车辆与 RSU_j 生成认证请求时实体间的信息交互如图 3 所示，具体步骤如下。

1) 车辆选择时间戳 T_{VR} 以及随机数 $N_{\mathrm{V}_1} \in Z_q^*$，计算 $N_{\mathrm{V}_1\mathrm{T}} = N_{\mathrm{V}_1} \oplus S_{\mathrm{T}}$、$E_{\mathrm{V}_1} = \mathrm{Enc}_{N_{\mathrm{V}_1}}(S_{\mathrm{V}_1})$。

2) 车辆计算其认证请求 $R_{\mathrm{V}} = H(T_{\mathrm{VR}} \| \mathrm{VID}_1 \| S_{\mathrm{V}_1} \| N_{\mathrm{V}_1\mathrm{T}})$。

3) 车辆把消息 M_1 发送给 RSU_j，其中 $M_1 = \{T_{\mathrm{VR}}, \mathrm{VID}_1, N_{\mathrm{V}_1\mathrm{T}}, E_{\mathrm{V}_1}, R_{\mathrm{V}}\}$。

4) 若 $T_{\mathrm{curr}} - T_{\mathrm{VR}} < \Delta t$ 成立，则 RSU_j 接收 M_1。

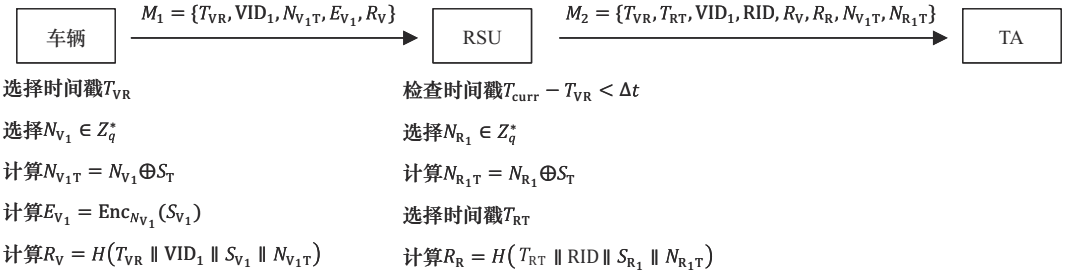


图3 车辆与RSU生成认证请求时实体间的信息交互

5) RSU_j 选择随机数 $N_{R_1} \in Z_q^*$，计算 $N_{R_1T} = N_{R_1} \oplus S_T$，并选择时间戳 T_{RT}，计算其认证请求 $R_R = H(T_{RT} \| RID \| S_{R_1} \| N_{R_1T})$。

6) RSU_j 把消息 M_2 发送给 TA，其中 $M_2 = \{T_{VR}, T_{RT}, VID_1, RID, R_V, R_R, N_{V_1T}, N_{R_1T}\}$。

3.2.2 TA验证并生成会话密钥阶段

TA验证并生成会话密钥时实体间的信息交互如图4所示，具体步骤如下。

1) 若 $T_{curr} - T_{RT} < \Delta t$ 成立，则TA接收 M_2。

2) 若TA验证 R_R、R_V 成立，则计算车辆的随机值 $N_{V_1} = N_{V_1T} \oplus S_T$ 和 RSU_j 的随机值 $N_{R_1} = N_{R_1T} \oplus S_T$。

3) TA选择 $N_T \in Z_q^*$，计算 $N_{TT} = N_T \oplus S_T$。

4) TA 计算 $F_R = H(R_R \| S_{R_1} \| N_{V_1T} \| N_{TT})$ 和 $F_V = H(R_V \| S_{V_1} \| N_{R_1T} \| N_{TT})$。

5) TA 记录 RSU_j 对车辆旅行表的访问时间 $Time_1$，计算 $TS_1 = H(Time_1)$，作为车辆与 RSU_{j+1} 认证参数，并计算 TA 与车辆之间的会话密钥 $K_{V_1T} = H(S_{V_1} \| S_T \| N_{V_1} \| N_T)$ 以及TA与 RSU_j 之间的会话密钥 $K_{R_1T} = H(S_{R_1} \| S_T \| N_{R_1} \| N_T)$。

6) TA 选择时间戳 T_{TR}，并把消息 M_3 发送给 RSU_j，其中 $M_3 = \{T_{TR}, F_R, F_V, TS_1, N_{TT}\}$。

3.2.3 RSU与车辆生成会话密钥阶段

RSU_j 与车辆生成会话密钥时实体间的信息交互如图5所示，具体步骤如下。

1) 若 $T_{curr} - T_{TR} < \Delta t$ 成立，则 RSU_j 接收 M_3。

2) 若 RSU_j 验证 F_R 成立，则计算 $N_{V_1} = N_{V_1T} \oplus S_T$、$S_{V_1} = Dec_{N_{V_1}}(E_{V_1})$、$N_T = N_{TT} \oplus S_T$ 和 $E_{R_1} = Enc_{N_{R_1}}(S_{R_1})$。

3) RSU_j 计算 RSU_j 与车辆之间的会话密钥 $K_{V_1R_1} = H(S_{V_1} \| S_{R_1} \| N_{V_1} \| N_{R_1})$ 以及 RSU_j 与TA之间的会话密钥 $K_{R_1T} = H(S_{R_1} \| S_T \| N_{R_1} \| N_T)$。

4) RSU_j 选择时间戳 T_{RV}，并把消息 M_4 发送给车辆，其中 $M_4 = \{T_{RV}, F_V, N_{TT}, N_{R_1T}, S_{R_1T}, TS_1\}$。

5) 若 $T_{curr} - T_{RV} < \Delta t$ 成立，则车辆接收 M_4，若车辆验证 F_V 成立，则计算 $N_{R_1} = N_{R_1T} \oplus S_T$、$S_{R_1} = Dec_{N_{R_1}}(E_{R_1})$ 和 $N_T = N_{TT} \oplus S_T$。

6) 车辆计算车辆与 RSU_j 之间的会话密钥 $K_{V_1R_1} = H(S_{V_1} \| S_{R_1} \| N_{V_1} \| N_{R_1})$ 以及车辆与TA之间的会话密钥 $K_{V_1T} = H(S_{V_1} \| S_T \| N_{V_1} \| N_T)$。

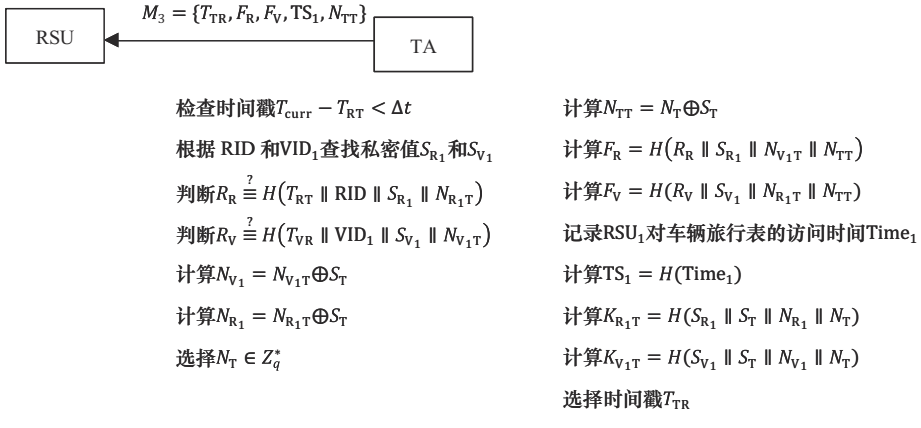


图4 TA验证并生成会话密钥时实体间的信息交互

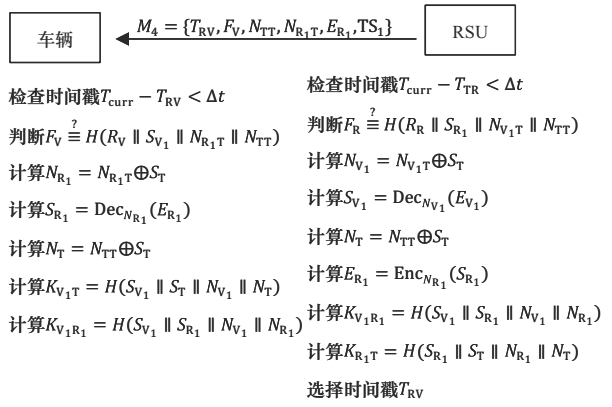


图5　RSU与车辆生成会话密钥时实体间的信息交互

3.3　快速认证阶段

本阶段主要完成车辆与RSU快速认证，实体间信息交互如图6所示，具体步骤如下。

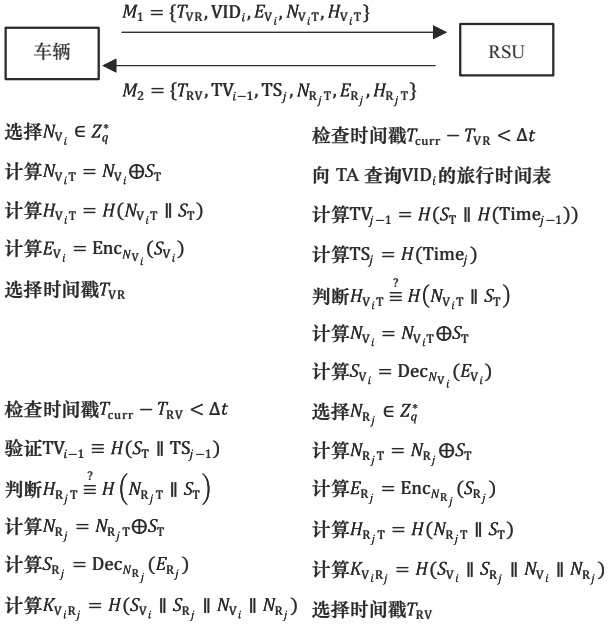


图6　快速认证阶段的实体间信息交互

1) 车辆选择$N_{V_i}\in Z_q^*$，计算$N_{V_iT}=N_{V_i}\oplus S_T$、$H_{V_iT}=H(N_{V_iT}\|S_T)$和$E_{V_i}=\mathrm{Enc}_{N_{V_i}}(S_{V_i})$。

2) 车辆选择时间戳T_{VR}，把消息M_1发送给RSU_j，其中$M_1=\{T_{VR},VID_j,N_{V_iT},H_{V_iT},E_{V_i}\}$。

3) 若$T_{curr}-T_{VR}<\Delta t$成立，则RSU_j接收M_1。

4) RSU_j向TA查询对应假名为VID_i的车辆，根据车辆旅行时间表中车辆途经的RSU_{j-1}对访问时间$Time_{j-1}$和TA私密值S_T计算时间验证值$TV_{j-1}=H(S_T\|H(Time_{j-1}))$。

5) RSU_j计算$TS_j=H(Time_j)$，若RSU_j验证H_{V_iT}成立，则计算$N_{V_i}=N_{V_iT}\oplus S_T$、$S_{V_i}=\mathrm{Dec}_{N_{V_i}}(E_{V_i})$。

6) RSU_j选择$N_{R_j}\in Z_q^*$，计算$N_{R_jT}=N_{R_j}\oplus S_T$、$E_{R_j}=\mathrm{Enc}_{N_{R_j}}(S_{R_j})$和$H_{R_jT}=H(N_{R_jT}\|S_T)$。

7) RSU_j计算RSU_j与车辆的会话密钥$K_{V_iR_j}=H(S_{V_i}\|S_{R_j}\|N_{V_i}\|N_{R_j})$，选择时间戳$T_{RV}$，发送$M_2=\{T_{RV},TV_{i-1},TS_j,N_{R_jT},E_{R_j},H_{R_jT}\}$给车辆。

8) 若$T_{curr}-T_{RV}<\Delta t$成立，则车辆接收M_2。

9) 若车辆根据TA私密值S_T和途经RSU_{j-1}发送给车辆的信息TS_{j-1}验证TV_{i-1}及H_{R_jT}成立，则计算$N_{R_j}=N_{R_jT}\oplus S_T$、$S_{R_j}=\mathrm{Dec}_{N_{R_j}}(E_{R_j})$。

10) 车辆计算车辆与RSU_j的会话密钥$K_{V_iR_j}=H(S_{V_i}\|S_{R_j}\|N_{V_i}\|N_{R_j})$。

3.4　密钥更新阶段

本阶段主要完成车辆与RSU_j的密钥更新以抵抗追踪攻击，具体步骤如下。

1) 车辆选择新的随机数$c_i^*\in Z_q^*$，计算$r_i^*=\mathrm{PUF}(c_i^*)$。

2) 车辆计算新的私密值$S_{V_i}^*=r_i^*G$，发给TA。

3) TA收到$S_{V_i}^*$后，将其私密值S_T发给车辆。

4) RSU_j选择新的随机数$c_j^*\in Z_q^*$，计算$r_j^*=\mathrm{PUF}(c_j^*)$。

5) RSU_j计算新的私密值$S_{R_j}^*=r_j^*G$，发给TA。

6) TA收到$S_{R_j}^*$后，将其私密值S_T发给RSU_j。

4　安全性证明与分析

本节采用BAN逻辑[19]和ProVerif工具[18]对LAKA协议的安全性进行形式化分析与验证。

4.1　BAN逻辑形式化分析

1) 初始化假设

A1：$V|\equiv\#(S_V,N_V)$

A2：$RSU|\equiv\#(S_R,N_R)$

A3：$V|\equiv RSU|\equiv V\overset{S_T}{\longleftrightarrow}RSU$

A4：$RSU|\equiv V|\equiv V\overset{S_T}{\longleftrightarrow}RSU$

A5：$V|\equiv RSU|\Rightarrow M_4$

A6：$RSU|\equiv V|\Rightarrow M_1$

A7：$V\triangleleft M_4$

A8：$RSU\triangleleft M_1$

2) 逻辑规则说明

R1（消息含义规则）：$\dfrac{P|\equiv Q\overset{K}{\longleftrightarrow}P,P\lhd\{X\}_K}{P|\equiv Q|\sim X}$

R2（消息新鲜性规则）：$\dfrac{P|\equiv\#(X)}{P|\equiv\#(X,Y)}$

R3（临时值验证规则）：$\dfrac{P|\equiv\#(X),P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$

R4（管辖规则）：$\dfrac{P|\equiv Q|\Rightarrow X,P|\equiv Q|\equiv X}{P|\equiv X}$

3) 证明目标

G1：$V|\equiv V\overset{K_{VR}}{\longleftrightarrow}RSU$，车辆相信会话密钥$K_{VR}$是安全的。

G2：$RSU|\equiv V\overset{K_{VR}}{\longleftrightarrow}RSU$，RSU相信会话密钥$K_{VR}$是安全的。

G3：$V|\equiv RSU|\equiv V\overset{K_{VR}}{\longleftrightarrow}RSU$，车辆相信RSU相信会话密钥$K_{VR}$是安全的。

G4：$RSU|\equiv V|\equiv V\overset{K_{VR}}{\longleftrightarrow}RSU$，RSU相信车辆相信会话密钥$K_{VR}$是安全的。

4) 证明过程

F1：根据A8、A6，有$RSU|\equiv V|\sim M_1$。

F2：根据A1、R2，有$RSU|\equiv\#(M_1)$。

F3：根据F1、F2和R3，$RSU|\equiv V|\equiv M_1$。

F4：根据A4、A8和R1，有$RSU|\equiv V|\sim\{S_V,N_V\}$。

F5：根据F2、F4和R3，有$RSU|\equiv V|\equiv\{S_V,N_V\}$。

F6：根据A2、F5和$K_{VR}=K_{V_iR_j}=H(S_{V_i}\|S_{R_j}\|N_{V_i}\|N_{R_j})$，有$RSU|\equiv V|\equiv V\overset{K_{VR}}{\longleftrightarrow}RSU$。

因此，目标G4得证。

F7：根据A6、F3和R4，有$RSU|\equiv M_1$。

F8：根据A6、F5和R4，有$RSU|\equiv\{S_V,N_V\}$。

F9：根据A2、F8和$K_{VR}=K_{V_iR_j}=H(S_{V_i}\|S_{R_j}\|N_{V_i}\|N_{R_j})$，有$RSU|\equiv V\overset{K_{VR}}{\longleftrightarrow}RSU$。

因此，目标G2得证。

F10：根据A7、A5，有$V|\equiv RSU|\sim M_4$。

F11：根据A2、R2，有$V|\equiv\#(M_4)$。

F12：根据F10、F11和R3，有$V|\equiv RSU|\equiv M_4$。

F13：根据A3、A7和R1，有$V|\equiv RSU|\sim\{S_R,N_R\}$。

F14：根据F11、F13和R3，有$V|\equiv RSU|\equiv\{S_V,N_V\}$。

F15：根据A1、F14和$K_{VR}=K_{V_iR_j}=H(S_{V_i}\|S_{R_j}\|N_{V_i}\|N_{R_j})$，有$V|\equiv RSU|\equiv V\overset{K_{VR}}{\longleftrightarrow}RSU$。

因此，目标G3得证。

F16：根据A5、F12和R4，有$V|\equiv M_4$。

F17：根据A5、F14和R4，有$V|\equiv\{S_R,N_R\}$。

F18：根据A1、F17和$K_{VR}=K_{V_iR_j}=H(S_{V_i}\|S_{R_j}\|N_{V_i}\|N_{R_j})$，有$V|\equiv V\overset{K_{VR}}{\longleftrightarrow}RSU$。

因此，目标G1得证。

综上所述，利用BAN逻辑分析LAKA协议，实现了4个安全目标。

4.2 ProVerif工具形式化验证

ProVerif代码中定义LAKA协议具有7个事件，其中，event(acc1)表示TA验证RSU成功，event(acc2)表示TA验证车辆成功，event(acc3)表示TA端会话密钥建立成功，event(acc4)表示RSU验证TA成功，event(acc5)表示RSU端会话密钥建立成功，event(acc6)表示车辆验证TA成功，event(acc7)表示车辆端会话密钥建立成功。ProVerif验证结果如图7所示，可知LAKA协议达到了预期的安全目标。

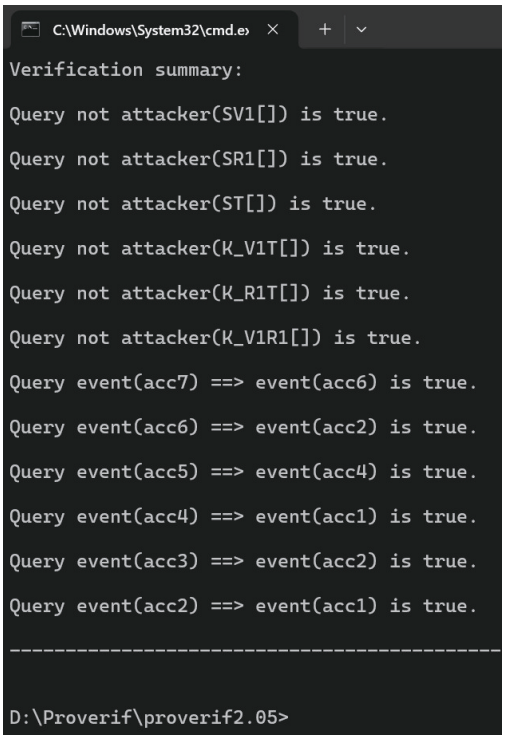


图7 LAKA协议ProVerif验证结果

4.3 LAKA协议安全性分析

LAKA协议不仅满足认证协议基本的安全隐私需求，还能够抵抗多种恶意攻击[20-21]，具体如下。

1) 车辆匿名性

车辆的真实身份通过安全信道提交给TA，在初始认证阶段通过公共信道使用假名VID_i与其他实体通信，A无法捕获车辆的真实身份。因此，LAKA协议满足车辆的匿名性。

2) 不可链接性

车辆使用不同的假名VID_i与RSU_j通信，当A捕获通信消息时，无法区分消息是否来自同一辆车。因此，LAKA协议满足不可链接性。

3) 身份可追溯性

车辆使用TA为其生成的假名与其他实体通信，若发现有恶意行为，则TA通过假名找到对应车辆的真实身份。因此，LAKA协议满足身份可追溯性。

4) 前向安全性

车辆、RSU_j和TA每次均选择不同随机值计算会话密钥。假设K_{i-1}和K_i分别是车辆第$i-1$次和第i次使用的会话密钥，即使A捕获到K_i，也无法得到K_{i-1}，因为K_{i-1}的计算依赖于第$i-1$次的随机值和私密值，因此，LAKA协议满足前向安全性。

5) 重放攻击

当A试图重放之前捕获的某个消息时，由于车辆、RSU_j和TA之间传递消息均由时间戳和相应私密值计算，接收方利用私密值和时间戳验证认证请求，只有验证通过后才会接收该消息，否则丢弃此消息，而A无法得到车辆与RSU的私密值。因此，LAKA协议能够抵抗重放攻击。

6) 秘密泄露攻击

假如A获取到车辆向RSU_j发送消息M_1中的$N_{\mathrm{V}_i\mathrm{T}}$、$S_{\mathrm{V}_i\mathrm{T}}$，由于$A$没有TA的私密值$S_{\mathrm{T}}$，因此无法计算得到车辆的随机值$N_{\mathrm{V}_i}$和私密值$S_{\mathrm{V}_i}$。同理，$A$也无法计算得到$\mathrm{RSU}_j$随机值$N_{\mathrm{R}_j}$和私密值$S_{\mathrm{R}_j}$，以及TA的随机值$N_{\mathrm{T}}$和私密值$S_{\mathrm{T}}$。因此，LAKA协议能够抵抗秘密泄露攻击。

7) 中间人攻击

A无法成功伪造车辆和RSU_j合法的认证请求发起中间人攻击。由于车辆和RSU_j的认证请求R_{V}、R_{R}包含相应的私密值S_{V_i}和S_{R_j}，而S_{V_i}和S_{R_j}只有TA和相应的合法实体拥有，A无法获取。因此，LAKA协议能够抵抗中间人攻击。

8) 冒充攻击

对于车辆而言，其私密值S_{V_i}仅由自己和TA保存，A无法获取，而$R_{\mathrm{V}}=H(T_{\mathrm{VR}}\|\mathrm{VID}_i\|S_{\mathrm{V}_i})$由其私密值$S_{\mathrm{V}_i}$计算得到，$A$无法伪造。对于$\mathrm{RSU}_j$而言，$R_{\mathrm{R}}=H(T_{\mathrm{RT}}\|\mathrm{RID}\|S_{\mathrm{R}_j})$由其私密值$S_{\mathrm{R}_j}$计算得到，$A$无法伪造。因此，LAKA协议能够抵抗冒充攻击。

9) DoS攻击

假设A截获到认证请求R_{V}和R_{R}，并尝试伪造大量R_{V}和R_{R}。由于认证请求R_{V}和R_{R}由车辆和RSU_j的私密值S_{V_i}、S_{R_j}计算得到，而A无法得到真实的私密值，从而无法伪造合法的认证请求。因此，LAKA协议能够抵抗DoS攻击。

10) 追踪攻击

在认证密钥协商过程中，车辆、RSU_j以及TA之间传输的消息都是动态变化的，如车辆向RSU_j发送的$N_{\mathrm{V}_i\mathrm{T}}$、$N_{\mathrm{V}_i}$和$R_{\mathrm{V}}$分别由随机数$N_{\mathrm{V}_i}$和时间戳$T_{\mathrm{VR}}$计算得到，$A$无法根据某个不变量追踪某个车辆信息。因此，LAKA协议能够抵抗追踪攻击。

综上所述，LAKA协议能够抵抗中间人攻击等多种恶意攻击，并实现了车辆的隐私保护。

5　协议性能对比

本节对LAKA协议和文献[13-17]方案在安全性和性能等方面进行对比与分析。

5.1　安全性对比分析

LAKA协议和文献[13-17]方案安全性对比如表1所示，其中，√表示方案满足该安全性，×表示方案不满足该安全性。

表1对比结果表明，文献[13-17]方案均满足不可链接性和前向安全性，能够抵抗追踪攻击，但LAKA协议在满足车辆匿名性和身份可追溯性方面优于文献[14]方案，在抵抗重放攻击方面优于文献[13]方案，在抵抗秘密泄露攻击方面优于文献[14,17]方案，在抵抗DoS攻击方面优于文献[13,17]方案，在抵抗冒充攻击方面优于文献[14-17]方案，在抵抗中间人攻击方面优于文献[17]方案。因此，LAKA协议更适用于车联网轻量级安全认证和密钥协商场景。

5.2　计算代价对比分析

利用密码学库cryptography和ecdsa在个人计算机（Windows11操作系统、主频2.60 GHz的i9-13900H的处理器、内存为32 GB）及PyCharm

表1 LAKA协议和文献[13-17]方案安全性对比

方案	车辆匿名性	不可链接性	身份可追溯性	前向安全性	重放攻击	秘密泄露攻击	中间人攻击	冒充攻击	DoS攻击	追踪攻击
文献[13]	√	√	√	√	×	√	√	√	×	√
文献[14]	×	√	×	√	√	×	√	×	√	√
文献[15]	√	√	√	√	√	√	√	×	√	√
文献[16]	√	√	√	√	√	√	√	×	√	√
文献[17]	√	√	√	√	√	×	×	×	×	√
LAKA协议	√	√	√	√	√	√	√	√	√	√

2024.2.3的编译环境下对文献[13-17]方案和LAKA协议所涉及的密码学操作进行模拟，结果为10万次密码学操作的平均运算时间，如表2所示。其中，T_h为Hash运算，T_{xor}为异或运算，T_{ecm}为椭圆曲线标量乘法运算，T_{eca}为椭圆曲线标量加法运算，T_{puf}为PUF运算，$T_{Enc/Dec}$为对称加解密运算。根据表2中的数据，LAKA协议和文献[13-17]方案在各实体处及总计算代价对比如表3所示。

LAKA协议和文献[13-17]方案的计算代价对比如图8所示。

在文献[13]方案中，各实体共进行15次Hash、15次异或和9次椭圆曲线标量乘法运算，总计算代价为$15T_h+15T_{xor}+9T_{ecm}\approx3.330$ ms。

表2 密码学运算的平均执行时间

密码学运算	平均执行时间/ms
T_h	0.000 8
T_{xor}	0.001 6
T_{ecm}	0.365 4
T_{eca}	0.002 7
T_{puf}	0.002 5
$T_{Enc/Dec}$	0.005 8

在文献[14]方案中，各实体共进行22次Hash、5次异或和22次椭圆曲线标量乘法运算，总计算代价为$22T_h+5T_{xor}+22T_{ecm}\approx8.062$ ms。

在文献[15]方案中，各实体共进行5次Hash、

表3 LAKA协议和文献[13-17]方案在各实体处及总计算代价对比

协议	V/ms	RSU/ms	TA/ms	总计算代价/ms
文献[13]	$3T_h+2T_{xor}+2T_{ecm}\approx0.737$	$3T_h+6T_{xor}+2T_{ecm}\approx0.745$	$9T_h+7T_{xor}+5T_{ecm}\approx1.848$	$15T_h+15T_{xor}+9T_{ecm}\approx3.330$
文献[14]	$8T_h+3T_{xor}+6T_{ecm}\approx2.204$	$5T_h+T_{xor}+6T_{ecm}\approx2.197$	$9T_h+T_{xor}+10T_{ecm}\approx3.661$	$22T_h+5T_{xor}+22T_{ecm}\approx8.062$
文献[15]	$2T_h+T_{ecm}\approx0.367$	$3T_h+4T_{ecm}+3T_{eca}\approx1.472$	0	$5T_h+5T_{ecm}+3T_{eca}\approx1.839$
文献[16]	$3T_h+3T_{ecm}+T_{eca}+T_{Enc/Dec}\approx1.107$	$3T_h+4T_{ecm}+3T_{eca}\approx1.472$	$2T_h+T_{ecm}+T_{Enc/Dec}\approx0.373$	$8T_h+8T_{ecm}+4T_{eca}+2T_{Enc/Dec}\approx2.952$
文献[17]初始认证阶段	$2T_h+2T_{xor}+3T_{ecm}\approx1.101$	$2T_h+T_{xor}+3T_{ecm}\approx1.099$	$5T_h+3T_{xor}+3T_{ecm}\approx1.106$	$9T_h+6T_{xor}+9T_{ecm}\approx3.306$
文献[17]快速认证阶段	$T_h+T_{xor}+2T_{ecm}\approx0.733$	$3T_h+T_{xor}+2T_{ecm}\approx0.735$	0	$4T_h+2T_{xor}+4T_{ecm}\approx1.468$
LAKA协议初始认证阶段	$4T_h+3T_{xor}+2T_{Enc/Dec}\approx0.022$	$4T_h+3T_{xor}+2T_{Enc/Dec}\approx0.022$	$7T_h+3T_{xor}\approx0.013$	$15T_h+9T_{xor}+4T_{Enc/Dec}\approx0.057$
LAKA协议快速认证阶段	$4T_h+2T_{xor}+2T_{Enc/Dec}\approx0.020$	$5T_h+2T_{xor}+2T_{Enc/Dec}\approx0.021$	0	$9T_h+4T_{xor}+4T_{Enc/Dec}\approx0.041$

5 次椭圆曲线标量乘法和 3 次椭圆曲线标量加法运算，总计算代价为 $5T_h+5T_{ecm}+3T_{eca}\approx1.839$ ms。

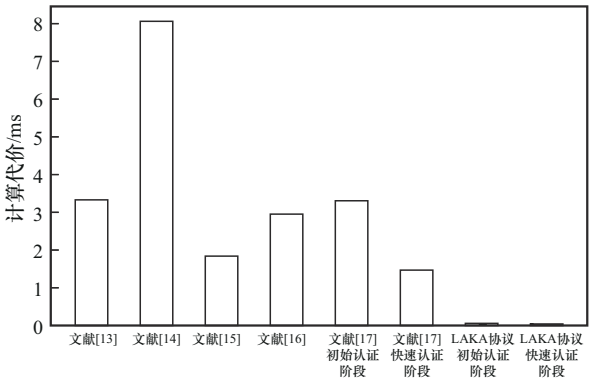


图 8　LAKA 协议和文献[13-17]方案的计算代价对比

在文献[16]方案中，各实体共进行 8 次 Hash、8 次椭圆曲线标量乘法、4 次椭圆曲线标量加法和 2 次对称加解密运算，总计算代价为 $8T_h+8T_{ecm}+4T_{eca}+2T_{Enc/Dec}\approx2.952$ ms。

在文献[17]方案中，各实体在初始认证阶段共进行 9 次 Hash、6 次异或和 9 次椭圆曲线标量乘法运算，该阶段总计算代价为 $9T_h+6T_{xor}+9T_{ecm}\approx3.306$ ms；快速认证阶段共进行 4 次 Hash、2 次异或和 4 次椭圆曲线标量乘法运算，该阶段总计算代价为 $4T_h+2T_{xor}+4T_{ecm}\approx1.468$ ms；因此，2 个阶段的总计算代价为 $13T_h+8T_{xor}+13T_{ecm}\approx4.774$ ms。

在 LAKA 协议中，各实体在初始认证阶段共进行 15 次 Hash、9 次异或和 4 次对称加解密运算，该阶段总计算代价为 $15T_h+9T_{xor}+4T_{Enc/Dec}\approx0.057$ ms；快速认证阶段共进行 9 次 Hash、4 次异或和 4 次对称加解密运算，该阶段总计算代价为 $9T_h+4T_{xor}+4T_{Enc/Dec}\approx0.041$ ms；因此，2 个阶段的总计算代价为 $24T_h+13T_{xor}+8T_{Enc/Dec}\approx0.098$ ms。

LAKA 协议和文献[13-17]方案在 RSU 数量不同时计算代价对比如图 9 所示。对比结果表明，由于 LAKA 协议初始认证阶段只需进行一次，后续均是车辆与 RSU 通过车辆旅行时间表进行快速认证。因此，LAKA 协议计算代价远低于文献[13-17]方案。

LAKA 协议和文献[13-17]方案密钥管理对比如表 4 所示，密钥管理包括密钥生成与密钥更新。表 4 对比结果表明，LAKA 协议的密钥管理效率低于文献[14-16]方案，高于文献[13,17]方案，但仅 LAKA 协议和文献[14]方案实现了密钥更新以抵抗追踪攻击，因此 LAKA 具有更强的安全性和隐私保护性以及较好的密钥管理效率。

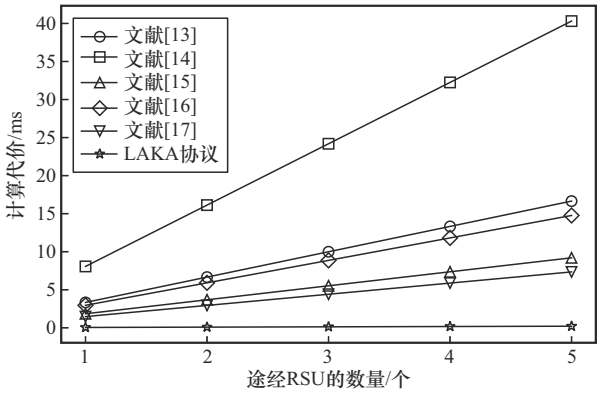


图 9　LAKA 协议和文献[13-17]方案在 RSU 数量不同时计算代价对比

表 4　LAKA 协议和文献[13-17]方案密钥管理对比

协议	密钥管理/ms
文献[13]	$3T_h+T_{ecm}\approx0.368$
文献[14]	$11T_h+4T_{xor}+5T_{ecm}\approx1.844$
文献[15]	$T_h+T_{xor}+5T_{ecm}\approx1.828$
文献[16]	$7T_h+T_{xor}+9T_{ecm}+3T_{Enc/Dec}\approx3.312$
文献[17]	$2T_{ecm}\approx0.730$
LAKA 协议	$4T_{puf}+4T_{ecm}\approx1.472$

5.3　通信开销对比分析

为了便于比较与分析，本文方案与文献[13-17]方案参数预设一致，椭圆曲线点乘、切比雪夫多项式、哈希摘要、异或、有限域元素、对称加密、时间戳和身份的大小分别为 320 bit、256 bit、160 bit、160 bit、160 bit、256 bit、32 bit、32 bit。LAKA 协议和文献[13-17]方案在各实体处及总通信开销对比如表 5 所示。其中，$|G|$ 为椭圆曲线点乘大小，$|C|$ 为切比雪夫多项式大小，$|H|$ 为哈希摘要大小，$|X|$ 为异或大小，$|Z_q^*|$ 为有限域元素大小，$|E|$ 为对称加密大小，$|T|$ 为时间戳大小，|ID| 为身份大小。

LAKA 协议和文献[13-17]方案的通信开销对比如图 10 所示。

在文献[13]方案中，各实体间共进行 4 次椭圆曲线点乘、7 次哈希、9 次异或的信息交换，总通信开销为 $4|G|+7|H|+9|X|=3\,840$ bit。

在文献[14]方案中，各实体间共进行 10 次切比雪夫多项式、9 次哈希、4 次异或、4 次时间戳的信息交换，总通信开销为 $10|G|+9|H|+4|X|+4|T|=4\,768$ bit。

表 5 LAKA 协议和文献[13-17]方案在各实体处及总通信开销对比

协议	V/bit	RSU/bit	TA/bit	总通信开销/bit
文献[13]	$\|G\|+\|H\|+\|X\|=640$	$3\|G\|+5\|H\|+5\|X\|=2\ 560$	$\|H\|+3\|X\|=640$	$4\|G\|+7\|H\|+9\|X\|=3\ 840$
文献[14]	$\|C\|+3\|H\|+\|X\|+\|T\|=928$	$6\|C\|+4\|H\|+3\|X\|+2\|T\|=2\ 720$	$3\|C\|+2\|H\|+\|T\|=1\ 120$	$10\|C\|+9\|H\|+4\|X\|+4\|T\|=4\ 768$
文献[15]	$4\|G\|+2\|Z_q^*\|+2\|T\|=1\ 664$	$4\|G\|+2\|Z_q^*\|+2\|T\|=1\ 664$	0	$8\|G\|+4\|Z_q^*\|+4\|T\|=3\ 328$
文献[16]	$3\|G\|+3\|Z_q^*\|+2\|T\|=1\ 504$	$3\|G\|+3\|Z_q^*\|+2\|T\|=1\ 504$	0	$6\|G\|+6\|Z_q^*\|+4\|T\|=3\ 008$
文献[17]初始认证阶段	$\|G\|+\|H\|+\|T\|+\|ID\|=544$	$4\|G\|+4\|H\|+3\|T\|+2\|ID\|=2\ 080$	$3\|G\|+3\|H\|+\|T\|=1\ 088$	$8\|G\|+8\|H\|+5\|T\|+3\|ID\|=4\ 096$
文献[17]快速认证阶段	$\|G\|+\|T\|+\|ID\|=384$	$\|G\|+2\|H\|+\|T\|+\|ID\|=704$	$2\|T\|=64$	$2\|G\|+2\|H\|+4\|T\|+2\|ID\|=1\ 152$
LAKA 协议初始认证阶段	$\|H\|+\|X\|+\|E\|+\|T\|+\|ID\|=640$	$4\|H\|+4\|X\|+\|E\|+3\|T\|+2\|ID\|=1\ 696$	$3\|H\|+\|X\|+\|T\|=672$	$8\|H\|+6\|X\|+2\|E\|+5\|T\|+3\|ID\|=3\ 008$
LAKA 协议快速认证阶段	$\|H\|+\|X\|+\|E\|+\|T\|+\|ID\|=640$	$3\|H\|+\|X\|+\|E\|+\|T\|=928$	$2\|T\|=64$	$4\|H\|+2\|X\|+2\|E\|+4\|T\|+\|ID\|=1\ 632$

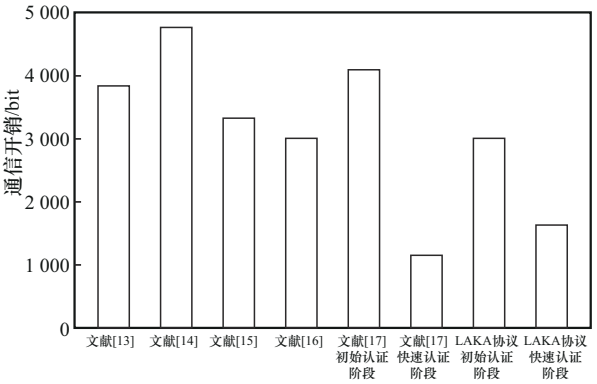


图 10 LAKA 协议和文献[13-17]方案的通信开销对比

在文献[15]方案中，各实体共进行 8 次椭圆曲线乘法、4 次有限域元素和 4 次时间戳的信息交换，总通信开销为 $8|G|+4|Z_q^*|+4|T|=3\ 328$ bit。

在文献[16]方案中，各实体共进行 6 次椭圆曲线乘法、6 次有限域元素和 4 次时间戳的信息交换，总通信开销为 $6|G|+6|Z_q^*|+4|T|=3\ 008$ bit。

在文献[17]方案中，各实体在初始认证阶段共进行 8 次椭圆曲线点乘、8 次哈希、5 次时间戳、3 次身份的信息交换，该阶段总通信开销为 $8|G|+8|H|+5|T|+3|ID|=4\ 096$ bit；快速认证阶段共进行 2 次椭圆曲线点乘、2 次哈希、4 次时间戳、2 次身份的信息交换，该阶段总通信开销为 $2|G|+2|H|+4|T|+2|ID|=1\ 152$ bit；因此，2 个阶段的总通信开销为 $10|G|+10|H|+9|T|+5|ID|=5\ 248$ bit。

在 LAKA 协议中，各实体在初始认证阶段共进行 8 次哈希、6 次异或、2 次对称加密、5 次时间戳、3 次身份的信息交换，该阶段总通信开销为 $8|H|+6|X|+2|E|+5|T|+3|ID|=3\ 008$ bit；快速认证阶段共进行 4 次哈希、2 次异或、2 次对称加密、4 次时间戳、1 次身份的信息交换，该阶段总通信开销为 $4|H|+2|X|+2|E|+4|T|+|ID|=1\ 632$ bit；因此，2 个阶段的总通信开销 $12|H|+8|X|+4|E|+9|T|+4|ID|=4\ 640$ bit。

LAKA 协议和文献[13-17]方案在 RSU 数量不同时通信开销对比如图 11 所示。对比结果表明，LAKA 协议初始认证阶段只需进行一次，后续均是车辆与 RSU 通过旅行时间表进行快速认证，因此 LAKA 协议通信开销低于文献[13-16]方案。然而，LAKA 协议在认证阶段通过异或和对称加密运算对私密值和随机值进行加密，与文献[17]方案相比通信开销略有增加，但 LAKA 协议避免了秘密泄露攻击、中间人攻击等恶意攻击，具有更强的安全性和隐私保护性。

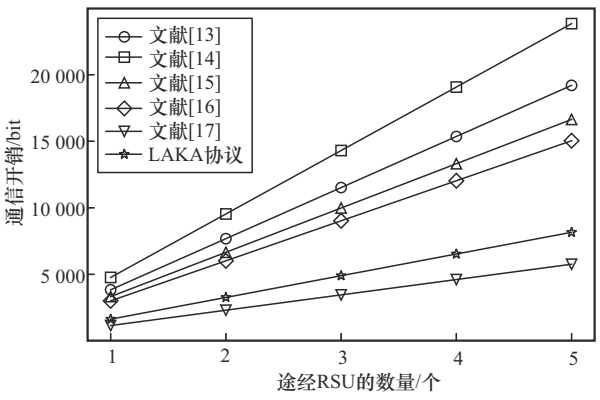


图 11 LAKA 协议和文献[13-17]方案在 RSU 数量不同时通信开销对比

本文在个人计算机（Windows11 操作系统、主频 2.60 GHz 的 i9-13900H 的处理器、内存为 32 GB）及 MATLAB R2025a 的编译环境下综合考虑计算代价和通信开销，LAKA 协议和文献[13-17]方案通信时延对比如图 12 所示。参考文献[16]方案参数设

置，道路长度为5 km，RSU 部署密度为500 m/个，车辆速度为5~40 m/s，传输速率为6 Mbit/s。对比结果表明，LAKA 协议的通信时延低于文献[13-17]方案。

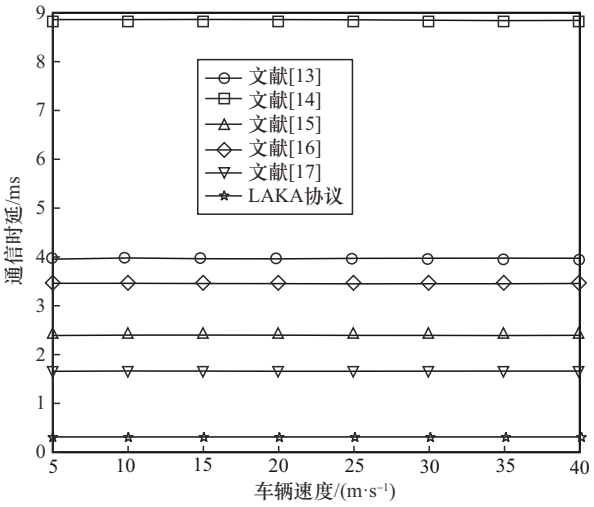


图12　LAKA 协议和文献[13-17]方案通信时延对比

LAKA 协议和文献[22-23]方案哈希计算代价对比和存储开销对比分别如表6和表7所示。对比结果表明，LAKA 协议的总哈希计算代价仅为$10T_h$≈0.010 ms（最低），存储开销仅为992 bit（最低）。

表6　LAKA 协议和文献[22-23]方案哈希计算代价对比

协议	总哈希计算代价/ms
文献[22]	$15T_h$≈0.015
文献[23]	$29T_h$≈0.029
LAKA 协议	$10T_h$≈0.010

表7　LAKA 协议和文献[22-23]方案存储开销对比

协议	总存储开销/bit
文献[22]	1 376
文献[23]	1 248
LAKA 协议	992

综上所述，与文献[13-17]方案相比，LAKA 协议在安全性和隐私保护性等方面具有显著优势，能够抵抗秘密泄露攻击、中间人攻击等攻击，具有更强的安全性和隐私保护性；与文献[22-23]方案相比，LAKA 协议具有更低的哈希计算代价与存储开销。因此，LAKA 协议更加适用于动态变化的轻量级车联网认证场景。

6　结束语

本文针对文献[17]进行安全性分析，指出其存在安全隐患，不能抵抗秘密泄露攻击、中间人攻击等多种恶意攻击。为了解决文献[17]所面临的安全隐患问题，本文提出了一种面向车联网的 LAKA 协议。通过异或和对称加密算法对各实体的私密值和随机值进行加密，确保私密值和随机值在传输过程中的安全性。BAN 逻辑和 ProVerif 工具的形式化分析和验证结果表明，LAKA 协议成功避免了文献[17]所面临的安全隐患，能够抵抗多种恶意攻击，具有更好的安全性和隐私保护性，适用于车联网认证的实际应用场景。下一阶段工作将在确保协议安全性和隐私保护性的同时，进一步降低通信开销以提高认证效率。

参考文献：

[1] MANASRAH A, YASEEN Q, AL-AQRABI H, et al. Identity-based authentication in VANETs: a review[J]. IEEE Transactions on Intelligent Transportation Systems, 2025, 26(4): 4260-4282.

[2] 于刊, 李东, 张奇勋, 等. 车联网泛在感知、潜在通信、融合计算、内生安全综述: 最新进展与未来方向[J]. 通信学报, 2024, 45(11): 223-243.
YU K, LI D, ZHANG Q X, et al. Survey of ubiquitons sensing, potential communication, integrated computing, and inherent security for Internet of vehicles: latest developments and future directions[J]. Journal on Communications, 2024, 45(11): 223-243.

[3] WU Q, ZHANG L, YANG Y F, et al. Certificateless signature scheme with batch verification for secure and privacy-preserving V2V communications in VANETs[J]. IEEE Transactions on Dependable and Secure Computing, 2025, 22(2): 1448-1459.

[4] SON S, LEE J, PARK Y, et al. Design of blockchain-based lightweight V2I handover authentication protocol for VANET[J]. IEEE Transactions on Network Science and Engineering, 2022, 9(3): 1346-1358.

[5] KHEZRI E, HASSANZADEH H, YAHYA R O, et al. Security challenges in Internet of vehicles (IoV) for ITS: a survey[J]. Tsinghua Science and Technology, 2025, 30(4): 1700-1723.

[6] 刘召曼, 杨亚芳, 宁建廷, 等. 基于新型可净化多重签名的车联网高效假名证书分发方案[J]. 通信学报, 2024, 45(11): 27-45.
LIU Z M, YANG Y F, NING J T, et al. Efficient pseudonym certificate distribution scheme for Internet of vehicles based on novel sanitizable multi-signature[J]. Journal on Communications, 2024, 45(11): 27-45.

[7] ALI I, CHEN Y, ULLAH N, et al. An efficient and provably secure ECC-based conditional privacy-preserving authentication for vehicle-to-vehicle communication in VANETs[J]. IEEE Transactions on Vehicular Technology, 2021, 70(2): 1278-1291.

[8] WANG Z L, ZHOU Y W, QIAO Z R, et al. An anonymous and revocable authentication protocol for vehicle-to-vehicle communications[J].

IEEE Internet of Things Journal, 2023, 10(6): 5114-5127.

[9] 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.

[10] LIANG Y F, LUO E T, LIU Y N. Physically secure and conditional-privacy authenticated key agreement for VANETs[J]. IEEE Transactions on Vehicular Technology, 2023, 72(6): 7914-7925.

[11] WEI L, CUI J, ZHONG H, et al. Proven secure tree-based authenticated key agreement for securing V2V and V2I communications in VANETs[J]. IEEE Transactions on Mobile Computing, 2022, 21(9): 3280-3297.

[12] XIE Q, DING Z X, ZHENG P P. Provably secure and anonymous V2I and V2V authentication protocol for VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(7): 7318-7327.

[13] AWAIS S M, WU Y C, MAHMOOD K, et al. Provably secure and lightweight authentication and key agreement protocol for fog-based vehicular ad-hoc networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2024, 25(12): 21107-21116.

[14] TOMAR A, TRIPATHI S. A Chebyshev polynomial-based authentication scheme using blockchain technology for fog-based vehicular network[J]. IEEE Transactions on Mobile Computing, 2024, 23(10): 9075-9089.

[15] ZHU F, YI X, ABUADBBA 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.

[16] LI X C, YIN X C, NING J T. RelCLAS: a reliable malicious KGC-resistant certificateless aggregate signature protocol for vehicular ad hoc networks[J]. IEEE Internet of Things Journal, 2023, 10(23): 21100-21114.

[17] 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, YU 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.

[18] BLANCHET B. Modeling and verifying security protocols with the applied pi calculus and ProVerif[J]. Foundations and Trends in Privacy and Security, 2016, 1(1/2): 1-135.

[19] BURROWS M, ABADI M, NEEDHAM R. A logic of authentication[J]. ACM Transactions on Computer Systems, 1990, 8(1): 18-36.

[20] AZAM F, KUMAR S, YADAV K P, et al. An outline of the security challenges in VANET[C]//Proceedings of the 2020 IEEE 7th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON). Piscataway: IEEE Press, 2020: 1-6.

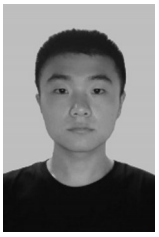
[21] HAMDI M M, DHAFER M, MUSTAFA A S, et al. Effect sybil attack on security authentication service in VANET[C]//Proceedings of the 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). Piscataway: IEEE Press, 2022: 1-6.

[22] MAHMOOD K, FATIMA M N, SHAMSHAD S, et al. A cost-effective key agreement encryption protocol for securing IIoT-enabled WSN communication[J]. IEEE Internet of Things Journal, 2025, 12(5): 5185-5193.

[23] LI Y, TIAN Y L. A lightweight and secure three-factor authentication protocol with adaptive privacy-preserving property for wireless sensor networks[J]. IEEE Systems Journal, 2022, 16(4): 6197-6208.

[作者简介]

刘亚丽（1981– ），女，江苏徐州人，博士，江苏师范大学教授、硕士生导师，主要研究方向为信息安全、认证协议、隐私保护技术、区块链安全、车联网安全、无人机安全、智慧医疗安全、密码算法和数据安全及其在物联网中的应用等。



庞小辉（2001– ），男，河南商丘人，江苏师范大学硕士生，主要研究方向为车联网安全、认证协议、密钥协商和隐私保护技术等。

陈东东（2000– ），男，江苏宿迁人，江苏师范大学硕士生，主要研究方向为无人机认证技术、物联网安全和隐私保护技术等。

王鹏超（2003– ），男，江苏徐州人，东南大学硕士生，主要研究方向为信息安全、RFID认证和隐私保护技术等。

周毅（2000– ），男，江苏徐州人，江苏师范大学硕士生，主要研究方向为无人机认证技术、区块链技术、数字签密技术和数据共享技术等。