专题：低空智联网与低空安全

基于物理不可克隆函数的车云轻量级匿名认证协议

柳亚男[1]，曹磊[1]，张正[1]，李戈[2]，邱硕[1]，王苏豪[1]
（1. 金陵科技学院网络安全学院，江苏 南京 211169；
2. 中国人民解放军陆军工程大学指挥控制工程学院，江苏 南京 210007）

摘　要：针对低空经济中车辆与云端应用服务器的通信场景，提出基于PUF-ECC-Kerberos的轻量级车云匿名认证协议PEKE。该协议利用物理不可克隆函数（physical unclonable function，PUF）改进传统Kerberos的认证模式，结合椭圆曲线密码学（elliptic curve cryptography，ECC）算法获得车辆假名，实现车辆与云服务器之间的双向匿名认证和密钥交换。结合Scyther形式化分析工具验证，该协议不仅能够有效抵御密钥泄露、伪装攻击、中间人攻击以及反射攻击等多种安全威胁，同时还能在低空经济环境中实现车辆通信的匿名性，提供可靠的安全保障。通过与其他协议进行性能分析比较，进一步证明了PEKE协议在计算和通信消耗方面具有显著优势，并能有效降低通信时延，从而提高系统的整体效率。

关键词：物理不可克隆函数；Kerberos；椭圆曲线密码学算法；匿名认证；车联网；低空经济
中图分类号：TP309
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2025096

PUF-based light-weighted anonymous authentication protocol between vehicles and cloud

LIU Yanan[1], CAO Lei[1], ZHANG Zheng[1], LI Ge[2], QIU Shuo[1], WANG Suhao[1]
1. School of Network Security, Jinling Institute of Technology, Nanjing 211169, China
2. School of Command and Control Engineering, Army Engineering University of PLA, Nanjing 210007, China

Abstract: In the context of vehicle-to-cloud application server communication within the low-altitude economy, a novel vehicle-to-cloud anonymous authentication protocol named PEKE was proposed, which was based on PUF-ECC-Kerberos. The protocol was enhanced by incorporating physical unclonable function (PUF) and integrating the elliptic curve cryptography (ECC) public-key encryption algorithm to obtain vehicle pseudonyms. This enabled mutual anonymous authentication and key exchange between vehicles and cloud servers to be achieved. Through formal analysis using the Scyther tool, it was demonstrated that the PEKE protocol not only effectively resisted various security threats such as key leakage, masquerade attacks, man-in-the-middle attacks, and reflection attacks, but also en-

收稿日期：2025−01−20；修回日期：2025−02−25
通信作者：曹磊，3389664953@qq.com
基金项目：国家自然科学基金青年项目（No.42101428）；江苏省“青蓝工程”项目；江苏省研究生科研与实践创新计划项目
Foundation Items: The National Natural Science Foundation of China Youth Project (No.42101428), Jiangsu Province “Qinglan Project”, The Postgraduate Research & Practice Innovation Program of Jiangsu Province

sured the anonymity of vehicle communications in the low-altitude economy, providing robust security guarantees. Furthermore, performance analysis comparisons with other protocols reveal that the PEKE protocol exhibited significant advantages in terms of computational and communication overhead, effectively reducing communication latency and thereby enhancing the overall system efficiency.

Key words: PUF, Kerberos, ECC algorithm, anonymous authentication, Internet of vehicles, low-altitude economy

0　引言

近年来，低空经济的快速发展为交通运输模式带来了新的可能性，尤其是在城市物流和空中出行等领域。低空经济的核心在于利用无人机及其他空中交通工具提升运输效率，满足日益增长的即时配送和短途出行需求。在这一背景下，车联网与低空经济之间的紧密联系愈发明显，车联网技术为低空经济提供了实时数据支持，有助于协调管理地面与空中交通，确保不同交通方式之间的安全与效率。此外，基于车联网实现的智能交通管理，可以优化无人机的物流配送路径，提升整体物流效率。这种跨越地面与空中的协同发展，标志着未来交通运输模式的融合与创新，为实现更加高效、安全的智能出行奠定了基础。

然而，随着车联网技术的快速发展，隐私保护和安全问题也日益凸显，特别是在匿名身份认证和密钥协商方面，如何在保护用户隐私的同时确保系统的安全性，已成为当前研究的焦点。2012 年，翟苗等[1]提出了一种基于双线性映射的车联网身份认证隐私保护机制，通过将用户身份标识和车辆射频识别（radio frequency identification，RFID）码映射成车辆私钥，实现了车辆与路侧单元（road side unit，RSU）的匿名密钥协商。2018 年，Dang 等[2]提出了一种基于身份的双方一轮身份验证和密钥协商方案 IB2PAKA，显著降低了密钥协商的时间消耗。2021 年，Deng 等[3]提出了 IB2PAKA 的改进方案，通过分离车辆发送的信息和公钥的关系，进一步提升了 IB2PAKA 方案的安全性。2024 年，刘健等[4]提出了可溯源的车联网匿名签名和批量验证协议，设计了 RSU 针对同一车辆和不同车辆发出的验证信息进行匿名验证的不同算法，提高了车辆身份验证的效率。同年，毕昌兵等[5]提出了由车辆本身生成假名的可追溯匿名消息认证方案，减少了系统对车辆假名生成和存储的资源消耗。

在低空经济中，车辆作为重要的信息节点，需要与云端应用服务器实现可靠的通信，以实现智能交通管理、车辆远程控制和紧急救援等功能。本文针对车联网中车辆与云端（vehicle-to-cloud，V2C）应用服务器之间的通信场景，提出一种高效且安全的车云匿名身份认证协议 PEKE。车云通信是指车辆通过蜂窝网络（如 4G、5G）与远程云服务器进行交互，支持车辆访问多种云服务，包括但不限于实时交通信息、地图更新、远程诊断和维护、娱乐内容下载、车队管理以及紧急救援等[6-7]。车云通信的核心挑战在于如何确保车辆与云服务器之间的通信安全与数据隐私，同时保持通信的高效性与低时延。PEKE 协议结合椭圆曲线密码学（elliptic curve cryptography，ECC）算法和单向哈希算法，使车辆获得假名，随后采用物理不可克隆函数（physical unclonable function，PUF）的挑战响应对替代 Kerberos 协议中认证服务器（authentication server，AS）和用户之间的口令认证，完成车辆与 AS 的双向认证，最后通过验证车辆假名和 Kerberos 协议中的票据授权服务器（ticket granting server，TGS）分发的票据，解决了车辆与云端应用服务器之间的身份认证与密钥协商问题。

1 相关工作

1.1 椭圆曲线密码学算法

ECC算法是一种基于椭圆曲线上离散对数的计算困难性的公钥加密技术，它通过在椭圆曲线上的点运算来实现加密和解密。相较于传统的RSA（Rivest-Shamir-Adleman）算法，ECC算法在保证同等安全性的情况下，使用更短的密钥长度提升效率，被广泛应用于数字签名、密钥交换等安全领域，已成为车联网中重要的加密方案[8-11]。

1.2 物理不可克隆函数

PUF的基本原理是利用硅基芯片在制造过程中微小不均匀性所产生的独特性，为芯片生成一个不可复制的标识[12]。这些标识可以作为唯一的密钥，用于加密操作。PUF不存储密钥，而是通过测量和分析物理特性来生成密钥。PUF用数学模型来描述，表示为：

$$P:C \to R:P(c)=r, c \in C, r \in R \quad (1)$$

其中，P为PUF用于映射输入激励值到输出响应值，C为挑战（challenge）集合，R为响应（response）集合，对于每一个挑战值c，函数P会生成一个唯一的响应值r，（c,r）被称为挑战响应对，而（c,r）的集合<C,R>被称为挑战响应集合。

PUF的响应基于设备内部独特的物理特性，这些特性既无法被精确复制，也无法被预测。因此，PUF具备强大的抗攻击性和防窃取性，广泛应用于硬件安全、身份验证、设备认证等领域，为车联网的身份认证和密钥协商提供了一种独特的解决方案[13-16]。

1.3 Kerberos协议

Kerberos协议最初由美国麻省理工学院（MIT）开发，是一种对称密钥加密的网络身份验证协议[17]。它通过在不安全的网络环境中使用“票据”（ticket）来安全地验证用户身份，有效防止身份欺骗和数据窃取[18]。在Kerberos协议中存在一个可信的第三方机构，即密钥生成中心（key generation center，KGC），其负责管理和分发密钥，从而提高了用户身份认证的安全性[19]。因此，Kerberos协议也逐渐被应用于解决车联网中车辆认证的安全问题。

2 PEKE协议

2.1 系统模型

在低空经济环境中，车联网拓扑结构的设计应当考虑安全性、效率和通信隐私等方面的要求，以保障空地一体化的交通系统能够实现车辆与云端应用平台之间的高效、稳定与安全通信。本文设计的车联网系统模型如图1所示，该模型主要包括3种设备：车辆、应用服务器和KGC。其中，KGC包含一个认证服务器（AS）、一个票据授权服务器（TGS）和一个数据库（data base，DB），其主要负责车联网中密钥和假名的生成与分发，以及对合法车辆申请票据的分发。若干个车辆主要与KGC进行双向认证和假名申请，并对应用服务器发起匿名通信服务申请。若干个应用服务器主要负责与合法车辆建立通信。应用服务器与车辆建立通信后，可向无人机（unmanned aerial vehicle，UAV）或无人机基站（base station，BS）发送地面交通信息，以实现空地一体化的高效协同。在这个过程中，为了保障车联网的稳定性和安全性，KGC与应用服务器之间的通信必须建立在可靠的认证机制之上，避免恶意攻击导致系统崩溃或信息泄露。

2.2 PEKE协议描述

PEKE协议中车辆和应用服务器的匿名认证与会话密钥交换分为5个阶段：系统初始化、车辆和应用服务器在KGC注册、车辆向AS请求假名和票据授权票据（ticket grangting ticket，TGT）、车辆匿名向TGS请求服务授权票据（service granting ticket，SGT）、车辆匿名与应用服务器建立会话密钥。本文使用的符号说明对照见表1。

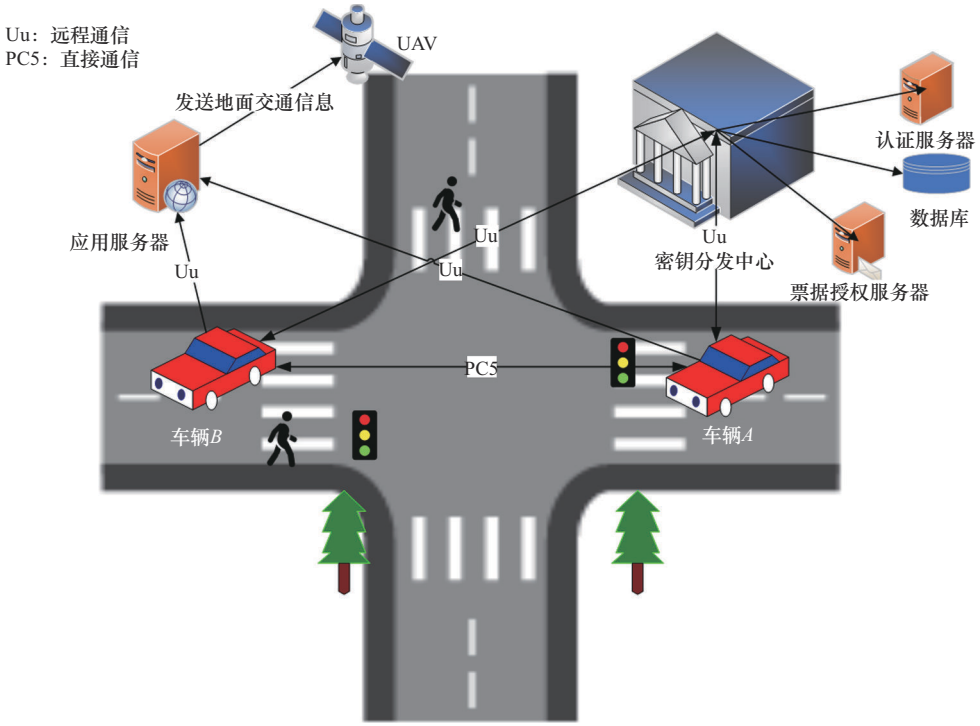


图1　车联网系统模型

表1　符号说明对照

符号	说明
V	车辆
X_id	设备X真实id
X_fid	设备X假名
C_V	PUF挑战值
R_V	PUF响应值
$<C_V,R_V>$	挑战响应对
CRP	挑战响应对集合
P	椭圆曲线基点
（pk-sk）	认证服务器公私钥对
K_{TGS}	票据授权服务器主密钥
$K_{X,Y}$	设备X与设备Y的会话密钥
t	时间戳
lifetime	生命周期
h_1、h_2	哈希函数

2.2.1　系统初始化

车辆配备了PUF结构，即PUF_V，并集成了公钥加密/解密算法、对称加密/解密算法和哈希函数h_1。车辆生成若干个随机数作为挑战集合C_V，将每个挑战输入PUF结构生成对应的响应R_V，每一个挑战C_V和对应的一个响应R_V组成一个车辆挑战响应对$<C_V,R_V>$。车辆生成的全部挑战响应对$<C_V,R_V>$构成车辆的挑战响应对集合CRP。

KGC的AS首先安装公钥加密/解密算法、对称加密/解密算法、哈希函数h_1和h_2，然后选一条椭圆曲线$Ep(a,b)$，并取椭圆曲线上一点作为基点P后选定一个比较大的数sk作为私钥，并生成公钥pk＝sk*P，将公私钥对（pk-sk）安全地存储在KGC的DB中。TGS生成主密钥K_{TGS}，并存储到DB中。

2.2.2　车辆和应用服务器在KGC注册

车辆将挑战响应对集合CRP以及真实id发送给KGC进行注册，KGC将车辆挑战响应对集合CRP按车辆的真实id索引，安全存储在KGC的DB中，KGC返回AS的公钥pk给车辆。

应用服务器App发送身份标识App_id到KGC的AS注册，AS根据应用服务器的身份标识

生成应用服务器和TGS的会话密钥$K_{App,TGS}$，AS保存App_id和$K_{App,TGS}$到DB并将$K_{App,TGS}$返回给应用服务器。KGC中AS和TGS对DB具备访问权限。车辆和应用服务器在KGC注册的过程如图2所示。

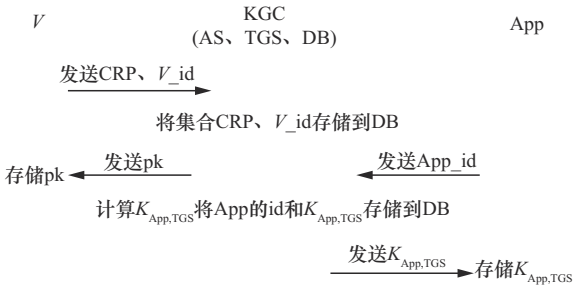


图2　车辆和应用服务器在KGC注册的过程

2.2.3　车辆向AS请求假名和TGT

车辆用pk加密车辆的真实id，用来向AS发送假名和TGT申请，即$E_{pk}(V_id)$。

AS收到消息后用sk解密$E_{pk}(V_id)$，得到车辆真实id，从DB中检索车辆真实id，检索成功后从车辆的挑战响应对集合CRP中任取一个挑战响应对$<C_V,R_V>$，生成与车辆通信的会话密钥$K_{V,AS}=h_1(R_V)$以及报文验证码（message authentication code，MAC）$MAC=h_1(C_V||R_V)$，若未检索到车辆真实id则退出。

AS根据车辆真实id生成车辆假名$V_fid=h_2(V_id)$，并随机生成车辆与TGS的会话密钥$K_{V,TGS}$，将车辆假名V_fid保存到DB中，用$K_{V,AS}$加密V_fid和$K_{V,TGS}$，得到$E_{K_{V,AS}}(V_fid, K_{V,TGS})$。AS访问到DB中TGS的主密钥$K_{TGS}$，用$K_{TGS}$加密生成TGT，即$E_{K_{TGS}}(\{V_fid, AS_id, TGS_id, t, lifetime, K_{V,TGS}\})$。

车辆收到AS发来的C_V、$E_{K_{V,AS}}(V\_fid, K_{V,TGS})$、MAC和TGT。车辆利用自己的$PUF_V$，生成挑战值$C_V$对应的响应值$R_V$，计算$MAC_V=h_1(C_V||R_V)$的值，若与收到的MAC值一致，则信任AS以及AS发送的消息。车辆生成与AS的会话密钥$K_{V,AS}=h_1(R_V)$，并用$K_{V,AS}$解密$E_{K_{V,AS}}(V_fid, K_{V,TGS})$，得到假名$V_fid$和$K_{V,TGS}$。

车辆向AS请求假名和TGT的过程如图3所示。

2.2.4　车辆匿名向TGS请求SGT

车辆用$K_{V,TGS}$加密想要请求通信的应用服务器身份标识App_id和车辆假名V_fid，即$E_{K_{V,TGS}}(App_id, V_fid)$。

车辆将$E_{K_{V,TGS}}(App_id, V_fid)$和TGT发送给TGS请求App_id对应的SGT。

TGS使用主密钥K_{TGS}解密TGT，得到$\{V_fid, AS_id, TGS_id, t, lifetime, K_{V,TGS}\}$，TGS使用$K_{V,TGS}$解密$E_{K_{V,TGS}}(App_id, V_fid)$并验证$V_fid$和TGT中的是否一致。若验证通过，则进行下一步；否则退出。

TGS生成车辆与应用服务器之间的随机会话密钥$K_{V,App}$，之后TGS用$K_{V,TGS}$加密V_fid、

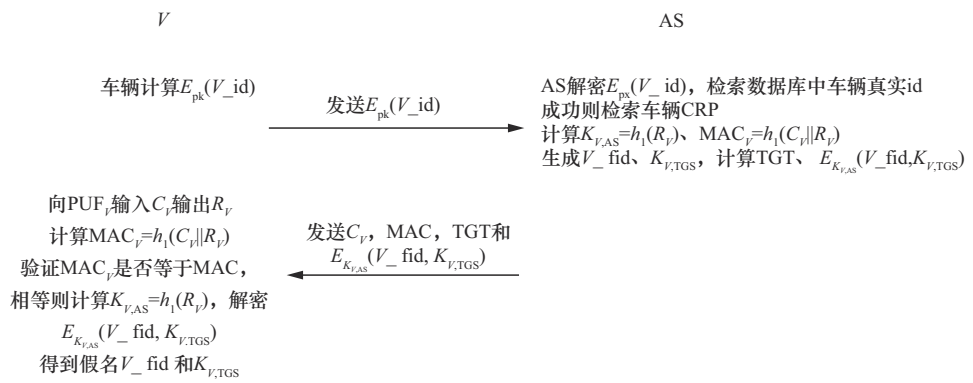


图3　车辆向AS请求假名和TGT的过程

App_id、$K_{V,\mathrm{App}}$，得到$E_{K_{V,\mathrm{TGS}}}(V_\mathrm{fid}, \mathrm{App_id}, K_{V,\mathrm{App}})$。TGS 根据应用服务器的标识 App_id，从 DB 中检索应用服务器和 TGS 的会话密钥$K_{\mathrm{App,TGS}}$，并生成用$K_{\mathrm{App,TGS}}$加密的 SGT，即$E_{K_{\mathrm{App,TGS}}}(\{V_\mathrm{fid}, \mathrm{App_id}, \mathrm{TGS_id}, t, \mathrm{lifetime}, K_{V,\mathrm{App}}\})$，随后 TGS 将$E_{K_{V,\mathrm{TGS}}}(V_\mathrm{fid}, \mathrm{App_id}, K_{V,\mathrm{App}})$和 SGT 发送给车辆。

车辆收到 TGS 发送来的$E_{K_{V,\mathrm{TGS}}}(V_\mathrm{fid}, \mathrm{App_id}, K_{V,\mathrm{App}})$和 SGT。车辆使用与 TGS 的会话密钥$K_{V,\mathrm{TGS}}$解密$E_{K_{V,\mathrm{TGS}}}(V_\mathrm{fid}, \mathrm{App_id}, K_{V,\mathrm{App}})$，得到$V$_fid、App_id 和$K_{V,\mathrm{App}}$。验证$V$_fid、App_id 与发送给 TGS 的是否一致，若一致，则信任 TGS 发送的 SGT 以及和应用服务器的会话密钥$K_{V,\mathrm{App}}$；否则退出。

车辆匿名向 TGS 请求 SGT 的过程如图 4 所示。

2.2.5　车辆匿名与应用服务器建立会话密钥

车辆用$K_{V,\mathrm{App}}$加密 App_id 和V_fid，得到$E_{K_{V,\mathrm{APP}}}(\mathrm{App_id}, V_\mathrm{fid})$。

车辆将$E_{K_{V,\mathrm{APP}}}(\mathrm{App_id}, V_\mathrm{fid})$和 SGT 发送给应用服务器。应用服务器利用其与 TGS 的会话密钥$K_{\mathrm{App,TGS}}$解密 SGT，得到{V_fid, App_id, TGS_id, t, lifetime, $K_{V,\mathrm{App}}$}。用解密得到的$K_{V,\mathrm{App}}$进一步解密$E_{K_{V,\mathrm{APP}}}(\mathrm{App_id}, V_\mathrm{fid})$，得到$V$_fid 和 App_id，验证$V$_fid 与 SGT 中的车辆假名是否一致，若一致则信任车辆，此后车辆与应用服务器之间使用$K_{V,\mathrm{App}}$进行通信；若不一致则退出。

车辆匿名与应用服务器 App 建立会话密钥的过程如图 5 所示。

3　安全性分析

3.1　Scyther 形式化分析

Scyther 是一种基于完美密码学假设的分析工具，主要用于对安全协议进行形式化分析，它能够帮助验证协议是否满足既定的安全属性，并检测协议是否存在潜在的安全漏洞或不符合特定安全要求的情况。

实验硬件环境为：8 GB 内存、Windows 11 操作系统、Python 2.7 以及 Scyther-w32-v1.1.3。定义 PEKE 协议中的 4 个角色为 V（车辆）、S（认证服务器）、T（票据授权服务器）、A（应用服务器）。将 PEKE 协议的角色和消息转换为 Scyther 的输入格式。Scyther 使用安全协议描述语言（security protocol description language，SPDL）来描述协议。PEKE 协议中各个角色的 SPDL 如图 6

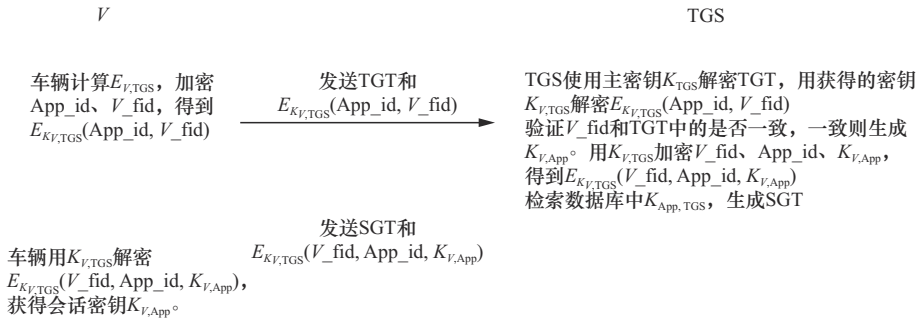


图 4　车辆匿名向 TGS 请求 SGT 的过程

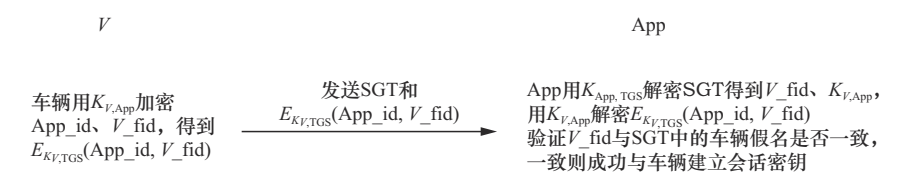


图 5　车辆匿名与应用服务器 App 建立会话密钥的过程

所示。

```
role V {
    send_1(V, S, {id}pk);
    recv_2(S, V, c, {fid,Kvt}H(puf(c)), tgt, H(c,puf(c)));
    send_3(V, T, {appid,fid}Kvt, tgt);
    recv_4(T, V, {appid,fid,Kva}Kvt,sgt);
    send_5(V, A, sgt, {appid,fid}Kva);
}
role S {
    recv_1(V, S, {id}pk);
    send_2(S, V, c, {fid,Kvt}H(puf(c)), tgt, H(c,puf(c)));
}
role T {
    recv_3(V, T, {appid,fid}Kvt, tgt);
    send_4(T, V, {appid,fid,Kva}Kvt,sgt);
}
role A {
    recv_5(V, A, sgt, {appid,fid}Kva);
}
```

图6　PEKE协议中各个角色的SPDL

完成PEKE协议描述之后，对其进行安全性验证。Scyther所有声明验证结果如图7所示，由图7可知，Scyther所有声明均成功通过验证。这表明，该协议即使在密钥泄露的情况下，认证机制仍能确保会话安全，保障其他安全属性不被破坏，抵御密钥泄露攻击；在伪装攻击中，通过模拟攻击者伪装成合法角色，Scyther确认协议能识别并拒绝伪装攻击；针对中间人攻击，该协议利用加密和PUF技术保障消息的完整性和保密性，从而阻止中间人篡改或解密消息。此外，通过反复发送合法消息，Scyther确认协议能防止攻击者利用反射消息进行攻击。

3.2　匿名性

在PEKE协议的第二阶段，车辆使用AS的公钥对真实id进行加密，向AS申请授权票据和假名。攻击者即使截获了车辆的申请假名信息，但由于缺乏AS的私钥，他们也无法解密以获取车辆的真实id。随后，AS根据车辆的真实id生成一个假名。车辆获得假名后，便使用该假名与TGS和应用服务器进行通信。由于假名是由AS独立生成的，攻击者无法从假名中推断出车辆的真实id，因此，该方案确保了匿名性。

3.3　身份双向认证

车辆与AS进行身份认证过程中，利用AS的公钥对真实id进行加密，并向AS发送假名和票据授权请求。AS使用私钥解密，获取车辆的真实id，并查询DB以验证。只有已完成注册车辆的真实id才能在DB中检索到，因此，AS在DB中检索到车辆的真实id后，即完成了对车辆身份的认证。AS随后向车辆发送TGT、假名、挑战C_V和MAC_V，收到消息后车辆利用安装的PUF系统输入挑战C_V以获取R_V，用以验证MAC_V。如果验证结果正确，则完成了车辆与AS之间的双向认证。

图7　Scyther所有声明验证结果

车辆与TGS申请SGT过程中，向TGS发送用会话密钥加密的假名和应用服务器身份标识，以及车辆的TGT。TGS解密TGT以获取车辆的假名和会话密钥，然后解密车辆发送的用会话密钥加密的假名和应用服务器身份标识，以验证假名是否与TGT中的相匹配。如果匹配，TGS即完成了对车辆的认证。TGS随后发送SGT和用车辆与TGS之间的会话密钥加密的车辆与应用服务器的会话密钥、车辆假名、应用服务器身份标识。车辆通过会话密钥解密，验证车辆假名和应用服务器身份标识是否与车辆用会话密钥加密发送的一致。如果一致，则完成了车辆与TGS之间的双向认证。

3.4　可追溯性

在密钥协商和身份认证过程中，KGC 和应用服务器 App 一旦检测到车辆发出恶意信息，KGC 的 AS 就可根据车辆的假名信息从 DB 中查询到车辆的真实 id，因此，PEKE 协议具有可追溯性。

3.5　抗伪造性

在密钥协商和身份认证过程中，攻击者即使截获车辆发送的信息，由于椭圆曲线离散对数问题的复杂性和 PUF 的不可克隆和不可预测性，攻击者无法伪造消息的发送身份。在协议中，消息的接收方会验证消息的发送者身份。因此，协议攻击者不可伪造消息进行发送。

3.6　前向后向安全性

每次 AS 向车辆发送的挑战 C_V 以及对应的 MAC_V 都具有随机性，攻击者无法根据当前的挑战 C_V 和 MAC_V 推断出之前或之后的 C_V 和 MAC_V。因此，PEKE 协议具备前向和后向安全性。

3.7　抵御重放攻击

AS 在生成 TGT 以及 TGS 生成 SGT 时都加入了时间戳和生命周期，TGS 在解密 TGT 以及应用服务器解密 SGT 时验证时间戳和生命周期，若消息超出生命周期则拒绝服务。因此，PEKE 协议可以抵御重放攻击。

3.8　抗侧信道攻击

在密钥协商和身份认证过程中，PEKE 协议设计采用了 ECC 算法和 PUF，这使得即使攻击者试图通过功耗分析、时间分析等侧信道攻击获取加密过程中的信息，也无法从中提取出私钥或其他敏感数据。椭圆曲线公钥加密的计算过程和 PUF 的生成过程具有较强的抗侧信道攻击能力，有效保障了密钥的安全性。

3.9　抗物理攻击

协议通过结合 PUF 在身份认证过程中生成唯一且不可预测的挑战响应，保证了密钥协商和身份认证的物理安全性。PUF 本身依赖于硬件的物理特性，具有强大的抗物理攻击能力，即使攻击者获得了设备的物理副本，也无法复制或伪造 PUF 的响应。与传统的密码存储机制不同，PUF 无法被逆向工程或克隆，从而有效防止了窃取设备密钥、破解硬件等物理攻击。

4　性能分析

本节主要探讨了 PEKE 协议中车辆与 KGC 和应用服务器之间的申请假名服务、身份认证以及密钥协商机制的计算资源开销，以及通信资源开销，并与其他相近方案[6-7]进行了对比。鉴于目前关于车辆与车联网中应用服务器之间通信的研究相对较少，本文还对比了车辆与车联网其他节点的身份认证及密钥协商方案[8,13]。

4.1　计算资源开销

密码学常用操作计算开销见表 2，以文献[20]中加密算法、哈希算法和 PUF 的操作计算开销为基础，对 PEKE 协议与文献[6-8]以及文献[13]所涉及的计算资源进行对比分析。PEKE 协议单次与其他方案单次认证和密钥协商计算开销对比见表 3。文献[6]提出的车辆与多服务器认证协议，系统总共需要执行 12 次椭圆曲线标量乘法运算和 10 次单向哈希函数运算。文献[7]提出的方案，系统总共需要执行 8 次椭圆曲线标量乘法运算和 9 次单向哈希函数运算。文献[8]提出的车辆与 RSU 密钥协商方案，系统总共需要执行 14 次椭圆曲线标量乘法运算和 15 次单向哈希函数运算。文献[13]提出的车辆与车辆之间的身份认证和密钥协商方案，系统总共需要执行 4 次椭圆曲线标量乘法运算、8 次单向哈希函数运算以及 2 次 PUF 运算。本文提出的协议需要执行 3 次椭圆曲线标量乘法运算、1 次 PUF 运算、11 次对称加解密运算和 5 次单向哈希函数运算。

由表 3 可知，PEKE 采用了较为轻量级的 Kerberos 协议和较少的椭圆曲线加密运算，相较于文献[6-8]中提出的基于大量椭圆曲线公钥加密的方案，不但能够显著节省计算资源，而且与同

样是轻量级协议的文献[13]相比，本文在PUF的使用上进行了优化，进一步提升了计算效率。

表2　密码学常用操作计算开销

符号	密码学操作说明	计算开销/ms
T_e	对称加解密运算	0.079
T_m	椭圆曲线标量乘法运算	5.900
T_h	单向哈希函数运算	0.026
T_{puf}	PUF运算	0.120

表3　PEKE协议单次与其他方案单次认证和密钥协商计算开销对比

协议	计算操作	总计算开销/ms
文献[6]	$12T_m+10T_h$	71.060
文献[7]	$8T_m+9T_h$	47.434
文献[8]	$14T_m+15T_h$	82.900
文献[13]	$4T_m+8T_h+2T_{puf}$	24.016
PEKE	$3T_m+1T_{puf}+11T_e+5T_h$	19.688

4.2　通信资源开销

PEKE协议中使用的参数通信大小见表4，由此可以计算出PEKE协议的通信资源开销。其中，车辆发送假名申请以及申请票据服务的总通信开销为1 024 bit，KGC中AS和TGS的通信开销为1 120 bit，因此，PEKE协议系统总通信开销为2 144 bit。

表4　PEKE协议中使用的参数通信大小

参数	长度/bit
哈希函数	256
对称密钥	64
椭圆曲线点	256
PUF挑战值	32
TGT票据	256
SGT票据	256

各方案单次认证和密钥协商通信成本对比见表5。由于PEKE协议在设计之初就充分考虑了数据传输的有效性，优化了数据包的结构并减少了冗余信息，相比文献[8]和文献[13]提出的方案，本文提出的协议有效降低了通信开销。虽然与文献[6]中车辆与服务器直接进行身份认证和密钥协商的方案相比，系统在整个通信开销上略高一些，但在协议的整体安全度，以及在车联网中服务器面对大量车辆申请通信的环境身份认证和密钥协商的效率上，PEKE协议具有显著优势。

表5　各方案单次认证和密钥协商通信成本对比

协议	总通信开销/bit
文献[6]	2 080
文献[8]	2 176
文献[13]	2 552
PEKE	2 144

4.3　多次认证和密钥协商资源开销

PEKE协议采用了基于Kerberos协议的认证方法，车辆在与多个服务器认证时只需要向AS发送一次假名和TGT服务请求，获得TGT后，在TGT的生命周期内，只需要多次向TGS发送对应的SGT匿名请求，TGS对车辆完成认证后返回对应的SGT，这样车辆即可与多个应用服务器完成认证并建立会话密钥。由于PEKE协议的车辆向AS请求假名和TGT会消耗大量计算和通信资源，而与多个服务器建立会话密钥时只需要车辆向AS发送一次假名和TGT请求，因此，PEKE协议在车辆与多个应用服务器匿名身份认证和建立会话密钥过程中，在计算开销和通信开销上展现出更佳的性能。多次身份认证密钥协商计算开销对比如图8所示，多次身份认证密钥协商通信开销对比如图9所示。

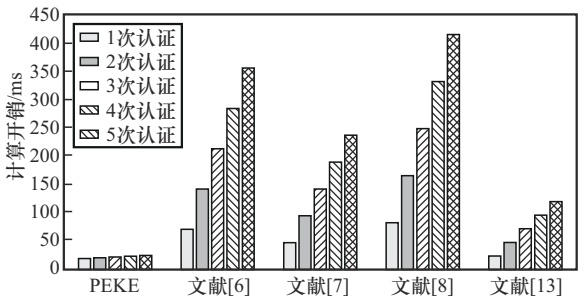


图8　多次身份认证密钥协商计算开销对比

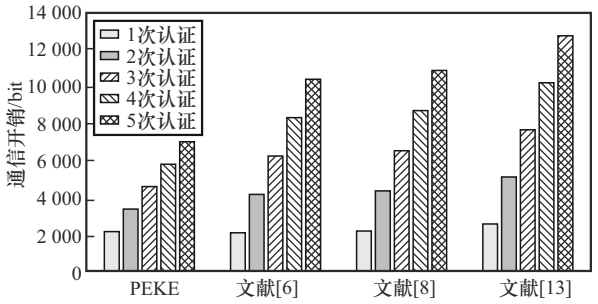


图9　多次身份认证密钥协商通信开销对比

4.4　仿真实验

为了测试PEKE协议在真实环境下的表现，本文在Window 11系统上使用OMNeT++、Veins和SUMO工具搭建车联网仿真平台。该仿真平台可以模拟真实道路环境中的车辆通信和移动行为，以评估PEKE协议在车联网环境中的性能。在该仿真平台上，本文选取了江宁大学城的一部分（5 km×5 km）道路地图进行仿真，使用IEEE 802.11p无线标准进行通信。车辆以20 m/s的车速通过该仿真道路，并通过模拟来部署PEKE协议，模拟过程包含车辆与KGC（该中心包含一个AS、一个TGS），以及车辆与应用服务器App之间的安全认证和密钥交换过程。随后，本文收集并分析实验数据，计算得到PEKE协议的平均消息时延，并将其与其他车联网身份认证协议进行对比，评估PEKE协议在真实场景下的表现。平均消息时延对比如图10所示。

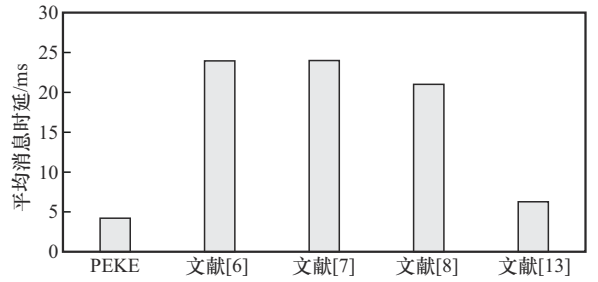


图10　平均消息时延对比

由仿真实验结果可知，PEKE协议展现出了优越的性能特点。在平均消息时延方面，PEKE协议的表现不仅明显优于文献[6-8]中基于椭圆曲线公钥加密的方案，而且与采用PUF运算的文献[13]相比，也具有显著优势。PEKE协议通过简化消息交互和中间步骤，并充分利用了Kerberos协议的轻量级特性，从而显著降低了通信时延，使得网络能够更快速地响应请求。

对计算开销、通信开销以及仿真实验结果的综合分析可以看出，PEKE协议在低空经济环境中展现出广泛的应用潜力，特别是在车联网、智能交通以及工业物联网等高度动态且资源受限的场景下，PEKE协议凭借其低时延和高效能特性，能够满足低空经济中对地面交通快速响应、实时数据处理和高效协同的需求。

5　结束语

本文针对车辆与云端应用服务器通信场景，提出基于PUF-ECC-Kerberos的车云匿名身份认证协议PEKE。该方案结合ECC算法与PUF，对传统Kerberos协议进行改进，实现了车辆通过可信第三方密钥生成中心与云端应用服务器之间的匿名身份认证和密钥交换。经过安全性和性能分析证明，该方案能够有效抵御密钥泄露、伪装攻击、中间人攻击以及反射攻击等多种安全威胁，并在保证安全性的前提下有效降低资源消耗。最后，本文通过仿真实验，验证了该协议在车联网环境下具备较好的性能表现，能够支持低空经济中动态的空地一体化交通系统的高效通信。未来，研究将进一步聚焦于车辆批量认证、密钥更新机制等方向，提升协议在大规模低空经济应用中的适应性与可扩展性。

参考文献：

[1] 翟苗, 拱长青, 刁俊胜, 等. 基于PKI的车联网安全通信与隐私保护机制[J]. 沈阳航空航天大学学报, 2012, 29(5): 59-63.
ZHAI M, GONG C Q, DIAO J S, et al. The PKI-based privacy protection mechanism for vehicle communication safety[J]. Journal of Shenyang Aerospace University, 2012, 29(5): 59-63.

[2] DANG L J, XU J, CAO X F, et al. Efficient identity-based au-

thenticated key agreement protocol with provable security for vehicular ad hoc networks[J]. International Journal of Distributed Sensor Networks, 2018, 14(4): 155014771877254.

[3] DENG L Z, SHAO J X, HU Z Y. Identity based two-party authenticated key agreement scheme for vehicular ad hoc networks[J]. Peer-to-Peer Networking and Applications, 2021, 14(4): 2236-2247.

[4] 刘健, 李艳俊, 郑继虎, 等. 可溯源车联网匿名签名和批量验证方案设计[J]. 计算机工程与应用, 2024, 60(23): 268-274.
LIU J, LI Y J, ZHENG J H, et al. The anonymous signature and batch verification scheme design of traceable Internet of vehicles[J]. Computer Engineering and Applications, 2024, 60(23): 268-274.

[5] 毕昌兵, 田有亮. 车联网中基于身份签名的匿名可追溯消息认证方案[J]. 计算机工程, 2024: 1-8.
BI C B, TIAN Y L. An anonymous traceable message authentication scheme based on identity signature in car networking[J]. China Industrial Economics, 2024: 1-8.

[6] 谢永, 吴黎兵, 张宇波, 等. 面向车联网的多服务器架构的匿名双向认证与密钥协商协议[J]. 计算机研究与发展, 2016, 53(10): 2323-2333.
XIE Y, WU L B, ZHANG Y B, et al. Anonymous mutual authentication and key agreement protocol in multi-server architecture for VANETs[J]. Journal of Computer Research and Development, 2016, 53(10): 2323-2333.

[7] 刘辉, 仲红, 许艳, 等. 车联网云环境下多服务器架构的匿名认证及密钥协商协议[J]. 南京信息工程大学学报(自然科学版), 2017, 9(5): 503-508.
LIU H, ZHONG H, XU Y, et al. Anonymous authentication and key agreement protocol in multi-server architecture for vehicular cloud computing[J]. Journal of Nanjing University of Information Science & Technology (Natural Science Edition), 2017, 9(5): 503-508.

[8] YADAV K A, 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): 473-489.

[9] 刘一丹, 马永柳, 杜宜宾, 等. 一种车联网中的无证书匿名认证密钥协商协议[J]. 信息网络安全, 2024, 24(7): 983-992.
LIU Y D, MA Y L, DU Y B, et al. A certificateless anonymous authentication key agreement protocol for VANET[J]. Netinfo Security, 2024, 24(7): 983-992.

[10] 杨小东, 李沐紫, 马国祖, 等. 车联网中支持非法签名定位的无证书匿名认证方案[J]. 计算机工程, 2024, 50(6): 157-165.
YANG X D, LI M Z, MA G Z, et al. Certificateless anonymous authentication scheme supporting illegal signatures localization for Internet of vehicles[J]. Computer Engineering, 2024, 50(6): 157-165.

[11] AL-SHAREEDA M A, ANBAR M, MANICKAM S, et al. An efficient identity-based conditional privacy-preserving authentication scheme for secure communication in a vehicular ad hoc network[J]. Symmetry, 2020, 12(10): 1687.

[12] RAI V K, TRIPATHY S, MATHEW J. LPA: a lightweight PUF-based authentication protocol for IoT system[C]//Proceedings of the 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). Piscataway: IEEE Press, 2023: 1712-1717.

[13] 侯琬钰, 孙钰, 李大伟, 等. 基于PUF的5G车联网V2V匿名认证与密钥协商协议[J]. 计算机研究与发展, 2021, 58(10): 2265-2277.
HOU W Y, SUN Y, LI D W, et al. Anonymous authentication and key agreement protocol for 5G-V2V based on PUF[J]. Journal of Computer Research and Development, 2021, 58(10): 2265-2277.

[14] 夏卓群, 苏潮, 徐梓桑, 等. 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[J]. 电子与信息学报, 2024, 46(9): 3788-3796.
XIA Z Q, SU C, XU Z S, et al. A lightweight and provably secure authentication protocol for Internet of vehicles using physical unclonable function[J]. Journal of Electronics & Information Technology, 2024, 46(9): 3788-3796.

[15] AWAIS S M, WU Y C, MAHMOOD K, et al. PUF-based privacy-preserving simultaneous authentication among multiple vehicles in VANET[J]. IEEE Transactions on Vehicular Technology, 2024, 73(5): 6727-6739.

[16] LAI C Z, WANG X W, ZHENG D. A PUF-based authentication and key distribution scheme for in-vehicle network[C]//Proceedings of the ICC 2023-IEEE International Conference on Communications. Piscataway: IEEE Press, 2023: 1591-1596.

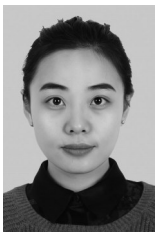
[17] NEUMAN B C, TS'O T. Kerberos: an authentication service for computer networks[J]. IEEE Communications Magazine, 1994, 32(9): 33-38.

[18] RAHAYU M, HOSSAIN M B, ALI M A, et al. An integrated secured vehicular ad-hoc network leveraging Kerberos authentication and Blockchain technology[C]//Proceedings of the 2023 Eleventh International Symposium on Computing and Networking Workshops (CANDARW). Piscataway: IEEE Press, 2023: 260-266.

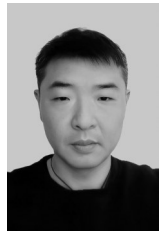
[19] 王冠, 苗艺雪. 基于Intel SGX的Kerberos安全增强方案[J]. 信息安全研究, 2021, 7(4): 374-383.
WANG G, MIAO Y X. Kerberos security enhancements based on Intel SGX[J]. Journal of Information Security Research, 2021, 7(4): 374-383.

[20] GOPE P. PMAKE: Privacy-aware multi-factor authenticated key establishment scheme for Advance Metering Infrastructure in smart grid[J]. Computer Communications, 2020(152): 338-344.

[作者简介]



柳亚男（1984– ），女，博士，金陵科技学院网络安全学院副教授，主要研究方向为车联网安全、密码协议。

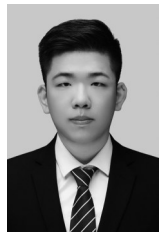


李戈（1982– ），男，博士，中国人民解放军陆军工程大学指挥控制工程学院讲师，主要研究方向为软件安全、网络攻防。

曹磊（2001– ），男，金陵科技学院网络安全学院硕士生，主要研究方向为车联网安全、软件安全。

邱硕（1989– ），女，博士，金陵科技学院网络安全学院副教授，主要研究方向为密码协议、大数据安全。

张正（1973– ），男，金陵科技学院网络安全学院研究员，主要研究方向为通信安全、网络攻防技术。



王苏豪（2000– ），男，金陵科技学院网络安全学院硕士生，主要研究方向为人工智能安全、入侵检测。