·车联网量子加密通信技术专题·

# 基于扩展量子密钥分发的车联网增强身份认证方案*

石琴[1] 李想[1] 程腾[1] 王川宿[2] 王文祥[2]

（1.合肥工业大学，自动驾驶汽车安全技术安徽省重点实验室 安徽省智慧交通车路协同工程研究中心，合肥 230009；2.奇瑞汽车股份有限公司，芜湖 241006）

【摘要】为实现车联网场景下的身份认证和密钥分发，提出一种基于扩展量子密钥分发的车联网增强身份认证方案。该方案的特征为：（1）在无线通信中通过量子安全模块和预置量子密钥完成量子密钥移动分发，在有线通信中通过量子密钥分发设备完成量子密钥的在线协商，实现了扩展的量子密钥分发；（2）基于后量子密码学的加密和签名算法进行基础身份认证，并通过预置的量子密钥实现增强认证。最后，通过安全性分析和性能测试，证实了本方案具有足够的安全性和较低的计算开销，总计算开销为1.689 ms，性能提升为60.43%~70.72%。

**主题词：车联网 量子保密通信 身份认证 量子密钥分发**

**中图分类号：**U495；TP309 **文献标识码：**A **DOI:** 10.19620/j.cnki.1000-3703.20230671

# Enhanced Identity Authentication Scheme for Internet of Vehicles Based on Extended Quantum Key Distribution

Shi Qin[1], Li Xiang[1], Cheng Teng[1], Wang Chuansu[2], Wang Wenxiang[2]

（1. Anhui Provincial Key Laboratory of Autonomous Vehicle Safety Technology, Anhui Provincial Intelligent Transportation Vehicle-Road Collaborative Engineering Research Center, Hefei University of Technology, Hefei 230009; 2. Chery Automobile Co., Ltd., Wuhu 241006）

**【Abstract】**In order to realize identity authentication and key distribution in Internet of Vehicle (IOV) scenario, this paper proposed an enhanced identity authentication scheme for the IOVs based on extended quantum key distribution. The features of this scheme are: (1) Quantum key mobile distribution was completed through quantum security module and preset quantum key in wireless communication, online negotiation of quantum key was completed through Quantum Key Distribution (QKD) equipment in wired communication, to achieve extended quantum key distribution; (2) Basic identity authentication based on post-quantum cryptography encryption and signature algorithms was conducted, and enhanced authentication through preset quantum keys. Finally, through security analysis and performance testing, it is confirmed that this scheme has sufficient security and low computational overhead. The total computational overhead is 1.689 ms, and the performance improvement is 60.43%~70.72%.

**Key words: Internet of Vehicles, Quantum secure communication, Identity authentication, Quantum key distribution**

**【引用格式】**石琴, 李想, 程腾, 等. 基于扩展量子密钥分发的车联网增强身份认证方案[J]. 汽车技术, 2023(10): 16-23.

SHI Q, LI X, CHENG T, et al. Enhanced Identity Authentication Scheme for Internet of Vehicles Based on Extended Quantum Key Distribution[J]. Automobile Technology, 2023(10): 16-23.

## 1 前言

伴随着智能网联汽车渗透率的逐渐提高，其涉及到的信息数据交换的场景也日益增多[1]，这些数据涉及到车主的敏感隐私数据[2]。黑客能够利用车联网平台的漏洞，非法获取这些数据，从而威胁用户的生命安全、财产安全以及隐私安全[3]。因此，有条件的身份认证和密钥协商机制被认为是保障车联网安全通信的有效措施[4]。

当前的车联网身份认证方案大多基于经典公钥密码算法[5]，如RSA、ECC、Diffie-Hellman，这些方法的安全

*基金项目：国家自然科学基金项目（82171012）；安徽省自然科学基金资助项目（2208085MF171）；中央高校基本科研业务费专项资金资助项目（JZ2023YQTD0073）；汽车标准化公益性开放课题资助项目（CATARC-Z-2022-01350）。

通讯作者：程腾（1983一），男，硕士研究生导师，副教授，主要研究方向为智能网联汽车信息安全，cht616@hfut.edu.cn。

性是建立在整数分解和离散对数这一系列数学问题上的。然而，这些传统密码算法已被证明可以被量子计算机破解[6]。因此，能够抵抗量子攻击的身份认证方案受到了研究者的关注，现有方案大多采用基于格的加密和签名算法[7-9]，依赖后量子密码（Post-Quantum Cryptography，PQC）算法的长期安全性，若PQC算法被破解，隐私数据将面临泄露的风险。

量子保密通信是保障未来通信安全的重要技术手段[10]。其中，量子密钥分发（Quantum Key Distribution，QKD）作为最先实用化的量子技术，是目前唯一被严格证明的无条件安全的密钥分发方式[11]。将QKD应用于车联网的实际场景中，可以极大地确保数据的前向安全性。

综合考虑车联网场景下的量子密钥分发方式和身份认证的安全性，本文提出了一种基于扩展量子密钥分发的车联网增强身份认证方案。该方案包括：

a. 提出适用于车联网的扩展量子密钥分发方法。在无线网络中，通过集成量子安全模块的车载通信终端与量子安全云服务器（Quantum Security Cloud Server，QSC）进行量子密钥协商；在有线网络中，通过布置在QSC与车辆云服务提供商（Vehicle Cloud Service Provider，VSP）的量子密钥分发设备，完成量子密钥的安全分发。

b. 提出适用于后量子时代的车联网身份认证方案。方案基于PQC的加密和签名算法进行初次身份认证，通过身份认证量子密钥进行增强认证，验证硬件的合法性。方案结合QKD与PQC算法完成车辆和VSP之间的身份认证和密钥协商，只需要PQC算法具有短时安全性。最后对方案进行安全分析和性能对比，以证明提出方案的安全性和适用性。

## 2 安全通信系统架构

针对车联网的车云通信场景，本文提出了如图1所示的系统架构。该系统架构包括QSC、VSP、QKD设备、智能网联汽车以及基础设施。

a. 量子安全云服务器（QSC）：QSC作为可信赖的量子安全中心，为系统中的所有用户和云服务提供商提供注册服务。QSC和VSP中集成的量子密钥分发设备可以相互进行身份认证，组成QKD网络。QSC通过对预置量子密钥的管理，在车云间形成扩展的QKD网络，实现量子密钥的无线分发。

b. 车辆云服务提供商（VSP）：VSP能够为车辆提供各种网络服务，例如智能交通服务、道路信息服务、智能停车服务等。VSP在与QSC身份认证成功后，能够为车辆提供所需要的云服务。VSP也部署有QKD设备，能够与QSC进行会话密钥的协商。

c. 量子密钥分发（QKD）设备：QKD设备成对部署，采用BB84协议通过经典信道和量子信道协商量子密钥。

d. 智能网联汽车：安装有车载通信终端（Telematics BOX，T-BOX）、车载单元（On Board Unit，OBU），具备联网和通信功能的智能车辆。车载通信终端集成了防篡改的量子安全模块（Quantum Security Entity，QSE），其可以安全存储预置的量子密钥，并在预置量子密钥的保护下，与QSC进行会话密钥的协商，实现量子密钥在扩展型QKD网络下的分发。

e. 基础设施：安装在道路两侧，具有快速传输速度的设备。其仅作为数据传输的中间介质，不具备计算能力，支持车辆通信的全域覆盖。

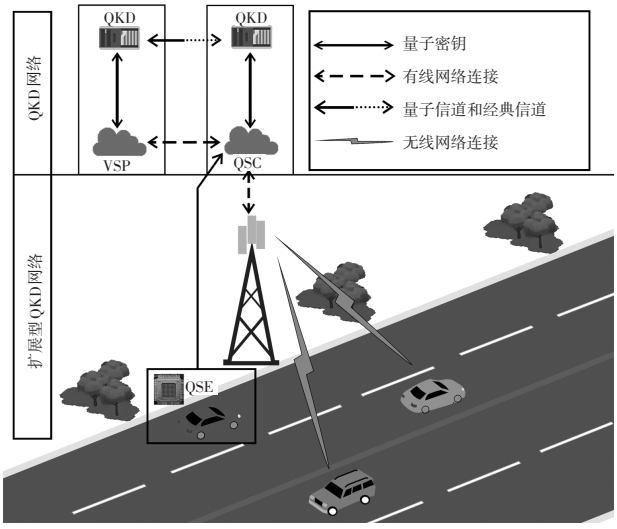


图1 系统通信架构

## 3 方案流程设计

本研究方案包括系统初始化、注册、身份认证和量子密钥协商4个流程。表1为方案设计所需使用的符号及对应定义。总体流程如图2所示。

### 3.1 系统初始化

QSC生成公私钥对$pk_Q$和$sk_Q$，并选择两个无碰撞的单向哈希函数$h$和$h_1$，然后QSC将所选择的系统参数$pk_Q$、$h$、$h_1$，选择对称加密算法（Advanced Encryption Standard，AES）进行公开。车辆生成签名公私钥对$pk_V$和$sk_V$，VSP生成签名公私钥对$pk_S$和$sk_S$，车辆和VSP向QSC公开签名公钥。

### 3.2 注册

注册阶段是由车辆、QSC和VSP通过安全通道执行的交互式协议。QSC负责管理车辆和VSP的身份信息。车辆的车载通信终端集成了已经充注了预置密钥

的量子安全模块，预置密钥的信息在QSC中也有记录存储。另外，VSP的可信存储空间存储有购买云服务的车辆的$VID_i$。

**表1　方案所需符号及相应定义**

| 符号 | 定义 |
|---|---|
| $SID$ | VSP的唯一标识 |
| $VID_i$ | 车辆的唯一标识 |
| $ID_{Ui}$,$PW_{Ui}$ | 用户的账号和密码 |
| $PEK_i$ | 存储在QSE中的认证量子密钥 |
| $QK_i$ | 用以生成$SK_i$的量子密钥 |
| $Ktag_i$ | 量子密钥的密钥标识 |
| $SK_i$ | 车和QSC的会话密钥 |
| $SK_j$ | QSC和VSP的会话密钥 |
| $sk_i$ | （车辆/QSC/VSP）私钥 |
| $En_{pk}()$,$De_{sk}()$ | 基于格的加密/解密算法 |
| $Sign(M,sk_i)$, | 使用$sk_i$对任意消息$M$进行签名 |
| $Verify(T_s,M,pk_i)$, | 使用$pk_i$检验签名值 |
| $h$,$h_1$ | 两个无冲突的单向哈希函数 |
| $A_i$,$B_i$,$Q_i$ | 认证参数 |
| $S_i$,$M_i$,$W_i$,$X_i$ | 哈希值 |
| $m_i$ | 认证消息 |

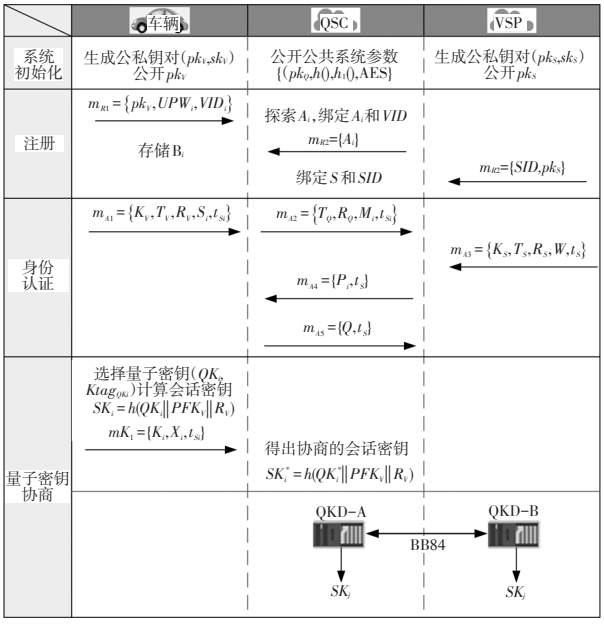


图2　方案整体流程

首先进行车辆注册，车辆用户需要加入车联网云服务网络，获得云服务功能。因此用户和车辆需要执行以下步骤提前向QSC注册：

a. 车辆用户设置登录账号$ID_{Ui}$和密码$PW_{Ui}$，并计算$UPW_i=h_1(ID_{Ui}\|PW_{Ui})$。通过安全通道，发送注册信息$m_{R1}=\{pk_V,UPW_i,VID_i\}$到QSC。

b. QSC接收到消息$m_{R1}$后，计算$A_i=h(UPW_i)\oplus VID_i$，将$A_i$在数据库的现有身份信息中进行检索。若检索成功，则拒绝注册请求。反之，将$UPW_i$和$VID_i$进行绑定，并在数据库中记录$\{A_i,pk_V\}$，向对应车辆发送注册反馈信息$m_{R2}=\{A_i\}$。

c. 车辆接收到$m_{R2}$之后，计算用户登录的验证参数$B_i=h(A_i\|VID_i)$，并存储到车载终端。

其次进行VSP注册，VSP需要提前在QSC进行注册，注册步骤为：

a. VSP提供唯一的身份标识$SID$，通过安全通道将注册消息$m_{R3}=\{SID,pk_S\}$发送到QSC。

b. QSC接收到$m_{R3}$后，将$S=h_1(SID)$和$SID$进行绑定，并在数据库中记录$\{S,pk_S\}$。

c. VSP将$S$安全存储。

### 3.3　身份认证

在车辆获得VSP提供的云服务之前，需要向QSC进行身份认证。QSC不仅校验车辆身份的合法性，还帮助车辆对VSP进行身份认证。车辆和VSP均需要通过向QSC的增强身份认证，以保证它们的身份和硬件的双重合法性，才能够进行后续会话密钥的协商。身份认证的具体流程如图3所示。


图3　身份认证具体流程

注册阶段完成后，车辆需验证用户身份的合法性。用户在车机端输入账号$ID_{Ui}$和密码$PW_{Ui}$。车辆终端收

到账号密码之后，计算 $B_i^*=h(A_i\|VID_i)$，并检查等式 $B_i^*=B_i$ 是否成立，若成立，则表明用户是合法的。

其次，车辆向QSC进行身份认证。为了抵御重放攻击，车辆选择量子随机数 $R_V$，然后从QSE中提取认证密钥 $PFK_V$ 及其对应的密钥标识 $Ktag_V$，并计算 $u_i=h(VID_i)\oplus PFK_V$。然后，使用QSC的公钥对密钥信息进行加密，获得 $K_V=En_{pk_Q}(u_i\|Ktag_V)$，并生成消息摘要 $D_V=h(K_V)$。接着，车辆使用私钥 $sk_V$ 对消息摘要进行签名，生成签名值 $T_V=\mathrm{Sign}(D_V\|R_V,sk_V)$。最后，计算哈希值 $S_i=h(K_V\|T_V\|t_{Si})$ 用于完整性校验。车端将认证请求消息 $m_{A1}=\{K_V,T_V,R_V,S_i,t_{Si}\}$ 发送给QSC。

最后，QSC收到 $m_{A1}$ 后，首先通过校验 $t_{Ri}-t_{Si}<\Delta t$，$S_i=h(K_V^*\|T_V^*\|t_{Si})$ 来确保消息的完整性和有效性。再通过 $Verify(T_V^*,D_V\|R_V,pk_V)$ 验证车辆的消息签名，完成车辆的第一次身份认证。

另外，QSC使用私钥 $sk_Q$ 对接收到的加密信息 $K_V^*$ 进行解密 $De_{sk_Q}(K_V^*)=(u_i^*\|Ktag_V^*)$，获得 $Ktag_V^*$ 后从数据库中提取认证量子密钥 $PEK_V^*$。随后，QSC在本地进行计算 $VID_i=A_i\oplus h(UPW_i)$，得到认证量子密钥 $PFK_V=h(VID_i)\oplus u_i^*$，通过比较认证量子密钥 $PFK_V^*$ 和 $PFK_V$ 是否一致，完成车辆的第二次身份认证。由于认证量子密钥是存储在车载通信终端的量子安全模块中，认证方案可以保证车辆硬件的合法性。

两次认证确认车辆合法后，QSC选择量子随机数 $R_Q$，计算消息摘要 $D_Q=h_1(VID_i)$ 和签名值 $T_Q=\mathrm{Sign}(D_Q\|R_Q,sk_Q)$，用于VSP的身份认证。最后QSC生成完整性校验码 $M=h(T_Q\|R_Q\|t_S)$，并将认证请求消息 $m_{A2}=\{T_Q,R_Q,M,t_S\}$ 发送给VSP。

VSP收到 $m_{A2}$ 后，首先通过校验 $t_R-t_S<\Delta t$、$M=h(T_Q^*\|R_Q^*\|t_S)$ 来确保消息的完整性和有效性。再通过 $Verify(T_Q^*,D_Q\|R_Q,pk_Q)$ 验证QSC的消息签名。VSP将 $D_Q$ 与存储空间中 $VID$ 的哈希值做匹配，若成功，则表示车辆具有VSP服务。

然后VSP从QSE中提取认证密钥 $PFK_S$ 及其对应的密钥标识 $Ktag_S$，并使用公钥 $pk_Q$ 对密钥信息进行加密，得到 $K_S=En_{pk_Q}(S\|PFK_S\|Ktag_S)$，并生成消息摘要 $D_S$。接着选择量子随机数 $R_S$，使用VSP的私钥 $sk_S$ 签名 $T_S=\mathrm{Sign}(D_S\|R_S,sk_S)$。最后产生完整性校验码 $W=h(K_S\|T_S\|R_S\|t_S)$，并将认证请求消息 $m_{A3}=\{K_S,T_S,R_S,W,t_S\}$ 发送给QSC。

QSC收到 $m_{A3}$ 之后，首先通过校验 $t_R-t_S<\Delta t$，$M=h(K_S^*\|T_S^*\|R_S^*\|t_S)$ 来确保消息的完整性和有效性。再通过 $Verify(T_S^*,D_S\|R_S,pk_S)$ 验证VSP的消息签名。并使用私钥 $sk_O$ 对 $K_S^*$ 进行解密 $De_{sk_O}(K_S^*)=(S^*\|PFK_S^*\|Ktag_S^*)$，通过检索 $S^*$ 是否在数据库中，完成VSP的第一次身份认证。

然后QSC由 $Ktag_S^*$ 提取量子密钥 $PFK_S^{**}$，并与解密消息中的 $PFK_S^*$ 进行比较，完成VSP的第二次身份认证。

最后，通过计算等式 $P_i=h(PFK_V^*\|VID_i\|t_{Si})$ 和 $Q=h(PFK_S^*\|S\|t_S)$，并发送消息 $m_{A4}=\{P_i,t_{Si}\}$ 到对应车辆，发送消息 $m_{A5}=\{Q,t_S\}$ 到VSP。

车辆收到 $m_{A4}$ 后，校验 $t_{Ri}-t_{Si}<\Delta t$ 和 $P_i=h(PFK_V\|VID_i\|t_{Si})$，成功则车辆认证完成。VSP收到 $m_{A5}$ 后，校验 $t_R-t_S<\Delta t$ 和 $Q=h(PFK_S\|S\|t_S)$，成功则VSP认证完成。

### 3.4 量子密钥协商

如图2所示，在量子密钥协商阶段，有两种密钥分发方式。第一种：QSC和VSP之间通过QKD网络有线连接完成量子密钥的分发，依赖的是量子密钥分发协议。第二种：在QSE中预置量子密钥，在车辆和QSC之间实现扩展的量子密钥分发。具体的密钥分发流程如下：

a. 车辆从量子安全模块中提取量子密钥 $QK_i$ 及其对应密钥标识 $Ktag_{QK_i}$，计算会话密钥 $SK_i=h(QK_i\|PFK_V\|R_V)$ 并保存。随后，计算 $K_i=h(Ktag_V\|t_{Si})\oplus Ktag_{QK_i}$，生成消息完整性验证码 $X_i=h(K_i\|t_{Si})$，并将请求同步会话密钥消息 $m_{K1}=\{K_i,X_i,t_{Si}\}$ 发送给QSC。

b. QSC收到消息 $m_{K1}$ 后，首先通过校验 $t_{Ri}-t_{Si}<\Delta t$，$X_i^*=X_i$ 来确保消息的完整性和有效性。然后通过计算 $K_i\oplus h(Ktag_V\|t_{Si})$ 求得量子密钥标识 $Ktag_{QK_i}^*$，依照对应关系获得量子密钥 $Q_i^*$，计算出会话密钥 $SK_i^*=h\left(QK_i^*\|PFK_V\|R_V\right)$ 并保存，量子密钥协商完成。

## 4 安全性证明

### 4.1 安全模型

参考其他研究者提出的认证协议[12-13]后，本研究使用真实或随机模型（Real or Random，ROR），假设方案中身份认证和密钥协商协议有用户、QSC和VSP三种实体。这些实体中包含的多个实例之间能够同时进行身份认证。每一个实例都能够看作一个独立的预言机。预言机存在三种状态，分别为："Accept"表示预言机接收到正确的信息；"Reject"表示预言机接收到错误信息；"⊥"表示预言机输出为空。设定 $U_i^a$ 是车辆的第 $a$ 个实例，$QSC_i^b$ 为QSC的第 $b$ 个实例，$VSP_i^c$ 为VSP的第 $c$ 个

实例。身份认证协议的安全性是在多项式时间攻击者A和挑战者C之间的“查询-响应游戏”证明的。

定义1（对手能力）：攻击者A可以执行以下查询来攻击认证方案，并获取挑战者的查询结果。

$h_i(m_i)$：当攻击者A通过$m_i$问询此预言机时，挑战者C在列表$L_{hi}$中生成一个随机数$r_i$，并将$(m_i, r_i)$储存在列表中。然后，挑战者C返回$r_i(i=1,2)$到攻击者。

Execute($U_i^a$, $QSC_i^b$, $VSP_i^c$)：监听模式。攻击者A能够访问可信实例间的认证过程。Oracles在接收到此查询时，根据认证和密钥协商协议，返回$U_i^a$、$QSC_i^b$与$VSP_i^c$之间的交互消息{$m_{A1}$, $m_{A2}$, $m_{A3}$, $m_{A4}$, $m_{A5}$, $m_{K1}$}。

Send($U_i^a$ / $QSC_i^b$ / $VSP_i^c$, $m_i$)：主动攻击，模拟攻击者A向$U_i^a$, $QSC_i^b$或$VSP_i^c$发送认证消息$m$。当消息$m$有效时，预言机会接受$m$，并根据认证和密钥协商方案将响应消息发送给攻击者A。否则返回拒绝响应。

Reveal($U_i^a$, $QSC_i^b$)：通过执行该查询，挑战者C会将相关的会话密钥$SK_i$ / $SK_j$发送给攻击者A。

Corrupt($U_i^a$, $VSP_i^c$)：通过执行该查询，攻击者A可以获得存储在$U_i^a$和$VSP_i^c$安全存储空间中的所有秘密参数。

Test($V_i^a$)：该查询会对会话密钥的语义安全性进行模拟。在游戏开始前，将硬币翻转，并且只有攻击者A知道硬币的值。这个值决定了此预言机的输出。若A执行此查询并建立了新鲜的会话密钥$SK_i$，当$b$=1时，挑战者C返回正确的会话密钥$SK_i$到A；否则当$b$=0时，C向A返回与$SK_i$长度相同的随机字符串。

定义2（语义安全）：攻击者A在执行完上述查询后，输出其在Test预言机中猜测的数值$b$。如果攻击者在没有执行过Reveal的前提下，猜测的数值是正确的，则认为攻击者成功破坏了认证和密钥协商方案(Authentication and Key Agreement, AKA)的语义安全性。其中A的优势如下：

$$Adv_{\Gamma}^{AKA}(A)=\left|2\Pr[b'=b]-1\right| \tag{1}$$

### 4.2 安全证明

在证明所提出的车联网增强身份认证方案在上述安全模型下能够满足AKA安全的前提下，定义$\Gamma$为所提出的方案。若攻击者A能够伪造正确的登录和认证信息，则认为攻击者A破坏了$\Gamma$。

定理1：如果攻击者A违反认证协议的优势在任何多项式时间内都可以被忽略，就称$\Gamma$是AKA安全的得到。$q_s$, $q_e$, $q_d$, $q_h$和$q_{h1}$分别表示发送查询、执行查询、加密/解密查询、$h$和$h_1$查询的次数。|$P$|、|$C$|和|$R$|分别表示用户密码、密文、随机数范围空间的长度。A在破解方案$\Gamma$的会话密钥安全性方面的优势可以估计为：

$$Adv_{\Gamma}^{A}\le\frac{q_h^2+q_{h1}^2+2q_S}{2^L}+\frac{(q_S+q_e)^2}{|R|}+\frac{q_d^2}{|C|}+\frac{q_S}{2^{L_n}|P|}+2q_S adv_{\Gamma}^{A,LWE}(t) \tag{2}$$

式中，$L$为哈希值长度；$L_n$为用户身份长度。

证明：构建如下游戏来证明攻击者A破解该方案的优势从游戏开始到游戏结束都可以被忽略，从而证明定理1。具体证明过程如下：

游戏0：在ROR模型中，A对$\Gamma$执行的实际攻击，成功的概率与攻破本方案协议的概率相同。由定义2可得：

$$Adv_{\Gamma}^{A}(t)=\left|2Adv_{\Gamma}^{A,Gm_1}-1\right| \tag{3}$$

游戏1：此游戏模拟了由哈希列表$L_{C-A}$维护的哈希预言机$h$和$h_1$。当A使用消息$m$执行查询时，C首先检查哈希列表，若对应的元组$(M, h(M))$值已存在，则返回该值。否则产生一个随机数并将值添加到哈希列表，同时将该值发送给A。对攻击者来说，游戏0和游戏1是无法区分的，由此得到：

$$Adv_{\Gamma}^{A,Gm_2}=Adv_{\Gamma}^{A,Gm_1} \tag{4}$$

游戏2：模拟游戏1中所有的预言机。如果发生以下碰撞事件，则游戏终止。基于生日悖论可以得到：

事件1：认证协议中使用的两个哈希函数$h$和$h_1$发生碰撞的最大概率是$\frac{q_h^2+q_{h1}^2}{2^{L+1}}$。

事件2：认证和密钥协商协议中发送的消息中的随机数$R_V$、$R_U$和$R_S$发生碰撞的概率是$\frac{(q_s+q_e)^2}{2|R|}$。

事件3：认证协议中使用签名和非对称加密发生碰撞的最大概率是$\frac{(q_d)^2}{2|C|}$。

如果上述事件发生，则$Adv_{\Gamma}^{A,Gm_3}=Adv_{\Gamma}^{A,Gm_2}$，A赢得挑战。由于游戏2和游戏1是不可区分的，因此根据差分引理得到：

$$\left|Adv_{\Gamma}^{A,Gm_2}-Adv_{\Gamma}^{A,Gm_1}\right|\le\frac{q_h^2+q_{h1}^2}{2^{L+1}}+\frac{(q_s+q_e)^2}{2|R|}+\frac{(q_d)^2}{2|C|} \tag{5}$$

游戏3：模拟了游戏2中所有的预言机。游戏中还假设，如果发生A可以不通过相应的哈希预言机查询，只通过Send查询就能够正确伪造身份认证流程中的关键参数$M$、Q、$W$、$P_i$、$S_i$、$X_i$的情况，则游戏3终止。除非车辆否认$S_i$，VSP否认$W$或者QSC否认$M$和$X_i$。因此得到：

$$\left|Adv_{\Gamma}^{A,Gm_3}-Adv_{\Gamma}^{A,Gm_4}\right|\le\frac{q_s^2}{2^L} \tag{6}$$

游戏4：修改发送查询。C随机选择一个匹配的实例($U_i^a$, $QSC_i^b$, $VSP_i^c$)，并按照图3的流程答复A的Send查询。设定一个用来解决基于格的签名和加密算法的

方案，并假定A可以在多项式时间内解决基于理想格问题的难题[14]，攻击者A的优势为：

$$\left|Adv_{\Gamma}^{A,Gm_4}-Adv_{\Gamma}^{A,Gm_5}\right|\leqslant q_s Adv_{\Gamma}^{A,LWE}(t) \tag{7}$$

在执行完Send查询后，A获得身份认证和密钥协商阶段的交互信息。随后，A将进行$q_S$次Corrupt($U_i^a$，$VSP_i^c$)询问，若能够成功区别$SK_i=h(QK_i\|S\|u_i)$和随机数，那么C结束游戏。此时认为A已经成功通过了身份认证和密钥协商协议，获得游戏的胜利。该结果需以下列事件发生为前提：

事件4：A想要成功模拟车辆用户并伪造消息$m_{A1}=\{K_V,T_V,R_V,S_i,t_{Si}\}$，其必须正确计算$S_i$、$R_V$和$(ID_{ui},PW_{Ui})$。A通过Corrupt($U_i^a$)获得车辆存储的秘密参数$(B_i,VID,PFK_V)$。若A想要从$B_i$正确猜测出用户($ID_{Ui}$,$PW_{Ui}$)组合，需要执行$q_S$次Corrupt($U_i^a$)，正确输出$m_{A1}$的概率为：

$$\frac{q_S}{2^{L_u}|P|} \tag{8}$$

事件5：A想要成功模拟VSP并伪造消息$m_{A3}=\{K_S,T_S,R_S,W,t_S\}$，那么必须正确计算$W$，通过Corrupt($VSP_i^c$)获得VSP存储的秘密参数$(Q,PFK_S,S)$。若A想要正确猜测出$W$和$R_S$的组合，需要执行$q_S$次Corrupt($VSP_i^c$)，正确输出$m_{A3}$的概率为：

$$\frac{q_S}{2^{L}|P|} \tag{9}$$

事件6：A身份认证成功后，想要模拟QSC并伪造密钥协商消息$m_{K1}=\{K_i,X_i,t_{Si}\}$，那么其必须获得$K_i$和$X_i$，正确输出$m_{K1}$的概率为：

$$\frac{q_S}{2^{L+K}} \tag{10}$$

事件7：A想要获取正确的会话密钥$SK_i=h(QK_i\|PFK_V\|R_V)$，在$h$预言机的帮助下，正确获得的概率为：

$$\frac{qh^2}{2^{L+1}} \tag{11}$$

因此，得到通过游戏5的可能性为：

$$P_r[Suc(G_{m4})]=1/2+\frac{q_S}{2^{L_u}|P|}+\frac{q_S}{2^{L}|P|}+\frac{q_S}{2^{L+K}}+\frac{qh^2}{2^{L+1}} \tag{12}$$

综上所述，可得到攻击者A的优势为：

$$Adv_{\Gamma}^{A}(t)\leqslant\frac{q_h^2+q_{h1}^2+2q_S}{2^{L}}+\frac{(q_S+q_e)^2}{|R|}+\frac{q_d^2}{|C|}+2q_S Adv_{\Gamma}^{A,LWE}(t) \tag{13}$$

## 5 性能分析

为了验证方案的有效性，搭建试验环境，将所提出方案的身份认证和密钥协商阶段的计算开销与现有方案进行比较，其中包括Ying[15]、Wang[16]、Cui[17]、Zhang[18]提出的方案。

### 5.1 试验环境搭建

在试验室中搭建模拟车联网真实场景的硬件环境。如图4所示，包括具备联网功能的ROS小车、搭载QSE且能够加密车端数据的车载通信终端、为车辆提供云服务的VSP、管理车辆和VSP身份认证、管理量子密钥的QSC、量子密钥分发设备QKD以及调试电脑。

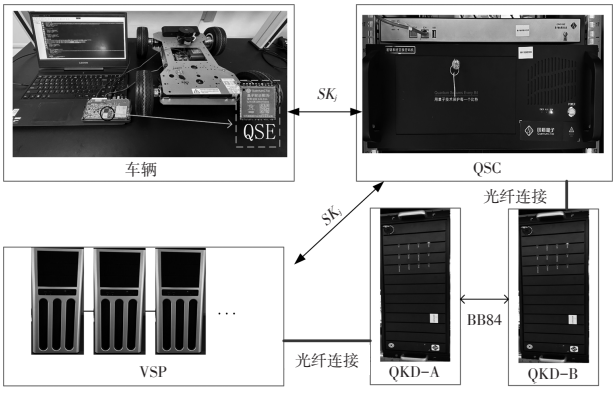


图4 硬件试验环境

### 5.2 计算开销对比

计算提出方案与对比方案所用到的重要密码算法的计算开销，并将认证方案中所用到的密码运算时间进行统计对比。这些密码算法包含：模指数运算、标量乘法运算、NTRU加密/解密运算、Falcon签名/验签运算、哈希运算。为了实现对比的客观性，设定Hash算法为SHA-256，对称加密算法为AES。通过参考NIST在局部模型下定义的第一类安全类别[19]和Zhang[15]提出方案中设定的参数，设定NTRU加密算法的关键参数为：$N$=503；$p$=3；$q$=2 048，设定Falcon签名算法的关键参数为：$k$=256；$R$=12 289。为了避免硬件差异，在同样的硬件（英特尔酷睿i7-12700H）上计算各算法的计算开销，结果如表2所示。

**表2 各算法的计算开销**

| 种类 | 描述 | 执行时间/ms |
|---|---|---|
| $T_h$ | 单向哈希 | 0.000 1 |
| $T_{pm}$ | 点乘 | 0.346 6 |
| $T_{pa}$ | 点加 | 0.009 7 |
| $T_{e,d}$ | 对称加密/解密 | 0.008 5 |
| $T_{En}$ | NTRU加密 | 0.126 9 |
| $T_{De}$ | NTRU解密 | 0.247 0 |
| $T_{Sign}$ | Falcon签名 | 0.284 1 |
| $T_{Verif}$ | Falcon验证 | 0.028 9 |

将各方案的计算开销进行对比,并假设是在单个车辆和单个VSP的场景下,分析车端和服务端的计算开销。Ying[15]、Wang[16]、Cui[17]的方案是建立在椭圆曲线密码算法的基础上。Zhang[18]和本方案则是基于格的密码算法来建立安全的身份认证方案。计算开销的方案对比如表3所示。

**表3　各方案的计算开销对比**

| 方案 | 车辆 | QSC<br>可信机构 | VSP<br>服务提供者 |
|---|---|---|---|
| Ying | $4T_{pm}+2T_{p}+7T_{h}$ | | $4T_{pm}+2T_{pa}+3T_{h}$ |
| Wang | $4T_{pm}+2T_{p}+6T_{h}$ | | $6T_{pm}+2T_{pa}+5T_{h}$ |
| Cui | $3T_{pm}+8T_{h}$ | $2T_{pm}+10T_{h}$ | $3T_{pm}+7T_{h}$ |
| Zhang | $2T_{En}+T_{h}$ | $3T_{De}+4T_{h}$ | $T_{En}+T_{h}$ |
| 本方案 | $T_{En}+T_{Sign}+7T_{h}$ | $2T_{De}+T_{Sign}+2T_{Verif}+10T_{h}$ | $T_{En}+T_{Sign}+T_{Verif}+5T_{h}$ |

在Ying[15]的方案中,车辆需要执行4次点乘、2次点加和7次单向哈希运算,开销为1.406 5 ms;服务端包括可信机构(QSC)和服务提供者(VSP),需要执行4次点乘、2次点加和3次单向哈希运算,开销为1.406 1 ms,总计算开销为2.812 6 ms。同理,可以计算出Wang[16],Cui[17]和Zhang[18]方案的总计算开销,分别是3.505 9 ms、2.775 3 ms和1.122 3 ms。在本研究提出的增强身份认证方案中,车辆需要执行1次加密、1次签名和7次单向哈希运算;QSC执行2次解密、1次签名、2次验签和10次单向哈希运算;VSP执行1次加密、1次签名、1次验签和5次单向哈希运算。总计算开销为1.689 ms。图5为各方案的计算开销结果。

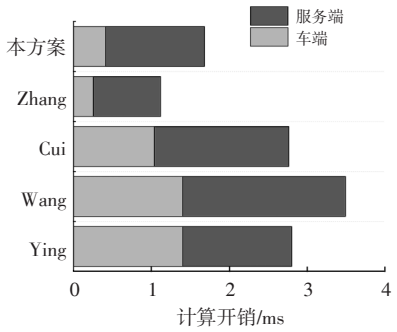


图5　计算开销测试结果

可以看出Zhang[18]的方案计算开销最小,这是因为其采用的是基于格的加密和签名算法,计算开销小于基于椭圆曲线的标量乘法运算。本研究的方案计算开销略大于Zhang的方案,是由于本方案对车辆、QSC以及VSP的消息进行了签名,保证了消息的不可否认性,方便在复杂交通环境下对车辆进行管理。因此本方案的安全性优于Zhang的方案,显著地减少了车端开销,性能提升为60.43%~70.72%。

## 6　结束语

本文提出了一种适用于后量子时代的车云通信场景下的增强身份认证方案。方案实现了可扩展的量子密钥分发,能够在车联网环境中兼顾无线和有线通信网络,进行安全高效的身份认证和密钥协商。对提出方案的安全性进行评估,并搭建了硬件实验环境,测试方案的通信性能和密钥协商过程,并与其他方案进行对比。结果表明,所提出的方案能够完成量子密钥在车联网通信场景的安全协商,适用于后量子时代的车联网领域。

## 参　考　文　献

[1] 王会杰, 杨燕红, 李志强. 我国智能网联汽车发展现状及策略分析[J]. 汽车实用技术, 2023, 48(6): 53-57.
WANG H J, YANG Y H, LI Z Q. Development Status and Strategy Analysis of Intelligent Networked Vehicles in My Country[J]. Automotive Practical Technology, 2023, 48(6): 53-57.

[2] 钟永超, 杨波, 杨浩男, 等. 智能网联汽车安全综述[J]. 信息安全研究, 2021, 7(6): 558-565.
ZHONG Y C, YANG B, YANG H N, et al. A Review of Intelligent Networked Vehicle Security[J]. Information Security Research, 2021, 7(6): 558-565.

[3] 暴爽, 李丽香, 彭海朋. 智能车联网信息安全研究[J]. 信息安全与通信保密, 2023(3): 10-20.
BAO S, LI L X, PENG H P. Research on Information Security of Intelligent Vehicle Networking [J]. Information Security and Communication Security, 2023(3): 10-20.

[4] 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. PUF-Based 5G Internet of Vehicles V2V Anonymous Authentication and Key Agreement Protocol [J]. Computer Research and Development, 2021, 58(10): 2265-2277.

[5] GULATI A, AUJLA G S, CHAUDHARY R, et al. Dilse: Lattice-Based Secure and Dependable Data Dissemination Scheme for Social Internet of Vehicles[J]. IEEE Transactions on Dependable and Secure Computing, 2019, 18(6): 2520-2534.

[6] 储美玲. 抗量子攻击的物联网安全认证方案研究[D].南京: 南京邮电大学, 2022.
CHU M L. Research on Internet of Things Security Authentication Scheme Against Quantum Attacks [D]. Nanjing: University of Posts and Telecommunications, 2022.

[7] CUI Y, CAO L, ZHANG X, et al. Ring Signature Based on Lattice and VANET Privacy Preservation[J]. Chin. J. Comput, 2017, 40(169): 1-14.

[8] LIU H, SUN Y, XU Y, et al. A Secure Lattice-Based Anonymous Authentication Scheme for VANETs[J]. Journal of the Chinese Institute of Engineers, 2019, 42(1): 66-73.

[9] ZHANG S, LIU Y, XIAO Y, et al. A Trust Based Adaptive Privacy Preserving Authentication Scheme for VANETs[J]. Vehicular Communications, 2022, 37: 100516.

[10] 姚光韬, 周琴. 量子保密通信技术及应用研究综述[J]. 通信与信息技术, 2020(1): 54-56+59.
YAO G T, ZHOU Q. A Review of Quantum Secure Communication Technology and Its Application[J]. Communication and Information Technology, 2020(1): 54-56+59.

[11] 贾其东. 量子密钥分发协议设计及其在IPSec协议中的应用研究[D]. 合肥: 中国科学技术大学, 2022.
JIA Q D. Design of Quantum Key Distribution Protocol and Its Application in Ipsec Protocol[D]. Hefei: University of Science and Technology of China, 2022.

[12] WANG J, WU L, WANG H, et al. A Secure and Efficient Multiserver Authentication and Key Agreement Protocol for Internet of Vehicles[J]. IEEE Internet of Things Journal, 2022, 9(23): 24398-24416.

[13] WANG Z, ZHONG Z, ZHAO D, et al. Vehicle-Based Cloudlet Relaying for Mobile Computation Offloading[J]. IEEE Transactions on Vehicular Technology, 2018, 67(11): 11181-11191.

[14] STEHLÉ D, STEINFELD R. Making NTRU as Secure as Worst-Case Problems Over Ideal Lattices[C]//Advances in Cryptology – EUROCRYPT 2011: 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings 30. Springer Berlin Heidelberg, 2011: 27-47.

[15] YING B, NAYAK A. Lightweight Remote User Authentication Protocol for Multi-Server 5g Networks Using Self-Certified Public Key Cryptography[J]. Journal of Network and Computer Applications, 2019, 131: 66-74.

[16] WANG J, WU L, WANG H, et al. A Secure and Efficient Multiserver Authentication and Key Agreement Protocol for Internet of Vehicles[J]. IEEE Internet of Things Journal, 2022, 9(23): 24398-24416.

[17] CUI J, ZHANG X, ZHONG H, et al. Extensible Conditional Privacy Protection Authentication Scheme for Secure Vehicular Networks in A Multi-Cloud Environment[J]. IEEE Transactions on Information Forensics and Security, 2019, 15: 1654-1667.

[18] ZHANG S, LIU Y, XIAO Y, et al. A Trust Based Adaptive Privacy Preserving Authentication Scheme for Vanets[J]. Vehicular Communications, 2022, 37: 100516.

[19] MOODY D, ALAGIC G, APON D C, et al. Status Report on The Second Round of the Nist Post-Quantum Cryptography Standardization Process[J]. US Department of Commerce, NIST, 2020, 2: 11-15.

（责任编辑　王　一）

修改稿收到日期为2023年9月5日。