·车联网量子加密通信技术专题·

面向车云网量子加密通信架构的轻量化身份认证方案研究*

石琴[1] 潘廷亮[1] 程腾[1] 王川宿[2] 张星[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】为解决车联网技术中身份认证问题，在车云网量子通信架构的基础上，设计了一种轻量化身份认证方案，认证过程由注册和认证2个阶段构成，车辆与车联网云平台间进行2轮认证以确保方案的安全性。试验结果表明，该方案计算开销仅为0.179 ms，通信开销为417 B，与其他4种相关方案相比，具有更低的计算开销和通信开销，在兼顾安全性的同时具备更高的效率，对于大多数低计算量和低通信量的车联网设备具有更高的适用性。

主题词：量子加密通信 身份认证 车联网 计算开销 通信开销

中图分类号：U495；TP309 **文献标识码：**A **DOI:** 10.19620/j.cnki.1000-3703.20230069

Research on Lightweight Authentication Scheme for Quantum Encrypted Communication Architecture in Vehicular Cloud Networks

Shi Qin[1], Pan Tingliang[1], Cheng Teng[1], Wang Chuansu[2], Zhang Xing[2]

（1. Key Laboratory for Automated Vehicle Safety Technology of Anhui Province, Engineering Research Center for Intelligent Transportation and Cooperative Vehicle-Infrastructure of Anhui Province, Hefei University of Technology, Hefei 230009; 2. Chery Automobile Company Limited, Wuhu 241006）

【Abstract】In this research, a lightweight authentication scheme was designed based on the quantum communication architecture of the Internet of Vehicle (IoV) cloud network. The authentication process consists of 2 stages: registration and authentication, and 2 rounds of authentication between the vehicle and the IoV cloud platform to ensure the security of the scheme. Test results show that this scheme has computational overhead of only 0.179 ms, and communication overhead of 417 B, which is lower than other 4 schemes, had has high efficiency while ensuring security, therefore it has high applicability for most IoV equipment with low computational amount and low communication volume.

Key words: Quantum encrypted communication, Authentication, Internet of Vehicle (IoV), Computational overhead, Communication overhead

【引用格式】石琴，潘廷亮，程腾，等. 面向车云网量子加密通信架构的轻量化身份认证方案研究[J]. 汽车技术，2023(10)：9-15.

SHI Q, PAN T L, CHENG T, et al. Research on Lightweight Authentication Scheme for Quantum Encrypted Communication Architecture in Vehicular Cloud Networks[J]. Automobile Technology, 2023(10): 9-15.

1 前言

在车联网各实体中，车-云间的通信是车联网技术的基础。车-云通信过程中，存在大量的车辆隐私和位置信息，以及云服务器的控制信令[1]。因此，车-云通信安全对于整个车联网交通安全具有重大影响。身份认证是车联网通信中最重要的步骤之一，可使合法车辆与车联网云平台进行信息交互，并将非法用户和各种类型的攻击拒之门外[2]。

在车-云通信过程中，密钥对于信息加密也有十分

*基金项目：国家自然科学基金项目（82171012）；中央高校基本科研业务费专项资金项目（JZ2023YQTD0073）；安徽省自然科学基金项目（2208085MF171）；安徽高校协同创新项目（GXXT-2020-076）；汽车标准化公益性开放课题项目（CATARC-Z-2022-01350）；安徽省新能源汽车暨智能网联汽车创新工程项目（JZ2021AFKJ0002）。

通讯作者：程腾（1983—），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。

重要的影响。密钥的生成往往基于随机数和口令，随机数的随机性会影响生成密钥的安全性[3]。在具有强大算力的计算机面前，通过种子信息、预设函数和常数常量等元素生成的伪随机数将会变得极其不安全[4]。而真随机数往往通过一些不可预测的物理现象产生，例如量子随机数发生器通过光子的物理现象产生随机数[5]。通过使用真随机数来生成量子密钥将会具有更高的安全性。目前，较为常用的量子密钥分发协议由Bennett和Brassard[6]于1984年提出，即BB84协议。

目前的身份认证机制主要分为基于公钥基础设施（Public Key Infrastructure，PKI）的认证方案、基于群签名的认证方案和基于身份的认证方案[7]。基于PKI的认证方案具有存储、通信和计算开销过大的缺陷。基于群签名的认证方案普遍具有如下问题：车辆离开一个群或加入一个新群，需要在可信实体（Trusted Authority，TA）的帮助下更新群密钥[8]，这不仅给TA带来了额外的负担，群密钥的频繁切换也带来极大的计算和通信开销[9]；群成员隐私信息的保护不易实现，难以保证匿名性和可追溯性。基于身份的认证方案相较于基于PKI的认证方案，在很大程度上减少了计算、通信和存储的开销，但密钥生成算法或者密钥存储设备的攻破会直接危害系统安全[10]。

本文针对部分车联网设备通信和计算能力有限的问题，在车云网量子通信架构的基础上，设计一种轻量化身份认证方案，主要通过量子随机数、逻辑运算和单向哈希函数[11-13]等进行运算，并与其他4种相关方案[14-17]进行对比验证。

2　车云网量子加密通信系统架构模型

车云网量子加密通信架构系统既支持广域网下车辆与车联网云平台之间通过线下储存的充注密钥进行会话密钥的无线分发，也支持局域网下车联网云平台与车载信息服务提供商（Telematics Service Provider，TSP）之间使用BB84协议实现量子密钥的有线协商。因此，该系统实现了混合网络下基于量子物理安全的加密通信。

车云网量子加密通信架构系统主要由车联网云平台、车辆、密钥充注系统（Key Filling System，KFS）和TSP组成，其架构如图1所示：

a. 量子云服务器（Quantum Cloud Server，QCS）车联网云平台。车联网云平台记录着每一辆车的ID、密码和充注密钥，以此验证车辆身份的合法性，也为车辆提供各种车联网服务。同时，QCS内还集成了一套量子密钥分发系统，可生成充注密钥和量子会话密钥，使其能够与车辆之间进行安全加密通信。QCS与TSP之间也具有量子密钥分发系统，保证QCS能够将车辆数据安全地传输给TSP。

b. 车辆。每一辆车都配备一个具有无线通信能力的设备，该设备可以是车载通信终端（Telematics-BOX，T-BOX）或车载诊断系统（On-Board Diagnosis，OBU）。同时，车辆的安全介质内存放着KFS生成并线下充注的密钥。在车辆与QCS完成认证并申请到会话密钥后，车辆能够使用密钥进行加密通信。

c. 密钥充注系统。KFS的主要作用是将QCS产生的足量的量子随机数以线下充注的方式储存到车辆的安全介质内。该随机数文件可以视为充注密钥。同时，充注密钥在QCS中也存有备份，并且与车辆ID绑定，充注密钥将会用于后续的车-QCS会话密钥的申请。

d. 车载信息服务提供商：TSP主要负责从QCS获取车辆的相关数据和请求后，提供相应的车联网服务。TSP与QCS之间通过光纤连接，并且集成了一套量子密钥分发系统。量子密钥分发系统能够保证两者之间的密钥分发和加密通信绝对安全。

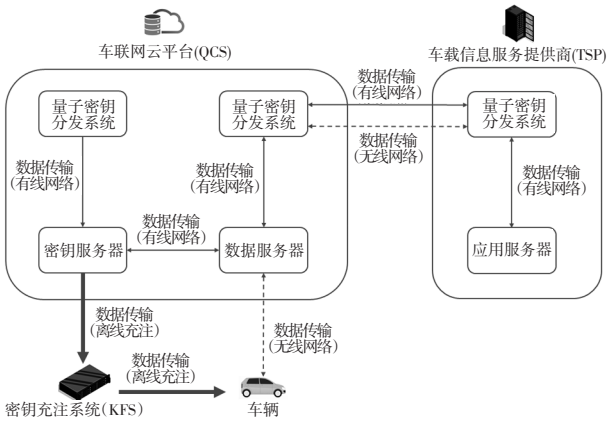

图1　车云网量子加密通信架构

3　身份认证流程

车辆与车联网云平台之间有2轮认证，认证过程如图2所示。车辆上电后，将与QCS建立连接，并发送第1轮登录认证消息。QCS在收到车辆第1条认证消息后，对车辆身份进行认证，认证通过后向车辆回复一条认证消息。车辆收到QCS回复的认证消息后，对QCS身份进行认证，认证通过后发送第2轮认证消息。QCS收到第2轮认证消息，验证通过后向车辆回复成功消息。至此，车辆与QCS之间的认证流程完成。

车辆与QCS身份认证的过程分为2个阶段，即注册阶段和认证阶段。表1所示为认证过程中的相关参数。

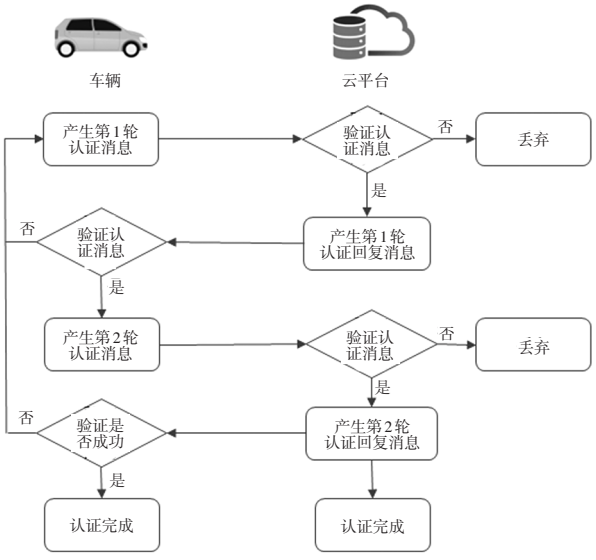

图2　车辆与云平台的身份认证流程

表1　登录认证协议参数

符号	定义
H_1	哈希函数(MD5算法)
H_2	哈希函数(SHA256算法)
H_3	哈希函数(SM3算法)
α、β、α_1、β_1	随机数
V_i	第i个车辆
M_i	车辆或云平台发送的消息
L	发送消息的长度
MT	消息类型标识符
Seq_i/Seq_j	消息序列号
H	消息头部
RID_i	V_i的真实身份
PW_i	V_i的密码
ID_i	V_i的匿名身份
R_i	第i轮认证
t_i	消息内时间戳
t^*	当前时间戳
Δt	时间戳有效期
MAC/MAC^*	消息完整性校验码
E	错误码
E_m	错误信息
R_m	应答消息
$\|\|$	连接操作
$\oplus$	异或操作

3.1　注册阶段

车辆通过线下的安全渠道向QCS注册登记,并向KFS获取充注密钥:

a. 车辆V_i选择其唯一真实身份信息RID_i和密码PW_i,并将信息上传QCS。

b. QCS收到注册信息后,计算$H_1(RID_i)$,并将计算结果与数据库现有身份信息进行对比。如果已经存在,则拒绝注册请求;反之,QCS将计算结果与RID_i绑定并记录在数据库内。同时,QCS将注册成功信息和3个安全哈希函数H_1、H_2、H_3发送给车辆。

c. 车辆收到信息后,记录下3个安全哈希函数并向KFS上报身份信息$H_1(RID_i)$,请求充注密钥。

d. KFS在收到充注请求后,请求QCS检查车辆合法性。完成检查后,将充注密钥传输到车辆的安全介质内。同时,KFS将车辆身份信息和充注密钥发送给QCS进行绑定和记录。

e. 车辆收到充注密钥后,将充注密钥存储在其安全介质内以完成注册过程。

3.2　认证阶段

认证阶段详细过程如图3所示:

a. 车辆V_i启动,登录云服务平台,生成第1轮登录认证消息。生成量子随机数α、随机序列号Seq_i和时间戳t_i。计算匿名身份信息$ID_i=H_1(RID_i)\oplus H_2(t_i)$,按照$\alpha_1=\alpha\oplus H_3(RID_i\oplus H_2(t_i))$计算随机数,并且组装生成认证消息头部,即$H=\{MT\|L\|t_i\|Seq_i\}$,计算$MAC=H_2(H\|R_i\|ID_i\|\alpha_1)$,最后生成消息$M_i=\{H\|ID_i\|\alpha_1\|R_i\|MAC\}$,将消息发送给云服务器。

b. 云服务器接收到消息M_i后,计算时间差$t^*-t_i<\Delta t$,检查消息的有效性,如果不满足条件则丢弃,如果满足时间戳有效性,则计算该消息$MAC^*=H_2(H\|R_i\|ID_i\|\alpha_1\}$,并检查式(1)是否成立:

$$MAC=MAC^*=H_2(H\|R_i\|ID_i\|\alpha_1) \tag{1}$$

如果不成立则丢弃该消息,否则查看消息类型MT,验证为登录认证消息。检查认证轮次R_i,验证为第1轮认证。取出ID_i,并根据时间戳t_i计算得出$H_1(RID_i)$,将数据库内的身份消息进行对比分析,查询得出车辆的RID_i,如果未能成功查询,则丢弃该消息,如果查询成功,则通过车辆的RID_i在数据库中找到对应的PW_i,并计算$\alpha=\alpha_1\oplus H_3(RID_i\oplus H_2(t_i))$,以及$R_m=H_2\{\alpha\|PW_i\}$。记录对方的$Seq_j$,同时生成量子随机数$\beta$、随机序列号$Seq_j$和时间戳$t_i$,计算$\beta_1=\beta\oplus H_3(RID_i\oplus H_2(t_i))$,组装生成认证消息头部,即$H=\{MT\|L\|t_i\|Seq_j\}$,然后计算消息完整性验证码$MAC=H_2(H\|R_i\|\beta_1\|R_m\|E\|E_m)$,最后生成消息$M_i=\{H\|\beta_1\|R_i\|E\|E_m\|R_m\|MAC\}$,将消息发送给车辆$V_i$。

c. 车辆V_i接收到消息M_i后,计算时间差$t^*-t_i<\Delta t$,检查消息的有效性,如果不满足条件则丢弃,如果满足时

间戳有效性,则计算该消息$MAC^*=H_2(H||R_i||\beta_1||R_m||E||E_m)$,并检查式(2)是否成立:

$$MAC=MAC^*=H_2(H||R_i||\beta_1||R_m||E||E_m) \quad (2)$$

如果不成立则丢弃该消息,否则查看消息类型MT,验证为登录认证消息。检查认证轮次R_i,验证为第1轮认证。车辆V_i将自己之前发送的量子随机数α与自己的密码PW_i进行计算,$R_m^*=H_2\{\alpha||PW_i\}$,并检查式(3)是否成立:

$$R_m=R_m^*=H_2\{\alpha||PW_i\} \quad (3)$$

如果不成立则丢弃该消息,否则检查消息内错误码E的值,如果表明登录认证消息失败,则根据错误信息E_m修改认证信息,并重新执行步骤a。如果消息内错误码E的值表明登录认证消息成功,则计算量子随机数$\beta=\beta_1\oplus H_3(RID_i\oplus H_2(t_i))$,将云服务器的量子随机数$\beta$与自己的密码$PW_i$进行计算,得到$R_m=H_2\{\beta||PW_i\}$。序列号$Seq_i$在之前的基础上增加1,同时生成时间戳$t_i$。组装生成认证消息头部,即$H=\{MT||L||t_i||Seq_j\}$,然后计算消息完整性验证码$MAC=H_2(H||R_i||ID_i||R_m)$,最后生成消息$M_i=\{H||ID_i||R_m||R_i||MAC\}$并发送给云服务器。

d. 云服务器接收到消息M_i后,计算时间差$t^*-t_i<\Delta t$,检查消息的有效性,如果不满足条件则丢弃,如果满足时间戳有效性,则计算消息$MAC^*=H_2(H||R_i||ID_i||R_m)$,并检查式(4)是否成立:

$$MAC=MAC^*=H_2(H||R_i||ID_i||R_m) \quad (4)$$

如果不成立则丢弃该消息,否则查看消息类型MT,验证为登录认证消息。检查认证轮次R_i,验证为第2轮认证。计算$R_m=H_2\{\beta||PW_i\}$,并检查式(5)是否成立:

$$R_m=H_2\{\beta||PW_i\} \quad (5)$$

如果不成立则丢弃该消息,否则对比Seq_i与之前记录的数值是否满足$Seq_i=Seq_i^*+1$,不满足则发送对应错误码给车辆V_i,如果符合条件,则回复认证成功消息。组装生成认证消息头部$H=\{MT||L||t_i||Seq_j\}$,然后计算消息完整性验证码$MAC=H_2(H||R_i||E||E_m)$,最后生成消息$M_i=\{H||R_i||E||E_m||MAC\}$,将消息发送给车辆$V_i$。

e. 车辆V_i接收到消息M_i后,计算时间差$t^*-t_i<\Delta t$,检查消息的有效性,如果不满足条件则丢弃,如果满足时间戳有效性,则计算该消息$MAC^*=H_2(H||R_i||E||E_m)$,验证式(6)是否成立:

$$MAC=MAC^*=H_2(H||R_i||E||E_m) \quad (6)$$

如果不成立则丢弃该消息,否则查看消息类型MT,验证为登录认证消息。检查认证轮次R_i,验证为第2轮认证。检查消息内错误码E的值,如果表明登录认证消息失败,则根据错误信息E_m修改认证信息,并重新执行步骤a。如果消息内错误码E的值表明登录认证消息成功,则认证结束,车辆进入通信流程下一阶段。

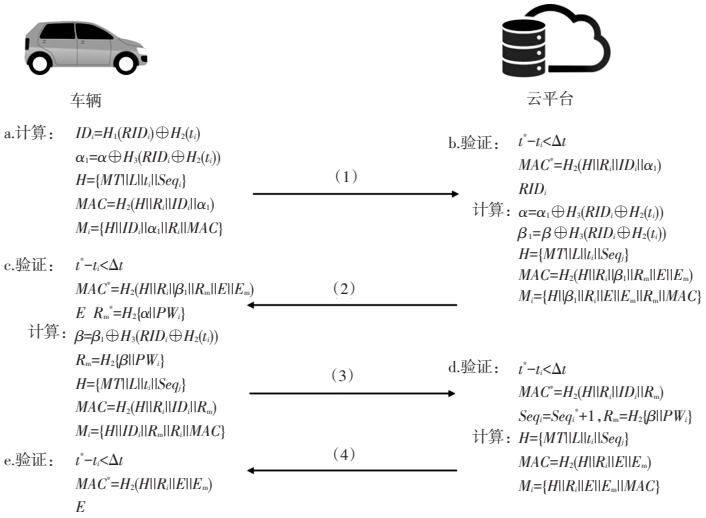

图3 身份认证详细流程

4 安全性分析

本文所提出的轻量化身份认证方案使用量子随机数提高了通信过程的安全性,因为量子加密通信具有无条件的安全性,这是由量子物理学的不可克隆原理和不确定性原理所决定的[18]。一方面,基于量子随机数所产生的量子密钥更加难以破解,具有更高的安全性,另一方面,量子密钥分发过程已被证明是绝对安全的,且任何第三方窃听行为都将会被及时发现[19]。本文对身份认证过程进行安全性分析,保证其符合安全性需求并能应对各种安全攻击手段:

a. 匿名性。因为在认证过程中车辆使用的ID_i并不是真实身份信息,所以在进行身份认证的过程中,攻击者不能依靠拦截认证消息获得用户的真实信息。因此,

本文方案具有匿名性。

b. 可追溯性。车辆的真实身份信息RID_i可以由QCS分析计算ID_i来获得。当网络内出现异常节点时,QCS能够通过分析ID_i来追踪到真实身份信息。因此,本文方案具备可追溯性。

c. 不可链接性。车辆生成的用于身份认证的匿名身份ID_i和认证消息M_i都使用了量子随机数和时间戳,因此,每一次认证使用的ID_i都不相同,攻击者无法通过长期追踪来锁定某个特定的车辆用户。

d. 抵抗伪造攻击。本文方案在建立通信前需要进行身份认证。合法节点的身份信息记录在QCS内,而且每次认证过程使用不同的量子随机数,攻击者难以伪装成车辆或者QCS。因此,该方案能够抵抗伪造攻击。

e. 抵抗重放攻击。假定攻击者具有截获车辆和QCS的身份认证消息M_i的能力,在一段时间后,攻击者将截获信息原封不动地发送给车辆或者QCS,并以此冒充合法身份。但是,M_i中存在着时间戳t_i、量子随机数和序列号Seq_i或Seq_j,都将造成攻击者发送的认证消息无效,从而使得攻击者无法完成身份认证。因此,本文方案对于重放攻击具有很强的抵抗能力。

f. 抵抗篡改攻击。假设攻击者在截获车辆和QCS之间的身份认证消息M_i后,篡改部分内容来通过身份认证。本文方案中,车辆与QCS的通信消息中都存在着完整性摘要MAC。当消息被篡改后,消息接受方在对消息进行完整性校验时将发现消息已经篡改,从而丢弃该条消息。

g. 抵抗中间人攻击。假设攻击者通过截获车辆和QCS间的通信消息,介入两者间的通信,达到欺骗对方、窃听和篡改信息的目的[20]。本文方案中,车辆和QCS之间会进行双向认证。同时,认证所需信息都进行加密并具有完整性摘要MAC,中间人既不能获取有效信息,也不能篡改消息内容。因此,本文方案具有抵抗中间人攻击的能力。

5 性能评估

5.1 计算开销

将所提出的轻量化认证方案与现有的其他相关方案[10-13]在认证过程的计算开销进行对比和分析。

试验中,使用一台笔记本电脑作为QCS或云服务提供商(Cloud Service Provider,CSP)来统计计算开销。该主机具有AMD Ryzen 7 5800H with Radeon Graphics处理器、16 GB内存和Ubuntu 16.04操作系统。对于每种计算开销的统计,以10 000次计算为一组,计算10组取平均值。试验主机如图4所示,试验中,使用试验车的T-BOX开发板统计车辆计算开销,开发板为移远AG35 QuecOpen硬件模组,具有ARM Cortex A7内核的基带处理器平台,T-BOX开发板如图5所示。对于每种计算开销的统计,同样以10 000次计算为一组,计算10组取平均值。异或运算执行时间远小于其他运算,对试验结果影响较小,因此在统计计算开销时忽略异或操作执行时间。设T_{h1}、T_{h2}、T_{h3}、T_{bp}、$T_{bp.m}$、T_{mtp}、$T_{W.m}$、$T_{M.m}$和$T_{c/d}$分别为以MD5算法执行单向哈希函数运算、以SHA256算法执行单向哈希函数运算、以SM3算法执行单向哈希函数运算、执行双线性对运算、执行双线性对乘法运算、执行Map-To-Point哈希运算、执行椭圆曲线群上的点乘运算、执行蒙哥马利曲线群上的点乘运算和执行对称加解密运算的消耗时间,各方案的加密操作执行时间如表2所示。

图4 实车试验

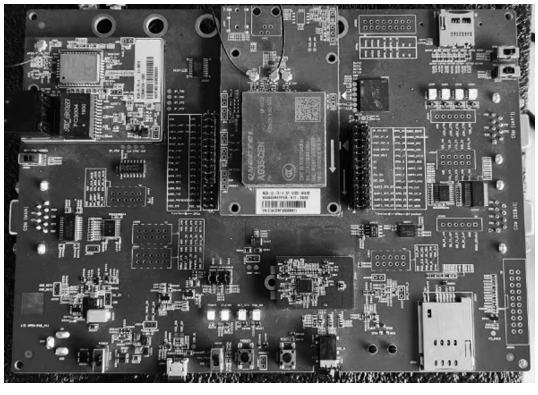

图5 T-BOX开发板

将本文所提出的轻量化身份认证方案与现有的其他相关方案在认证过程的计算开销进行对比,结果如表3所示。

由表3可以看出,与其他方案相比,本文设计的轻量化方案在认证阶段所需的总时间大幅缩短。

5.2 通信开销

将所提出的轻量化认证方案与其他现有的相关方

案在认证过程的通信开销进行对比和分析。

本文提出的认证方案主要有4条消息:$M_1=\{H||ID_i||\alpha_1||R_i||MAC\}$、$M_2=\{H||\beta_1||R_i||E||E_m||R_m||MAC\}$、$M_3=\{H||ID_i||R_m||R_i||MAC\}$、$M_4=\{H||R_i||E||E_m||MAC\}$。假设哈希函数的输出大小为32 B、时间戳为4 B,4条消息中ID_i、MAC、α_1、β_1、R_m均属于哈希函数。H中MT、L、t_i、Seq_i(Seq_j)的大小分别是3 B、4 B、4 B和3 B,R_i和E的大小均为1 B,E_m的大小为2 B。因此消息M_1~M_4的通信开销分别为142 B、114 B、111 B和50 B。最终,本文方案的通信开销为417 B。

表2 各方案的加密操作执行时间 ms

加密操作	车端	云端
T_{h1}	0.011	0.001
T_{h2}	0.015	0.002
T_{h3}	0.012	0.003
T_{bp}	6.543	1.271
$T_{bp.m}$	1.881	0.174
T_{mtp}	0.146	0.025
$T_{W.m}$	0.438	0.087
$T_{M.m}$	0.219	0.043
$T_{e/d}$	0.032	0.006

表3 各方案的计算开销 ms

方案	车辆计算开销	QCS/CSP计算开销	总计算开销
文献[11]	$T_{bp}+T_{bp.m}+2T_{mtp}+2T_{e/d}$	$T_{bp}+2T_{bp.m}+2T_{e/d}$	10.113
文献[12]	$3T_{W.m}+4T_{h1}$	$4T_{W.m}+4T_{h1}$	1.714
文献[13]	$3T_{W.m}+8T_{h1}$	$3T_{W.m}+7T_{h1}$	1.670
文献[10]	$3T_{M.m}+9T_{h1}+T_{e/d}$	$3T_{M.m}+7T_{h1}$	0.924
本文方案	$T_{h1}+8T_{h2}+2T_{h3}$	$9T_{h2}+2T_{h3}$	0.179

本文所提出的轻量化认证方案与其他现有的相关方案在认证过程的通信开销对比结果如表4所示。由表4可知,本文方案的通信开销低于其他4种方案。

表4 各方案的通信开销 B

方案	通信开销						
	M_1	M_2	M_3	M_4	M_5	M_6	总开销
本文方案	142	114	111	50			417
文献[10]	132	112	164	136			544
文献[13]	136	4	136	196	164	32	668
文献[12]	132	328	260	228			948
文献[11]	1 172	1 556	1 636	1 636	384		6 384

6 结束语

本文在车云网量子通信架构的基础上,设计了一种轻量化身份认证方案。通过对认证流程的详细分析,论证了该方案符合安全性需求且能应对各种安全攻击手段。试验结果表明,该方案相较于其他相关方案,有更低的计算开销和通信开销,故对于大多数低计算量和低通信量的车联网设备具有更高的适用性。

参 考 文 献

[1] 李慧. 车联网隐私保护关键技术研究[D]. 成都: 电子科技大学, 2021.
LI H. Research on Key Technologies for Privacy Protection in Vehicle Networking[D]. Chengdu: University of Electronic Science and Technology, 2021.

[2] 骆毅. 互联网时代社会协同治理研究[D]. 武汉: 华中科技大学, 2015.
LUO Y. Research on Collaborative Social Governance in the Internet Era[D]. Wuhan: Huazhong University of Science and Technology, 2015.

[3] 骆汉光. 面向物联网的轻量级安全协议及关键技术研究[D]. 成都: 电子科技大学, 2019.
LUO H G. Research on Lightweight Security Protocols and Key Technologies for the Internet of Things[D]. Chengdu: University of Electronic Science and Technology, 2019.

[4] 安雪碧. 量子密码协议与实验研究[D]. 合肥: 中国科学技术大学, 2018.
AN X B. Quantum Cryptographic Protocols and Experimental Research[D]. Hefei: University of Science and Technology of China, 2018.

[5] 周泓伊, 曾培. 量子随机数发生器[J]. 信息安全研究, 2017, 3(1): 23-35.
ZHOU H Y, ZENG P. Quantum Random Number Generator [J]. Information Security Research, 2017, 3(1): 23-35.

[6] BENNETT C H, BRASSARD G. Quantum Cryptography: Public Key Distribution and Coin Tossing[J]. Theoretical Computer Science, 2014, 560: 7-11.

[7] 王琳杰. 物联网数据安全及跨域认证模型研究[D]. 贵阳: 贵州大学, 2021.
WANG L J. Research on IoT Data Security and Cross-Domain Authentication Model[D]. Guiyang: Guizhou University, 2021.

[8] 张鹏飞. 面向车联网的匿名认证与密钥协商协议研究[D]. 成都: 电子科技大学, 2022.
ZHANG P F. Research on Anonymous Authentication and Key Negotiation Protocol for Vehicular Networking[D]. Chengdu: University of Electronic Science and Technology, 2022.

[9] 王朋. 车联网消息认证关键技术研究[D]. 桂林: 桂林电子科技大学, 2022.
WANG P. Research on Key Technology of Message Authentication for Vehicle Networking[D]. Guilin: Guilin

University of Electronic Science and Technology, 2022.

[10] 高博远. 一种基于区块链的物联网设备身份认证系统设计与实现[D]. 北京: 北京工业大学, 2021.
GAO B Y. A Blockchain- Based Identity Authentication System Design and Implementation for IoT Devices[D]. Beijing: Beijing University of Technology, 2021.

[11] 钱睿硕. 基于GPU加速的MD5哈希函数加密算法研究[D]. 武汉: 华中科技大学, 2009.
QIAN R S. Research on MD5 Hash Function Encryption Algorithm Based on GPU Acceleration[D]. Wuhan: Huazhong University of Science and Technology, 2009.

[12] 李妮. MD5和SHA-256算法研究与FPGA实现[D]. 长沙: 湖南大学, 2021.
LI N. Research on MD5 and SHA- 256 Algorithms and FPGA Implementation[D]. Changsha: Hunan University, 2021.

[13] 刘宗斌, 马原, 荆继武, 等. SM3哈希算法的硬件实现与研究[J]. 信息网络安全, 2011(9): 191-193+218.
LIU Z B, MA Y, JING J W, et al. Hardware Implementation and Research of SM3 Hash Algorithm[J]. Information Network Security, 2011(9): 191-193+218.

[14] ZHANG J, ZHONG H, CUI J, et al. SMAKA: Secure Many- to- Many Authentication and Key Agreement Scheme for Vehicular Networks[J]. IEEE Transactions on Information Forensics and Security, 2020, 16: 1810-1824.

[15] LIU Y B, WANG Y H, CHANG G H. Efficient Privacy-Preserving Dual Authentication and Key Agreement Scheme for Secure V2V Communications in an IoV Paradigm[J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(10): 2740-2749.

[16] MA M M, HE D B, WANG H Q, et al. An Efficient and Provably- Secure Authenticated Key Agreement Protocol for Fog- Based Vehicular Ad- Hoc Networks[J]. IEEE Internet of Things Journal, 2019, 6(5): 8065-8075.

[17] CUI J, ZHANG X Y, 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, 2020, 15: 1654-1667.

[18] 光旗胜. 两方量子通信协议及其安全性的研究[D]. 南京: 南京大学, 2020.
GUANG Q S. Research on Two- Party Quantum Communication Protocol and Its Security[D]. Nanjing: Nanjing University, 2020.

[19] 侯芬. 基于单光子干涉的认证量子密钥分发协议研究[D]. 重庆: 重庆大学, 2021.
HOU F. Research on Authenticated Quantum Key Distribution Protocol Based on Single Photon Interference [D]. Chongqing: Chongqing University, 2021.

[20] 王华. 量子密钥分发网络生存性关键技术研究[D]. 北京: 北京邮电大学, 2021.
WANG H. Research on Key Technologies for Survivability of Quantum Key Distribution Networks[D]. Beijing: Beijing University of Posts and Telecommunications, 2021.

（责任编辑　斛　畔）

修改稿收到日期为2023年2月3日。