多云环境下基于区块链的车列协同认证方案*

曹尚贵[1]　邓佳宾[2,3]　王文冲[1]　程腾[2,3]

（1.奇瑞汽车股份有限公司，芜湖 241000；2.合肥工业大学 自动驾驶汽车安全技术安徽省重点实验室，合肥 230009；3.安徽省智慧交通车路协同工程研究中心，合肥 230000）

【摘要】为了增强智能网联汽车无线信道云服务访问的安全性与即时性，提出基于区块链的匿名身份认证方案。利用Bennett-Brassard 1984（BB84）协议完成多个云服务器间的密钥协商，建立车辆与多云服务器连接；通过车端量子随机数生成的匿名凭证，实现认证过程的隐私保护；使用区块链记录成员车的相关信息，减少认证通信轮次并提高效率。试验结果表明：提出方案的车端计算开销为711.7 μs，通信开销为412 B，兼具安全性与高效性。

主题词：多云服务　条件匿名　身份认证　量子随机数

中图分类号：U495；TP309　　**文献标志码：**A　　**DOI:** 10.19620/j.cnki.1000-3703.20250338

Blockchain-Based Authentication Scheme for Vehicle Platooning in Multi-Cloud Environments

Cao Shanggui[1], Deng Jiabin[2,3], Wang Wenchong[1], Cheng Teng[2,3]

（1. Chery Automobile Co., Ltd., Wuhu 241000; 2. Key Laboratory for Automated Vehicle Safety Technology of Anhui Province, Hefei University of Technology, Hefei 230009; 3. Engineering Research Center for Intelligent Transportation and Cooperative Vehicle-Infrastructure of Anhui Province, Hefei 230000）

【Abstract】To enhance the security and immediacy of wireless channel cloud service access for intelligent connected vehicles, a blockchain-based anonymous identity authentication scheme is proposed. This paper employs the Bennett-Brassard 1984 (BB84) protocol to establish key agreements among multiple cloud servers, thereby enabling vehicle connectivity with these cloud resources. Anonymity certificates generated via quantum random number generation at the vehicle end ensure privacy protection during authentication. Blockchain technology is utilized to record member vehicle information, thereby reducing authentication communication rounds and enhancing operational efficiency. The results indicate that the proposed solution entails a computational overhead of 711.7 μs at the vehicle end and a communication overhead of 412 B, combining both security and efficiency.

Key words: Multi-cloud services, Conditional anonymity, Authentication, Quantum random number

【引用格式】曹尚贵, 邓佳宾, 王文冲, 等. 多云环境下基于区块链的车列协同认证方案[J]. 汽车技术, 2026(3): 38-45.

CAO S G, DENG J B, WANG W C, et al. Blockchain-Based Authentication Scheme for Vehicle Platooning in Multi-Cloud Environments[J]. Automobile Technology, 2026(3): 38-45.

1　前言

随着车联网（Internet of Vehicle，IoV）服务的加速渗透，智能网联汽车具备访问云服务器提供商（Cloud Server Provider，CSP）多元化增值服务能力，如智能交通优化、娱乐与互联网服务、远程诊断和实时停车等[1-2]。而车辆与云服务器间缺乏可靠的认证机制和密钥协商流程[3-4]，在面对潜在的恶意攻击时，如仿冒攻击、数据篡改及信息窃取等[5-6]，用户的隐私信息与驾驶安全将受到严重威胁，同时云服务器的稳定运行亦面临考验[7-8]。

在车联网环境中，随着车辆与交通基础设施互联、

*基金项目：安徽省科技创新攻坚计划项目（202423r06050003，202423e12050001，202523f12050013）；中央高校基本科研业务费专项资金（PA2025GDSK0045）；芜湖市“赤铸之光”重大科技项目（2023zd01）。

互通程度的显著提升，车联网领域亟需加强用户隐私保护。现有的匿名认证方案在认证前向安全性和后向安全性的协同保障方面存在局限[9]。Maurya等[10]基于路侧单元生成基础参数，构建车辆伪身份和与之绑定的批量、可验证签名，但依赖半可信路端参数，易引发身份冒充、签名伪造风险。杨小东等[11]提出一种无证书匿名认证方案，降低了证书管理带来的风险，但增加了车辆的计算负担和能耗。Jiang等[12]引入易受环境变化和制造差异影响的物理不可克隆函数，提高了认证的安全性，但需要额外的稳定措施。

在动态开放的车载网络环境中，传统基于固定基础设施的认证方案难以满足高速移动场景下的低时延、高可靠认证需求。Miao等[13]提出一种基于椭圆曲线加密技术的无人机辅助车联网认证协议；Zhang等[14]针对无网络覆盖地区，设计一种智能无人机辅助匿名认证和5G/B5G车载自组织网络的密钥协议。上述方案虽扩展了网络覆盖范围，但不可避免地增加了系统部署成本与运维复杂度。

现阶段，车云服务已从车辆与单一云服务商间的简单认证，发展为需要同时对接多个云服务平台的复杂场景[15]。传统的单车辆-单云服务器直接认证模式增加了系统认证负载，导致认证延迟和性能下降，还会因频繁的认证请求引发网络拥塞和带宽压力[16]。Zhang等[17]通过整合车联网中车辆的冗余计算与存储资源，构建分布式车载云以提供低成本服务，但中继车辆选择时未考虑车辆移动性与连接稳定性，缺乏高效的动态选择策略。Cui等[18]提出一种多云认证方案，由可信机构管理的云代理负责连接所有的云服务，但大幅增加了机构负担。

为此，可通过BB84（Bennett-Brassard 1984）协议克服多云协同场景下的安全瓶颈，构建云服务器间的物理层安全通道[19]。该协议利用量子态非正交性与测量扰动效应实现无条件安全密钥分发[20]，发送方随机选择矩形或对角偏振基调制光子态（0/1），接收方随机选择基测量。通信双方通过经典信道比对偏振基矢信息（过程中不泄露任何比特数据），筛选出基矢匹配的测量结果作为初始密钥；随后随机抽取部分比特进行误码率校验，若误码率低于预设阈值，则依次执行纠错与隐私放大操作，最终生成具有无条件安全性的量子密钥。本文基于BB84协议提出一种车列协同场景下的分层认证方案，实现多云安全互联、头车代理认证及成员车隐私接入。同时，经安全分析和系统性能测试，验证本文方案的合理性和有效性。

2 系统架构

在多云环境中，本文提出的车列协同与云服务器架构如图1所示，相关符号和定义如表1所示。

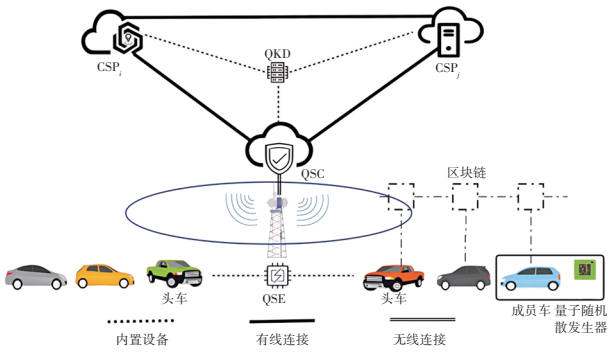


图1 系统架构

表1 符号定义

符号	定义
UID	用户身份
PW	登录密码
ID	头车真实身份标识
VID	成员车真实身份标识
HID	头车匿名身份标识
PID	区块链上车辆匿名身份参数
FID	成员车匿名身份标识
CID	CSP真实身份标识
PQK	头车预置量子密钥
PQK_{tag}	预置量子密钥标识
p	区块链索引
$E_{key}(X)$	使用密钥对X进行加密
$D_{key}(X)$	使用密钥对X进行解密
$T_{s,i}$	消息发送时间戳
T_s	本地时间戳
$\|\|$	连接符
$\oplus$	异或操作
$H(\ )$	单向哈希函数（SHA3-256）
$h(\ )$	单向哈希函数（BLAKE2b-256）

该架构由量子安全云（Quantum Security Cloud，QSC）、云服务器提供商、车列中的头车与成员车组成：

a. 量子安全云：一个可信的权威机构，为所有车辆和CSP提供注册服务。其配备了集成的量子密钥生成和分发设备，是协助车辆和CSP相互认证的中介。

b. 云服务器提供商：作为多云环境的服务载体，由多个分布式云服务平台组成并接入互联网，为车列协同场景下的智能网联汽车提供多元化车联网服务，包括智能停车调度、道路事故信息实时共享、实时路况推送等。

c. 头车：配备车载通信终端，如车载远程信息处理终端（Telematics Box，T-BOX）和车载单元（On-Board Unit，OBU），作为成员车的云服务代理，负责网络连接。其终端集成了量子安全加密模块和量子随机数发生器，在预置密钥的保护下，车载终端可与QSC进行会话密钥协商。

d. 成员车：配备量子随机数发生器，可自行生成匿名凭证。部分匿名身份参数经注册阶段记录于区块链，成员车基于该记录与头车完成身份认证及会话密钥协商，依据头车已建立的多云服务连接，间接接入云服务。

3 主体方案

本文方案可分为4个阶段，分别为初始化阶段、注册阶段、认证阶段和车列协同阶段。

3.1 初始化阶段

初始化阶段由QSC完成系统参数的选择和发布，QSC选择有限域Z_q中一条以O为无穷远点的椭圆曲线$E_q(\alpha,\beta)$，其形式为$y^2 = x^3 + \alpha x + \beta(\mathrm{mod}\,q)$，其中，$q$为大素数，$\alpha$、$\beta \in Z_q^*$，满足非奇异条件$4\alpha^3-27\beta^2 \neq 0(\mathrm{mod}\,q)$。

选择椭圆曲线的基点P、两类单向哈希函数（$H()$计算消息完整性校验参数，$h()$生成认证参数与派生密钥）和对称加密（Advanced Encryption Standard，AES）算法，用于保障后续数据加密与密钥传输的机密性。其中，$\begin{cases} P \in E_q(\alpha,\beta) \\ n \cdot P = O \end{cases}$，$O$为椭圆曲线原点。QSC公布系统参数、函数$\{\alpha,\beta,q,P,H(),h()\}$与算法AES。

头车出厂时，在量子安全加密（Quantum Secure Encryption，QSE）模块中充注一定数量的PQK，QSC可根据密钥标签PQK_{tag}检索对应的PQK，识别并记录QSE充注的密钥。当头车中剩余的PQK数量低于预设阈值时，需对QSE补充注入PQK。

3.2 注册阶段

注册阶段包含头车、成员车和CSP的身份注册，授予头车读写区块链权限，并将成员车的匿名信息记录在区块链中。

头车向QSC注册流程为：

a. 用户（头车管理员）设置身份UID和密码PW，计算用户登录验证$UPW = h(UID\|\|PW)$。车辆将自身及用户身份标识ID、UID和UPW组包注册消息$M_{\mathrm{r1}} = \{ID,UID,UPW\}$，通过安全通道发送至QSC。

b. QSC接收到M_{r1}后，核验数据库中该车ID的注册情况：若数据库中已存在该车辆ID对应的注册记录，则拒绝本次注册请求；反之，QSC确认其身份后，选择一个长期密钥r，并计算认证哈希参数$A = h(r\|\|ID\|\|UPW)$，存储$\{ID,UID,UPW,A\}$，授权该车成为合法区块链节点，支持链上相关记录查询。QSC组包消息$M_{\mathrm{r2}} = \{r,A\}$，通过安全通道发送给车辆。

c. 车辆收到M_{r2}后，计算$A = h(r\|\|ID\|\|UPW)$，对比消息中A是否一致，一致则确认其注册成功，并安全保存$\{r,A\}$。

成员车向QSC注册流程为：

a. 车辆选择其唯一的身份标识VID，组包消息$M_{\mathrm{r3}} = \{VID\}$，通过安全通道发送至QSC。

b. QSC检查数据库中该成员车VID注册情况，若存在则拒绝注册；反之，QSC为其生成匿名身份参数$PID = h(VID)\oplus r$，并上传区块链，生成区块链索引p，组包消息$\begin{cases} M_{\mathrm{r4}} = \{R,p\} \\ R = r \cdot P \end{cases}$，通过安全通道发送至成员车，其中，$P$为椭圆曲线基点。

c. 车辆收到消息M_{r4}后，将R和p安全保存。

CSP向QSC注册流程为：

a. CSP生成随机数n，将身份CID组包消息$M_{\mathrm{r5}} = \{n,CID\}$，通过安全通道发送至QSC。

b. QSC生成随机数m，计算云端认证哈希参数$C = h(CID\|\|m\|\|n)$，存储$\{CID,m,n,C\}$，将C通过安全通道发送至CSP。

c. CSP接收C并保存。

3.3 认证阶段

认证阶段实现QSC、头车和CSP间的身份认证和密钥协商，如图2所示。

QSC认证头车的流程为：

a. 用户输入身份UID和密码PW，车辆计算$UPW = h(UID\|\|PW)$，对比存储的UPW，一致则用户身份验证成功。头车生成一个量子随机数a，计算匿名身份$HID = h(a,ID,UID)$，并提取QSE中量子密钥加密生成$S = E_{\mathrm{PQK}}(UPW,A\oplus a)$，生成当前时间戳$t_{s,h}$，计算消息完整性参数$L = H(HID,S,t_{s,h})$，组包消息$M_{\mathrm{a1}} = \{HID,PQK_{\mathrm{tag}},S,L,t_{s,h}\}$发送至QSC。

b. QSC接收消息M_{a1}后，生成本地时间戳T_{s}，并验证$T_{\mathrm{s}} - t_{s,h} < \Delta T$是否符合要求，确认消息即时性。验证通过后，根据消息内容计算$L = H(HID,S,t_{s,h})$，检验消息完整性。随后根据密钥标签PQK_{tag}提取密钥PQK解密S，获得UPW和$(A \oplus a)$，通过UPW查找数据库存储$\{ID,UID,UPW,A\}$，计算$a = A\oplus a\oplus A$和车辆匿名身份$HID = h(a,ID,UID)$，对比消息中车辆匿名身份HID是否

一致,符合则认证通过。

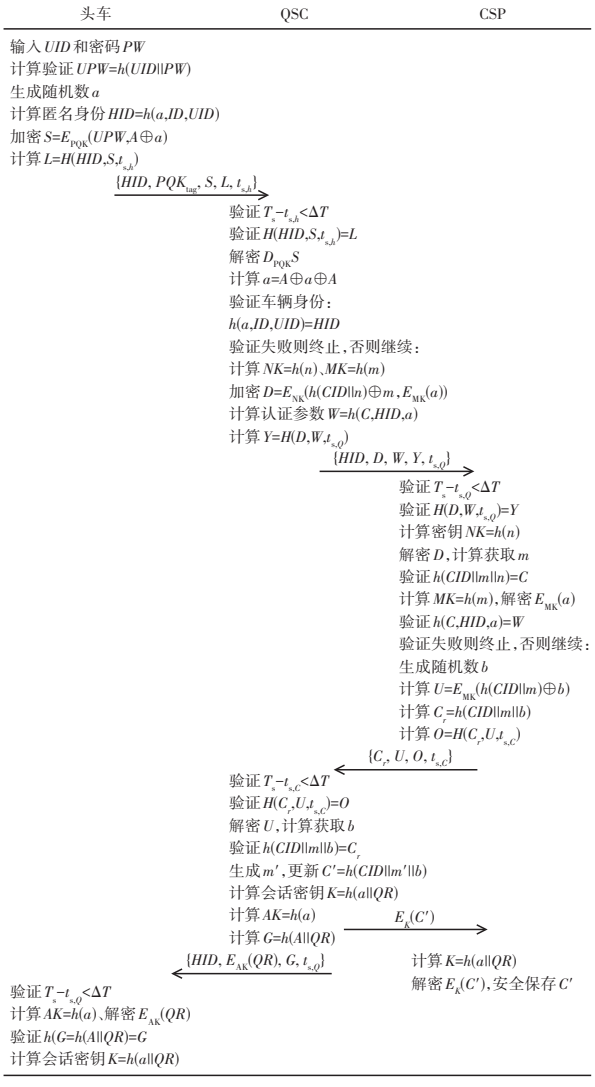


图2　认证阶段流程

QSC协助CSP认证头车的流程为:

a. QSC选择一个CSP,计算加密密钥 $\begin{cases} NK = h(n) \\ MK = h(m) \end{cases}$,进行加密计算 $D = E_{NK}(h(CID||n)\oplus m)$,$E_{MK}(a)$ 生成时间戳 $t_{s,Q}$,计算认证参数 $W = h(C,HID,a)$ 和消息完整性参数 $Y = H(D,W,t_{s,Q})$,组包消息 $M_{a2} = \{HID,D,W,Y,t_{s,Q}\}$,发送至该CSP。

b. CSP接收消息 M_{a2} 后,生成本地时间戳 T_s 验证 $T_s - t_{s,Q} < \Delta T$ 是否符合要求,确认消息即时性。验证通过后,根据消息内容计算 Y 并检验消息完整性。提取自身随机数 n 计算密钥 $NK = h(n)$,解密 D 获得 $(h(CID||n)\oplus m)$ 和 $E_{MK}(a)$,计算得到 $m = h(CID||n)\oplus m\oplus h(CID||n)$,再判断 $C = h(CID||m||n)$ 与数据库存储的一致性。使用 m 计算密钥 $MK = h(m)$ 解密 $E_{MK}(a)$,获得车辆随机数 a,验证 W 与消息是否一致,一致表明车辆身份和QSC可信,并保存随机数 a。

c. CSP重新生成随机数 b,计算 $\begin{cases} U = E_{MK}(h(CID||m)\oplus b) \\ C_r = h(CID||m||b) \end{cases}$,生成当前时间戳 $t_{s,C}$,计算消息完整性参数 $O = H(C_r,U,t_{s,C})$,组包消息 $M_{a3} = \{Cr,U,O,t_{s,C}\}$,发送至QSC。

d. QSC接收消息 Ma_3 后,生成本地时间戳 T_s 验证 $T_s - t_{s,C} < \Delta T$ 是否符合要求,确认消息即时性。验证通过后,根据消息内容计算 $O = H(C_r,U,t_{s,C})$ 检验消息完整性。解密 U,计算 $b = h(CID||m)\oplus b\oplus h(CID||m)$,再验证 $C_r = h(CID||m||b)$ 是否与消息一致,一致则CSP身份认证成功。QSC更新存储 $\{CID,m,b,C'\}$,其中,$C' = h(CID||m'||b)$,m' 为新生成的随机数。

e. 已验证双方根据BB84协议通过内置量子密钥分发设备生成量子随机数 QR,计算会话密钥 $K = h(a||QR)$。QSC使用 K 加密 C',发送至CSP。CSP解密更新 C 并保存 C'。

QSC协助头车认证CSP的流程为:

a. QSC计算加密密钥 $AK = h(a)$,组包消息 $M_{a4} = \{HID,E_{AK}(QR),G,t_{s,Q}\}$ 发送至车辆,其中,$G = h(A||QR)$ 为认证参数。

b. 头车接收消息 Ma_4 后,确认身份 HID,生成本地时间戳并验证 $T_s - t_{s,Q} < \Delta T$ 是否符合要求。计算密钥 $AK = h(a)$,使用 AK 解密加密内容 $E_{AK}(QR)$ 获得 QR,计算 $G = h(A||QR)$,确认QSC身份后,计算会话密钥 $K = h(a||QR)$,若使用该会话密钥能够申请云服务,则表明头车与CSP双方认证成功。

3.4　车列协同阶段

在车列协同阶段,头车先对成员车完成身份认证,再与成员车协商会话密钥,并依托头车已建立的多云服务连接,为成员车搭建至云服务器的间接通信链路,如图3所示。

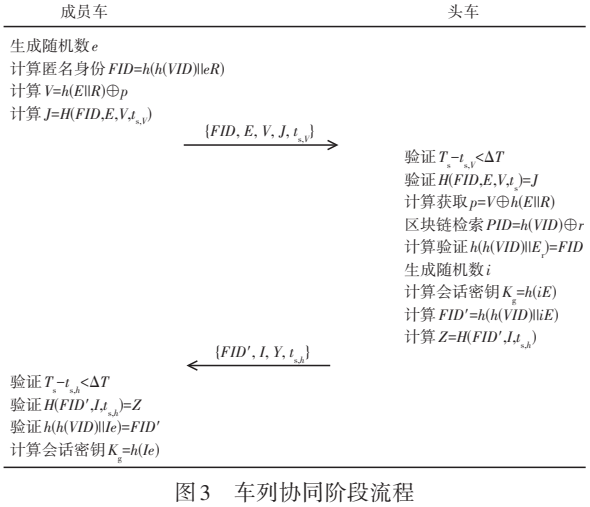


图3　车列协同阶段流程

a. 成员车生成随机数 e，计算匿名身份 $FID = h(h(VID)\|e\cdot R)$，构建 $\begin{cases} V = h(E\|R)\oplus p \\ E = e\cdot P \end{cases}$，生成时间戳 $t_{s,V}$，计算完整性参数 $J = H(FID,E,V,t_{s,V})$，组包消息 $M_{a5} = \{FID,E,V,J,t_{s,V}\}$ 发送至头车。

b. 头车接收消息 M_{a5} 后，生成本地时间戳 T_s 验证 $T_s - t_{s,V} < \Delta T$ 是否符合要求，确认消息即时性。验证通过后，根据消息内容计算 J，检验消息完整性。根据消息内容计算 $p = V\oplus h(E\|R)$，由 p 检索区块链内容 $PID = h(VID)\oplus r$，进而获取 $h(VID) = PID\oplus r$。使用车辆匿名身份 $FID = h(h(VID)\|E_r)$，对比消息中的车辆匿名身份是否一致。若一致表明验证通过，头车生成随机数 i，计算会话密钥 $K_g = h(i\cdot E)$，生成当前时间戳 $t_{s,h}$，计算消息完整参数 $\begin{cases} Z = H(FID',I,t_{s,h}) \\ I = i\cdot P \end{cases}$，组包消息 $\begin{cases} M_{a6} = \{FID',I,Z,t_{s,h}\} \\ FID' = h(h(VID)\|I\cdot E) \end{cases}$ 发送至成员车。

c. 成员车接收消息 M_{a6} 后，生成本地时间戳 T_s 验证 $T_s - t_{s,h} < \Delta T$ 是否符合要求，确认消息及时性。验证通过后，根据消息内容计算 Z 检验消息完整性。根据消息中 I 以及自身随机数 e 计算 $FID' = h(h(VID)\|I\cdot E)$ 对比消息中 FID'，一致表明头车身份可信，进而计算会话密钥 $K_g = h(I\cdot e)$，用于向头车申请代理云服务等。

4 安全性分析

4.1 BAN逻辑推理规则

采用BAN（Burrows-Abadi-Needham）认证逻辑分析方法证明本文方案的安全性[21-22]，该方法通过对协议中的消息传递、信任关系以及消息含义的细致分析，揭示协议中可能存在的安全漏洞，抵御各种潜在的安全威胁。相关的公式符号及含义如表2所示。

表2 公式符号定义

符号	含义
$P\|\equiv X$	P 相信消息 X 为真
$P\lhd X$	P 收到消息 X
$P\sim X$	P 曾发送消息 X
$P\|\Rightarrow X$	P 对 X 有管辖权
$P\xleftrightarrow{K}Q$	K 为 P 和 Q 间的共享密钥
$\#(X)$	X 具有即时性
$\{X\}_K$	密钥 K 加密 X 后的密文
$P\xleftrightarrow{X}Q$	X 为 P 和 Q 的共享秘密

本文使用的BAN逻辑推理规则主要包括：

a. 消息含义规则：主体 P 收到用密钥 K 加密的消息 X，且 P 相信 K 为 P 和 Q 间的共享密钥，则 P 相信 Q 曾经发送过包含 X 的消息。可定义为：

$$\frac{P|\equiv Q\xleftrightarrow{K}P,P\lhd\{X\}_K}{P|\equiv Q\sim X} \tag{1}$$

b. 临时值验证规则：主体 P 相信 X 是即时的，且 P 相信 Q 曾发送过包含 X 的消息，则 P 相信 Q 相信 X 是为真。可定义为：

$$\frac{P|\equiv \#(X),P|\equiv Q|\sim X}{P|\equiv Q\equiv X} \tag{2}$$

c. 管辖规则：主体 P 相信 Q 相信 X 为真，且 P 相信 Q 对 X 有管辖权，则 P 相信 X 为真。可定义为：

$$\frac{P|\equiv Q|\Rightarrow X,P|\equiv Q\equiv X}{P|\equiv X} \tag{3}$$

d. 接收消息规则：主体 P 相信 K 为 P 和 Q 间的共享密钥，且 P 接收到使用密钥 K 加密 X 的密文，则 P 接收到 X。可定义为：

$$\frac{P|\equiv Q\xleftrightarrow{K}P,P\lhd\{X\}_K}{P\lhd X} \tag{4}$$

e. 消息即时性规则：主体 P 相信 K 是即时的，则 P 相信包含 X 的消息也是即时的。可表达为：

$$\frac{P|\equiv \#(X)}{P|\equiv \#(X,Y)} \tag{5}$$

4.2 安全证明目标和假设

根据车列协同方案，安全证明的目标为：

$$Q|\equiv Q\xleftrightarrow{HID}H \tag{6}$$

$$Q|\equiv Q\xleftrightarrow{C}P \tag{7}$$

$$P|\equiv P\xleftrightarrow{HID}H \tag{8}$$

$$P|\equiv P\xleftrightarrow{C}Q \tag{9}$$

$$H|\equiv H\xleftrightarrow{K}P \tag{10}$$

$$V|\equiv V\xleftrightarrow{K_g}H \tag{11}$$

式中：Q 为QSC，P 为CSP，H 为头车，V 为成员车。

安全假设是方案自身设计所隐含的预设可信条件，是开展安全性形式化证明的必要前提，为BAN逻辑的推理提供基础支撑。PQK 为头车预先充注的密钥，所以 PQK 为头车与QSC间的共享密钥：

$$H|\equiv H\xleftrightarrow{PQK}Q \tag{12}$$

随机数 a 和 n 均由各自量子随机数发生器生成，且具备真随机性，所以QSC认为头车和CSP对随机数具有管辖权：

$$\begin{cases} Q|\equiv H\Rightarrow a \\ Q|\equiv P\Rightarrow n \end{cases} \tag{13}$$

QR由BB84协议协商获得,因量子态具有不可克隆性,为了保障QR的安全性,所以QR为P和Q共享的密码值:

$$P| \equiv P \overset{QR}{\longleftrightarrow} Q \tag{14}$$

随机数e和i均由各自的量子随机数发生器生成,且具备真随机性,因此,头车和成员车认为双方对随机数具有管辖权:

$$\begin{cases} H| \equiv V \Rightarrow e \\ V| \equiv H \Rightarrow i \end{cases} \tag{15}$$

4.3 安全证明

车列协同认证方案中,各主体在不同认证阶段的消息收发行为记录,是开展方案安全属性验证的核心前置条件,其与认证流程各环节的主体交互逻辑形成精准对应关系:

a. 条件1:$Q \lhd \{HID, PQK_{\text{tag}}, S, L, t_{s,h}\}$,头车向QSC发送认证消息。

b. 条件2:$P \lhd \{HID, D, W, Y, t_{s,Q}\}$,QSC向CSP发送认证消息。

c. 条件3:$Q \lhd \{C, U, O, t_{s,C}\}$,CSP返回QSC认证消息。

d. 条件4:$H \lhd \{HID, E_{\text{AK}}(QR), G, t_{s,Q}\}$,QSC向头车发送认证消息。

e. 条件5:$H \lhd \{FID, E, V, J, t_{s,V}\}$,成员车向头车发送认证消息。

f. 条件6:$V \lhd \{FID', I, Y, t_{s,h}\}$,头车返回成员车认证消息。

根据条件1和式(1)、式(4)、式(5),如果$t_{s,h}$被验证是即时的,可得:$\begin{cases} Q \lhd \{E_{\text{PQK}}(UPW, A \oplus a)\} \\ Q| \equiv H| \sim (a) \\ Q| \equiv \#(a) \end{cases}$。由式(2)、式(12)、式(13)可得$Q| \equiv H \equiv (a)$,因$HID$由$a$生成,进而推导出式(6)。

根据条件2和式(1)、式(4)、式(5),如果$t_{s,Q}$被验证是即时的可得:$\begin{cases} P \lhd \{E_{\text{NK}}(h(CID \| n) \oplus m), W\} \\ P| \equiv Q| \equiv H| \sim (a), P| \equiv Q| \sim W \\ P| \equiv \#(a), P| \equiv \#(W) \end{cases}$。由式(2)、式(3)、式(13)可得$P| \equiv H \equiv (a)$,因$W$由$C$、$HID$和$a$生成,进而推导出式(8)~式(9)。

根据条件3和式(1)、式(4)、式(5),如果$t_{s,Q}$被验证是即时的,可得:$\begin{cases} Q \lhd \{E_{\text{MK}}(h(CID \| m) \oplus b)\} \\ Q| \equiv P| \sim (U) \\ Q| \equiv \#(U) \end{cases}$,由式(13)可推导出式(7)。

根据条件4和5和式(1)、式(4)、式(5),如果$t_{s,h}$被验证是即时的,可得:$\begin{cases} H \lhd \{E_{\text{AK}}(QR)\} \\ H| \equiv Q| \sim (QR) \\ H| \equiv \#(QR) \end{cases}$,由式(2)、式(14)可得$H| \equiv P| \equiv (QR)$,进而推导出式(10)。

根据条件6和式(1)、式(4)、式(5),如果$t_{s,h}$被验证是即时的,可得:$\begin{cases} V \lhd \{FID', I\} \\ V| \equiv H| \sim (FID', I) \\ V| \equiv \#(I) \end{cases}$,由式(3)、式(15)可得$V| \equiv H| \equiv (i)$,进而推导出式(11)。

基于BAN逻辑规则,严格证明了QSC与CSP、CSP与头车及头车与成员车间的匿名双向认证与会话密钥协商。头车与CSP通过云端量子随机数QR与车端随机数a,建立的会话密钥K具备即时性和机密性。头车与成员车间的密钥协商基于双方各自生成的量子随机数e和i,保证了会话密钥K_g的不可预测性和抗伪造性。通过BAN逻辑的形式化分析,本方案在满足理想信道假设的条件下,能够实现双向认证、前后向安全性,为多云车联网环境提供了理论可证的安全保障。

5 性能分析

5.1 计算开销

为了准确评估车联网通信系统中关键计算操作的性能开销,本文基于Qt 5.13框架构建测试环境。试验平台采用Intel Core i7-10750H处理器(6核12线程,基准频率2.60 GHz),搭配64位Ubuntu 20.04长期支持(Long Term Support,LTS)操作系统,禁用非必要后台进程以降低系统干扰。在测试方案中,各实体间的认证及密钥协商过程中涉及的密码学计算开销,主要包括椭圆曲线运算、哈希计算、对称加密/解密等核心操作。针对每种目标操作执行10万次循环计算,取算术平均值作为最终结果。各计算操作的符号定义及平均耗时测试结果,如表3所示。

表3 操作符号定义和耗时 μs

符号	含义	耗时
T_{ecc}	椭圆曲线点乘	352.219
T_{eca}	椭圆曲线点加	0.111
T_{bp}	双线性配对	3 353.557
T_{enc}	对称加密	4.117
T_{dec}	对称解密	4.088
T_{aenc}	非对称加密	63.542
T_{adec}	非对称解密	31.300
T_{h}	256位哈希计算	1.461

本文选取3种典型的车联网通信方案进行对比分析，各方案的服务端均为云端，中继端的类型不同（文献[13]~[14]以无人机为中继，文献[16]以量子云服务器为中继，本文方案以头车为中继），各方案的计算开销如表4所示。本文方案的车端开销低于其他方案，能够有效减少本地算力；中继端开销与文献[14]基本持平，兼顾中继效率；服务端开销远低于同类方案，大幅减轻云端负载。

表4　不同方案各端计算开销　　μs

方案	车端	代理端	服务端
文献[13]	$3T_{ecc}+6T_h+T_{eca}\approx$ 1 066.995	$3T_{ecc}+4T_h\approx$ 1 062.501	$4T_{ecc}+8T_h+T_{enc}+T_{dec}\approx$1 428.769
文献[14]	$3T_{ecc}+7T_h+T_{enc}\approx$ 1 071.001	$2T_{ecc}+6T_h+2T_{enc}\approx$ 721.438	$T_{ecc}+9T_h+3T_{dec}\approx$ 377.632
文献[16]	$3T_{ecc}+8T_h\approx$ 1 068.345	$3T_{ecc}+7T_h\approx$ 1 066.884	$3T_{ecc}+10T_h\approx$ 1 071.267
本文	$2T_{ecc}+5T_h\approx$ 711.743	$2T_{ecc}+8T_h+T_{enc}+T_{dec}\approx$720.243	$17T_h+4T_{enc}+4T_{dec}\approx$57.657

将云端认证的车辆从10辆逐步增加至50辆，结果如图4所示。本文方案通过代理车辆与云端的一次认证，简化成员车辆与云端的认证流程，表现出最优的计算效率，其开销较次优方案（文献[14]）在10辆和50辆规模下，分别降低33.14%和32.96%，更适合高密度车联网环境的应用需求。

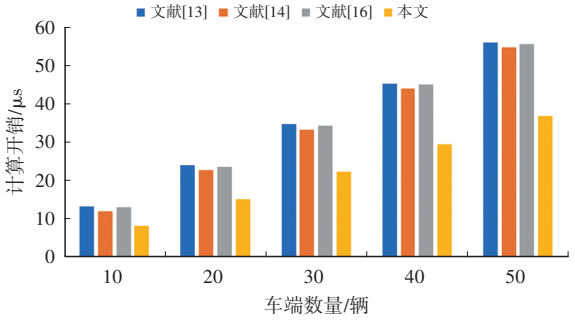


图4　不同方案计算开销对比

5.2　通信开销

针对本文所提协议与现有同类协议的通信开销进行对比分析。根据文献[14]的参数设定，定义群G单个点的长度为40 B。假定身份标识信息、哈希函数输出、随机数、对称加解密操作和时间戳的输出长度分别为20 B、20 B、20 B、16 B和4 B。通信开销对比试验结果显示：文献[13]、文献[14]、文献[16]和本方案开销分别为484 B、304 B、416 B和412 B。其中，本文方案在保证系统安全性的前提下，通信开销显著优于文献[13]（降低14.9%）。综合考虑安全认证机制和系统可靠性要求，本文方案实现了通信效率与安全性能的良好平衡，在控制通信负载的同时确保了严格的安全保障。

6　结束语

本文提出了一种基于量子密钥分发与区块链技术的车联网多云架构，有效解决了双向匿名认证隐私泄露、认证效率不足以及单一云服务资源受限等关键问题。通过将QSC的量子密钥管理和头车作为云服务代理，不仅实现了车辆在多云环境下的无缝切换与负载均衡，还增强了通信的安全性与隐私保护。同时，动态匿名认证机制与高效的认证管理策略显著提升了系统的整体性能。通过与其他相关方案进行对比，本文方案在安全性、计算开销和通信开销等关键指标上均取得明显提升，验证了方案设计的有效性。

参　考　文　献

[1] OLADIMEJI D, GUPTA K, KOSE N A, et al. Smart Transportation: An Overview of Technologies and Applications[J]. Sensors, 2023, 23(8).

[2] LIN I, CHENG C, CHEN H. A Real-Time Parking Service with Proxy Re-Encryption in Vehicular Cloud Computing[J]. Engineering Applications of Artificial Intelligence, 2019, 85: 208-213.

[3] BAGGA P, DAS A K, WAZID M, et al. On the Design of Mutual Authentication and Key Agreement Protocol in Internet of Vehicles-Enabled Intelligent Transportation System[J]. IEEE Transactions on Vehicular Technology, 2021, 70(2): 1736-1751.

[4] 石琴, 朱俊杰, 程腾, 等. 基于车端量子密钥的车联网数据访问控制研究[J]. 汽车技术, 2023(10): 24-31.
SHI Q, ZHU J J, CHENG T, et al. Research on Data Access Control in Internet of Vehicles Based on Vehicle-Side Quantum Key[J]. Automobile Technology, 2023(10): 24-31.

[5] YANG Z, SHI Q, CHENG T, et al. A Security-Enhanced Authentication Scheme for Quantum-Key-Distribution (QKD) Enabled Internet of Vehicles in Multi-Cloud Environment[J]. Vehicular Communications, 2024, 48.

[6] 赵宗渠, 王瀚博, 李英, 等. 车联网中格上基于身份的隐私保护协议[J]. 重庆邮电大学学报（自然科学版）, 2024, 36(1): 49-58.
ZHAO Z Q, WANG H B, LI Y, et al. Identity Based Privacy Protection Protocol in the Internet of Vehicles[J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2024, 36(1): 49-58.

[7] 况博裕, 李雨泽, 顾芳铭, 等. 车联网安全研究综述: 威胁、对策与未来展望[J]. 计算机研究与发展, 2023, 60(10): 2304-2321.
KUANG B Y, LI Y Z, GU F M, et al. Review of Research on Internet of Vehicles Security: Threats, Countermeasures, and Future Prospects[J]. Journal of Computer Research and

Development, 2023, 60(10): 2304-2321.

[8] 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.

[9] 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. Lightweight Identity Authentication Scheme for Quantum-Encrypted Vehicle-Cloud Communication Architecture[J]. Automobile Technology, 2023(10): 9-15.

[10] MAURYA C, CHAURASIYA V K. Efficient Anonymous Batch Authentication Scheme with Conditional Privacy in the Internet of Vehicles (IoV) Applications[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(9): 9670-9683.

[11] 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 Z G, et al. Certificateless Anonymous Authentication Scheme Supporting Llegal Signatures Localization for Internet of Vehicles[J]. Computer Engineering, 2024, 50(6): 157-165.

[12] JIANG Q, ZHANG X, ZHANG N, et al. Three-Factor Authentication Protocol Using Physical Unclonable Function for IoV[J]. Computer Communications, 2021, 173: 45-55.

[13] MIAO J F, WANG Z S, NIGN X, et al. A UAV-Assisted Authentication Protocol for Internet of Vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2024, 25(8): 10286-10297.

[14] ZHANG J, CUI J, ZHONG H, et al. Intelligent Drone-Assisted Anonymous Authentication and Key Agreement for 5G/B5G Vehicular Ad-Hoc Networks[J]. IEEE Transactions on Network Science and Engineering, 2020, 8(4): 2982-2994.

[15] YANG Z, SHI Q ,CHENG T, et al. A Security-Enhanced Authentication Scheme for Quantum-Key-Distribution (QKD) Enabled Internet of Vehicles in Multi-Cloud Environment[J], Vehicular Communications, 2024, 48: 100789-100789.

[16] CHENG T, WU Z X, WANG C S, et al. Research on Vehicle-to-Cloud Communication Based on Lightweight Authentication and Extended Quantum Key Distribution[J]. IEEE Transactions on Vehicular Technology, 2024, 73(8): 12082-12095.

[17] ZHANG L, MENG X Y, CHOO K R, et al. Privacy-Preserving Cloud Establishment and Data Dissemination Scheme for Vehicular Cloud[J]. IEEE Transactions on Dependable and Secure Computing, 2020, 17(3): 634-647.

[18] 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, 2019, 15: 1654-1667.

[19] TERMOS H. Quantum Authentication Evolution: Novel Approaches for Securing Quantum Key Distribution[J], Entropy, 2024, 26(6).

[20] DJAOUIDA B, ALI S. Theoretical and Simulation Investigation of Practical QKD for Both BB84 and SARG04 Protocols[J], International Journal of Quantum Information, 2024, 22(4).

[21] PATIL R Y, DEVANE S R. Formal Verification of Secure Evidence Collection Protocol Using BAN Logic and AVISPA[J]. Procedia Computer Science, 2020, 167: 1334-1344.

[22] CHENG T, LIU Q, SHI Q, et al. Efficient Anonymous Authentication and Group Key Distribution Scheme Based on Quantum Random Numbers for Vanets[J]. IEEE Internet of Things Journal, 2024, 11(13): 23544-23560.

（责任编辑　瑞　秋）

修改稿收到日期为2025年8月13日。