·车联网量子加密通信技术专题·

基于车端量子密钥的车联网数据访问控制研究*

石琴[1] 朱俊杰[1] 程腾[1] 杨泽[2] 王川宿[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】为实现车联网相关数据的安全传输和隐私保护，提出了一种基于车端量子密钥的车联网数据访问控制方案。设计了基于预充注量子密钥的身份认证和密钥协商机制，提出了基于量子随机数发生器的车辆数据访问控制方案，在车载通信终端集成量子随机数发生器以生成量子加密密钥，并由车辆所有者对来自外部设备的车联网数据访问请求进行管控，以防止非授权访问、高权限人员恶意侵入和车辆隐私数据的不当开放。最后，对提出的方案进行了安全性和性能分析，结果表明，该方案具有较强的安全性，具有比其他主要方案更小的计算开销（0.395 ms）和通信开销（420 B）。

主题词：身份认证 访问控制 量子保密通信 车辆自组网

中图分类号：U495；TP309 **文献标识码：**A **DOI:** 10.19620/j.cnki.1000-3703.20230426

Research on Data Access Control for Vehicular Networks Based on Vehicle Terminal Quantum Key

Shi Qin[1], Zhu Junjie[1], Cheng Teng[1], Yang Ze[2], Wang Chuansu[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】 To realize secure transmission of vehicular network related data and privacy protection, this article proposed a quantum key based identity authentication and data access control scheme for the vehicular networks. An identity authentication scheme and key agreement mechanism based on pre-charge quantum keys were designed, vehicle data access control scheme based on quantum random number generator was proposed to generate quantum encryption keys, allowing the vehicle owner to control access requests for vehicle networking data from external devices to prevent unauthorized access, malicious intrusion by high-privileged personnel and improper opening of vehicle privacy data. Finally, this article conducted security and performance analysis, analysis results show that this scheme has good security, with a computational cost of 0.395 ms and a communication cost of 420 B, which are lower than that of other schemes.

Key words: Authentication, Access control, Quantum secure communication, Vehicular network

【引用格式】 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 for Vehicular Networks Based on Vehicle Terminal Quantum Key[J]. Automobile Technology, 2023(10): 24-31.

1 前言

随着智能网联汽车的快速发展，车辆所产生的数据量越来越丰富[1]，这些数据不仅涉及车辆信息，也包括车辆所有者的私人敏感信息[2]。因此，车辆面临着私人信息未经车辆所有者授权而被不当开放的威胁[3]。为此，

*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。

车辆数据的安全传输和云存储数据的限制性访问需要得到重视。

在数据传输过程中，攻击者可能通过对传输的消息进行修改、模仿或重放等手段威胁通信安全[4]；在访问控制方面，车辆敏感信息可能受到未经授权的访问[5]。因此，身份认证和密钥协商机制是车联网信息安全中重要的一环[6]。现有的车辆安全通信方案大多通过有条件的身份认证来识别未经授权的数据访问[7-9]。这些方案虽然可以在一定程度上保护车辆数据在传输过程中不会受到未经批准的访问，但并未考虑数据在云端存储后的隐私数据访问限制与管控。

随着量子计算研究的不断深入，大型量子计算机一旦出现，许多常用的密码系统将被快速破解，当前的加密方案面临着严峻的挑战[4]，车联网的通信安全也将受到威胁[10]。量子保密通信是在抗量子计算攻击的特定需求下的全新的、有效的密码学补充手段[11]。常见的是量子密钥分发（Quantum Key Distribution，QKD）与其他能够抵抗量子计算攻击的对称密钥加密算法结合使用，从而形成安全的量子保密通信系统[12]。

针对车联网数据在传输和存储过程中面临的攻击者恶意侵入与非授权访问的问题，本文提出一种基于车端量子密钥的车联网数据访问控制方案，包括基于预充注量子密钥的身份认证和密钥协商机制，以及基于量子随机数发生器的车辆数据访问控制方案，通过在车载通信终端集成量子随机数发生器生成量子加密密钥，由车辆所有者管理外部访问者对车辆隐私数据的访问请求，防止非授权访问和高权限人员的恶意侵入。方案融合了量子密钥进行加密通信，可应对以量子计算为代表的超能力计算机的威胁。最后对方案与其他主要研究方案进行安全性与性能对比分析。

2　系统架构

本文系统的通信架构如图1所示，包括集成量子随机数发生器（Quantum Random Number Generator，QRNG）的车载通信终端（Telematics BOX，T-BOX）、量子密服平台（Quantum Security Server，QSS）、车辆信息服务提供平台（Telematics Service Provider，TSP）、车辆电子控制单元（Electronic Control Unit，ECU）、车辆所有者（Owner）、访问者（Visitor）。

T-BOX负责接收车辆数据M_{Data}，并将其加密生成密文（C_{Data}）上传到TSP。T-BOX可以与QSS进行通信完成量子会话的密钥加密密钥（Key Encryption Key，KEK）生成，即会话密钥的协商，并通过预充注量子密钥（Pre-Fill quantum Key，PFK）保护KEK的安全传输。T-BOX通过集成的QRNG提取内容加密密钥（Contents Encryption Key，CEK），并加密车辆数据。T-BOX使用KEK对CEK进行加密获得加密会话密钥（Keyed CEK，KCEK）。最后，根据车辆所有者授权的指令将KCEK分发到TSP。

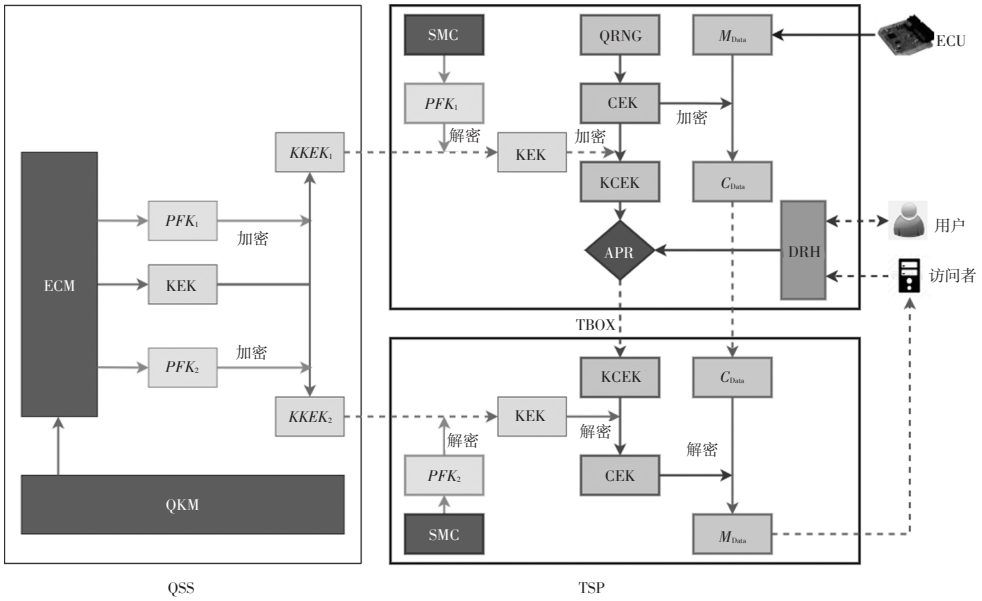

图1　系统通信架构

TSP的安全存储芯片（Secure Memory Chip，SMC）中存有大量预充注量子密钥PFK。TSP接收到QSS分发的KCEK后，从SMC中取出对应的PFK，解密后得到会话密钥KEK。当TSP收到T-BOX发送的KCEK后，用KEK解密得到量子加密密钥CEK，并使用CEK将车辆数据密文（C_{Data}）解密生成车辆明文数据（M_{Data}）发送给访问者。TSP以有线方式连接到互联网，为车辆提供各种网络接入服务。

QSS存储所有注册T-BOX和TSP平台的信息，从而能够对T-BOX和TSP的身份合法性进行认证。QSS还集成了量子密钥分发系统（Quantum Key Distribution，QKM）和电子密码机（Electronic Code Machine，ECM）。ECM从QKM获取量子随机数，生成PFK和KEK。QSS负责将KEK分发到T-BOX和TSP。

访问者意图读取车辆隐私数据，并发送数据请求到TSP。车辆所有者接收TSP转发的车辆数据读取请求，完成车辆隐私数据读取的授权。

3 系统工作流程

本文方案包括注册阶段、身份认证和密钥协商阶段、数据访问控制阶段，相关协议参数定义如表1所示。

表1 协议参数及其定义

符号	定义
SN	T-BOX序列号
$ICCID$	T-BOX集成电路卡标识
TID	TSP的真实ID
VID,NID	T-BOX和TSP的假名
PFK	预充注量子密钥
KEK_i	第i次会话的会话密钥
$KKEK_i$	第i次会话密钥的加密结果
CEK_i	第i次会话的内容加密密钥
$KCEK_i$	第i次内容加密密钥的加密结果
CTR_i	加密会话计数器的值
$Req,VInf$	访问请求、请求者信息
TR_i,TS_i	消息收、发时间戳
TS_{ij}	会话密钥失效时间
$E_k(\ )/D_k(\ )$	使用密钥k对称加解密操作
h	单向哈希函数
$H,S_i,V_i,W_i,X_i,Y_i,Z_i$	哈希结果
m	消息内容

3.1 注册阶段

注册阶段由QSS、T-BOX、TSP在可信环境下进行。QSS负责管理所有注册体的身份信息。T-BOX在交付前，由TSP后台将T-BOX的数据（SN、$ICCID$）录入数据库并在平台上完成T-BOX的注册。注册阶段需要TSP和T-BOX在QSS处注册。本文方案中的T-BOX、TSP均安装了SMC。整车生产线上使用量子密钥预充注设备对T-BOX的安全芯片进行密钥充注；TSP后台的SMC预充注量子密钥。QSS中记录了所有预充注量子密钥信息。

TSP需要提前在QSS进行注册，注册流程如下：

a. TSP选取唯一的TID，计算$h(TID)$并将结果组包消息$m_{R1}=\{h(TID)\}$发送到QSS。

b. QSS收到消息m_{R1}后，首先，从ECM中随机提取预充注量子密钥PFK_T用于生成TSP的注册信息。然后，验证$h(TID)$是否已经注册，若没有注册，计算$NID=h(h(TID)||PFK_T)$，并记录NID。组包消息$m_{R2}=\{NID\oplus PFK_T\}$，发送到TSP。

c. TSP收到消息m_{R2}后，从SMC中提取预充注量子密钥PFK_T^*，计算$NID=(NID\oplus PFK_T)\oplus PFK_T^*$，最后TSP存储注册信息。

同理，如果车辆终端意图加入车联网使用某些服务提供商提供的某些服务，需要提前向QSS注册，执行以下步骤：

a. T-BOX提取内存中的SN、$ICCID$，并计算$h(SN||ICCID)$，然后组包消息$m_{R4}=\{h(SN||ICCID)\}$，发送到QSS。

b. QSS收到消息m_{R4}后，首先从ECM中提取PFK_V，然后检索$h(SN||ICCID)$是否已经注册，若没有注册，生成新的用户信息$VID=h(h(SN||ICCID)||PFK_V)$，将$VID$记录到注册表中，最后，组包消息$m_{R5}=\{VID\oplus PFK_V\}$，发送到T-BOX。

c. T-BOX收到消息m_{R5}后，从SMC提取出PFK_V，计算$VID=(VID\oplus PFK_V)\oplus PFK_V^*$。最后，T-BOX存储注册信息。

3.2 身份认证和密钥协商阶段

如图2所示，身份认证和密钥协商流程为：

a. T-BOX向QSS发起身份认证，计算$Q_i=h(PFK_V\oplus VID)$，生成时间戳t_{Si}，并组包消息m_{A1}发送到QSS：

$$m_{A1}=\{Q_i,h(Q_i||t_{Si}),t_{Si}\} \tag{1}$$

b. QSS接收到m_{A1}后，生成时间戳t_{Ri}。定义超时时间Δt，通过计算$t_{Ri}-t_{Si}<\Delta t$检验消息的有效性；通过计算对比$h(Q_i^*||t_{Si}^*)=h(Q_i||t_{Si})$校验消息的完整性，若消息不匹配，则退出会话。然后，计算T-BOX的身份信息$VID^*=Q_i\oplus h(PFK_V)$并验证其合法性。随机选择新的预充注密钥PFK_{Vi}，计算加密后的会话密钥$KKEK_{Vi}=E_{PFK_{Vi}}(KEK_i)\oplus VID^*$。接着，计算哈希值$R_i=h(KKEK_{Vi}||PFK_{Vi}||t_{Si})$，其中$t_{Si}$为当前发送消息的时间戳。最后，组包消息$m_{A2}$到T-BOX：

$$m_{A2}=\{KKEK_{Vi},R_i,t_{Si}\} \tag{2}$$

c. T-BOX收到m_{A2}的同时产生时间戳t_{Ri}，通过计算$t_{Ri}-t_{Si}<\Delta t$检验消息时效性。然后，通过校验$h(KKEK_{Vi}^*||PFK_{Vi}||t_{Si})=R_i$检查完整性，其中$KKEK_{Vi}^*$为从

m_{A2}中解析或计算获得的加密后的会话密钥。最后，通过SM4解密算法计算QSS分发的会话密钥$KEK_i^*=D_{PFK_{Vi}}(KKEK_{Vi}\oplus VID)$。计算$W_i=h(SN\|ICCID)\oplus KEK_i^*$后，组包消息$m_{A3}$发送到QSS：

$$m_{A3}=\{W_i,h(W_i\|KEK_i^*)\} \tag{3}$$

d. QSS提取m_{A3}的消息内容，并通过计算$h(W_i^*\|KEK_j)=h(W_i\|KEK_i^*)$检验消息的完整性，其中$W_i^*$为从$m_{A3}$中解析或计算获得的哈希结果。若消息完整，则计算$S_i=h(PFK_{Ti})\oplus NID$用于验证TSP的身份，其中$PFK_{Ti}$为从QSS本地存储的预充注量子密钥随机取出的密钥。计算$KKEK_{Ti}=E_{PFK_{Ti}}(KEK_i)\oplus NID$进行量子保护密钥的分发，并组包消息$m_{A4}$发送到TSP：

$$m_{A4}=\{KKEK_{Ti},S_i,W_i,t_{Si}\} \tag{4}$$

e. TSP提取消息m_{A4}的内容。首先，TSP验证等式$S_i\oplus h(PFK_{Ti})=NID$是否成立，若成立，则表明QSS是受信任的平台。然后，通过解密计算得到$KEK_i^*=D_{PFK_{Ti}}(KKEK_{Ti}\oplus VID)$并存储。接着，TSP计算$h(SN\|ICCID)^*=W_i^*\oplus KEK_i^*$，并从注册信息中提取T-BOX的序列号和集成电路卡标识SN^*、$ICCID^*$验证T-BOX的身份信息，$h(SN\|ICCID)=h(SN\|ICCID)^*$，若验证通过，计算$V_i=h(KEK_i^*\|SN^*\|ICCID^*\|t_{Si})$，并组包消息$m_{A5}$发送到T-BOX：

$$m_{A5}=\{V_i\} \tag{5}$$

f. T-BOX收到m_{A5}后，通过计算$t_{Ri}-t_{Si}<\Delta t$验证消息的时效性。然后，计算$V_i^*=h(KEK_i^*\|SN\|ICCID\|t_{Si})$并验证等式$V_i^*=V_i$，若等式成立，则T-BOX、QSS、TSP间完成了身份认证。

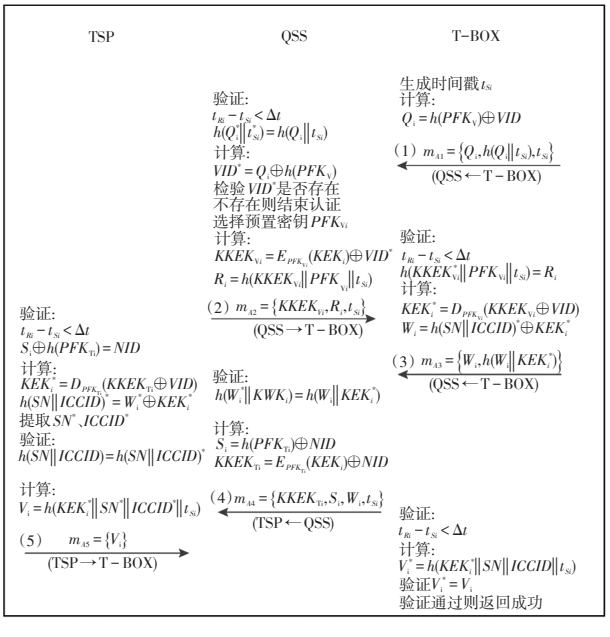

图2　身份认证和密钥协商流程

3.3　数据访问控制阶段

如果访问者意图获取车辆信息，需要生成请求信息$VInf$，等待车辆所有者授权，只有获得授权后，T-BOX才会将量子加密密钥的加密结果$KCEK_i$发送到TSP，TSP解密后最终得到数据明文M_{Data}，数据访问控制流程如图3所示：

a. T-BOX向QRNG获取16 B（本方案中的CEK长度为16 B）的量子随机数QR作为量子加密密钥CEK_i，$CEK_i=Str_{16}(QR)$，用CEK_i对车辆数据进行加密，$C_{Data}=E_{CEK_i}(M_{Data}\oplus CTR_i)$。$CTR_i$为加密会话的计数器，防止密钥与其加密密钥泄露时攻击者伪造数据。然后，通过T-BOX与QSS协商的量子会话密钥密钥KEK_i加密量子加密密钥CEK_i，$KCEK_i=E_{KEK_i}(CEK_i)\oplus CTR_i$。$KCEK_i$为加密后的密钥。最后，生成消息$m_{k1}$，并发送到TSP：

$$m_{k1}=\{C_{Data}\} \tag{6}$$

b. TSP接收T-BOX发送的m_{k1}，提取密文数据C_{Data}，并进行存储。

c. T-BOX内部的数据访问处理模块（Data Request Handler，DRH）根据访问者的，生成访问请求者的信息$VInf$。T-BOX将消息组包发送m_{k2}到车辆所有者：

$$m_{k2}=\{Req,VInf\} \tag{7}$$

d. 车辆所有者根据T-BOX发送的$VInf$，对访问者的请求进行授权，提供请求通过信息（Approval，APR）。同时，车辆所有者设定本次授权的有效时长TS_i，计算$Y_i=h(APR\|TS_i\|t_{Ui})$，其中t_{Ui}为车辆所有者进行授权操作的时间戳。消息组包m_{k3}发送并到T-BOX：

$$m_{k3}=\{APR\|TS_i\|t_{Ui},Y_i\} \tag{8}$$

e. T-BOX接收到车辆所有者对数据读取请求的授权后，判断授权操作是否超时$TS_j-t_{Ui}\leqslant\Delta t$与$h(APR\|TS_i\|t_{Ui})=Y_i$是否成立，其中$TS_j$为T-BOX接收到消息$m_{k4}$的时间戳。如满足，检查车辆所有者是否授权访问者的访问请求，若未授权则退出当前会话。然后，计算用户授权的失效时间$TS_{ij}=TS_i^*+TS_j$，生成摘要$Z_i=h(KCEK_i\|CTR_i\|TS_{ij})$。最后，组包消息$m_{K4}$，发送消息TSP：

$$m_{K4}=\{KCEK_i,CTR_i,Z_i\} \tag{9}$$

f. TSP收到来自T-BOX的m_{K4}后，先计算$Z_i^*=h(KCEK_i\|CTR_i\|TS_{ij})$，验证条件$Z_i^*=Z_i$是否成立，若不成立，说明消息内容不准确，结束会话，验证通过后，TSP计算出量子加密密钥$CEK_i=D_{KEK_i}(KCEK_i\oplus CTR_i)$。最后，通过计算$M_{Data}=D_{CEK_i}(C_{Data}\oplus CTR_i)$得到解密后的车辆数据明文$M_{Data}$，通过安全通信通道发送给访问者。

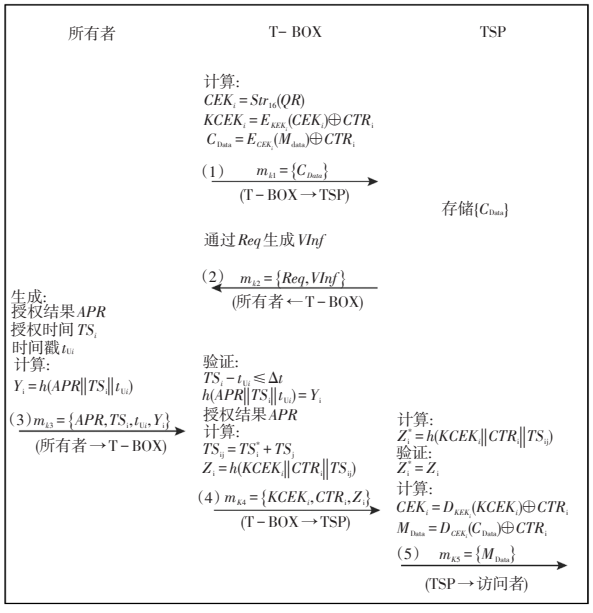

图3　数据访问控制流程

4　安全性分析

本文使用真实或随机（Real Or Random，ROR）模型进行形式化分析，验证所提出的方案中会话密钥的安全性。基于ROR模型的会话密钥的安全性证明已经用于多个研究者提出的认证协议[13-15]。同时，分析本文方案可以抵御的典型的攻击。

4.1　安全模型

假设本文方案中身份认证和密钥协商协议有V_i（T-BOX）、QSS、TSP 3种类型的实体，这些实体包含了多个实例并能够同时进行身份认证。每一个实例都能视为一个独立的预言机。预言机的状态有3种：接受（Accept），预言机接收到正确的信息；拒绝（Reject），预言机接收到错误信息；空（⊥），预言机输出为空。设V_i^a为车辆i的第a个实例，TSP^b、QSS^c分别为TSP的第b个实例和QSS的第c个实例。V_i^a状态变为接受后，V_i^a和TSP^b之间协商获得相同的会话密钥。但是，车辆所有者和访问者对会话密钥的安全不产生影响。同时，他们不参与加密操作，也不存储任何有效信息，故不考虑车辆所有者和访问者。

定义攻击者A可以执行以下查询来分析得到会话密钥：

a. Execute(V_i^a，TSP^b，QSS^c)：此查询为窃听模式。攻击者A通过执行此查询能够获得V_i^a、TSP^b、QSS^c间的所有信息$\{m_{A1}, m_{A2}, m_{A3}, m_{A4}, m_{A5}\}$。

b. Send(V_i^a，TSP^b)：此查询为主动攻击。如果攻击者A意图拦截并修改V_i^a发出的消息，A需要执行此查询。

c. Reveal(V_i^a)：当攻击者A执行此查询时，V_i^a会将会话密钥CEK发送给A。

d. Test(V_i^a)：此查询模拟会话密钥的语义安全性。在游戏开始前，将硬币翻转，并且只有A了解硬币的值d，这个值决定了此预言机的输出。如果A执行此查询并建立了新的会话密钥：当d=1时，Test返回正确的会话密钥；当d=0时，Test输出随机值，否则输出为空（⊥）。

e. Corrupt(V_i^a，TSP^b)：通过执行该查询，攻击者A可以获得存储在注册的参与者实例V_i^a、TSP^b的SMC中的所有秘密参数。

定理：设A是针对本方案在多项式时间t内运行的攻击者，若A不能以可忽略的优势$Adv^A(t)$成功攻击本方案，那么提出的方案是安全的。设q_s、q_e、q_h和q_{h1}分别表示发送查询、执行查询、h查询和h1查询的数量，$|H|$、$|H_1|$分别表示哈希值的范围空间，A在破解会话密钥安全性方面的优势可以估计为：

$$Adv^A(t) \le \frac{q_h^2}{|H|} + \frac{q_{h_1}^2}{|H_1|} + \frac{(q_s+q_e)^2+q_s}{2^{L-1}} + \max\left\{\frac{q_s}{2^{2L-1}}, \frac{q_s}{2^{2L_c-1}}\right\} \quad (10)$$

式中，L为密钥长度；L_c为计数器的最大长度。

通过5个连续的博弈（Gm_0~Gm_4）来证明方案的安全性。$\Pr[Suc^A_{Gm_i}]$用来表示在博弈Gm_i中，A猜测了$d'=d$。定义攻击者A在博弈Gm_i中的获胜优势$\Pr[Suc^A_{Gm_i}] = Adv^{A,Gm_i}$。

Gm0：A在ROR模型中对本文方案执行的实际攻击对应于游戏Gm0。在这个游戏中，硬币d在开始时被选择。因此：

$$Adv^A(t) = \left|2Adv^{A,Gm_0} - 1\right| \quad (11)$$

Gm1：Gm1对应窃听攻击。A通过Execute查询来获取身份认证和密钥协商的过程中的$m_{A1}=\{Q_i, h(Q_i \| t_{Si}), t_{Si}\}$、$m_{A2}=\{KKEK_{Vi}, R_i, t_{Si}\}$、$m_{A3}=\{W_i, h(W_i \| KEK_i^*)\}$、$m_{A4}=\{KKEK_{Ti}, S_i, W_i, t_{Si}\}$和$m_{A5}=\{V_i\}$。此询问结束后，A执行Reveal和Test查询，验证获取的CEK是真实密钥或随机数。然而，会话密钥CEK通过$h(QR \| KEK \| VID)$得到，A无法获得生成会话密钥CEK的参数。因此，通过窃听消息，A不能增加其在Gm1中获胜的概率。所以，Gm0与Gm1是不可区分的。得到以下结果：

$$Adv^{A,Gm_1} = Adv^{A,Gm_0} \quad (12)$$

Gm2：Gm2和Gm1的区别是增加了Send和Hash预言器的模拟。Gm2模拟了一种主动攻击，A试图欺骗参与者接受其编造的消息。A反复查询哈希预言机以查找冲突。根据生日悖论可得：

事件E1：认证协议中用到的2个散列函数h、h1发生碰撞的最大概率为：$\frac{q_h^2}{2|H|} + \frac{q_{h_1}^2}{2|H_1|}$。

事件E2：认证协议中随机数QR、PFK_i是随机均匀分布的，因此QR和PFK_i碰撞的概率为$\frac{(q_s^a+q_s^b+q_e)^2}{2^{L+1}}$。

如果事件E1和事件E2都发生，Gm_2和Gm_1则是不可区分的。因此可得：

$$\left|Adv^{A,Gm_1}-Adv^{A,Gm_2}\right|\leqslant\frac{q_h^2}{2|H|}+\frac{q_{h_1}^2}{2|H_1|}+\frac{(q_s^a+q_s^b+q_e)^2}{2^L} \quad (13)$$

Gm3：Gm3模拟了Gm2中的所有预言。若A不通过随机预言查询可以伪造身份认证流程中的关键参数(Q_i,R_i,W_i,S_i,V_i)，则方案终止运行。但是这种情况只会出现在Send查询中，故A无法区分Gm3和Gm2，因此：

$$\left|Adv^{A,Gm_2}-Adv^{A,Gm_3}\right|\leqslant\frac{q_s^a+q_s^b}{2^L} \quad (14)$$

Gm4：Gm4模拟Gm3中所有预言。攻击者A意图获取会话密钥$CEK=h(QR\|KEK_i\|VID)$，A需要执行Corrupt(V_i^a)查询获得SMC中PFK、VID、NID和KCEK。攻击者A可以通过执行以下2个独立的事件来获取会话密钥CEK：

a. 通过执行q_s次Send询问获得(QR,KEK_i)，对应的可能性为$q_s/2^{2L}$。

b. 对称加密后的会话密钥$KCEK_i=E_{KEK_i}(CEK_i)\oplus CTR_i$获得会话密钥。攻击者A通过执行$q_s$次Send询问得到$(CTR_i,KEK_i)$，对应的可能性为$\frac{q_s}{2^{L+L_c}}$。

因此，可得：

$$\left|Adv^{A,Gm_3}-Adv^{A,Gm_4}\right|\leqslant\max\left\{\frac{q_s}{2^{2L-1}},\frac{q_s}{2^{2L_c-1}}\right\} \quad (15)$$

在上述比赛中，容易得到$Adv^{A,Gm_4}=\Pr\left[Suc_{Gm_4}^{A}\right]=\frac{1}{2}$。因此，攻击者A的优势为：

$$Adv^{A}(t)=\frac{q_h^2}{2|H|}+\frac{q_{h_1}^2}{2|H_1|}+\frac{(q_s+q_e)^2+q_s}{2^{L-1}}+\max\left\{\frac{q_s}{2^{2L-1}},\frac{q_s}{2^{2L_c-1}}\right\} \quad (16)$$

4.2 安全分析

分析本文所提出方案对典型攻击的抵御情况：

a. 根权限内部攻击：假设攻击者A可以获得开发根（root）权限，从而通过身份认证与密钥协商。A意图读取车辆数据，需要得到加密后的会话密钥KCEK。然而，KCEK只有在车辆所有者本人授权读取请求后才会发送到云端，攻击者无法在未经授权的情况下获得车辆数据明文信息。所以，本文方案可以抵抗根权限内部攻击。

b. 重放攻击：假设攻击者A可以监视并获取T-BOX、QSS、TSP之间的通信，并在一段时间后重放该条消息。但是在密钥协商和数据加密消息中包含时间戳，并且在数据加密后加密会话计数器的计数值会更新，A无法获得有效的信息。假设攻击者A记录所有的身份认证请求消息m_{A1}，并将其重播到密钥管理服务器QSS，以模拟T-BOX获取保护密钥。然而，VID受到单向哈希函数和对称量子密钥加密保护，A不能通过m_{A1}获得T-BOX的假名，无法通过身份认证。因此本文方案能够抵抗重放攻击。

c. 前向安全：本文方案中内容加密密钥CEK由加密会话密钥KEK进行加密后传输，即$KCEK_i=E_{KEK_i}(CEK_i)\oplus CTR_i$。在车辆所有者授权的有效期限内，每次会话的$CTR_i$都会进行更新。因此，对于车辆数据加密，每一次会话密钥是无关联的，本文方案具有前向安全。

d. 模拟攻击：在本方案中，认为TSP、所有者、QSS三者之间的通信通道是安全可信的。因此，本文方案面临QSS模拟攻击和T-BOX的模拟攻击。T-BOX模拟攻击中，攻击者A劫持T-BOX发送的消息$m_{A1}=\{Q_i,h(Q_i\|t_{Si}),t_{Si}\}$、$m_{A3}=\{W_i,h(W_i\|KEK_i^*)\}$。同时，A试图从劫持的消息中获得有效参数来生成合法的请求消息m_{A1}和m_{A3}来欺骗与QSS的身份验证。但是，消息m_{A1}和m_{A3}中包含参数VID、PFK、KEK，A无法获得，因此，A不能生成有效的请求消息m_{A1}和m_{A3}。同样，QSS的消息m_{A2}中包含了参数PFK_i、VID、NID，攻击者也无法获取这些参数。因此本文方案可以抵抗模拟攻击。

e. 中间人攻击：本方案中量子会话密钥CEK是通过KEK加密进行传输的。因此，攻击者A意图获取会话密钥CEK，需要通过QSS与T-BOX之间的身份认证。而PFK存储在SMC中，A无法获取，故A无法通过身份认证。因此本文方案可以抵御中间人攻击。

5 性能分析

本文将所提出的方案与现有的相关方案在认证和密钥协商阶段的计算和通信开销进行对比。

5.1 计算开销分析

对本文方案的身份认证部分的通信开销和计算开销进行测试。由于车辆所有者授权操作只在有访问请求时才会进行，所以，车辆所有者的授权时间与访问者的访问时间不进行计算。使用一台计算机作为QSS来统计计算开销。该主机具有AMD Ryzen 5 5600H with Radeon Graphics处理器、16 GB内存和Ubuntu 18.04操作系统。用T-BOX统计车辆端的计算开销，实物图如

图4所示，该T-BOX包括移远AG35-GEN通信模组、KF32MCU以及量子安全模块等硬件资源。

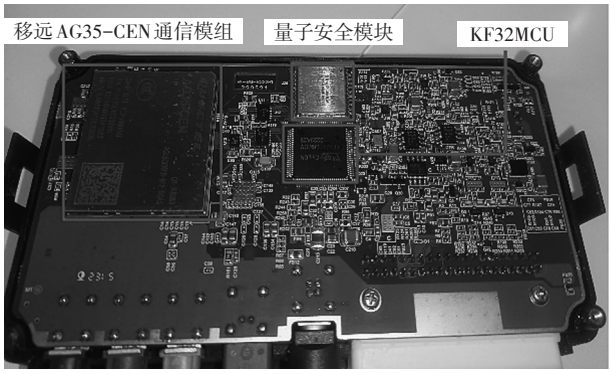

图4　T-BOX实物图

通过对每种计算开销进行统计，以10 000次计算为一组，计算10组取其平均值。T_h、$T_{s,m}$、$T_{m,e}$、T_{bp}、$T_{W.m}$、$T_{M.m}$、$T_{e/d}$、T_{mtp}分别为单向Hash函数、标量乘法运算、模指数运算、双线性对运算、魏尔斯特拉斯（Weierstrass）椭圆曲线点乘操作、蒙哥马利（Montgomery）椭圆曲线点乘操作、对称密钥加/解密操作、加密Hash运算的时间消耗，异或（exclusive OR，XOR）操作忽略不计。具体时间开销如表2所示。

表2　不同操作的开销　ms

操作	开销	
	服务端	车端/T-BOX
T_h	0.001	0.023
$T_{s,m}$	0.103	0.979
$T_{m,e}$	0.529	6.547
T_{bp}	5.327	33.176
$T_{W.m}$	0.482	2.819
$T_{M.m}$	0.346	1.964
$T_{e/d}$	0.025	0.168
T_{mtp}	0.031	0.366

在本文提出的方案中，从开始登录到完成认证，车辆端需要进行1次对称加密计算和6次单向Hash计算，车端计算开销为$T_{e/d}+6T_h\approx0.306$ ms。服务端需要进行3次对称加密和14次单向Hash计算，服务端计算开销为$3T_{e/d}+14T_h\approx0.089$ ms。因此，方案计算共消耗0.395 ms。表3列出了各方案的计算开销，其中使用的哈希算法为SHA-256，对称加密密算法为SM4。

本文方案采用预充注量子密钥和对称加密的方法进行身份认证，因此认证过程中的计算开销更小，可以更快完成身份认证。

5.2　通信开销分析

假设哈希函数的输出大小为32 B、时间戳大小为4 B、对称加密输出大小为16 B。本文方案的通信开销总数为300 B+120 B=420 B。同理，文献[16]、文献[14]、文献[17]、文献[18]方案的通信开销分别为216 B、2 296 B、668 B、544 B。显然，文献[14]、文献[17]、文献[18]方案要比文献[16]方案通信开销高。这是因为其身份认证的消息中包含了较多密钥相关的MAC值。然而，本文方案中采用预充注密钥进行对称加密，认证消息中减少了大量的密钥相关的信息，故具有更小的通信开销。

表3　各方案计算开销　ms

方案	车端/T-BOX	服务端	总开销
文献[14]	$T_{s,m}+T_{bp}+2T_{mtp}+T_{e/d}\approx35.055$	$T_{s,m}+T_{bp}+5T_{mtp}+T_{e/d}\approx5.610$	40.665
文献[16]	$T_{s,m}+T_{m,e}+6T_h+T_{e/d}\approx7.832$	$T_{s,m}+T_{m,e}+4T_h+T_{e/d}\approx0.661$	8.493
文献[17]	$3T_{W.m}+8T_h\approx8.641$	$5T_{W.m}+17T_h\approx2.427$	11.068
文献[18]	$3T_{M.m}+9T_h+T_{e/d}\approx5.457$	$5T_{M.m}+17T_h+T_{e/d}\approx1.772$	7.229
本文方案	$6T_h+T_{e/d}\approx0.306$	$14T_h+3T_{e/d}\approx0.089$	0.395

6　结束语

本文提出了一种基于车端量子密钥的车联网数据访问控制方案，设计并详细分析了基于预充注量子密钥的T-BOX、量子密服平台（QSS）、车辆信息服务云平台（TSP）之间的身份认证和密钥协商流程，以及基于量子随机数发生器的车辆数据的访问控制流程。对所提出的方案进行形式化安全分析并论证了其可以抵御的典型攻击，通过试验对所提出的方案进行性能分析，并与其他相关方案进行对比，结果表明，本文方案具有更高的安全性和更好的性能。

参　考　文　献

[1] 王军雷, 吕惠, 王亮亮, 等. 基于专利分析的智能网联汽车决策技术发展现状分析[J]. 汽车技术, 2019(12): 12-17.
WANG J L, LÜ H, WANG L L, et al. Analysis of the Development Status of Intelligent Connected Vehicle Decision Technology Based on Patent Analysis[J]. Automobile Technology, 2019(12): 12-17.

[2] 邓雨康, 张磊, 李晶. 车联网隐私保护研究综述[J]. 计算机应用研究, 2022, 39(10): 2891-2906.
DENG Y K, ZHANG L, LI J. Overview of Privacy Protection Research on the Internet of Vehicles[J]. Computer Application Research, 2022, 39(10): 2891-1906.

[3] 启明星辰智能网联汽车安全研究团队. “新基建”下车联网所面临的安全态势、建议和对策[J]. 中国信息安全, 2020(7): 57-58.
Qiming Xingchen Intelligent Connected Vehicle Safety

Research Team. The Security Situation, Suggestions, and Countermeasures Faced by the "New Infrastructure" Vehicle Networking[J]. China Information Security, 2020(7): 57-58.

[4] 杨红梅, 王亚楠. 我国车联网安全相关管理政策及技术标准研究进展[J]. 保密科学技术, 2021(7): 11-15.
YANG H M, WANG Y N. Research Progress on Management Policies and Technical Standards Related to Vehicle Networking Security in China[J]. Confidentiality Science and Technology, 2021(7): 11-15.

[5] 宋涛, 李秀华, 李辉, 等. 大数据时代下车联网安全加密认证技术研究综述[J]. 计算机科学, 2022, 49(4): 340-353.
SONG T, LI X H, LI H, et al. Overview of Research on Secure Encryption and Authentication Technology for Vehicle Networking in the Era of Big Data[J]. Computer Science, 2022, 49(4): 340-353.

[6] JIANG Q, NI J B, MA J B, et al. Integrated Authentication and Key Agreement Framework for Vehicular Cloud Computing. IEEE Network, 2018, 32(3): 28-35.

[7] BHOI S K, PANDA S K, RAY S R, et al. TSP-HVC: A Novel Task Scheduling Policy for Heterogeneous Vehicular Cloud Environment[J]. International Journal of Information Technology, 2019, 11(4): 853-858.

[8] HUANG X, CHEN X, LI J, et al. Further Observations on Smart- Card- Based Password- Authenticated Key Agreement in Distributed Systems[J]. IEEE Transactions on Parallel & Distributed Systems, 2014, 25(7): 1767-1775.

[9] JIANG M, WANG H, ZHANG W, et al. Location- Based Data Access Control Scheme for Internet of Vehicles[J]. Computers & Electrical Engineering, 2020, 86.

[10] 彭鹏. 量子通信技术在车联网中的应用探讨[J]. 江苏通信, 2022, 38(2): 71-74.
PENG P. Exploration of the Application of Quantum Communication Technology in the Internet of Vehicles[J]. Jiangsu Communication, 2022, 38(2): 71-74.

[11]《量子"Q波"技术白皮书》发布,量子无线密钥分发技术得到初步验证[J]. 信息网络安全, 2022, 22(8): 91.
The White Paper on Quantum "Q-Wave" Technology was Released, and Quantum Wireless Key Distribution Technology Has Been Preliminarily Verified[J]. Information Network Security, 2022, 22(8): 91.

[12] JI S Y. A Simple Review of Quantum Communication and Quantum Communication Experiments in Three Different Mediums[J]. The Frontiers of Society, Science and Technology, 2022, 4(6): 1-11.

[13] 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.

[14] CHANG C C, LE H D. A Provably Secure, Efficient, and Flexible Authentication Scheme for Ad Hoc Wireless Sensor Networks[J]. IEEE Transactions on Wireless Communications, 2016, 15(1): 357-366.

[15] DUA A, KUMAR N, DAS A K, et al. Secure Message Communication Protocol Among Vehicles in Smart City[J]. IEEE Transactions on Vehicular Technology, 2018, 67(5): 4359-4373.

[16] YING B D, NAYAK A. Anonymous and Lightweight Authentication for Secure Vehicular Networks[J]. IEEE Transactions on Vehicular Technology, 2017, 66(12): 10626-10636.

[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, 2019, 15: 1654-1667.

[18] 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.

(责任编辑 斛 畔)

修改稿收到日期为2023年7月17日。