

基于云端量子密钥池的车载轻量化安全通信系统

吴成加¹, 吴嘉熙², 黄荣胜³

(1. 劲旅环境科技股份有限公司, 合肥 230011; 2. 中国科学院上海微系统与信息技术研究所, 上海 200233;

3. 安徽航途智能科技有限公司, 合肥 230031)

摘要:为应对智能网联汽车面临的量子计算安全威胁,本文提出一种基于云端量子密钥池的车载轻量化安全通信系统。该系统通过云端量子密钥分发网络分发并集中管理量子密钥,而车端则由硬件安全模块负责密钥的安全存储及加密运算,从而建立“一次一密”的安全信道。实车验证结果表明,该系统在保证信息论安全的同时,兼具低延迟、高可靠性和低功耗等优点,有效解决了量子密钥分发给在车载环境中部署难、成本高的问题,为智能网联汽车提供了兼具高安全性与实用性的通信安全保障。

关键词:量子密钥分发; 车联网安全; 云端密钥池; 硬件安全模块; 一次一密

中图分类号:U463.67; TN918 文献标志码:A DOI:10.15917/j.cnki.1006-3331.2026.04.001

A Lightweight In-vehicle Secure Communication System Based on Cloud Quantum Key Pool

WU Chengjia¹, WU Jiayi², HUANG Rongsheng³

(1. Jinglv Environment Science and Technology Co., Ltd., Hefei 230011, China;

2. Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200233, China;

3. Anhui Hangtu Intelligent Technology Co., Ltd., Hefei 230031, China)

Abstract:To address the quantum computing security threats facing intelligent connected vehicles, this paper proposes a lightweight, vehicle-mounted secure communication system based on a cloud-based quantum key pool. The system distribution and centrally manages quantum keys through a cloud-based quantum key distribution network. The vehicle side relies on a hardware security module to securely store the keys and perform encryption operations, thereby establishing a “one-time pad” secure channel. The real vehicle test results demonstrate that the system not only ensures information-theoretic security but also offers advantages such as low latency, high reliability, and low power consumption. It effectively resolves the difficulties and high costs associated with deploying quantum key distribution in vehicular environments, providing intelligent connected vehicles with secure communication guarantees that combine high security and practicality.

Key words:quantum key distribution; internet of vehicles security; cloud key pool; hardware security module; one-time pad

随着汽车“新四化”的加速推进,智能网联汽车与云端平台的数据交互呈现爆发式增长,所传输的内容已从传统车辆状态扩展到控制指令、生物特征、高精度地图等高敏感数据^[1]。这些数据在无线传输过程中面临被窃取或篡改的风险,可能引发严重的隐私泄露与安全事故^[2]。现阶段车云通信主要采用基于非对称密码体系的公钥基础设施(Public Key Infrastructure, PKI)进行认证与密钥协商,同时结合对称

加密实现数据保护^[3]。然而,量子计算技术的快速发展对传统非对称密码构成了严重威胁^[4]。作为应对方案的后量子密码虽在发展中,但标准化工作尚未完成,且其安全性仍依赖于特定数学问题的计算复杂度^[5-6]。量子密钥分发(Quantum Key Distribution, QKD)基于量子力学原理,可在物理层面实现信息论安全的密钥分发,对包括量子计算在内的任何计算攻击具备免疫性^[7]。但 QKD 设备通常成本高昂、体积

收稿日期:2025-11-11。

第一作者:吴成加(1971—),男,高级工程师,主要从事新能源汽车电控与车载智能装备的关键技术研究及产业化应用。E-mail:wuchengjia@126.com。

庞大、功耗较高,且依赖专用通信链路,难以直接应用于移动车载环境。因此,业界亟需一种既能继承 QKD 安全特性,又能适应车联网移动场景的创新架构。为此,本文提出一种基于云端量子密钥池的车载轻量化安全通信系统^[8]。该系统通过在云端集中部署 QKD 资源并建立共享密钥池,为车辆提供密钥服务;车端则借助轻量化安全硬件实现密钥的安全使用,从而在保障超高安全性的同时,满足车载环境对实用性与低成本部署的要求。

1 系统总体方案设计

本系统的设计核心在于将复杂且高成本的量子密钥生成过程转移至固定的云端基础设施,而将车端设计为一个低成本、低功耗、高安全的密钥使用终端。系统总体架构如图 1 所示,主要由云端量子密钥服务层和轻量化车载安全执行层组成,二者通过经典的无线网络(如 4G/5G)进行连接。

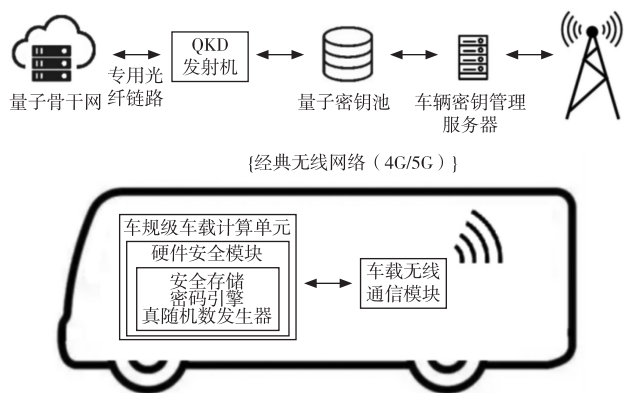


图 1 系统总体架构

1.1 云端量子密钥服务层

云端量子密钥服务层是本系统的安全基础,负责量子密钥的产生、存储及分发的全生命周期管理。该层由以下三个核心组件构成:

1) QKD 网络接入设备。该设备通过专用物理安全的光纤链路,接入国家或区域量子保密通信骨干网,并与固定量子网络节点持续进行 QKD 协议交互,生成具备信息论安全性的量子密钥流,其具有真随机性和不可预测性。

2) 量子密钥池管理服务器。该服务器接收来自 QKD 设备的原始量子密钥流,并实施池化管理,是一个具备高可用性、高并发处理和容灾能力的大规模分布式存储与计算系统。其核心功能如下:

①密钥存储与索引:对海量量子密钥进行分块、

分类存储,并建立高效索引机制,确保密钥的快速检索。

②生命周期管理:包括生成时间戳记录、状态标记(未使用、已分配、已使用、已销毁)及过期密钥的定期清理等。

③密钥隔离与安全:为每辆注册车辆维护独立的密钥上下文和逻辑隔离的密钥存储区域,确保车辆间密钥绝不重复,杜绝密钥复用带来的安全风险。

3) 车辆密钥管理服务器。该服务器是面向车辆的服务平台,负责车辆身份管理、身份认证、会话密钥分配与下发。

①车辆身份管理:存储和管理所有注册车辆的标识信息(如 VIN 码),以及与该标识信息绑定的数字证书或预共享的根密钥,该根密钥可作为密钥加密密钥(Key Encryption Key, KEK)使用。

②身份认证:接收来自车辆的密钥申请请求,并验证其身份合法性。认证可基于数字证书签名验证,或基于预共享密钥的挑战响应机制实现。

③会话密钥分配与下发:验证通过后,服务器先从量子密钥池中为该车辆分配一段指定长度(如 256 位)的一次性真随机数,作为本次通信的量子会话密钥(Quantum Session Key, QSK)。随后,服务器使用与该车辆唯一绑定的 KEK,通过高强度对称加密算法(如 AES-256)对 QSK 进行加密,形成量子数据包。最终通过传输层安全协议(Transport Layer Security, TLS)链路下发给车辆。

1.2 轻量化车载安全执行层

轻量化车载安全执行层是本系统在车辆端的实现终端,其设计目标是安全地使用密钥,而非生成密钥,以此实现极致的轻量化。该层嵌入车辆网关、T-BOX 或智能座舱域控制器中,主要包括以下组件:

1) 车规级车载计算单元。作为主处理器,该单元负责运行车辆应用逻辑、通信协议栈,并协调硬件安全模块(Hardware Security Module, HSM)的工作。其需具备较强的通用计算能力和丰富的接口,以连接各类车载网络。

2) HSM。作为车载安全执行层的核心,HSM 提供安全存储、密码运算及真随机数生成等关键安全功能。其设计符合 AEC-Q100 Grade 2 或以上等级的车规级标准,并满足 ISO 26262 ASIL-B 功能安全等级要求,从而确保在车载严苛环境下的可靠运行。

3) 真随机数发生器。其基于物理噪声源(如环形振荡器、隧穿效应)产生密码学强度的高质量随机

数,为本地所需的随机数生成提供熵源。

4) 车载无线通信模块。该模块负责与云端建立无线通信连接,用于接收加密的量子密钥数据包,并发送加密后的应用数据。

2 系统关键技术与实现细节

2.1 云端量子密钥池的构建与管理机制

量子密钥池是一个大规模、高可用的密钥资源库。其技术实现的关键在于以下环节:

1) 量子密钥后处理。QKD 设备接收的原始量子密钥需经完整处理后,方可成为最终可用的安全密钥。首先通过纠错协议(如 Cascade 协议或 LDPC 码)消除传输过程中的误码,实现密钥协商;随后进行隐私放大处理,利用通用哈希函数压缩密钥,以消除潜在信息泄露。此过程确保了密钥的一致性、机密性和完整性。

2) 密钥更新策略。量子密钥池管理服务器采用动态密钥更新机制,包括基于时间周期(如 24 小时自动更新)和基于使用状态(单次使用后立即废弃)的双重更新策略。量子密钥池会实时监控密钥使用状态,对即将过期的密钥提前预警,并自动从 QKD 网络获取新密钥进行补充,确保密钥池中可用密钥充足。

3) 抗量子攻击的存储安全机制。为应对未来量子计算攻击,云端量子密钥池采用多层防护架构。首先,使用抗量子加密算法(如基于格的加密方案)对存储的密钥进行加密保护;其次,采用物理隔离的分布式存储,将密钥分片存储在多个安全区域;最后,实施严格的访问控制和实时入侵检测,确保密钥存储在量子攻击场景下仍具有高安全性。

4) 分布式存储架构。云端量子密钥服务层的底层存储采用分布式存储系统(如 HDFS 或 Ceph)存放密钥数据,并利用多副本或纠删码机制实现数据冗余,防止单点故障导致密钥服务中断。

5) 应用程序编程接口(Application Programming Interface, API)。车辆密钥管理服务器提供基于 RESTful API 或 HTTP/2 RPC(如 gRPC)的接口。车载终端可通过调用接口(例如 POST/api/v1/keys/request)来申请密钥。云端将返回一个 JSON 格式的响应,包含经加密与 Base64 编码的密钥数据(encrypted_key)及其唯一标识符(key_id),供终端安全获取与后续使用。

2.2 轻量化车载安全模块的硬件选型与安全启动

本设计选用通过 AEC-Q100 Grade 2 或 Grade 1

认证的国产车规级安全芯片。该芯片内置的 HSM 作为车载端的安全核心与信任根,需满足车规级可靠性要求^[9],并具备以下关键安全特性:

1) 物理防篡改的安全存储区域。设有采用物理防篡改技术(如金属屏蔽层、传感器网格)保护的安全存储区,用于安全存放车辆的唯一身份证书、与云端预共享的 KEK 及解密后的明文 QSK。所有敏感密钥材料在任何时刻都不以明文形式出现在 HSM 芯片外部。

2) 集成密码算法硬件加速引擎。集成专用的密码协处理器,该处理器至少支持对称加密(AES-256,用于高速数据加密解密)、非对称加密(NIST P-256 曲线,用于基于数字签名的身份认证)、哈希算法(SHA-256,用于数据完整性校验),此外还全面支持国密算法套件(SM2、SM3、SM4),以满足国家信息安全合规性要求^[10-13]。

3) 基于物理噪声源的真随机数发生器。集成基于物理噪声源(如环形振荡器、隧穿效应)的随机数发生模块,产生密码学强度的高质量随机数,为本地所需的随机数生成提供熵源。

为确保终端自身固件的安全,系统实现了安全启动机制。安全启动机制是一套从硬件信任根开始,逐级验证后续启动组件完整性与真实性的安全链条,其核心作用是防止未经授权的固件与软件在系统启动过程中运行,从而建立终端设备的初始安全状态。其具体实现流程如下:

1) 车载计算单元上电后,Boot ROM 代码首先运行,使用 HSM 中存储的公钥或根证书验证主引导加载程序 Bootloader(如 U-Boot)的数字签名。

2) 验证通过后,加载主 Bootloader,再由主 Bootloader 验证 Linux 内核和设备树的签名^[14-15]。

3) 内核启动后,进一步验证关键系统服务和应用程序的完整性。

此链条式验证确保从硬件加电到应用层启动的每一个环节都未被篡改,防止恶意固件的植入。

2.3 基于统一诊断服务协议的安全通信会话流程

借鉴汽车行业广泛应用的统一诊断服务(Unified Diagnostic Services, UDS)协议,本系统定义了一套标准化的安全会话建立与通信流程(如图 2 所示)。该流程分为初始化认证、密钥分发、数据加密和会话终结四个阶段,涉及车端 HSM 与云端服务两大核心实体。车端 HSM 作为车辆侧的密码运算与密钥存储核

心,其内部可完成所有加密、解密、签名及密钥安全存储操作,形成物理级的安全边界;云端服务则集中负责密钥生成、身份认证、密钥分发与生命周期管理。流程图中,二者以独立的框体呈现,这种设计旨在突出安全通信的端到端信任链:从云端量子密钥池到车端 HSM,明文量子会话密钥仅存在于这两个安全域内,而所有跨域传输环节均采用加密保护。

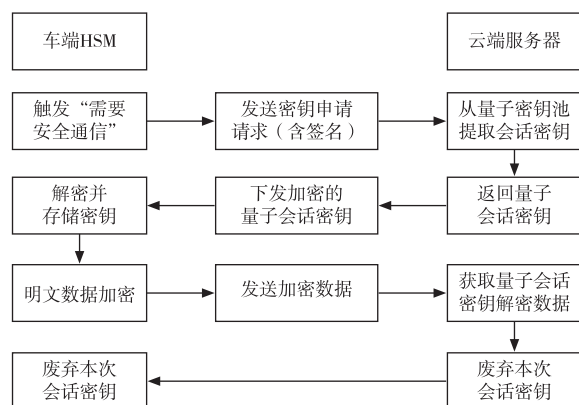


图2 安全会话建立与数据加密传输流程

1) 会话初始化与身份认证。本阶段对应 UDS 中的会话控制与安全访问服务(0x10 和 0x27)。流程由车辆应用需求触发,例如上传数据或接收控制指令。车载安全中间件随后向云端密钥管理服务器申请密钥。该申请报文至少包含车辆唯一标识(VIN 码)和一个用于防重放的随机数(Nonce),并使用车载 HSM 内的设备私钥进行数字签名。云端服务器接收到请求后,使用该车辆预置的公钥验证签名,并检查 Nonce 的有效性。若验证通过,则确认车辆身份合法。

2) 量子会话密钥的安全分发。本阶段借鉴了 UDS 中的数据下载与传输服务(如 0x34、0x36、0x37)。认证通过后,云端服务器从量子密钥池中为该车辆分配一段 256 位的真随机数,作为本次通信的 QSK。为确保 QSK 在传输过程中的安全,服务器使用与该车辆共享的 KEK,通过 AES-256 算法对 QSK 进行加密,形成量子密钥数据包,并通过 TLS 链路下发给车辆。车端 HSM 在接收到数据包后,使用内部存储的相同 KEK 进行解密,提取出明文 QSK 并安全存储,完成密钥的安全注入。

3) 安全数据加密传输。本阶段对应 UDS 中的数据写入服务(如 0x2E)。车载应用处理器将待传输的敏感数据(如心电数据)送入 HSM。HSM 使用本地安全存储的 QSK,通过硬件加速的 AES-256-GCM

算法对数据进行加密并生成完整性认证标签。加密后的密文、认证标签及本次会话的 key_id 被一同发送至云端应用服务器。该设计确保 QSK 始终受到 HSM 内的物理与逻辑保护,有效避免了密钥在车端泄露的风险。

4) 云端数据解密与会话终结。本阶段对应 UDS 中的例程控制服务(如 0x31 服务用于停止例程)。云端应用服务器根据收到的 key_id,向密钥管理服务器请求获取本次会话的 QSK,并利用该 QSK 对接收到的密文进行解密和完整性验证,从而还原出原始数据。本次数据传输任务完成后,系统立即执行协同密钥销毁:车载 HSM 将本次使用的 QSK 置为无效状态;云端密钥管理服务器也将量子密钥池中对应的 QSK 标记为已使用并安全销毁。双方协同实现“一次一密”,彻底杜绝密钥重用风险,完成安全会话全生命周期管理。

2.4 核心密钥分发与数据加密机制

图3进一步示意了本系统的核心安全机制,即量子会话密钥的端到端保护过程,并展示了从密钥池到 HSM 的信任链传递机制。

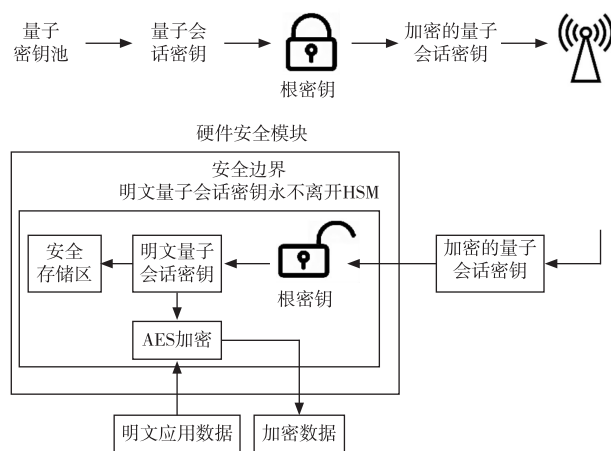


图3 密钥分发与数据加密机制示意图

1) 信任链传递。系统的安全建立在初始预置的 KEK 之上。KEK 保护了 QSK 的传输安全,而 QSK 又保护了应用数据的安全,从而形成了“根密钥→量子会话密钥→应用数据”的信任链。

2) 安全边界。图中清晰地表明,处于明文状态的 QSK 仅存在两个最安全的核心区域:云端量子密钥池的安全存储区内及车载 HSM 的安全存储区内。在跨越此边界的任何传输过程中,QSK 均以 KEK 加密后的密文形式存在。

3 系统实现与实车验证

为验证本系统的可行性与性能,已在一款 18 t 纯电动道路洗扫车平台上完成了系统部署与全面测试。

3.1 系统部署与初始化

部署过程严格依据图 4 所示的流程执行,包括云端部署、车端硬件安装、软件初始化及根密钥预置四个主要步骤。

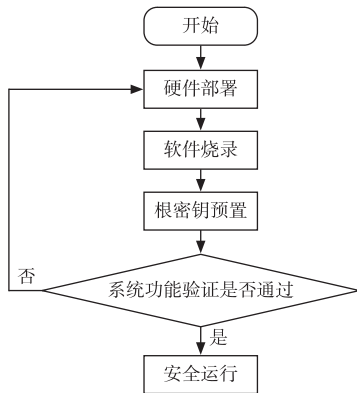


图 4 系统部署与初始化流程图

- 1) 云端部署。在公有云或私有云数据中心部署 QKD 网络接入设备、量子密钥池管理服务器、车辆密钥管理服务器,并通过专线接入合肥量子通信网络。
- 2) 车端硬件安装。选用一款国产车规级 ARM Cortex-A53 双核处理器作为主计算单元,并外挂一颗通过 AEC-Q100 Grade 2 认证的国产安全芯片作为 HSM。该安全芯片通过 SPI 接口与主处理器通信。
- 3) 车端软件初始化。在主处理器上移植 Linux 操作系统,并开发安全通信中间件,该中间件通过调用 HSM 的驱动接口来实现所有密码操作。
- 4) 根密钥预置。在车辆生产线的安全密室内,

使用专用设备将每辆车的唯一数字证书和预共享的 KEK,通过 HSM 的调试接口安全地注入到其安全存储区中。同时,在云端密钥管理服务器中完成该车辆信息的注册及其相同 KEK 的录入。此过程建立了端到端的初始信任链。

3.2 功能与性能测试

本测试模拟车辆在日常作业中实时上传加密数据(如驾驶员状态监控数据)的典型场景。

1) 安全通信建立测试。使用 CANoe 软件模拟车辆应用并触发密钥申请。通过 Wireshark 抓包可观察到车端与云端成功建立了 TLS 连接,并完成了认证密钥申请和加密密钥下发。图 5 所示的串口日志记录(捕获了 Key_Request 与 Key_Response 的成功交互)进一步印证了该过程。

```
[INFO] Vehicle Secure Middleware: Sending Key_Request (Signed)...
[DEBUG] HSM: Signing request with device private key.
[INFO] Cloud Key Server: Received request from VIN: LS123456789ABCDEF, Auth PASS.
[INFO] Cloud Key Server: QSK allocated and encrypted with KEK.
[INFO] Vehicle Secure Middleware: Received Key_Response.
[DEBUG] HSM: Decrypting QSK packet... SUCCESS.
[INFO] HSM: Quantum Session Key stored securely.
```

图 5 安全会话建立过程日志截图

至此,系统已完成身份认证、密钥分发、安全存储、信任建立的核心任务。此后,车辆即可使用 HSM 内安全存储的 QSK 对上述敏感数据(如心电数据、控制指令)进行加密,云端则用同样的密钥进行解密。

2) 加密性能测试。在车辆运行状态下,持续向云端服务器上传大小为 1 kB 的心电数据包,以模拟真实的车联数据上报场景。加密性能与资源占用等关键指标的测试结果见表 1。

表 1 系统性能测试结果

测试项目	测试条件	指标	测试结果
密钥申请延迟	5G 网络,RTT 30 ms	从发起应用到云端响应	≤150 ms
密钥分发延迟	5G 网络	从发起应用到 HSM 成功存储 QSK	平均 85 ms
数据加密延迟	HSM 内 AES-256-GCM 加密 1 kB 数据	加密单包数据	平均 0.8 ms
数据解密延迟	HSM 内 AES-256-GCM 解密 1 kB 数据	解密单包数据	平均 0.7 ms
端到端通信延迟	5G 网络	应用层数据发出到云端解密完成	平均 12 ms
密钥分发成功率	连续 1 000 次申请	成功完成密钥分发的比率	99.7%
系统功耗	车载安全通信子系统(主 CPU+HSM)待机与工作	相较未启用本系统的功耗增加值	<2.5 W
平均功耗	持续加密传输数据	系统平均运行功耗	1.2 W
高低温工作	分别在-30 ℃和 85 ℃的环境箱中运行 8 h	系统通信功能正常性	通信正常,无错误
内存占用	系统正常运行	安全中间件+HSM 驱动占用 RAM	约 12 MB

3) 多场景性能测试。为全面评估系统在不同环境下的性能表现,设计了多场景测试方案,包括不同网络质量(强信号、弱信号、高丢包率)及多车辆并发接入(10 辆、50 辆、100 辆车同时连接)等场景。测试结果见表 2。

表 2 多场景性能测试数据

测试场景	会话建立成功率/%	平均延迟/ms	丢包率/%	备注
强信号	100	25	0.1	—
弱信号 (RSRP<-110 dBm)	98.5	45	2.3	重传机制有效
高丢包率(>5%)	97.2	60	5.5	丢包重传后成功
10 辆车并发	100	30	0.2	响应时间稳定
50 辆车并发	99.8	40	0.5	系统负载适中
100 辆车并发	99.5	55	1.2	延迟可控,服务正常

从表 2 可知,系统在 5G 强信号环境下表现最优,平均延迟低于 50 ms,丢包率趋于 0。在弱信号环境下,系统通过重传机制将丢包率控制在 5%以内,仍能保持较高的可靠性。在 100 辆车并发测试中,系统平均延迟为 55 ms,较 10 辆车并发时的 30 ms 有所增加,但仍处于可接受范围内,表现出良好的可扩展性。

4) 与传统方案对比测试。为验证本系统的轻量化优势,在相同测试环境下与传统 PKI+TLS(RSA-2048+AES-256-GCM)方案进行对比。两者的加密延迟、内存占用及功耗对比结果见表 3。

表 3 本系统与传统 PKI+TLS 方案性能对比结果

性能指标	本系统(QSK+HSM)	传统 PKI+TLS
加密延迟(1 kB)/ms	0.8	3.2
内存占用(RAM)/MB	约 12	约 28
平均功耗(峰值)/W	1.2	2.8
启动时间 HSM(初始化)/ms	120	不适用

从表 3 可知,本系统在加密效率、资源占用和能耗方面均显著优于传统方案,尤其适合资源受限的车载环境。

5) 安全性与可靠性测试。为了验证系统的核心安全与可靠运行特性,对其进行了专项测试,主要涵盖以下三个维度:

①抗攻击测试:在实验室环境中,模拟中间人攻击(篡改密钥申请报文)与重放攻击,云端均能因签名验证失败或 Nonce 重复而有效识别并拒绝该请求。

②断线续传测试:在密钥下发或数据传输过程中,手动中断 5G 网络连接。网络恢复后,系统能根据会话状态重新发起申请或恢复传输,未出现数据错乱或密钥状态不一致的情况。

③代码回滚测试(密钥版本管理):尝试使用已销毁的旧 key_id 解密数据,云端与车端均能正确识别并报错,确保了密钥的前向安全性。

4 结束语

本文设计并验证了一种基于云端量子密钥池的车载轻量化安全通信系统。该系统通过创新的“云池车端”架构,将量子密钥分发的高安全特性引入移动车联网环境,有效克服了量子终端车载化的工程瓶颈,在保障信息论安全、抵御量子计算威胁的同时,还具备良好的实用性与经济性。实车验证表明,该系统在延迟、可靠性与功耗等方面均表现优异,满足智能网联汽车对高安全的应用需求。

参考文献:

[1] 李克强,戴一凡,李升波,等. 智能网联汽车(ICV)技术的发展现状及趋势[J]. 汽车安全与节能学报,2017, 8(1): 1-14.

[2] 王跃建,刘传金,王楠. 车联网安全威胁分析及防护技术研究综述[J]. 计算机研究与发展,2019, 56(10): 2049-2068.

[3] 姚卓尔,赵永耀,赵利军. 基于 PKI 的车联网通信安全认证方案[J]. 吉林大学学报(工学院),2020, 50(3): 1071-1079.

[4] GIDNEY C,EKERÅ M. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits[J]. Quantum,2021(5):433.

[5] 陈宇,汪婧,王鹏. 后量子密码学研究进展及标准化综述[J]. 密码学报,2021,8(2):203-227.

[6] 刘伟,张强,李静. 面向车联网的后量子密码技术研究进展[J]. 通信学报,2023,44(5):112-125.

[7] 潘建伟,陈宇翔,范靖云. 量子保密通信技术前沿与应用展望[J]. 中国科学院院刊,2016,31(9): 1064-1073.

[8] Chevalier C,Hermouet P,Vu Q-H. Security models and cryptographic protocols in a quantum world[J]. Foundations and Trends® in Theoretical Computer Science,2025,17(1-2): 1-140.

[9] AEC-Q100. Failure-mechanism-based stress test qualification for integrated circuits[S].

2) 若 ADS 策略得分低于或等于驾驶员策略得分,则 ADS 辅助驾驶员执行该策略。例如,在中风险环境且驾驶员置信度为 0.9 的场景下,驾驶员的减速策略得分为 8.5,ADS 的匀速策略得分为 7.5。此时,若驾驶员踩制动踏板的力度不足,ADS 自动补充制动压力,保证减速效果;同时,系统持续监测驾驶员操作是否合规,如检测到减速过慢等操作偏差,则自动发出提醒信息。

该处理逻辑有效解决了传统技术缺乏一致性判断的问题,同时通过量化评估简化了决策流程,确保快速完成冲突处理并做出正确决策。该方法既能满足车辆实时性需求,又能兼顾行驶安全与驾驶员意愿,有助于提升人机协同信任度。

3 结束语

本文所提出的考虑不确定性智能车行车态势评估与交互性决策方法,以环境风险、驾驶员状态双重不确定性数据作为核心指标,精准量化了风险等级;基于博弈建模的决策流程可有效实现应急接管阶段指令一致性检测与冲突处理,降低了计算复杂度,更好地满足了实时性响应需求。未来可从 3 个方面进一步优化评估决策体系:一是拓展不确定性维度,引入突发事件概率、交通流预测等动态数据,进一步提升态势评估精度;二是融合强化学习算法,进一步提升人机协同决策的适应性;三是开展实车测试,如模拟突发障碍物场景、暴雨环境等,验证所提方法的可行

性及应用效果,加速新技术落地。

参考文献:

- [1] 贾庆东,刘骄阳,蒲超,等.基于态势感知的线网级智能行车调度系统方案研究[J].自动化与仪表,2025,40(8):5-8.
- [2] 鲍明喜.考虑周车行为不确定性的智能车辆横向决策研究[D].长春:吉林大学,2025:4-8.
- [3] 钟沂平,孙心悦,罗清玉.高密度交通流下自动驾驶车辆行车安全态势评估方法[J].公路,2024,69(12):325-331.
- [4] 武巍.考虑驾驶风格的智能车态势评估及换道决策规划研究[D].长春:吉林大学,2024:7-8.
- [5] 刘禹祺.基于车载视频数据的行人过街轨迹预测与行车安全态势分析[D].长春:吉林大学,2024:19-22.
- [6] 张娅.考虑不确定性的智能车行车态势评估和交互性决策[D].杭州:浙江大学,2022:2.
- [7] 侯文静,杨广东.基于 DSP 的智能车控制系统设计[J].信息技术与信息化,2020(5):234-235.
- [8] 邹晓越.基于机器视觉的驾驶员面部多特征疲劳检测系统研究[D].济南:山东交通学院,2025:4-8.
- [9] 苏卫星,赵晓雯,温永刚,等.基于环境风险的自动驾驶局部路径规划算法[J].信息与控制,2023,52(3):369-381.
- [10] 周晓冰.弯道动态环境下无人驾驶汽车路径规划与跟踪策略研究[D].西安:长安大学,2022:41-43.
- [11] 周润发.融合动态场景信息和 DDPG 算法的智能车决策规划方法研究与应用[D].成都:电子科技大学,2021:14-16.

(上接第 6 页)

- [10] GM/T 0002—2012 SM4 分组密码算法[S].
- [11] GM/T 0003.2—2012 SM2 椭圆曲线公钥密码算法 第 2 部分:数字签名算法[S].
- [12] GM/T 0003.3—2012 SM2 椭圆曲线公钥密码算法 第 3 部分:密钥交换协议[S].
- [13] 王海涛,陈晓峰,刘建伟.基于国密算法的车载安全通信

- 系统设计与实现[J].密码学报,2022,9(4):345-358.
- [14] 吴成加,郑磊,夏宇生,等.基于 UDS 协议的车辆 OTA 开发[J].客车技术与研究,2024,46(3):39-44.
- [15] 吴成加,夏宇生.基于 Linux 的客车全液晶仪表设计[J].客车技术与研究,2021,43(1):36-39.