智能网联汽车量子通信技术及其安全应用标准化研究

一、研究背景及概述

随着智能网联汽车的飞速发展，汽车不再仅仅是一个交通工具，而是一个能够与其他设备进行信息交互的移动智能终端。由于通信终端、传输信道、服务器等多个环节均存在着安全性隐患，网络信息安全面临着严重的威胁。通常，人们可以采用身份认证、传输加密、数字签名等手段来确保信息安全。在传统信息安全体系中，这些手段都是通过依赖于计算复杂度的加密算法来实现。然而一旦拥有足够强大的计算能力，所有依赖于计算复杂度的加密算法都可能会被破解。量子通信克服了经典加密技术内在的安全隐患，能够确保身份认证、传输加密以及数字签名等技术手段的无条件安全，可以从根本上解决信息安全问题。量子通信是最早走向实用化和产业化的量子信息技术，普遍被国际上认为是事关国家信息安全的战略性必争领域。因此智能网联汽车量子通信技术及安全应用的研究就十分有意义。

本课题深入探讨了量子通信技术在智能网联汽车信息安全领域的应用与发展建议。文章首先分析了智能网联汽车在不同通信场景下的安全需求，包括车辆与云端、云-云、车辆与行人、车辆与基础设施、车辆与车辆以及车辆内部的通

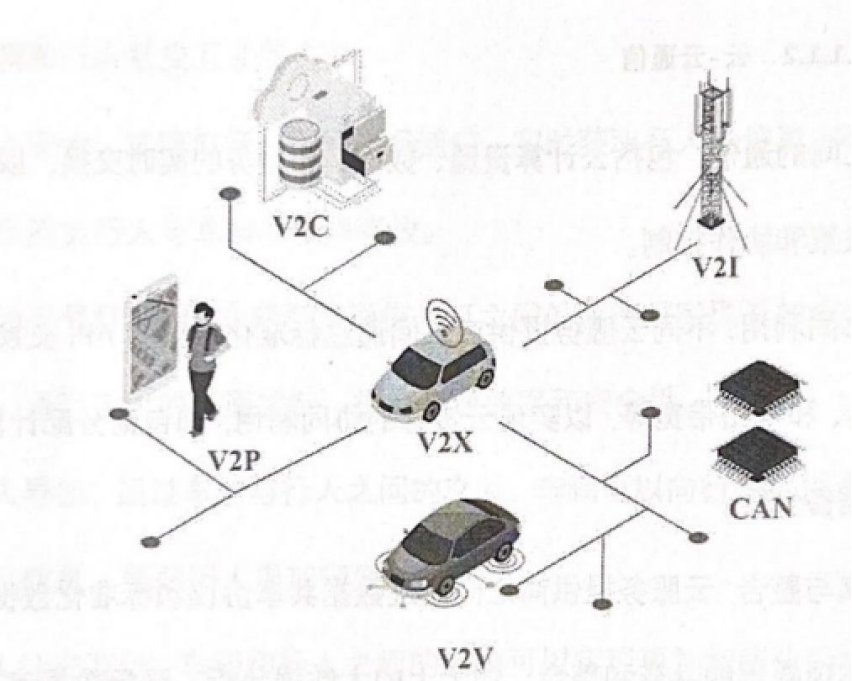
信。接着，文章详细阐述了量子密码在汽车信息安全中的典型应用，如身份认证和数据加密，并明确了其保障范围。此外，文章还通过具体案例介绍了量子密码在智能网联汽车中的实际应用，包括关键共性技术(如量子密钥的分发和管理)以及典型应用场景(如场景验证设备信息、车-云-云应用场景和 V2X 应用场景)。文章旨在为智能网联汽车的信息安全发展提供有益的参考和建议,推动量子通信技术在该领域的广泛应用。

课题基于以上研究成果，完成智能网联汽车量子通信技术及其安全应用标准化前瞻研究的行业报告 1 份。

二、研究内容

（一）智能网联汽车典型通信场景安全需求分析

车联网利用新一代信息和通信技术，将车辆、人员、路况、服务平台等多个方面进行全方位网络连接，实现智能化和自动驾驶能力的提升，构建全新的汽车和交通服务业态，从而提高交通效率，改善汽车驾乘感受，为用户提供智能、舒适、安全、节能、高效的综合服务。智能网联汽车通信以“两端一云"为主体，路基设施为补充，涉及车辆与行人、车辆和云端、车辆与基础设施、车辆与车辆之间以及车内通信的 5 个典型通信应用场景，如图所示。



（二）量子密码在智能网联汽车中的典型案例

1、关键共性技术

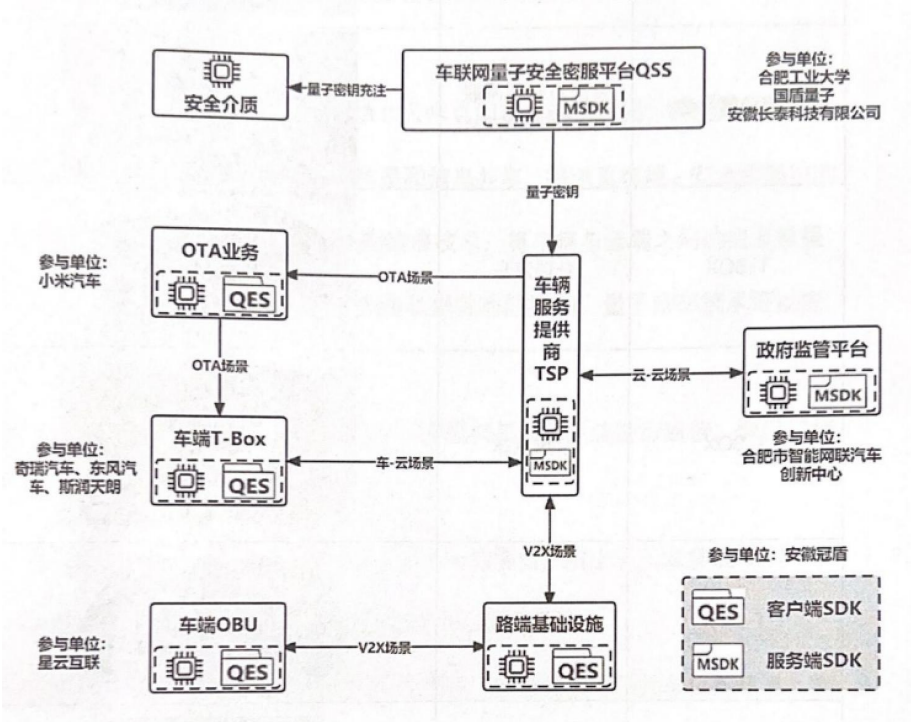
量子密码技术为智能网联汽车提供了一种卓越的数据传输和安全通信解决方案。其中包含许多关键共性技术。在移动通信和有线通信场景中，量子密钥分发技术扮演了关键的角色，确保了通信的安全性和保密性。在移动通信中,量子密钥分发中心充当协调者，通过生成、分发量子加密密钥，以确保云端和车端>间的通信是高度安全的。而在有线通信中，量子密钥协商中心使用两个独立生成的量子密钥片段的传输和验证，然后合并这些片段以生成共享的量子密钥，这个共享密钥用于加密和解密通信，确保通信的安全性。

密钥管理系统是一个包含多个模块的系统，提供了未来信息安全的基础,用于全面管理量子密钥对的生命周期。它包括量子密钥生成、存储、分发、备份更新、撤销、归档以及恢复等功能。其提供了强密码学安全性、密钥分发高效率性、

远距离密钥传输、密钥的实时监测和更新、减少传统加密方法的脆弱性。这使得量子密钥管理系统在智能网联汽车信息安全领域具有革命性潜力。总之，量子密码技术在智能网联汽车中为数据安全提供了卓越的解决方案包括量子密钥分发、管理等关键共性技术。这些技术的应用确保了密钥的生成存储、分发和更新，以确保密钥的安全性和可用性，有助于确保车辆之间的通信安全，防止潜在的数据泄漏和攻击，为未来智能交通系统的发展提供了坚实的基础。

2、典型应用场景、

车联网是指按照一定的通信协议和数据交互标准，实现人、车、路、网、云之间无线通信和信息交换的网络。量子密码典型的应用场景主要包含了车-云通信，云-云通信，V2X通信等。具体的场景验证架构图如下所示:



本部分内容节选自该课题研究报告，非全部内容，仅供

参考了解。