智能网联汽车 量子通信技术及其安全应用标准领航研究

全国汽车标准化技术委员会
智能网联汽车分技术委员会

2023 年 11 月

前　言

在此衷心感谢参加研究报告编写的各单位、组织及个人。

组织单位：全国汽车标准化技术委员会智能网联汽车分技术委员会

牵头单位：中国汽车技术研究中心有限公司、南京中科齐信科技有限公司

参与单位：科大国盾量子技术股份有限公司、合肥工业大学、北京航空航天大学、小米汽车科技有限公司、东风汽车集团有限公司研发总院、重庆长安汽车股份有限公司、一汽-大众汽车有限公司、中国第一汽车股份有限公司、上海机动车检测认证技术研究中心有限公司、东软集团股份有限公司、泛亚汽车技术中心有限公司、安徽江淮汽车集团股份有限公司。

参与人员：李宝田、徐忱、周雷、程腾、李雨冉、杨世春、孙航、曹小峰、陈思井、何凯、王博、于欢、王宏多、陈静相、华宇铖、王林林、赵毅恒、石琴、陈治通、李强伟、徐娟、宋军庆、李木犀、张荣沛。

目 录

1. 引言

2014 年 4 月 15 日，国家主席习近平同志主持召开中央国家安全委员会第一次会议时，首次提出了国家安全观概念，并对总体国家安全观的基本内涵、指导思想和贯彻原则作了重要讲话。2015 年 7 月 1 日，第十二届全国人大常委会第十五次会议通过《中华人民共和国国家安全法》并颁布施行。国家安全不是多个领域安全的简单叠加，而是一张环环相扣的多元化生态网络。不同领域的安全相互关联、相互影响，在一定条件下可以相互融合，具有传导效应和联动效应。维护国家安全，不仅要保障各个领域的安全，还要维护整体和系统的安全。

网络安全作为总体国家安全观所涵盖的细分领域之一，要求各级党政机关和相关企事业单位准确把握国家安全形势变化，坚决维护国家政权安全、制度安全和意识形态安全，巩固国家安全人民防线。本次应用研究将根据国内外法律法规及标准政策要求，以国家安全观为核心思想，分析智能网联汽车的发展趋势，验证智能网联汽车的安全防护情况，探索量子通信技术赋能智能网联汽车的应用价值，并针对智能网联汽车当前面临的网络安全挑战提出标准化与产业化建议，为提升智能网联汽车安全防护水平、构建智能网联汽车安全标准体系奠定了良好的基础。

1.1 量子通信技术的发展与产业现状

1.1.1 量子技术的发展与产业现状

量子信息技术是量子物理与信息科学交叉的新生学科。自从量子信息科学创立以来，已经先后孕育出激光、核磁共振等新技术，成为 20 世纪最重要的科学创新之一。进入 21 世纪，迎来量子科技革命的第二次浪潮，催生了量子通信、量子计算和量子测量等一批新兴技术，在确保信息安全、提高运算速度、保障测量精度等方面突破经典技术的瓶颈，极大地改善人类采集、传输和处理信息的方式和能力。

（1）量子通信

量子通信是量子信息科学的重要分支，它是指利用量子比特作为信息载体来进行信息交互的通信技术。在量子密钥传输过程中，基于量子力学基本原理保证数据无法被窃听。量子通信的典型应用形式包括量子密钥分发（Quantum Key Distribution，QKD）和量子隐形传态（Quantum Teleportation, QT）等。量子密钥分发可用来实现经典信息的安

全传输；而量子隐形传态是传递量子信息的有效手段，未来路有望成为分布式量子计算网络等应用中的主要信息交互方式。

（2）量子计算

量子计算利用量子叠加和干涉等原理进行量子并行计算，可以在特定问题上相对于经典计算提供指数级加速，为若干大规模计算难题提供了解决方案。量子计算机广义上包括通用量子计算机和专用量子模拟机。量子计算研究分为三个阶段。第一阶段是实现“量子优越性”，即量子模拟机针对特定问题的计算能力超越经典超级计算机，这一阶段性目标已经实现；第二阶段是实现具有应用价值的专用量子模拟系统，可在组合优化、量子化学、机器学习等方面发挥效用；第三阶段是实现可编程的通用量子计算机，能够在经典密码破解、大数据搜索、人工智能等方面发挥巨大作用。实现通用可编程量子计算机还需要全世界学术界的长期艰苦努力。

（3）量子测量

随着量子测量技术的快速发展，计量标准将进入“量子时代”。这将全面提高七个基本物理量（长度、质量、时间、电流、温度、物质的量和发光强度）的测量精度，并可广泛用于授时、导航、医学检测、乃至包括引力波探测在内的基础物理检验。得益于量子效应，量子精密测量能在诸如时间、重力、磁场、成像、遥感等领域，提供比现有技术更高的测量灵敏度、精度和速度。量子精密测量技术将在下一代时间基准、精确导航、基本物理常数测量、粒子探测、核磁共振成像、远程目标识别、全球地形测绘、引力波或暗物质的感应探测等广泛领域发挥重要作用。

随着信息安全重要性不断提升、国际环境日趋复杂，量子保密通信技术及产业发展成为各国关注的焦点。包括中国、英国、美国、日本、欧洲等在内的世界主要大国和地区陆续启动了量子技术研究计划，加大对量子技术的研发投入。世界领先的头部科技企业中，亚马逊、IBM、富士通、微软、思科、爱立信等均围绕量子技术展开布局。

我国量子通信技术正处于蓬勃发展的阶段，前瞻布局量子技术未来产业

2016 年 7 月国务院发布的《“十三五”国家科技创新规划》指出，面向 2030 年，量子通信与量子计算机被选择纳入体现国家战略意图的重大科技项目之一，重点开发量子信息技术。2022 年 1 月国务院发布的《“十四五”数字经济发展规划》提出瞄准传感器、量子信息等前瞻性领域，提高数字技术基础研发能力，强化关键产品自给保障能力。

目前，中国在量子信息技术在产业化的探索之路上披荆斩棘，特别是在量子通信领域，在国际上率先实现了广域量子保密通信技术路线图，在国际标准化方面也取得了重

要的话语权。实现了远程量子共享、量子网络和量子安全通信等技术的成功应用。在国内多个城市建立了量子通信骨干网络，正在研制的中高轨道量子卫星，未来高轨卫星和低轨卫星的组合将构建广域量子通信网络。并成立了多个量子通信研究实验室，极大推动了量子技术的全面发展。

深圳量子研究院、福州大学、清华大学的研究人员在超导量子线路系统上实现量子纠错突破性实验进展。研究人员通过实时重复的量子纠错技术延长了量子信息的存储时间，首次超越盈亏平衡点，展示了量子纠错优势。其超导量子计算团队在低温低噪声放大器研发方面取得重要进展，其自主研发的低温低噪声放大器（型号：SIQA-LNA1.0）可在 4K 环境温度下工作，具有低功耗、高增益和低噪声的性能特点，解决了低温测量系统中关键元器件的国产化问题，并为量子计算的规模化提供了技术支持和产品保障。

中国科大、悉尼科技大学、南方科技大学、河南量子信息与密码重点实验室、荷兰代尔夫特大学的联合团队研究“切割”大规模量子线路从而可使用小规模线路进行处理的架构，并实验演示了使用至多 4 个物理量子比特模拟 33 量子比特的线性簇态，实验发现对于 12 量子比特的线性簇态，切割模拟的保真度可以达到 0.734，比直接使用 12 量子比特提高 19%。

中国科大与济南量子技术研究院等研究人员利用绝缘体上铌酸锂平台设计加工了一种低噪声频率上转换波导，在实现通信波段和近可见光波段的光子频率转换的同时还能够继续保持其他维度的量子态。该芯片波导的频率上转换效率为 73%，噪声 900cps；基于该芯片也制作了一个单光子探测器系统，可以实现探测效率 8.7%，噪声 300cps。

南京大学、矩阵时光公司的研究人员提出了一种利用双光子干涉进一步提高双场 QKD 效率的协议，该协议相对于相位匹配式协议可以容忍更高的干涉错误，相对于发或不发式协议提高计数强度。仿真显示了该方案在密钥容量、极限距离等条件下的优势。

英国发布新的政府计划和国家量子战略

英国科学、创新和技术部于 2023 年 3 月发布新的政府计划-《科学和技术框架》，以推动英国在 2030 年成为科技超级大国。该计划由超过 3.7 亿英镑的政府资金支持，用于促进基础设施建设、科研投资和技能培养，覆盖量子技术、超级计算、人工智能等前沿领域。紧随其后同月颁布了《国家量子战略》，将量子技术确定为未来十年保障英国繁荣和安全的重中之重，并为英国国家量子技术计划提供了十年愿景和扩展行动计划。该行动计划分为两个五年阶段进行，将在 2024 年至 2034 年提供 25 亿英镑的政府投资，并吸引至少 10 亿英镑的额外私人投资。在该计划指导下，英国政府随后发布《国际技

术战略》，提出加大与其他国家的深入合作，并将量子技术列为英国重点关注的 5 项关键技术之一。

英国牛津大学的研究人员构建了一个基于离子阱的量子存储网络节点，（锶）离子-光子纠缠被传送到钙离子，并映射到离子阱存储比特，存储比特的退相干速度比离子-光子退相干速度低约 70 倍，使用动态退相干技术进一步延长存储时间，测量发现离子-光子纠缠在 10 秒后的保真度依然达到 0.81。

英国赫瑞瓦特大学的研究人员实验演示了能够在 10℃范围内实现光谱不可区分性的 QKD 光源。该光源由宽谱的超发光发光二极管（SLED）和窄带滤波器的组合，其温度稳定性在卫星载荷等可能存在温度梯度的场景中更为适用。

4 月 19 日，英国国家量子计算中心（NQCC) 和爱丁堡大学信息学院签署了一份关于合作共建量子软件实验室（QSL）的谅解备忘录。该实验室将基于一个名为“量子优势探路者（QAP）”的核心研究项目，对新量子软件的开发进行关键研究。

美国参议员提出两党法案应对新威胁，各大科研院所共同研究量子应用

2023 年 3 月，多名两党参议员联合提出《限制出现危及信息和通信技术的安全威胁（RESTRICT）法案》，旨在通过更好地授权商务部审查、预防和减轻对美国国家安全构成不当风险的信息通信和技术交易，全面解决外国对手的技术所带来的持续威胁。法案在信息和通信技术领域，列出量子密钥分发、量子通信、量子计算等技术。

美国耶鲁大学、加拿大舍布鲁克大学的研究人员实现了可稳定纠错的量子逻辑比特，纠错效益超过“收益”平衡点。研究人员通过改进超导量子电路制造工艺和无模型强化学习调控，实现纠错的相干增益达到 G=2.27±0.07（G 定义为同一系统中主动纠错逻辑量子比特与同一系统中最佳无源量子比特编码的相干时间的比值，G=1 即达到盈亏平衡点）。

4 月，亚马逊云科技 AWS 宣布与 Element Six 进行新的研究合作，探索开发和改进用于量子网络的人造金刚石的方法。量子互联网通信中的量子中继器通过将光子上编码的信息传输到可以存储和校正信息的固定存储量子比特来工作，缺陷量子比特（如金刚石中的色心 NV 和 SiV）成为量子中继器存储器的主要候选者，这两类色心位于金刚石中，可以与各种半导体工艺兼容。双方正在合作开发新技术，使金刚石成为一种更灵活、更易于获得的材料，帮助推动这项技术的增长和进步。

量子安全公司 Qunnect 宣布扩大其在布鲁克林海军造船厂的设施。名为“GothamQ Network”的网络研究中心将支持 Qunnect 的网络技术，不仅承载其新形式的安全通信，

还将支持其他量子设备，包括计算机和传感器，并部署在现有的电信光纤基础设施上，这些功能将成为量子互联网建设的基础。

美国能源部（DOE）阿贡国家实验室下的阿贡量子铸造厂正式启用，该铸造厂由阿贡的能源部国家量子信息科学研究中心 Q-NEXT 领导，其建立和运营是 Q-NEXT 的重要组成部分，将被建设为量子研究中心。阿贡量子铸造厂将专注于开发、测试和制造半导体量子比特。

加拿大国防部门推出量子科学与技术战略实施计划

2023 年上半年，加拿大国防部和武装部队推出量子科学与技术战略实施计划——《Quantum 2030》。该计划为期 7 年，是确保国防部和武装部队为量子技术对国防与安全的颠覆性潜力做好准备的路线图。该计划确定了四项具有国防与安全应用前景的量子技术，分别是：量子增强雷达、量子增强型光探测和测距（激光雷达）、用于国防和安全的量子算法、量子网络。

加拿大 D-Wave 公司、美国波士顿大学等的研究人员实验演示了在 5000（超导）量子位上，基于退火算法测量三维自旋玻璃中的动力学，相对于基于蒙特卡罗算法的慢随机动力学模拟显示出显著的优越性。

日本富士通携手大阪大学开发全新量子计算架构

3 月 23 日，富士通联合大阪大学公布了一种新型高效模拟旋转量子计算架构。新架构使得量子纠错所需的物理量子比特数量（实现容错量子计算的先决条件）大幅减少，从 100 万量子比特减少到 1 万量子比特。未来富士通和大阪大学将进一步完善这一新架构，以引领早期量子计算机的发展，旨在将量子计算应用于广泛的实际社会问题，包括材料开发和金融。随后，日本理化学研究所等开放了首台下一代超高速计算机“量子计算机”的使用权。该机使用了超导技术，量子比特数为 64，集成在长宽各 2 厘米左右的芯片上。理化学研究所称该机初期的使用对象是大阪大学等共同研究机构的研究人员，今后将逐步扩大至产业界等。

印度正在研究基于卫星的量子通信并积极探索军民领域的应用

印度拉曼研究所 （RRI）的研究人员展示了使用量子密钥分发（QKD）在固定源和移动接收器之间建立的安全通信。RRI 发布声明表示，此次演示能帮助印度设计和提供安全的通信信道，特别是用于国防和战略目的，增强网络安全并使在线交易比当下更安全，为未来基于地面到卫星的安全量子通信铺平道路。

印度海得拉巴国际信息技术研究所（IIITH）与 Synergy Quantum 印度公司建立合

作伙伴关系，以建立印度首个量子解决方案实验室。该实验室将专注于研究和开发量子通信技术，特别关注后量子加密、量子密钥分发、量子随机数发生器、量子传感，包括量子导航等，旨在开发经济上可行的量子技术及其在军事和民用领域中的应用。近日印度海军武器和电子系统工程机构（WESEE）与印度拉曼研究所（RRI）签署了谅解备忘录，以促进量子在海事用例中的研究。

欧盟扩大超导量子计算机研究计划，并发布量子技术标准化路线图

欧洲标准化委员会（CEN）和欧洲电工标准化委员会（CENELEC）发布了两份重要文件：标准化路线图和量子技术用例报告，全面阐述了欧洲对量子通信、量子计算和量子计量的标准化需求，并重点介绍了以 QKD 技术为主的量子通信设备、组件标准化发展情况。这些文件代表了欧洲标准化工作在该领域的里程碑，由 CEN-CENELEC 量子技术焦点小组编写。

欧洲电信标准化协会（ETSI）随后发布了用于量子密钥分发（QKD）模块安全评估的保护轮廓（PP）标准—ETSI GS QKD 016。该标准规范将帮助制造商提交成对的 QKD 模块，以便在安全认证过程中进行评估。同时，它还规定了直到最终密钥输出过程的制备和测量型 QKD 协议物理实现的高阶要求。

德国资助三个量子通信相关项目，将开发可以接收量子密钥的光学地面站

德国激光通信产品供应商 Mynaric 宣布被选中参与三个量子通信相关的技术开发项目，这些项目是德国联邦教育和研究部资助的 QuNET 计划第二阶段的一部分。在 2023 年至 2025 年期间，Mynaric 的技术开发将获得总额 560 万欧元的共同资助。三个项目分别为：开发能从太空接收量子密钥的光学地面站；演示可以通过空对空、空对地链路交换量子密钥的机载高空平台光通信终端；探索实现固定和移动网络节点的量子密钥激光通信的紧凑型光学技术。

德国帕德博恩大学、奥地利维也纳大学的研究人员在一次和二次量子化条件下对量子纠缠进行了严格描述，并发现在一些例子中，粒子纠缠与场纠缠是两个独立的效应，该分析完善了基础认识和并有助于纠缠应用。

1.1.2 量子安全的发展与产业现状

回顾往年的量子世界可谓是日新月异，量子安全囊括量子密钥分发（QKD）和后量子密码（PQC）、量子安全攻防、量子密码应用等多个细分领域，已然形成量子信息科技的一个重要发展方向，凸显出综合性强又相对独立性的前进脉络。这些新一代加密技

术可嵌入在整个网络的不同环节，担负起抵御量子时代的信息安全重任。

QKD 密码技术在 QaaS、区块链、无人机、金融、电网等领域已有大量应用，拓宽下游发展空间，但仍处于发展阶段；基于数学算法的现代密码学体系已完善且大量应用，PQC 已在 VPN、IC 卡等方面有小规模试用。但密码破解技术却一直在挑战和刺激着新一代密码技术不断演进。

QKD技术应用发展现状

（1）基于光纤传输的 QKD 线路刷新距离，为千公里陆基 QKD 打下坚实的基础。基于光纤的传输在 2022 年在 QKD 和量子安全直接通信(QSDC)两类技术上均刷新了长度纪录。在 QKD 网络建设方面，中国合肥量子城域网(中国最大量子城域网，包含 8 个核心网站点和 159 个接入网站点，光纤全长 1,147 公里，可为市、区两级近 500 家党政机关提供量子安全接入服务。纵观全球在 QKD 网络基础设施建设中，中国是成果最多的国家。

（2）高性能光源、量子中继器等核心上游器件是重要提升点之一。除了在安全性这一核心方面在提升，QKD 系统也在核心组件级方面做出效果，例如高品质光源。除了在 QKD 系统中应用，量子光源技术还可能赋能量子计算和量子精密测量，因此，发展新一代光源这一基础技术及器件，将为多个未来应用提供可能性。

（3）目前 DI-QKD 和 MDI-QKD 为主要前沿技术提升方向，尚不构成商业应用的能力。设备无关量子密钥分发(DI-QKD)和测量设备无关量子密钥分发(MDI-QKD)协议是 2022 年度学术论文成果展现的重要方向，MDI 是解决攻击方控制探测器，DI 是解决攻击方控制所有设备。这些技术都是假设攻击方能力非常强大的实验验证，目前离产业化还很远。

（4）基于卫星的 QKD 已有多国参与研究，发射微纳卫星以验证组网技术。卫星传输是除光纤传输之外的重要传输方式，也是目前量子通信的主要发展技术。由量子通信卫星组成的天地一体的量子网络进一步展开实验，各国均希望在网络安全和通信方面的拥有自主权，通过印证卫星组网的方案，将量子保密通信网络向经济化、小型化、商业化发展。

（5）交叉研究正成为量子通信技术走向实用化的必经之路。5G 甚至 6G 与量子通信与安全的结合，以及计算网络等更多领域与量子通信与安全的结合都是基于当前的已有的成熟技术展而开交叉性研究。无论量子通信与安全技术本身怎样发展，与全行业的交叉研究是使这项技术真正走向实用化必经的阶段。

PQC 技术应用发展现状

后量子密码（Post Quantum Cryptography）产生的历史不短，1978 年第一个基于纠错编码的具备抗量子特性的 McEliece 公钥密码算法就被提出了。时至今日，PQC 的应用需求变得日益明确和紧迫，现在不具备量子安全能力的公钥密码应用到哪里，未来 PQC 就可能替代到哪里，它可用来保证密钥生成、密码管理、密码服务的全过程都是量子安全的。

从现今密码技术应用场景可知，PQC 的应用场景非常广泛，从技术层面就包括涉及终端设备的加密与认证，网络基础设施上的传输加密，云上数据中心的计算与数据安全，新型数据存储与计算架构的区块链应用等，不一而足。PQC 应用推进牵涉面较广，不仅涉及 PKI 等国家和企业运营的安全基础设施，还涉及用户侧使用的密码模块、密码软件等软硬件的变更。也正源于此，PQC 密码的标准化工作就尤为重要，这是 PQC 落地应用的第一步。在实现算法标准化后，才会到实际系统研发和基础设施推广建设阶段，逐步形成产业规模。根据 Inside Quantum Technology 的一份最新报告，到 2029 年，PQC 功能将嵌入到众多设备和计算环境中，相关软件和芯片的市场将增至 95 亿美元。

（1）NIST 标准化项目、算法应用研发、推广迁移部署是 PQC 现阶段三大重要工作。短短几年时间内要推出能有效抵御量子和经典攻击又适用性强的公钥算法并非易事，且目前针对 PQC 算法发布的各类攻击成果也可能会对标准的发布造成影响：2022 年已经有多个 PQC 算法被传统方法破解的案例，如基于多变量密码（MQ）的 Rainbow 算法和基于格的 LWE 算法分别被经典算法成功攻击。

（2）据 NIST 专家 Dustin Moody 表示，基于超奇异椭圆曲线的 SIKE 算法在第四轮中“不太可能”存活下来，但目前还没有计划在第四轮中增加新的加密候选者来取代它。而基于格的 PQC 算法抗量子攻击能力近期也受到一些研究者的质疑。

（3）网络安全、物联网、半导体等领域公司进军 PQC，展开自研或合作研发。2022 年，有更多的网络安全公司、物联网和半导体公司开展量子通信与安全业务，因为这类公司有着强大的应用结合，其传统业务离不开为信息安全传输。

（4）PQC 目前不具备立即商业化的条件，经典密码向抗量子密码的过渡仍有挑战。由于还缺乏公众认可和权威部门政策包括标准化等方面的支撑，PQC 产品推进尚显乏力，2022 年主要表现为面向商用市场推出了一些应用范围有限的、多用于端到端安全加密的试水性质产品。

（5）美国当前是 PQC 推进的主导者，在标准化和实际推行方面动作频繁。2022 年

5 月，美国众议院通过了一项立法提案——“针对量子计算的网络安全准备行动法案”(The Quantum Computing Cybersecurity Preparedness Act)，以推动美国政府 IT 系统向抗量子密码技术的迁移。该法案明确提出超越传统计算能力的量子计算的快速发展使对手有可能用“现在存储、未来解密”的方法依靠强大的量子计算机解密当前产生的密文数据，因此美国政府要制定 IT 系统向后量子密码迁移的战略，关注 NIST 主导的 PQC 标准化进程，评估不使用 PQC 会导致的安全风险。

2. 智能网联汽车信息安全发展简介

2.1 智能网联汽车信息安全发展现状

早在 20 世纪中期，世界各国已经开始了对智能网联汽车的探索和研究。进入 21 世纪后，随着半导体、物联网、人工智能、5G 等新型技术的迅速发展，智能网联汽车逐渐走向大众视野，但当前汽车智能化程度依然有限，只能实现辅助驾驶或在特定的封闭环境下实现自动驾驶。

在汽车迈向智能化、网联化的过程中，尤其是车载网络接口愈加丰富，网络架构趋于复杂化，从外部信息的感知到车载内部系统之间的交互逐渐频繁，打破了汽车电子系统原有的封闭环境。当前智能网联汽车搭载上百台小型车载电脑，运行代码上升至 1 亿行，无人驾驶运行代码甚至在 2 亿行以上，代码量增多导致代码漏洞威胁持续扩大，造成更多网络安全风险。通过 T-BOX、车载网关、数字钥匙、智能驾驶模块、影音娱乐设备及应用、车载网络、车用传感器、OBD、移动介质等途径对智能网联汽车发起近程攻击；通过车载蓝牙、WIFI、4G/5G 等无线网络进行中程攻击；通过第三方内容和服务、TSP 等方式对车辆进行远程攻击。

结合智能网联汽车目前面临的信息安全风险并进行实地调研、分析，发现智能网联汽车存在的典型安全风险以及相应安全防护措施包括不限于以下内容：

（1）**云平台安全风险：**云端后台被利用/仿冒节点/网络数据劫持等造成敏感信息泄露或非法控车。可通过基于 PKI 的身份认证和通讯加密、车控加密、协议安全启动、车内通讯安全的防护手段，实现车云通讯身份认证、通讯链路加密、通讯数据加密。

（2）**数据安全风险：**ECU 等控制单元会不断感知分析道路信息、车辆工况以及用户个人信息，存在被非法更新或敏感信息泄露风险，目前主要通过调试接口关闭/升级包

签名加密/安全启动等方式来实现防调试/防逆向/防篡改的安全目标。

（3）**通信传输安全风险：**恶意节点攻击 WIFI 连接造成敏感数据泄露，可通过基于 PKI 的身份认证和通讯加密来保障协议安全、通信数据安全；车端数据被非法窃听一般采用关闭调试接口/身份认证/安全启动等措施来实现物理接口关闭或连接认证保护数据不被泄露。

（4）**终端本体安全风险：**智能网联汽车安装有大量传感器，通过对车载 GPS 传感器终端发送虚假信号造成 GPS 定位偏移、误导自动驾驶和导航。通常可采用 GPS/RTK/蜂窝定位融合 GNS、反欺骗方法保护 GPS 信号不受干扰、丢失或欺骗。

2.2 智能网联汽车信息安全关键技术发展研判

随着人工智能、5G 通信、大数据及云计算架构等新一代信息技术产业的飞速发及其与传统汽车工业的融合创新，汽车的电动化、智能化、网联化、共享化将成为未来行业发展的新趋势。到 2025 年、2030 年，部分自动驾驶、有条件自动驾驶智能网联汽车销量占当年汽车总销量的比例分别为 50%、70%。

在智能移动终端时代汽车产品形态全面革新，边界不断延展，汽车成为万物互联的节点。安全风险既涉及车辆零部件、总线，又涉及无线通信、软件，还包括交通路侧设备、云管理平台、物联网终端等。智能网联汽车的信息安全风险主要包括车外网络安全风险(包括短距离无线网络、远距离移动网络、V2X 网络、OBD、TSP 云平台、App 等安全风险)、车内网络安全风险(包括 CAN 总线、T-BOX、IVI、OTA 等安全风险)和其他网络安全风险(包括车辆数据安全风险、充电桩安全风险)。

2.2.1 端-管-云协同成为智能网联汽车发展的技术路线

智能网联汽车信息安全是国家安全范畴中重要的领域之一。目前整车的汽车安全不单单是功能安全，还需要考虑到信息安全。由于自动化能力要求的升级，智能网联汽车信息安全需要最少包含“云、管、端”三方面。随着 LTE-V2X 通信技术和路侧智能设备的不断成熟，车联网逐渐从车内智能、单车智能向“端-管-云”协同智能的方向发展。T-Box 前装比例不断提升，车联网信息服务推广加速。随着支持 4G 的 T-Box 技术逐渐成熟、电信运营商“提速降费”不断推进，新车型前装 T-Box 成本不断降低、前装比例不断提升，为车联网信息服务的快速发展提供了终端基础。一汽宣布从 2019 年起实现全系产品，标配车联网系统；长安启动“北斗天枢”战略，从 2020 年起实现新车全部

联网且搭载驾驶辅助系统，从 2025 年起实现新车全部具备人机交互功能。此外，主流汽车厂商积极推动定位导航、行车安全、远程控车、休闲娱乐、售后服务等业务，并从基础性联网信息服务向安全预警、高带宽业务和辅助驾驶服务演进。东风启辰发布“智·趣科技”的品牌理念，深化车联网战略，并联合高德地图和科大讯飞合作推动智能网联汽车平台建设。上汽集团不断升级 inkaNet 智能行车系统，提供全面高效的车载信息服务。

车联网数据服务平台、云控中心等在国内快速发展并进入验证阶段。中国移动在无锡部署了高性能 V2X 应用服务平台，实现与交管信息平台、TSP 及图商平台的交互，实现定位导航服务、交管信息推送、速度引导等多项信息服务功能。北京、上海等车联网示范区积极推进自动驾驶测试数据中心建设，并在此基础上构造虚拟场景库，打造无限化、批量化、自动化、可扩展的虚拟测试场景，提高自动驾驶仿真测试效率。同时，数据中心汇总、分析车辆测试数据，为自动驾驶方案商提供数据反馈支持。网络运营商、通信设备商、汽车厂商深度合作，合力推动远程驾驶、智能调度等云网端协同的场景应用。中国移动联合华为与上汽、中国联通联合爱立信与驭势先后演示了基于 5G 的远程遥控驾驶能力。

网联式自动驾驶技术路线逐渐获得共识，车路协同概念备受关注。车路协同通过加强路侧智能设备与智能网联汽车的信息交互与融合，可以有效降低车载终端的计算压力与性能成本，促进更高效地开展车辆主动安全控制和道路协同管理策略。此前百度发布了支持车路协同的 Apollo 版本，并将于 2018 年底开源，全面支持网联式自动驾驶。随后百度与中国信科签署战略合作协议，推进在车路协同等领域的全面合作。2018 年 9 月，阿里巴巴宣布全面升级汽车战略，打造车路协同系统，联合交通部公路院等成立了“2038 超级联盟”，协同产业力量共同落地“智能高速公路”。在未来产业发展进程中，服务运营主体将不断分层细化，路侧智能基础设施、区域内自动驾驶及行车安全服务、城市级导航及智慧出行服务等将衍生出不同的运营主体。因此，需推动构建统一的云控服务平台架构，规范数据接口与服务流程，建设分层协同的自动驾驶服务系统。

目前，产业内一般所采用的架构在云端安全主要包括:整车云如 TSP 以及 OTA 服务等，第三方云如零部件厂家的云等，管端安全主要包括 4/5G 蜂窝网络的通信信道、蓝牙、NFC、RFID、Wi-Fi、外部智能硬件等；车端安全主要包括:总线、T-BOX、IVI、OBD 以及终端 App 等。

从整车企业信息安全布局情况来看，国外主要对奔驰、奥迪、宝马、特斯拉、福特

汽车、博世、大陆集团等公司的信息安全布局进行介绍，从多方面防护汽车信息安全。在我国整车企业中，主要包括北汽新能源、小鹏汽车、蔚来汽车等，上述企业不仅在合作共赢中优势互补，在信息安全相关建设中也各自积极探索。除此之外，华为、腾讯、百度、360 等各大互联网企业也积极加快车联网和智能网联汽车信息安全相关建设。

随着汽车发展日趋电动化、智能化、自动化，信息安全问题是汽车智能化和网联化发展的必然产物。为了保证整车安全的更高要求，不仅需要保证车辆的功能安全，也需要保障车云的安全，即车内和车外网络以及云端安全。然而，由于车联网存在技术痛点、人才痛点以及管理痛点，就需自上而下，由内向外去加强技术防护、人才培养以及智能网联汽车信息安全相关的标准体系。

相较于传统的信息安全体系，针对智能网联汽车的信息安全问题，需制定整车企业信息安全发展思路。首先，构建以”检测-保护-响应-恢复”为体系的全生命周期智能网联汽车信息安全体系，以及制定针对智能汽车不同安全等级的响应机制和恢复策略，这是未来智能网联汽车信息安全的主要发展方向。从长远来看，智能网联汽车信息安全已经成为汽车产业甚至全社会关注的焦点，其信息安全防护需要从端、管、云多个角度进行考虑，分析汽车所面临的威胁，加强数据在全生命周期的访问控制，完善车辆使用过程中的身份认证体系，搭建贯通“端管云”三个层面的信息安全主动防护体系。

智能网联汽车的信息安全防护不只是保障车辆本身的信息安全，而是一个由通信、云平台和外部的新兴生态系统组成的整体性生态安全预警和防护。这种安全预警需要长期地进行，需要定期地对整个生态系统做好安全性检测，以便于发现潜在的危害性。因此，智能网联汽车的信息安全整体架构可以依据国际普遍采用的“云”“管”“端”“路侧单元”信息安全架构四个方面进行描述。

云平台肩负着控制指令的下达、信息汇集和存储等重要职责，其中对于信息安全进行防护的手段主要包括：利用成熟云平台安全技术保障车联网服务平台安全；部署云平台集中管控能力，保障云平台数据安全。车联网通信信息安全防护主要针对“车-云”通信，以加强访问控制并开展异常流量监测为主，主要防护手段有：加强车载端访问控制、实施分域管理，降低安全风险；基于 PKI 和通信加密，构建可信“车-云”通信，网络侧进行异常流量监测，提升车联网网络侧信息安全防护能力。

车端的信息安全防护工作主要从硬件安全、操作系统安全、应用安全和对内对外通信安全四个层面开展，主要的防护措施有：利用硬件安全模块，保障车端硬件安全；通过身份权限管理和访问控制机制，保证操作系统层面安全；应用层具备安全更新、抵抗

攻击、数据加密存储能力；对内对外通信层面保证数据的保密性、完整性及通信质量。路侧单元信息安全架构主要防护手段包括：对 RSU 配置专用的硬件加密模块并实施通信加密，保障设备安全管理，对 PC5 接口上的 C-V2X 消息认证鉴权以及保障业务功能安全管理。

2.2.2 V2X 无线通信技术发展进入爆发期

世界各方都已经将 V2X 无线通信技术发展看作是未来技术创新、产业培育和交通运输服务变革的重要方向。目前国际上主流的 V2X 无线通信技术有 IEEE802.11p 和 C-V2X（Cellular-V2X）两条技术路线。IEEE802.11p 技术方面，恩智浦、Autotalk 等芯片公司已开发 802.11p 商用芯片，CohdaWireless、Savari 等已可以提供车载单元设备（OnBoardUnit，OBU）和路侧单元设备（RoadSideUnit，RSU）。C-V2X 技术包含当前的 LTE-V2X 技术以及向后演进的 5G-V2X 技术，目前大唐可对外提供 DMD31 商用模组、华为可对外提供商用 Balong765 芯片组、高通可对外提供 9150 芯片组；与此同时，华为、大唐、星云互联、东软、万集、金溢、千方科技、华砺智行、Savari、中国移动等公司基于商用模组和芯片已经可以提供 OBU 和 RSU 设备。

国际社会在 V2X 技术路径选择上仍存竞争。由于 802.11p 技术成熟相对较早，美国政府倾向部署 802.11p 技术，而当地电信运营商、福特等更倾向于 LTE-V2X 技术。欧洲政府方面，欧盟 DGMove(欧盟运输总司)和 DGConnect（欧盟信息总司）持有不同意见；企业方面，大众、雷诺和博世支持 802.11p 技术，奥迪、宝马、标志雪铁龙等国际主流汽车厂商出于自动驾驶技术演进的考虑，支持 C-V2X 技术。日本一方面在 755.5-764.5MHz 专用频段开展基于 802.11p 的技术性能评估，另一方面在 5770-5850MHz 候选频段采取技术中立，将 LTE-V2X 作为另一个备选技术。

美欧日技术试验、应用示范培育 V2X 技术成熟和推广。美国交通部在密歇根对 802.11p 技术进行了大规模的测试验证，同时支持在纽约、怀俄明州、弗罗里达州三个地方开展利用 802.11p 技术的安全性评估；美国产业界积极推进 C-V2X 商用，2017 年 10 月福特、诺基亚、AT&T 和高通宣布开展美国首个 C-V2X 试验项目，2018 年 6 月福特、松下、高通以及加利福尼亚州的科罗纳多交通局宣布商用 C-V2X 技术。欧盟连续多年组织开展基于 ETSIITS-G5 的 Plugtest 技术试验，欧洲 5GAA 联盟联合汽车业和电信业共同推动 C-V2X 的技术成熟和产业化。日本丰田、本田、电装等汽车厂商和零部件供应商积极推进“ITS-Connect”技术产品研发和试验验证。

我国已具备大力发展 C-V2X 技术的基础条件。相比于 802.11p 技术，我国在 C-V2X 标准制定、产品研发、应用示范、测试验证等方面都取得了积极进展，为 V2X 产业化奠定了良好基础。在标准化方面，国内 LTE-V2X 标准体系建设和核心标准规范也基本建设完成，包括总体技术要求、空中接口技术要求、安全技术要求以及网络层与应用层技术要求等各个部分。在产品研发方面，我国已建成全球最大的 4G 网络，并初步形成了覆盖 LTE-V2X 系统、芯片、终端的产业链。在应用示范方面，工信部、交通部从车联网、车路协同不同角度积极推动国家示范区建设，无锡建成世界首个车联网（LTE-V2X）城市级开放道路示范样板，为跨行业产业协同营造有力条件，上海支持开展了世界首个跨通信模组、终端设备、整车厂商的“三跨”互联互通应用展示，验证了中国 V2X 标准的全协议栈有效性。在测试验证方面，IMT-20205G 推进组 C-V2X 工作组协同跨行业各方完成了实验室和小规模外场环境下的 LTE-V2X 端到端通信功能、性能和互操作测试，为大规模应用示范和商用部署奠定了基础。

V2X 安全需求发展

V2X 安全需求主要分为三个部分：直连通信安全防护、通信系统认证管理和通信系统持续监测。

在直连通信安全防护需求方面，要充分平衡信息完整性、真实性的防护和隐私保护。同时，还要结合 V2X 通信的高移动性的特点，以及低时延的要求，系统全面地构建 V2X 安全认证防护体系。

在通信系统认证管理需求方面，在对交通参与者签发证书的时候，要根据参与者的身份进行确权，从证书的类型上对其权限进行区别。执行确权操作、签发证书的功能需要分配给相应的主体并定义相关的流程。此外，还需要通过设定证书的有效期等方式，对参与者所赋予的权限进行时效管理；需要各种匿名化技术对参与者的隐私信息进行保护；需要通过证书撤销的机制限制已经具有 V2X 通信功能的参与者。

在通信系统持续监测需求方面，V2X 通信系统需要通过技术措施保护消息的安全性。在 V2X 安全系统中需要部署一种能够检测网络中异常行为终端的机制，检测具有异常行为的车辆，阻止其负面影响并确保 V2X 功能的长期可靠。

V2X 安全认证与管理体系发展

CCSA 的 YD/T3957-2021《基于 LTE 的车联网无线通信技术安全证书管理系统技术要求》明确了 V2X 安全管理体系架构，如图所示。图中左侧框内系统组件，实现对 V2X 设备进行数字证书签发的功能，从而该设备能够参与 V2X 通信；而右侧框内的组件，

主要实现的是对参与 V2X 通信的设备进行监测，发现判定异常行为并进行相应处置的组件。这两部分互相配合，形成 V2X 安全管理的闭环，确保 V2X 安全通信系统能够持续安全地正常工作。

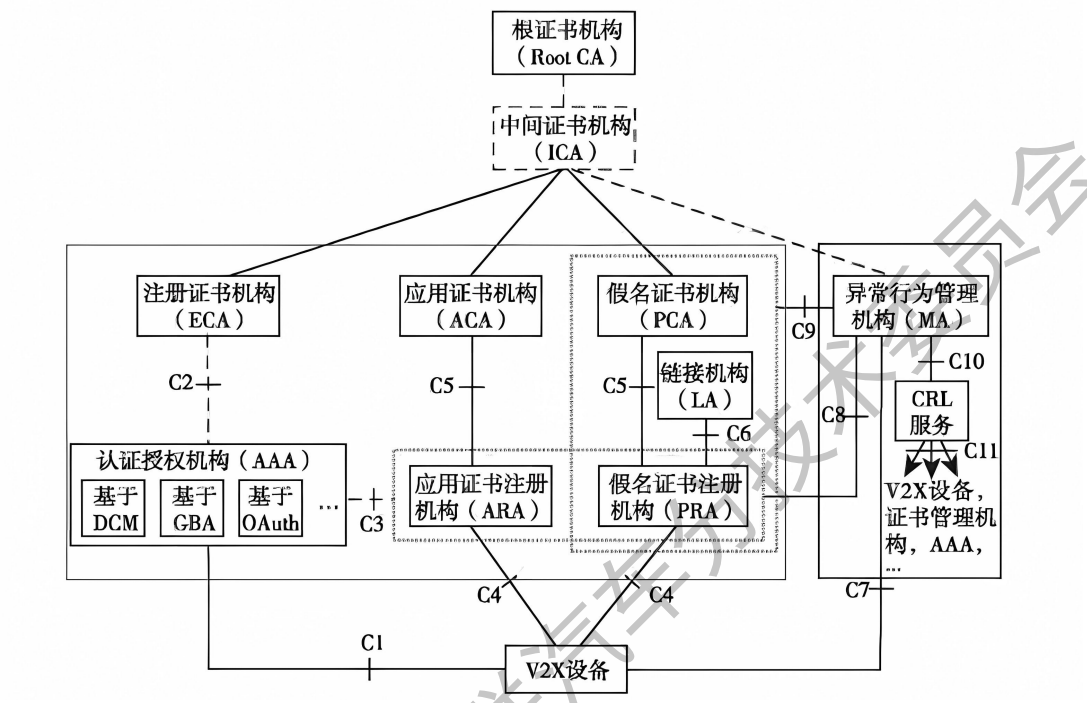


图 1 V2X 安全管理体系架构图

V2X 安全认证系统的信任机制和行为管理

1.集中式信任体系：在各行业根之上，部署全局根 CA,所有的子 CA 都在同一个根 CA 下管理，形成完整的证书链，建立集中式信任体系。由全局根 CA 签发各行业根 CA 证书，各行业根 CA 再签发各自行业内的子 CA 证书。

2.分布式信任体系：在分布式 CA 认证架构中，不同 CA 之间通过 CTL 实现交叉认证。CTL 包含全部受信任 CA 的证书，用于传达信任关系，取代基于证书链的交叉认证方式。可基于选举人机制由多个选举者共同维护 CTL,也可由专门的信任管理机构创建 CTL,建立多 CA 之间的信任关系。信任管理机构在新增、更新和撤销根 CA 证书时对 CTL 进行更新，使用信任管理机构的签名私钥对 CTL 进行签名，并通过专用通道将 CTL 下发至信任域内所有信任体。

3.异常行为管理：异常行为管理机构主要负责接收上报的异常行为报告，分析、识别系统中的异常行为者，然后形成对异常行为者的处置建议，如吊销证书等。在 V2X 异常管理的初期，异常行为管理机构主要通过接收来自车辆的上报，后续可能进一步拓展为与其他云端的态势感知系统进行联动，全面地对车联网进行监测和响应。识别异常

行为需要定义一些特征和检测方法，包括异常行为实例、报告机制和流程，从而进一步规划响应的方式，如定义需要被撤销证书的异常行为。

2.2.3 边缘计算助力智能网联汽车进入智能化深水区

多接入边缘计算（Multi-accessEdgeComputing，MEC）技术通过在网络边缘处部署平台化的网络节点，为用户提供低时延、高带宽的网络环境以及高算力、大存储、个性化的服务能力。面向车联网的应用场景，通过建设基于 MEC 的 LTE 网络架构，一方面可以通过减少数据传输的路由节点来降低 Uu 模式的端到端网络时延；另一方面可以利用 MEC 区域覆盖的特点，支持部署具备地理和区域特色的车联网服务。

MEC 与 LTE-V2X 相结合，丰富和扩展车联网业务应用场景。一方面，相比传统 Uu 模式通信连接中心云的服务模式，将 V2X 服务器部署在 MEC 上能够在降低网络及中心云端负载压力的同时，以更低的时延提供闯红灯预警、行人碰撞预警、基于信号灯的车速引导等场景功能；另一方面，利用 MEC 可实现 V2I2V 通信，在提供更可靠的网络传输同时确保满足低延时要求，实现前向碰撞预警、交叉路口碰撞预警等场景功能。此外，基于 MEC 的 LTE 网络环境具备强力的计算、存储、传输资源，配合路侧智能设备，具有对大量交通要素进行快速、准确的组织协调能力，可以进一步扩展 LTE-V2X 网络可支持的应用场景，如车辆感知共享、十字路口的路况识别与综合分析、高精度地图的实时分发、大规模车辆协同调度等。

ICT 企业纷纷布局 MEC 在车联网领域的应用。三大电信运营商及华为、中兴、诺基亚等设备商从 2016 年起先后开展各类 MEC 试点示范应用，但多数集中在边缘网关、边缘 CDN、边缘解码等场景。随着车联网和自动驾驶应用逐渐受到关注，2017 年底至今，国内各家 CT 企业相继将车联网视为 MEC 的重点应用方向，并积极从车联网应用场景与技术需求、MEC 与 LTE 融合的组网结构和关键技术、商业运营与推广模式等方面开展深入研究。中国信通院联合中国电信、中国联通等单位牵头在中国通信标准化协会开展面向 LTE-V2X 业务的 MEC 系列标准研制工作。此外，IT 企业开始进军基于 MEC 的车联网领域。2018 年 3 月阿里宣布战略投入边缘计算领域，并于 8 月与铁塔公司签署相关战略合作协议，随后宣布启动在杭绍甬高速部署 MEC 及路侧智能基础设施，开展服务应用试点。此外，滴滴、腾讯等互联网企业也在面向车联网的 MEC 领域积极探索并开展试验研究。

产业各界协同推动 MEC 在车联网领域的持续发展。在 LTE 网络中部署 MEC 可以

利用 Uu 通信模式构建低时延、大带宽、高可靠的网络环境，Uu 模式的 OBU 相对 PC5 模式具有更高的成熟度，有利于车厂在短期内开展业务部署与示范验证。ICT 企业积极开展基础设施建设，面向典型应用场景搭建测试床和开发基础应用，为业务验证与接口标准化提供支撑。智能交通与自动驾驶企业利用 MEC 作为车路协同系统中重要的边缘节点，积极推动在 MEC 部署并提供各类集感知、计算、通信于一体的智能交通和自动驾驶服务，构建安全、高效的道路环境。

在未来产业发展过程中，汽车、交通、信息通信等行业将持续协同推动 MEC 在车联网领域的持续发展：攻关诸如低抖动低时延的可靠传输、跨运营商业务连续性、数据与业务安全性等一系列技术问题;规范车载终端与 MEC 平台之间、MEC 平台与部署业务之间的接口协议，明确 MEC 与路侧基础设施的部署、运营、管理权限与责任，丰富 MEC 平台上车联网业务应用，构建全面完整的车联网 MEC 生态。

2.2.4 智能网联汽车信息安全芯片产业蓬勃发展

安全芯片即安全单元，是一种内部集成了密码算法并具备物理防御攻击设计的集成电路。安全芯片具有数据的加解密、身份认证鉴权、安全存储密钥的功能和防攻击设计。基于安全芯片全方位、高可靠、功能强大的安全机制，可为各类物联网设备提供身份认证、数据传输加密、敏感信息保护等安全服务。随着汽车的智能化、网联化，汽车内部越来越广泛地使用各类安全芯片。汽车电子应用中的安全芯片又需要具备产品设计“高安全性和高可靠性”、批量生产“高稳定性”的特点。本小节总结安全芯片的关键技术、产品形态和应用，介绍当前国内外主流安全芯片企业的动态，预测未来安全芯片的行业发展趋势，并给出安全芯片产业的发展启示。

芯片内部主要集成了微处理器、程序存储器、数据存储器、数据与程序、安全电路与传感器管理模块、密码运算协处理器等功能部件，根据使用者对芯片性能的不同要求，微处理器的性能、存储器的容量、芯片的性能均有所不同。安全芯片的防御技术主要包括加密算法实现、防侧信道攻击、防故障攻击、防物理攻击、高安全 CPU、存储设备防护和总线防护技术，配合其他软件可实现安全启动、安全存储、身份认证、密码算法实现等功能，可应用于关键组件系统加固、传感器安全防护、T-box 安全隔离、OTA 安全升级、车云通信安全防护、V2X 通信安全防护等场景。

智能安全芯片行业中游企业运营模式主要分为 IDM 模式与 Fabless 模式。IDM 模式，是集 IC 设计、制造、封测甚至下游电子终端产品生产于一体的模式，是早期多数集成

电路企业采用的运营模式，代表企业有紫电集团、NXP，英飞凌等；Fabless 模式，只负责芯片的电路设计与销售环节，将生产、测试、封装等环节向其他企业外包，代表企业有握奇数据、瑞达信安、晨元数据等。由于涉及国家安全，国内的安全芯片行业倾向于生产带国密算法的产品代表性的厂商有华大电子、华虹集成、大唐微电子、同方微电子、天津国芯、国民技术、复旦微电子公司，而智能卡成卡供应商则数量众多，主要有握奇数据、东信和平、华虹、华大、恒宝、明华公司等企业。

随着电子电器在汽车产业的应用范围逐渐扩大，2017-2022 年全球汽车电子市场规模将以 6.7%的复合增速保持增长态势，预计至 2022 年全球市场规模将超过 2 万亿元，而国内市场规模将接近万亿元大关。而技术发展将呈现功能日趋融合、高性能、自主可控等趋势，安全芯片需求开始受到车厂的重视。目前国内厂商信大捷安、华大电子、紫光同芯、天津国芯、上海芯钛均推出了车规级安全芯片，芯片产品获得 AEC-QlOO 认证，应用于 V2X、ECU 控制、车机控市、车载 eSIM、ETC 电子收费等领域，其竞争亦日趋激烈。

随着国际芯片市场竞争的加剧，安全芯片的发展直接关系到国家信息安全，为了国家的“信息主权”研制采用国产密码算法的、自主可控的安全芯片势在必行。从信息技术和控制技术发展的角度来看，物联网应用领域对安全芯片的发展具有极大的战略意义，也是安全芯片未来应用机会最多、潜力最大的主要市场。

2.3 量子技术发展对智能网联汽车的安全威胁

对于智能网联汽车而言，智能汽车本身的信息安全问题在应用系统和密钥安全方面更为凸显，其采用的数据传输加密技术主要用于线路加密与端—端加密两种。线路加密侧重在线路上而不考虑信源与信宿，是对保密信息通过各线路采用不同的密钥提供保护。端—端加密指信息由发送端自动加密，并且由 TCP/IP 进行数据包封装，然后作为不可阅读和不可识别的数据穿过通信网络，当这些信息被接收后，将被自动重组、解密，而成为可读的数据。

作为现有超级计算机的“接班人”，量子计算机正处于蓬勃发展之中，它在分析数据及处理复杂运算时其速度是远超我们的商用传统计算机。正在探索的所有潜在质量控制技术，有十分之一的技术可以用于汽车行业。汽车将成为量子计算的重要价值池之一，它能推进科学和技术发展进步。预计到 2025 年汽车行业相关进展的评估对汽车业务将产生重大的经济影响，估计其价值在 20 亿至 30 亿美元之间。量子计算非常适用于解决

智能网联汽车研究人员长期以来一直困扰的特定问题，包括车辆导航、自动驾驶安全性、路线优化，材料耐用性和燃料电池优化等问题。

依托于量子技术的更新迭代，量子计算攻击接踵而至。量子计算攻击会对传统车联网安全通信体系造成极大冲击。倘若被黑客恶意利用会对智能网联汽车带来巨大安全威胁，尤其是对传统加密算法是不小的挑战。目前，智能网联汽车涉及人-车-路-云间大量而广泛的信息传输及控制应用场景采用的传统加密算法主要是建立在数学计算的基础上，传统计算机需要数万年甚至亿万年才能将密钥暴力破解。而现有量子计算在数字分解和数据库算法检索中能极大缩短时间和减少使用资源，这种能力使得智能网联汽车通信网络中的公钥加密在量子计算面前变得不堪一击。这将彻底颠覆和破解现代信息系统所依赖的数字加密技术，导致基于公钥加密的全球现存通信系统、安全设备毫无安全性可言。

智能网联汽车信息交互的保密性、完整性和真实性，不仅涉及个人隐私、企业经济效益，甚至影响人身安全、社会繁荣稳定。而量子保密通信利用量子力学原理，传输读取加密信息的“密钥”，理论上难以盗取及破解密码，为对抗未来量子计算带来的信息安全风险，使用量子安全技术才能保障智能网联汽车全生命周期安全。量子保密通信能够在链路加密、端到端传输加密、存储加密、密钥管理、数据完整性认证等方面发挥重大价值。它是保障信息安全的利器，将会为智能网联汽车领域信息交互安全问题提供新思路。

2.4 量子技术带来的新威胁

量子技术的发展可能会带来一些新的威胁和挑战，尤其是在密码学、通信安全和数据隐私领域。

2.4.1 量子计算对现有加密系统的威胁

量子计算具有破解传统加密技术的潜力，例如 RSA 和 DSA。量子计算的 Shor 算法和 Grover 算法可以在相对较短的时间内解决复杂的数学问题，这可能会使当前的加密标准不再安全。因此，需要开发抵抗量子计算攻击的后量子加密技术。传统加密技术是建立在数学难题上的，这些难题基于当前计算机系统的计算能力，被认为是困难解决的。这些算法包括 RSA、DSA、ECC 等，它们在信息传输、数据存储和身份验证中广泛使用。RSA（Rivest-Shamir-Adleman）加密技术，例如，基于大整数分解问题。大整数分

解问题的难度在于将大的合数分解为其素因数。RSA 的安全性依赖于计算机无法有效地分解极大整数，因为这需要大量时间和计算资源。同样，其他传统加密技术也依赖于类似的数学难题，如离散对数问题和椭圆曲线离散对数问题。然而，量子计算的威胁在于它具有超越经典计算机的能力来解决这些数学难题。

Shor 算法是一种用于因子分解的量子算法，可以在多项式时间内分解大整数。这个算法的速度比传统算法快得多，这意味着 RSA 等基于大整数分解问题的加密技术可以在相对短的时间内被破解。这是一个巨大的威胁，因为很多互联网安全协议和数据加密都依赖于这些加密技术。

Grover 算法用于在无序数据库中搜索特定项。它可以在平均 O(√N)时间内找到一个项，而经典计算机需要 O(N)时间。这使得传统密码学中的散列函数、对称密钥加密等算法变得不再那么安全，因为攻击者可以更容易地破解密码。

量子计算的威胁不仅局限于破解加密技术，还可能对数字签名、身份验证、数据隐私和金融交易等领域产生广泛影响。它具有破解传统加密技术的潜力，从而危及信息安全和隐私。在面对这一威胁时，科研人员和安全专家正在积极寻找解决方案，包括量子安全加密方法和后量子加密技术。随着量子技术的不断发展，信息安全领域将面临巨大的挑战，但也将迎来创新和改变，以确保数据和通信的安全性。

2.4.2 数据隐私威胁

量子计算可能会威胁到现有的数据隐私保护方法。如果加密的数据被窃取并在未来被解密，那么敏感信息可能会暴露。这可能对金融、医疗保健和其他行业的数据安全产生影响。数据隐私一直是信息时代的重要问题，而随着量子计算技术的不断发展，传统的数据隐私保护方法可能会受到新的威胁。在当前的数字化时代，数据隐私保护已经成为了一项关键任务。组织和个人存储和传输大量敏感信息，包括个人身份信息、财务数据、医疗记录等。为了保护这些数据，采用了一系列加密和安全措施，传统数据隐私保护方法当中包括：

1)对称密钥加密：使用相同的密钥进行加密和解密，这种方法有效，但需要确保密钥的安全传输和存储。

2)非对称密钥加密：这种方法使用一对密钥，一个用于加密，另一个用于解密。私钥是保密的，公钥是公开的，但它们之间的数学关系保证了数据的安全。

3)数据哈希和签名：数据哈希用于验证数据的完整性，数字签名用于验证数据的来

源和完整性。

4)访问控制和身份验证：访问控制列表、用户身份验证和多因素认证等方法用于确保只有授权用户能够访问敏感数据。

然而，这些传统数据隐私保护方法的安全性在面对量子计算的威胁时可能会受到严重挑战。量子计算对数据隐私的潜在威胁可能对各行各业产生广泛影响其中包括：1）金融业：金融机构处理大量敏感的财务数据，包括交易记录、客户身份信息和账户信息。如果这些数据暴露，将导致巨大的财务损失和信誉风险。2）医疗保健：医疗保健行业存储大量的患者医疗记录，这些记录包含患者的个人健康信息和医疗历史。数据泄露可能导致个人隐私泄露和医疗诊断的泄露。3）政府部门：政府部门处理包括国家安全、法律执法和公共政策等重要信息。数据泄露可能危及国家安全和公共利益。4）企业和知识产权：企业存储大量的商业机密和知识产权，这些信息可能价值巨大。如果这些数据泄露，将损害企业竞争力和创新。

2.4.3 量子技术滥用

量子技术可能被用于不法用途，例如破坏传统的加密和安全系统、网络攻击和间谍活动。政府和企业需要加强监管和国际协作，以防范潜在的滥用。量子技术的崛起代表了科学和技术领域的重大突破，但同时也引发了对其滥用的担忧。虽然量子技术有着巨大的潜力，但它们也可能被用于不法用途，威胁到信息安全、隐私和国际关系。

量子技术的滥用可能包括以下方面：1)破坏传统的加密和安全系统：量子计算具有破解传统加密算法的潜力，如 RSA 和 DSA。这意味着加密的数据和通信可能不再安全，因为攻击者可以使用量子计算来解密敏感信息。2)网络攻击：量子计算可以用于进行网络攻击，如分布式拒绝服务（DDoS）攻击、恶意软件传播和网络渗透。量子技术可能使攻击更加复杂和具有破坏性。3)窃听和间谍活动：量子技术可以被用于进行大规模的通信窃听和间谍活动。窃听者可以利用量子技术来窥探敌对国家、政府机构、企业和个人的机密通信。4)金融犯罪：量子技术可能被用于进行金融犯罪，如盗取银行和金融机构的财务数据、窃取信用卡信息和进行欺诈交易。5)恶意用途的量子通信：尽管量子通信本身是为了提高安全性而设计的，但它也可能被用于不法用途，如加密和隐瞒恶意行为，以逃避监测和追踪。

为了应对量子技术的潜在滥用，政府、国际组织和企业需要采取一系列措施，包括政府应制定相关法规和政策，以规范量子技术的开发和使用。这些法规应明确禁止滥用，

并规定滥用量子技术的惩罚。政府和监管机构应加强对量子技术的监管，确保其合法使用，同时防止不法用途。国际社群应加强合作，以制定国际标准和协议，以应对量子技术的滥用。这可以包括信息共享、技术合作和共同打击跨境犯罪。政府和国际组织应加强对公众和企业的教育和宣传，提高他们对量子技术滥用的认识，以便更好地应对潜在威胁。政府和企业应加强网络安全措施，以应对量子技术带来的网络攻击。这包括采用先进的入侵检测和网络监控工具。为了应对量子技术的滥用，必须进行更多的技术研究和发展，以开发新的安全解决方案和反滥用工具。国际谈判和协作将发挥关键作用，以防范量子技术的滥用。国际组织和国家应共同努力，制定相关政策，建立合作机制，以应对共同的威胁。

随着量子技术的不断发展，对其滥用的担忧也日益增加。尽管量子技术具有广泛的应用潜力，但它们也可能被用于不法用途，威胁到信息安全、隐私和国际关系。为了应对这一挑战，政府、国际组织和企业需要采取一系列措施，包括制定法规、加强监管、国际协作、教育和技术研究。只有通过合作和共同努力，我们才能更好地应对量子技术滥用的潜在威胁，确保其安全和合法使用。

2.4.4 数字签名和身份验证

量子计算可能对数字签名和身份验证造成威胁，因为它们依赖于传统的加密技术。新的量子安全数字签名和身份验证方法将需要开发和采纳。数字签名和身份验证是现代通信和信息安全中至关重要的组成部分。它们用于确保数据的完整性、真实性和不可否认性，以及确认通信双方的身份。然而，随着量子计算技术的发展，传统的数字签名和身份验证方法可能会受到威胁，因为量子计算的独特能力使得传统加密技术容易受到攻击。

传统数字签名和身份验证是基于数学算法的，这些算法依赖于当前计算机系统的计算能力，被认为是困难解决的问题。以下是一些传统数字签名和身份验证方法的关键要素：

1) 传统数字签名使用非对称密钥加密，其中一个密钥用于加密，另一个用于解密。私钥是保密的，而公钥是公开的。签名者使用私钥创建数字签名，而验证者使用公钥来验证签名的真实性。
2) 数字证书是一个包含公钥和身份信息的电子文档，由可信的证书颁发机构（CA）签发。数字证书用于确认公钥的真实性，以防止中间人攻击。

3) 哈希函数用于生成消息的摘要，该摘要可以被数字签名。它确保消息的完整性，因为任何对消息的更改都会导致不同的摘要。

4) 数字签名算法用于生成数字签名，它依赖于私钥和消息内容。一旦签名创建，验证者可以使用公钥来确认签名的真实性。

5) 身份验证过程通常涉及用户提供凭证，如用户名和密码，以证明他们的身份。多因素身份验证也包括生物识别、智能卡和令牌等。

量子计算的崛起威胁到了传统数字签名和身份验证的安全性，这主要归因于两个重要的量子算法：Shor 算法和 Grover 算法（具体见 2.4.1）。量子算法的威胁不仅影响数字签名和身份验证的安全性，还可能对数据隐私、金融交易和政府通信等领域造成广泛影响。为了应对量子计算的威胁，正在研究和开发新的量子安全数字签名和身份验证方法随着量子技术的发展，需要认识到它带来的潜在威胁，并采取适当的措施来保护信息安全和隐私。这可能需要投资于量子安全技术的研发和部署，以及更新和升级现有的加密和安全系统，以应对这些新威胁。

3. 量子通信技术的发展趋势

3.1 量子通信技术简介

量子通信作为量子信息科学的重要分支，是利用量子态作为信息载体来进行信息交互的通信技术。现阶段，量子通信的典型应用形式包括量子密钥分发（Quantum Key Distribution，QKD）和量子隐形传态（Quantum Teleportation, QT）等。量子密钥分发可用来实现经典信息的安全传输；而量子隐形传态是传递量子信息的有效手段，有望成为分布式量子计算网络等应用中的主要信息交互方式。

量子保密通信是指以具备信息理论安全性证明的 QKD 技术作为密钥分发功能组件，结合适当的密钥管理、安全的密码算法和协议而形成的加密通信安全解决方案。

3.1.1 量子通信技术的理论基础记框架

量子密钥分发是最先实用化的量子信息技术，是量子通信的重要方向。量子密钥分发可以在空间分离的用户之间以信息理论安全的方式共享密钥，这是经典密码学无法完成的任务。基于国际学术界的广泛共识，包括 2010 年沃尔夫物理学奖获得者 Anton Zeilinger 教授等在内的众多国际学者通常将量子密钥分发就称为量子通信；美国物理学

会的学科分类系统 PhySH 将量子密码作为量子通信条目下的一个子条目；欧盟最新发布的量子技术旗舰计划《量子宣言》，将以量子密钥分发为核心的量子保密通信作为量子通信领域未来的主要发展方向。

现有实际量子密钥分发系统主要采用 BB84 协议，由 Bennett 和 Brassard 于 1984 年提出。与经典密码体制不同，量子密钥分发的安全性基于量子力学的基本原理。即便窃听者控制了通道线路，只要窃听者没有掌握能攻入合法用户设备内部的侧信道，量子密钥分发技术就能让空间分离的用户共享安全的密钥。学术界将这种安全性称之为“信息理论安全”（也可称为“无条件安全”），它指的是拥有严格数学证明的安全性；依赖的基础是量子物理学原理，即要求窃听者不能拥有违反量子物理学原理的技术，但是可以拥有任何不违反量子物理学原理的技术，例如计算能力任意强大的计算机，包括量子计算机。量子密钥分发的这种安全性，与计算复杂度无关，因此不论对手拥有多大的计算能力，其安全性都不会受到影响。

量子密钥分发安全性基于以下量子物理原理：

1. 单量子不可分割

量子是物理量变化的最小单元，单个量子不可分割。量子密钥分发若采用单个量子（通常为单光子）作为信息载体，则攻击者无法通过窃取单量子一部分并测量其状态的方法来获得密钥信息。

2. 未知单量子态无法精确测量

根据海森堡测不准原理（现在多称为不确定性原理），量子的一对非对易物理量不能被同时测准。在量子密钥分发双方随机选择非对易物理量的其一进行编解码时，攻击者即使截取了量子信号，也无法有效测准单量子的状态。如果攻击者根据测量结果重新制备一个量子发送给接收方，将不可避免地改变单量子状态，导致解码结果与编码不一致。量子密钥分发双方可通过检测误码率来判断攻击行为及其强度，并在后处理中进行消除。

3. 未知单量子无法精确复制

量子相干叠加（同时处于多种状态）的特性使得不存在通用的方法获得任意未知单量子的多个精确一致拷贝。在量子密钥分发双方随机调制单量子态时，如果攻击者试图在截获量子信号后复制多个拷贝，将不可避免地导致复制态与初始态存在偏差，进而导致解码结果与编码不一致，量子密钥分发双方同样可进行检测发现和后处理消除。

以上述物理原理为基础，目前对于一部分量子密钥分发协议，如：BB84、E91、

MDI-QKD 协议等，已经给出了严格的数学推导，可证明其信息理论安全性。量子密钥分发协议相对传统密钥分发在安全性方面有以下优势：量子密钥分发的安全性基于如上所述的量子力学基本原理，不依赖于对计算复杂性的要求和假设，其安全性和理论完备性能够得到充分保证；即使在量子计算技术成熟的条件下，其密钥分发过程也具有可靠的安全性。量子密钥分发可以有效应对计算技术以及量子计算飞速发展给传统密码体系带来的严重威胁。

量子保密通信是在抗量子攻击等特定需求下的全新的、有效的密码学补充手段，依据结合方式的不同，量子保密通信系统可具有多种类型。例如，可证明信息理论安全的 QKD 技术与同样可证明信息理论安全的一次性密码本（One Time Pad，OTP）加密方案和 Wegman-Carter 认证方案相结合，形成具备信息理论安全性的量子保密通信系统。又如：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，可实现可支持大带宽业务的、具备前向安全性的量子保密通信系统。

参考传统的网络架构模型，量子保密通信系统体系架构框架如下：

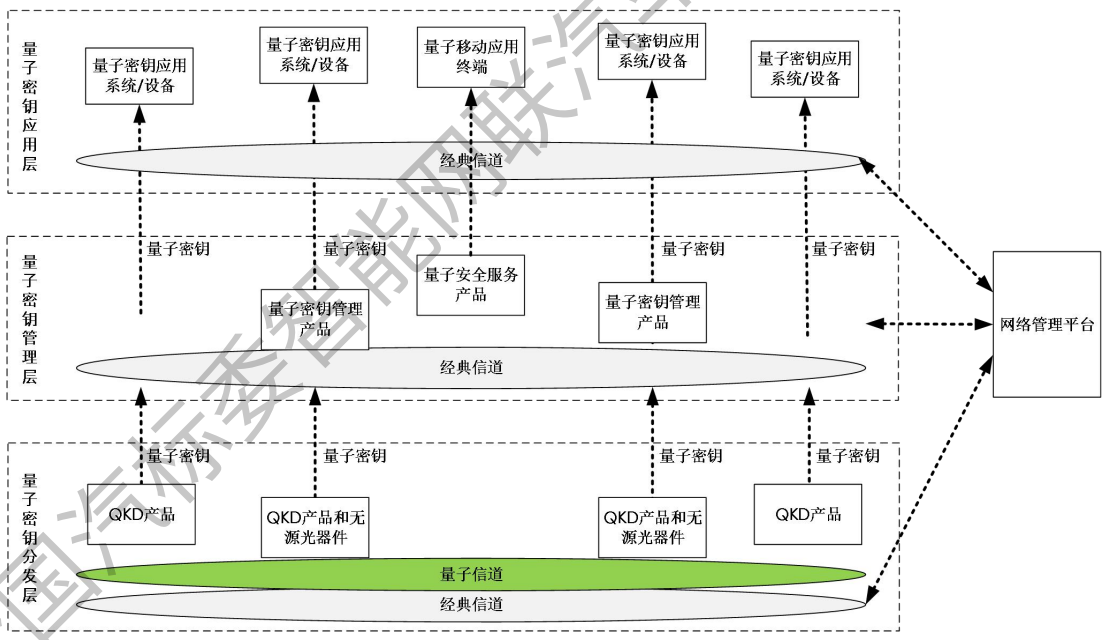


图 2 量子保密通信系统架构图

量子密钥分发层：主要包括量子密钥分发产品、无源光器件等，借助经典信道和量子信道，完成量子密钥的协商和分发，可为量子密钥管理层提供量子密钥。

量子密钥管理层：可在经典信道中实现量子密钥的存储、传输和中继，为量子密钥应用层系统提供量子密钥的服务。

量子密钥应用层：主要包括量子密钥应用系统、设备和移动应用终端，使用量子密钥管理层提供的量子密钥对量子密钥的应用提供安全服务。

网络管理层：主要包括量子网络管控系统，管控对象包括量子保密通信网络内的被管设备。实现对量子通信网络的监控和管理。

3.1.2 关键共性技术及其成熟度

量子保密通信应用的实现面临多方面的挑战，包括如何低成本、高效率地部署量子通信网络，如何高效地利用现有网络资源，适应复杂的网络拓扑、业务环境，如何实现差异化服务以满足各类用户的安全需求，如何保证网络的兼容性和安全性要求等。以下本报刚将分别针对高性能量子密钥分发技术、可信中继技术、可信中继安全性增强、密钥中继路由选择和经典量子波分复用等关键技术进行说明：

高性能量子密钥分发技术

1） 高性能诱骗态光源产生技术

人类在确保通信安全方面不断提出更高的要求，但经典的通信方式基于数学复杂性，存在其固有的不安全性。而基于量子力学基本原理的量子保密通信是唯一被证明是信息理论无条件安全的通信方式。然而由于技术的限制，在现有的实现中，不存在低成本的实用化单光子源。物理实现上使用的弱相干光源所产生的并非真正的单个光量子，会有一定的几率出现多光子情形，从而导致现实量子保密通信的安全距离一度限制在 30km 以下。因此采用诱骗态方案，使用几种不同光子数密度的弱相干态光源，分别作为信号态和诱骗态，对比接收到的信号态和诱骗态的个数和错误率，通过物理和数学的分析处理就可以得到在最坏情况下窃听者能够得到的最大信息量，进而得到该系统的安全密钥成码率。

诱骗态方案极具实用化价值，使得弱相干光在安全性上可以和完美的单光子源相媲美，而在速率、成本上都远优于单光子源，最重要的是相干激光技术及其成熟，这使得量子保密通信的实用化大幅提高。

诱骗态方法可以把安全距离大大扩充，达到实用化阶段。基于诱骗态的量子保密通信技术，已经在基于弱相干光的 BB84 方案中大大提高了安全通信的距离和密钥产生速率，显示出了巨大的优势。并由于只需对原有弱相干光源做很小的改造即可实现，因而具有相对单光子源低成本、易操控的优势，为量子保密通信的实用化奠定了重要的技术基础。

国内科研团队对诱骗态 BB84 方案的安全性证明、效率策略均有深入的研究，在 PRL、PRA、NJP 等国际刊物上发表多篇理论文章；在国际上最早完成了 100 公里以上的诱骗

态量子保密通信实验，后又率先完成 200 公里的诱骗态量子保密通信实验，已经发展出了成熟、可靠的诱骗态实现方案。

高速诱骗态光源是目前实用化的量子保密通信系统实现的关键组件。和经典通信相比，量子密钥分发光源要求实现高速光脉冲输出，具备低抖动、脉宽窄、高消光比等特点。其次，为了实现诱骗态方法，要求能控制光源随机地改变输出脉冲强度。同时光源需要具备强度衰减功能，衰减至每脉冲单光子能量级别时，仍需要保持非常好的光强稳定性。

目前，国内已开发并掌握具备光强反馈功能的外调制技术，调制激光二极管的输出的光脉冲强度，产生光强稳定的信号态，诱骗态和真空态。

2） 高性能近红外单光子探测技术

单光子探测系统是量子密钥分发系统中处于核心地位的器件，其参数指标直接制约着量子保密通信系统的性能，其性能提升对于量子保密通信系统起着基础性的作用。针对远距离、高速率实用化量子保密通信系统中所必需的关键技术和关键器件突破，在提升关键器件性能的基础上可以提高通信网络的容量，扩展通信网络的通信速率。为最终实现多用户环境下的量子保密通信网络应用奠定坚实的技术基础，并可推动量子保密通信大规模实际应用。

当前，国际上通用的通信波段单光子探测器有：超导探测器、铟镓砷雪崩二极管单光子探测器。超导探测器利用工作在 4K 低温下的铌化锂超导纳米线吸收单光子，单光子的能量可以使纳米线温度改变，出现电阻，从而实现单光子探测。超导探测器具有暗计数低（10Hz 左右），时间分辨好（时间晃动约 70ps）等优点，但商用超导探测器需要连续的液氦制冷才能维持有效工作，液氦制冷设备体积大、成本昂贵，为量子密码实用化设立了障碍。因此，性能良好、成本经济的铟镓砷雪崩二极管单光子探测器是量子保密通信产品和量子保密通信网络中最佳的候选。

3） 铟镓砷雪崩二极管单光子探测

探测器利用工作于盖革模式（Geiger Mode，工作偏压大于雪崩电压）的 InGaAs/InP 雪崩光电二极管（APD）进行红外单光子探测。光子入射到光敏面后，以一定的概率激发光生载流子，随后被加速、雪崩，产生可甄别的宏观雪崩电流。

高速正弦门控技术是实现探测器速率提升、门控信号压窄的重要技术之一。目前我国已掌握关键技术并研制成功高速正弦门控探测器。该类探测器采用射频滤波和正弦门控技术，具有元器件工艺成熟、性能稳定、高度集成化等特点。探测器还集成 TEC 深

度制冷技术、后脉冲识别与抑制技术，信噪比达到了国际上同类高速探测器最好的结果。高信噪比的雪崩探测信号保证了探测器不会因为电子学噪声而出现误探测事件，提升了探测器的性能，可保障百公里级别光纤传输下量子保密通信系统的性能。

后脉冲效应是 InGaAs/InP 单光子探测器的重要效应，也是限制探测器性能的最主要因素之一。InGaAs/InP 探测器在每次雪崩之后，由于倍增层材料的杂质和缺陷会捕获部分雪崩过程中产生的载流子。这部分被捕获的载流子会有一定的寿命，寿命的长短取决于多种因素包括温度。然而，当被捕获的载流子释放时，如果雪崩光电二极管仍然工作在盖革模式即反偏电压大于雪崩电压，那么这个释放的载流子就有可能再次激发一次雪崩信号，这种效应称为后脉冲效应，开发探测器后脉冲抑制技术，可以减小探测器后脉冲对于量子保密通信错误率的贡献，有助于提升系统最大工作距离和提高成码率。目前国内已研发后脉冲抑制技术，通过输出脉冲时域分布进行脉冲判断，若为后脉冲则抛弃该计数，进而减小后脉冲影响，满足高速率远距离量子保密通信需求。

4） 高性能偏振反馈补偿技术

偏振编码容易实现光开关切换，正常运行错误率低，接收方固有插入损耗比相位编码低。但在光纤传输过程中，光的偏振状态会产生变化，而且随着环境变化还会改变。需要高速偏振反馈补偿技术，补偿光纤信道对于偏振态的扰动，将通过光纤信道传输之后的偏振态回复到初始状态。目前已研发高性能偏振反馈补偿系统，通过主动对光纤产生形变，利用光纤形变引起的偏振状态改变可以补偿光传输过程中的偏振变化。

技术途径：偏振反馈模块以基矢比对错误率输出作为数据的入口，启动过程中先进行 HV 偏振反馈，再进行+-偏振反馈，反馈控制需要通过高压板的高压输出来控制电控偏振控制器，调节相应的对比度。设置对比度调节阈值，如 100:1。在实现过程中结合粗步长和细步长扫描方式，可以迅速扫描到对比度峰值位置。

一般的反馈方案是在信号光之外加强参考光进行偏振反馈，通常这需要中断系统的工作流程。目前较新技术方案利用信号态和诱骗态随时实现偏振状态检测，实现反馈补偿。因此，在偏振反馈补偿时，不需要中断系统的工作状态，可提高系统效率；同时还可以及时压制噪声，有效地提高系统成码率。该高速偏振反馈补偿技术应具有以下特点：高效的闭环偏振反馈控制算法，提高了收敛精度和收敛速度，提高了设备的可用性和总体的成码速率。新颖的即时反馈实现方案，利用信号态和诱骗态随时实现偏振状态检测，实现反馈补偿。适用于偏振相对缓变的工作环境，可随时压制噪声，提高信噪比，有效提高系统成码率和工作效率。

QKD 网络可信中继技术

远距离通信需要克服传输介质损耗对信号的影响。经典通信中，可采用放大器增强信号。但在量子网络中，由于量子不可克隆定理，放大器是无法使用的。基于量子纠缠交换，可以实现量子纠缠的中继，进而实现远距离量子通信。但量子中继技术难度很大，还不能实用。目前，为构建远距离量子密钥分发基础设施采用的过渡方案是可信中继器方案。

其具体原理是：考虑两个端节点 A 和 B，及其之间的可信中继器 R。A 和 R 通过量子密钥分发生成密钥 KAR。类似地，R 和 B 通过量子密钥分发生成密钥 KRB。A 和 B 则通过 R 产生共享会话密钥 KAB 的过程如下图所示：A 将 KAB 通过 KAR 以一次性密码本（One-time-pad，OTP）加密后发送至 R，R 解密得到 KAB。R 使用密钥 KRB 重新加密 KAB，并将其发送给 B。B 解密后获得 KAB。A 和 B 通过共享密钥 KAB 进行加密通信。这种将密钥以一次一密的方式从 A 传递至 B，可以实现信息理论安全的密钥分发，理论可防止任意的外部窃听者攻击。但这种方案要求任何一个中继节点必须是安全可信的。

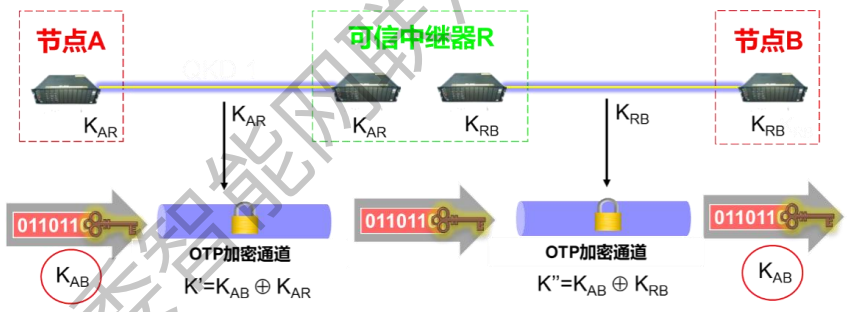


图 3 可信中继原理图

可信中继安全性增强技术

在可信中继节点，密钥已经失去量子特性，不再受量子原理的保护，结合传统的信息安全技术对节点进行防护，同时改进密钥中继方案，可有效降低可信中继的防护难度。一种改进的密钥中继技术是异或中继技术，在中继节点处只会暂存经过异或后的量子密钥。因此在中继节点除了量子密钥刚刚生成后极短的时间内，其他时间都不会出现量子密钥明文。攻击者只有在刚刚生成量子密钥时就攻入系统才可能窃取到量子密钥，进而破获用户密钥；在其他时刻攻击中继，都无法影响用户密钥的安全。这种方案可以很大程度上减轻中继节点的安全防护难度。异或中继的原理如下图所示：

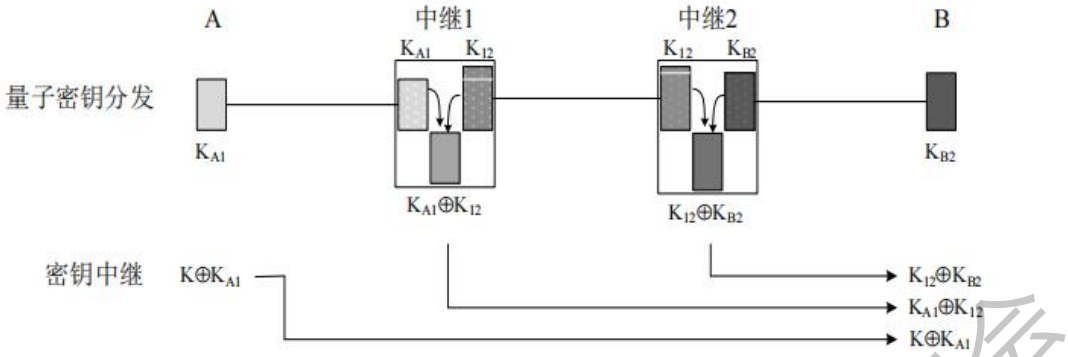


图 4 密钥异或中继技术原理

为了减少用户密钥被网络提供者记录的风险，还可以利用端到端的密钥共享方案。用户可以将 QKD 网络提供的当前密钥和其他来源共享密钥组合起来使用，这样记录 QKD 网络的当前密钥并不能直接获得用户密钥。其他来源的共享密钥并不一定需要额外的密钥分发技术，它们也可以是 QKD 网络历史上提供的密钥。在这种情况下，QKD 网络记录并获取用户密钥的难度和成本会大大提高。采用端到端的密钥共享方案有双重的好处，既可以减少用户密钥被网络提供者记录的风险，也有助于提高中继密钥的安全性——即使攻击者在一时一地攻破中继节点，也不能获得用户密钥——从而大幅减低了用户密钥被窃听破解的风险。

支持灵活组网的密钥中继路由技术

密钥中继的路由技术是支撑量子保密通信网络灵活组网的关键。量子保密通信网络一般使用密钥生成速率、密钥缓存量和密钥中继消耗速率等参数描述链路的状态，并评价链路质量。所有链路的状态、连接关系、质量等构成一个动态的网络拓扑数据库。量子保密通信网络中的中继路由表即根据这个数据库，按照距离优先、链路质量优先或者综合评定等策略来决策并动态地给出密钥中继路由。网络中各个节点实时地更新网络拓扑数据库，共同维护路由表或者委托核心节点/网络来维护路由表。对于大规模的量子保密通信网络，一般通过分域和分层管理来减低路由表维护的难度，提高路由收敛的速度；从而实现灵活组网，提高网络的兼容性和可扩展性。

量子密钥分发与经典光通信共纤传输技术

通过量子信道与经典光信道复用光纤传输，可有效节省量子保密通信网络部署所需的纤芯管道资源，利用现有光通信网络资源，实现经济、高效建网的目标。该技术主要需要解决的问题是功率较强的经典通信光信号的功率谱噪声和拉曼散射、四波混频等非线性噪声对量子通信的干扰问题。共纤传输的方案包括波分复用、时分复用、空分复用

等，其中波分复用方案和现网的光通信系统最容易融合，但其主要的困难在于长距离和强经典光功率条件下拉曼散射噪声难以滤除。

如图所示，基于波分复用的共纤技术将量子光信号、同步光信号和协商光信号分别安置在不同的波长上，通过窄带滤波和波分复用器合成一路进行传输。目前，量子/经典共纤传输波分复用方案已经具备实用化能力，并得到了实验验证和现网演示，下一步需要提高技术的成熟度，提高共纤传输距离。

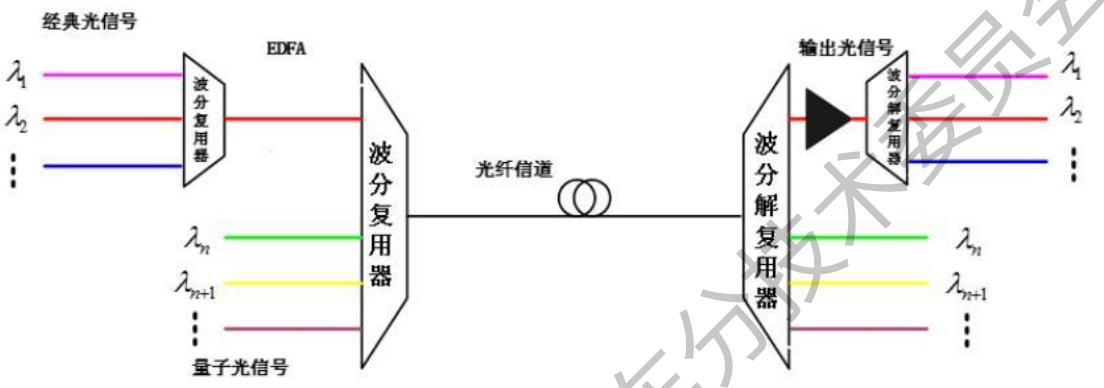


图 5 基于波分复用的量子密钥分发与经典光通信共纤传输原理

量子安全服务系统技术

量子安全服务系统技术主要实现将量子密钥资源，通过安全加密机制拓展到量子密钥分发专网以外的网络，使用量子安全介质产品融合到移动终端，并对终端密钥进行动态管理，为用户提供任意多点间密钥协商、接入认证、访问控制、安全存储等功能服务，从而使得更多的用户享有高安全等级的服务；能够快速响应用户需求实现定制开发，各行各业基于这个平台发挥各自的专业和产业优势，形成新的量子密钥应用，保障通信安全。

量子安全服务系统技术基于量子密钥分发和一次一密算法进行会话密钥的分发，量子密钥分发和一次一密算法可以保证会话密钥的安全性，理论上具备信息论安全，可以为移动应用业务数据传输提供高安全的解决方案。

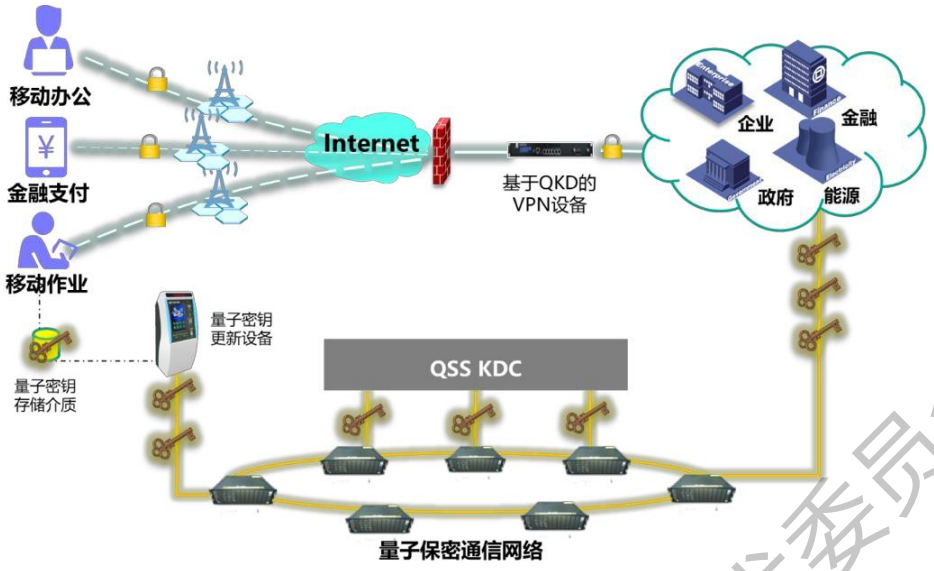


图 6 量子安全服务系统架构

量子安全服务系统技术基于量子密钥分发网络和量子随机数技术，将量子技术和传统密码技术相结合，可以为用户提供高安全等级的无线网络（4G/5G）安全通信解决方案，相比于传统的公私钥体系，主要具备以下特点：

1、密钥来自于可理论证明安全的量子密钥分发和量子随机数，密钥具有真随机性；

2、密钥分发采用量子密钥分发技术（QKD）和一次一密（OTP），理论上具备信息论安全性；

3、密钥加密存储，采用一机一密，用后即毁，保证密钥安全性；

4、采用对称密码算法对数据加密，可根据业务需求，设置合理的密钥更新策略。

3.1.3 量子通信技术在智能网联汽车上的应用优势与局限性

应用优势

量子通信技术在智能网联汽车领域的优势在于可抵御量子计算等算力破解对智能网联汽车数据加密的威胁；量子密钥实时生成和分发，可支撑智能网联汽车实现密钥快速更新，进一步提升数据安全性；同时，每个智能网联汽车终端或模块使用独立的量子密钥；可有效防止单个密钥泄露引起的智能网联汽车整体系统安全风险。

1.抵御量子计算算力破解

Shor 算法破解目前公钥算法的计算复杂度仅为 $O(n^2(\log n)(\log(\log n)))$,对于 RSA2048,破解计算步骤仅需约 $P \approx 2^{27}$次。若有一个 GHz 主频的量子计算机，则破解 RSA2048 仅需要几十毫秒。即使将密钥长度提高到 1Mbit,使用运行 shor 算法的 GHz 量子计算机破解 RSA 也只需要几十个小时。然而此时用单核 CPU 生成 1Mbit 的 RSA 密钥

的时间甚至将超过数十个小时。因此，在量子计算威胁下目前的公钥密码算法基本上丧失了安全性和可用性。

而量子密钥分发基于诱骗态的 BB84 协议，该协议的核心思想基于量子不确定性原理，窃听者在量子力学的理论范围内不能对这个量子态进行有效的窃听。因此也就不能得到密钥。根据 QKD 的安全理论分析，即使攻击者能够具有无限计算能力的经典和量子计算机，对于 QKD 设备所分发的 n 比特密钥也只能窃取到极少的信息量（对于目前的 QKD 设备可以达到远小于10^{-15}n 比特）。换而言之，即使 QKD 设备累计分发了 100 万 G 比特密钥，就算使用具有无限大计算能力的攻击者也窃听不到 1 个比特。

2.密钥快速更新

会话密钥长期不更新存在着风险。NIST 建议对 AES 算法一个会话密钥加密数据不超过 64Gbyte。事实上，只有在安全的密钥分发的前提下，更新密钥才有意义。这时，如果能够获得更快的密钥更新频率，则攻击者利用算法的弱点进行攻击的难度就越大，加密的安全性也就越高。利用 QKD 的密钥分发方式，在保证密钥分发安全性的同时，可以获得更快的密钥更新频率，使得每个会话密钥加密数据远远小于 64Gbyte。从而大幅提高了安全性。

3.密钥独立性

每个车联网应用设备或模块使用不同的量子密钥，单个应用设备被攻击不影响其它设备，发现车联网应用设备失密后可以在对端侧将其删除；会话密钥分发每次使用后即销毁也保证了系统的安全，避免出现单个密钥泄露导致整个车联网密码系统被破解，进而引起整车密码系统失效。

局限性

量子通信技术与智能网联汽车方向应用需要结合智能网联汽车的实际情况，目前存在部分技术局限和融合对接的问题有待攻关和解决。

1.单一应用方案的完整性

量子通信能很好的解决端到端的密钥分发问题，能很好的与对称密码技术相结合解决加密和部分的认证问题，但对于当前应用广泛的数字签名场景，目前 QKD 仍然没有好的解决途径。

2.效能和成本

目前的量子通信系统比现有经典密码系统的硬件设备昂贵。同时，QKD 系统的维护涉及到的技术领域要比仅基于电子元器件的密码机设备多，维护的技术难度和成本也

可能更高一些。但随着技术研究和工程应用技术的提升，QKD 系统成本也将逐步降低，同时，规模化应用也将降低单个汽车终端应用的成本。

3.1.4 量子计算、量子测量的发展情况和规划展望

量子力学刻画微观粒子系统中的叠加性与纠缠性等独特性质，为新的计算范式提供了物理基础。量子计算是迄今已知的，可以提供与当今计算机相比，运算处理能力指数级加速的唯一计算模型。

量子计算机研发已经成为全球主要国家在前沿科技领域攻关突破的重点方向之一，近年来取得样机研制与技术验证主要代表性成就如图所示。大规模可容错通用量子计算机仍是需要长期探索和努力的目标，量子计算领域的发展与竞争也将是一场科技马拉松。

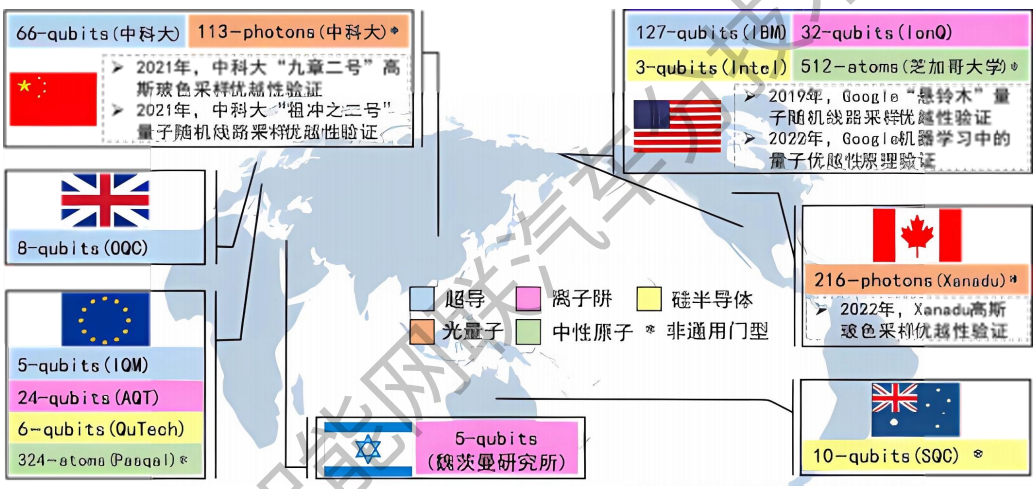


图 7 全球量子计算样机研发与技术验证代表性成果

量子计算硬件技术主要分两大类，一类是以超导和硅半导体为代表的人造粒子路线，另一类是以离子阱、光量子和中性原子为代表的天然粒子路线。量子计算硬件研发目前处于各种技术路线并行发展和开放竞争阶段，近期科研不断取得进展，亮点成果纷呈。

超导量子计算处理器核心器件为超导约瑟夫森结，具有可设计、可扩展、易控制、易耦合等优势，近年来衍生出 Transmon、Xmon、Fluxonium 等多种新型超导量子比特。近期超导技术路线在比特数量和保真度方面均有突破。2022 年 5 月，IBM 发布新技术路线图，2022 年底发布 433 量子比特 Osprey 处理器，2023 年推出 1121 量子比特 Condor 处理器，并探索并行芯片扩展方案，2025 年实现 3 处理器集成 4000+量子比特系统。2022 年 7 月，阿里报道实现 Fluxonium 系统中双比特门的 99.72%保真度。2022 年 8 月，百度发布超导量子计算机乾始。超导技术路线是通用量子计算有力竞争者之一，得到众多科研机构、科技企业和初创公司支持，比特数量稳步提升，每秒电路层操作数(CLOPS)

等指标占优。

硅半导体量子计算处理器在硅或者砷化镓等半导体材料制备门控量子点来编码量子比特，优势在于可扩展性好，且与成熟 CMOS 工艺相兼容。硅半导体量子比特主要分光门控和电门控两类，前者通常使用光学活性缺陷或量子点来诱导光子间的强有效耦合，后者通过施加在光刻金属门上的电压来限制和操纵形成量子比特的电子。硅半导体技术路线近期主要进展在于量子比特数量和保真度提升。2022 年 1 月，《自然》杂志发表澳大利亚 UNSW 大学、荷兰 Delft 理工和日本理化研究所三个团队成果，不同方案硅基量子处理器的双量子比特门保真度均达到 99%以上。未来，克服电子自旋易受电磁环境影响，将是硅半导体科研攻关的主要目标。

光量子处理器利用单光子或光压缩态的多种自由度进行量子态编码和量子比特构建，优势在于光子受环境影响小、可常温环境工作、相干时间长等。光量子计算主要挑战是在不同光子态之间构建的双量子比特门和实现逻辑操作，典型策略是在线性光学量子计算中通过单光子操作和测量的结合实现双比特逻辑门，或是利用集成光学的体系结构实现光子间相互作用。近期光量子技术路线科研进展主要是量子优越性证明和光子纠缠操控实验。2022 年 6 月，加拿大 Xanadu 报道 Borealis 光量子计算机完成 216 压缩态高斯玻色采样实验，再次验证光量子计算优越性。2022 年 8 月，德国马克斯-普朗克研究所报道实现 14 个光子纠缠操控新纪录。未来，光量子技术路线需进一步探索新型光源和探测器技术，以及光量子逻辑门操控。

量子测量是量子信息领域三驾马车之一，被认为是距离实用化最近的量子技术方向，传感单元是量子态制备、操控和测量的载体，根据物理媒介和制备操控方式不同，存在冷原子、热原子蒸气、氮空位(NV)色心、里德堡原子、量子纠缠、单光子等多种技术路线，如图所示。国内外研究机构和初创企业在陆续推出了冷原子钟、重力仪、磁力计、光量子雷达等样机和产品，并逐步走向商业应用。

图 8 量子测量主要技术方向

冷原子干涉是一种测量精度较高的量子测量技术路线。利用冷原子相干叠加特性可实现频率、重力、重力梯度、角速度等物理量精密测量。主要优势在于测量精度高，相干时间长，但是由于激光冷却操控测量装置较为复杂，冷原子干涉仪集成度不高，体积较大，成本高，主要应用于基础科研、计量基准等对体积、成本、功耗不敏感，但对测量精度要求高的领域。国内外公司推出基于冷原子的时钟、重力仪等产品，尝试在车载、船载、恶劣自然环境中部署，主要面向科研院所、授时机构、地质勘探等专业用户。

热原子蒸气是目前成熟度较高的一种技术路线，已广泛应用于时频同步领域，目前商用铯钟、铷钟都是基于热原子蒸气能级跃迁进行频率或时间测量，并逐步向小型化和芯片化方向演进。热原子蒸气中原子核和电子具有自旋的内禀属性，会与外界场产生耦合，也可用于磁场和角速度测量。基于热原子蒸气的量子磁力计已开始商用化，特别是 SERF 磁力计，具有超高灵敏度的优点，相比超导干涉仪而言，具备无冷却装置、维护费用低、可近距离探测等优点，有望成为下一代心磁和脑磁等人体微弱磁场检测方案。

氮空位(NV)色心是近年来发展起来的新兴测量技术。金刚石 NV 色心是一种特殊的发光点缺陷，由氮原子与其紧邻碳原子空位组成，可通过光学和微波脉冲对其量子态进行制备、操控以及读取。NV 色心对外界磁场十分敏感，室温相干时间可达毫秒级，空间探测分辨 率可达纳米级，与待测样品间距可小于 5 纳米。NV 色心单量子传感器可实现样品表面纳米级精度扫描磁成像，为研究单活体细胞、蛋白质、DNA 等新材料和生命科学领域应用带来全新测量手段。金刚石 NV 色心量子测量技术初步成熟，初创企业已推出商用产品。

单光子探测主要应用于目标探测和成像领域，以提高探测效率方式提升雷达性能，

单光子探测器需要极高增益又要保持极低噪声。单光子探测可分为硬目标和软目标探测，硬目标探测是对飞行器等实体目标进行百公里级、三维、非视域成像；软目标探测是对风场、气溶胶、云层分布等非实体目标进行检测。单光子探测技术产品已相对成熟，目前在环境、交通、气象等领域落地应用。

3.2 量子通信基础设施建设状态

目前量子通信技术设施主要包括适用于固网应用的安全基础设施和适用于无线应用的安全基础设施，适用于固网应用的量子安全基础设施主要为以量子密钥分发技术和量子安全中继技术为核心构建的量子保密通信网络，如量子“京沪干线”、国家量子保密通信骨干网等面向广域应用的量子保密通信网络；北京、上海、济南、合肥、武汉、成都、重庆、海口等的量子保密通信城域网等面向城域网用户提供量子安全服务；面向电力、政务和金融等行业的量子安全专线，上述量子网络主要为固网应用提供量子安全服务支撑。采用量子安全服务技术以 QKD 密钥和量子随机数密钥为核心，面向无线应用提供量子安全服务，如量子安全密话、量子安全对讲、量子安全监控和量子安全电力配电终端等。

3.2.1 适用于固网应用的量子安全基础设施

1.基于量子通信的传输信道加密

使用 QKD 技术，配合现用各类对称密码算法，能够建立端到端的量子安全传输通道，能够实现终端与业务系统间、以及各类业务系统间重要敏感信息的加密传输。典型的是在 IP 层 VPN 系统中用 QKD 技术生成对称密钥对实现 VPN 通道加密等。

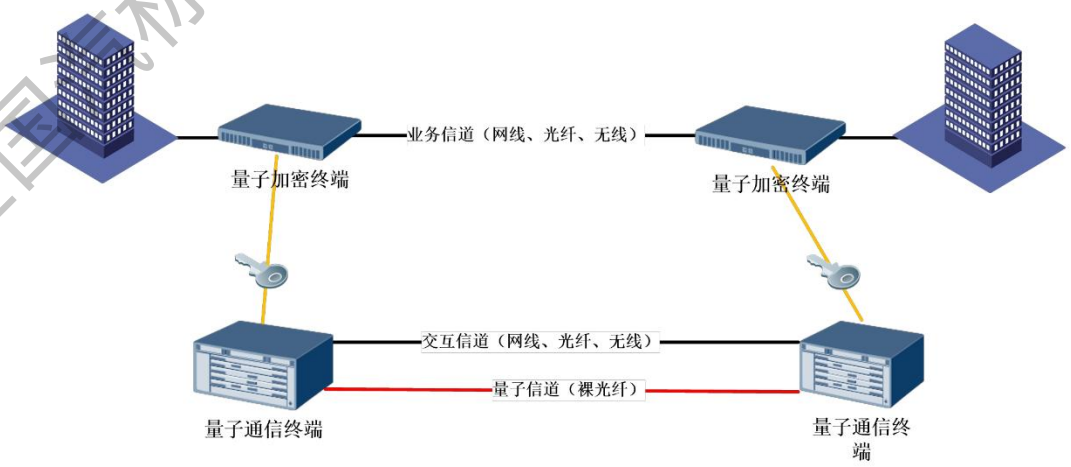


图 9 量子通信传输加密示意图

2.安全密钥管理

基于 QKD 设备、QKD 网络构建密钥管理系统，能够实现端到端或中心到多个终端的在线量子密钥从生成、分发、更新到删除的全生命周期密钥管理功能。其优势在于能够基于 QKD 设备为用户实时分发具有真随机性的各类密钥（用户可以按需指定类别如工作密钥、会话密钥等），也可以形成量子随机密钥池供用户需要时按需取用,且能够不依赖于公钥数字证书基础设施而独立运行，适合于具有抗量子攻击的长期安全需求和高安全防护等级需求的政府、行业用户。

3.存储加密

QKD 不仅可以支持传输加密，还可以支持本地或云上数据的存储加密，在此使用的加密算法与传输加密相同，仍然可以是对称密码算法或 OTP 算法，与传输加密的区别是在此使用 QKD 提供的随机密钥作为存储加密密钥，配合应用层、文件系统层或磁盘层等传统存储加密功能模块和技术。

以量子密钥分发为核心的量子通信能够与信息通信系统常用的 TCP/IP 参考模型中的数据链路层、网络层、传输层和应用层等分别进行结合应用，如下图所示。

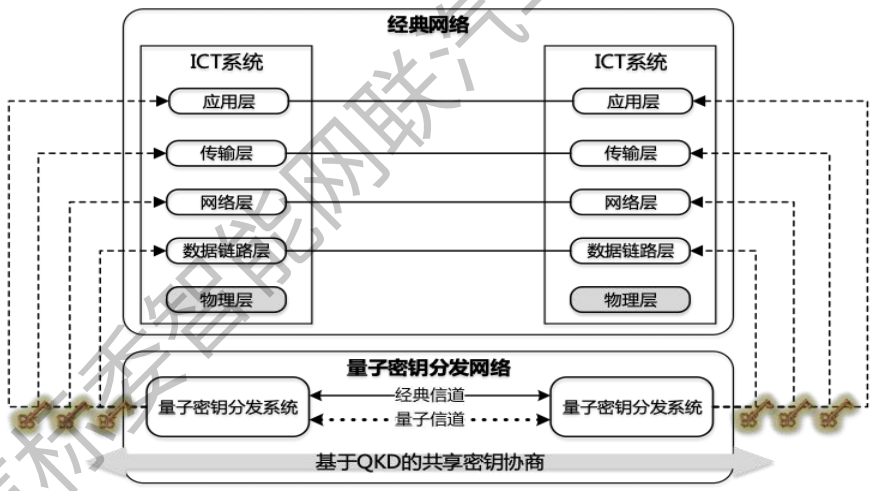


图 10 QKD 在 ICT 系统中的应用示意图

1）数据链路层应用

最简 QKD 系统是光纤连接量子密钥分发收发设备构成点对点链路。将 QKD 与传统的链路加密机进行集成，构成基于 QKD 的量子链路加密机。这种用于点对点链路加密的 QKD 应用，可称为基于 QKD 的虚拟专用网（VPN）隧道技术。对应的产品类型例如为使用 QKD 分发密钥的 VPN 设备。

2）网络层应用

互联网安全协议（IPSec）是用于保障 IP 协议通信安全的一组协议套件，IPSec 协议簇中的互联网密钥交换协议（IKE）负责建立安全的网络连接，QKD 可提供共享密钥

与 IKE 协议进行融合。对应的产品类型例如为使用 QKD 分发密钥的 IPSec VPN 以及加密路由器。

3）传输层应用

TLS 及其前身 SSL 是工作在传输层的安全协议，用于在传输层为网络通信提供端到端的安全服务。QKD 产生的密钥可以用于替换 TLS 中的会话密钥，也可以用于进行一次性密码本方式的加密传输，另外还可以用于实现消息认证，替换 TLS 协议中消息认证码（HMAC）或 SSL 协议中伪随机数函数的相应功能。对应的产品类型例如为使用 QKD 分发密钥的 SSL VPN。

4）应用层应用

在 OSI 模型传输层之上的应用层中，QKD 也可以与各类应用程序进行灵活的集成，这些应用利用 QKD 为通信收发两端提供的对称共享密钥，既可以用于进行用户的身份认证或鉴权，也可以用于实现传输载荷的加密传输。对应的产品类型例如加密语音/视频通话或会议、移动 OA、即时通信工具等。

网络基础设施加密是指数据在整个网络基础设施传输中依赖网络自身实施加密以保护数据完整性、保密性、真实性。包括广域网(WAN)、城域网或局域网，以及链接他们的主干网加密。在网络基础设施加密方面，规模最大、网络拓扑最广、最广为人知的就是如图所示我国建设的广域星地一体 QKD 量子通信网。

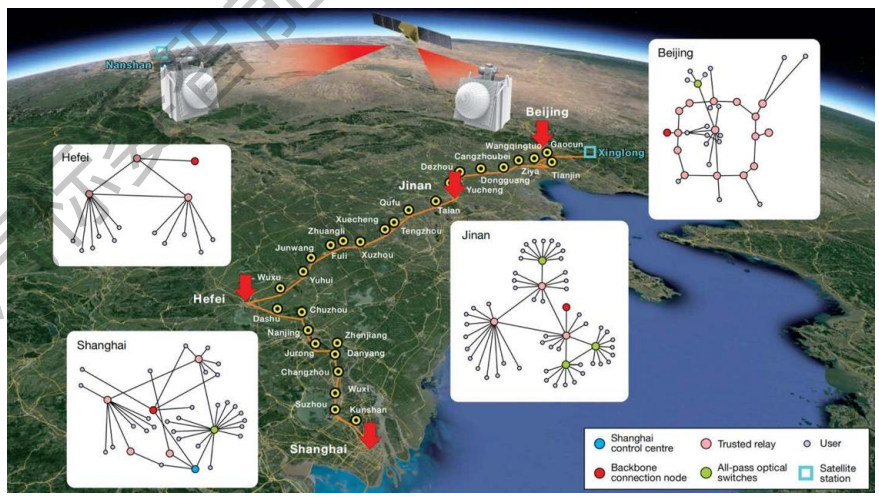


图 11 广域星地一体 QKD 量子通信网络图

3.2.2 适用于无线应用的量子安全基础设施

量子安全服务平台用于面向移动应用场景，实现量子密钥再分发和应用。量子安全服务平台包含量子安全服务移动引擎、密钥系统交换密码机、充注终端软件、安全介质、

量子随机数发生器、终端软件开发套件 SDK 等子系统。

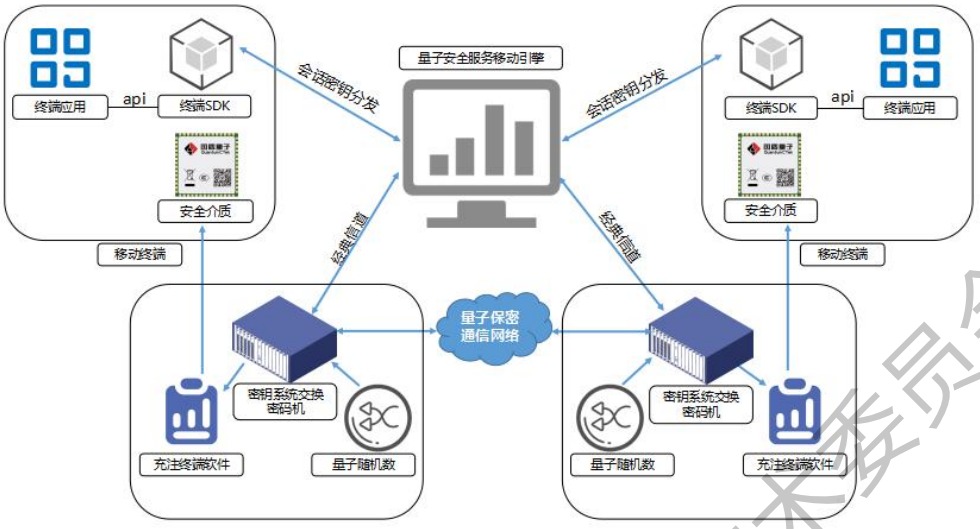


图 12 量子安全服务平台系统架构

量子安全服务移动引擎是整个量子安全服务平台的核心控制管理软件，基于量子随机数或量子密钥分发网络与密钥系统交换密码机为移动终端等设备提供密钥服务，支撑用户实现安全通信等业务。

密钥系统交换密码机是量子安全服务平台的核心设备，负责获取量子随机数或量子密钥分发网络的密钥，并进行密钥的存储管理，提供密钥终端充注，将获取量子密钥作为会话密钥提供给移动终端用于加密通信。

充注终端软件，是对安全终端或安全介质进行量子密钥充注的软件，可安装于特定充注机或普通 PC 终端上，并为安全介质进行发卡绑定和密钥充注功能。

终端软件开发套件(SDK)运行在应用终端操作系统中，封装了安全介质的调用接口以及量子安全服务平台的交互接口，并通过 API 给应用层 APP 提供统一密钥应用服务，包括会话密钥获取，数据加解密等功能。

量子安全服务平台可应用的领域包括：国防、金融、政务、交通、能源、云计算、大数据等。典型的应用方式如下：

1) 量子安全通话

图 13 量子安全通话场景拓扑图

量子安全服务平台结合移动通信终端提供量子安全通话服务。通过使用量子安全服务平台对通话提供高安全防泄漏功能，为通话保密性要求高的用户提供服务。

通过安全 SIM 卡中的量子密钥对拨打安全通话时的语音数据加密，从而防止语音传送过程泄漏。其中“安全 SIM 卡”结合了普通 SIM 卡功能和安全芯片功能，既可提供运营商入网的鉴权等普通 SIM 卡功能，又可提供安全芯片的相关功能。

2) 量子安全物联网

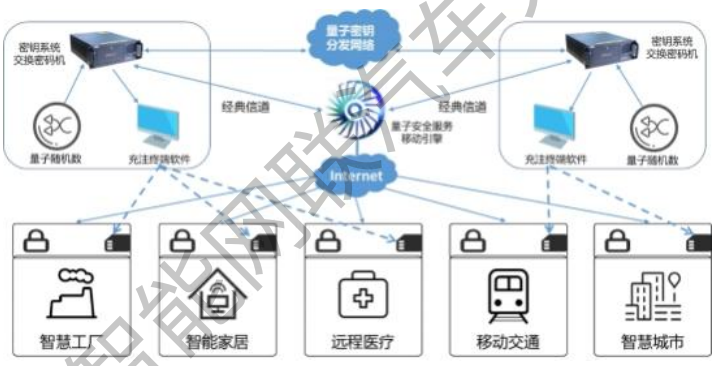


图 14 量子安全物联网场景拓扑图

基于量子安全的物联网场景，可实现对物联网数据、控制信令等进行加密传输，也可对设备进行身份认证，实现采集终端和中控设备的安全通信。

3) 量子安全移动办公

图 15 量子安全移动办公场景拓扑图

在量子安全的移动办公场景中，VPN 服务端通过直接与密钥系统交换密码机相连的

方式安全的获取量子密钥，VPN 客户端基于已进行密钥充注的安全介质实现用户数据安全的多维度保障。

3.3 量子通信领域标准分析

近年来量子信息技术领域成为标准化新兴热点，如下图所示。欧洲电信标准协会（ETSI）自 2008 年就开始布局量子密钥分发（QKD）标准化相关的工作，目前已发布 10 项规范；随后，到 2016 年电气与电子工程师协会（IEEE）量子通信标准化项目开始启动。可以看到，随后各国际/区域标准化组织如 ISO、IEC、ITU、IETF 等在两三年的时间内纷纷开始加速布局量子信息标准化工作，发展趋势迅猛。

图 16 国际/区域标准化组织启动量子信息标准化的时间线图

尤其在量子保密通信技术方面，随着量子保密通信技术产品研发和应用探索发展，国际电信联盟（ITU-T）、国际标准化组织及国际电工委员会（ISO/IEC）、欧洲电信标准化协会（ETSI）、中国通信标准协会（CCSA）和密码行业技术标准化委员会（CSTC）均开展了标准化研究并取得阶段性进展。截至 2022 年底，ITU-T SG13 已发布 QKD 网络架构、管控、服务需求等 12 项 Y.38xx 系列标准，SG17 已发布 QRNG 架构、QKD 网络安全框架和安全设计等 5 项 X.17xx 系列标准，SG11 开始研究 QKD 网络接口协议相关标准。ETSI 已发布 QKD 器件、内部接口、应用接口、控制接口等 13 项标准，并进一步对安全性要求、认证和网络架构等开展研究。ISO/IEC 持续开展 QKD 系统安全性要求和测试评估方法两项标准研究，目前已完成国际标准草案投票。CCSA 在 ST7 开展 2 项国家标准、19 项行业标准和 2 项协会标准研究，已发布和报批量子通信术语定义、量子保密通信应用场景、QKD 系统技术要求、测试方法、网络架构等标准 11 项。CSTC

目前已发布了量子密钥分配产品技术规范和检测规范 2 项。量子保密通信领域的系统设备、核心器件、网络架构和接口协议等方面的技术标准体系初步形成。量子保密通信标准化研究工作取得阶段性成果，对系统功能性能、现实安全性和组网业务能力的标准测评验证须加强。

4. 量子通信技术赋能智能网联汽车发展建议

4.1 智能网联汽车量子通信典型需求分析

4.1.1 应用场景

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。

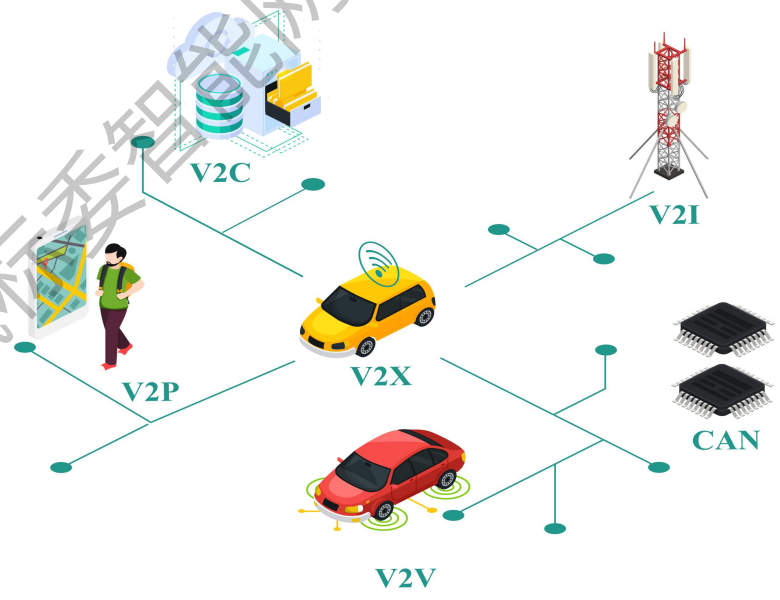


图 17 车联网应用场景

车云通信（V2C）

车辆和云端之间的通信，包括车辆远程控制、车辆数据上传和下载、车辆诊断和维护、车辆安全监控和车辆智能化服务等。

车辆远程控制：通过 TSP 平台，车辆可以与云端进行快速、准确的信息交换，实现远程控制，如启动、熄火、锁车等。

车辆数据上传和下载：车辆将车辆内部数据上传至云端，云端也可以将车辆需要的数据下载至车辆，如地图数据、路况信息等。

车辆诊断和维护：车辆将车辆状态、故障信息上传至云端，云端可以对车辆进行诊断和维护，从而提高车辆的可靠性和安全性。

车辆安全监控：车辆将车辆行驶过程中的数据上传至云端，云端可以对车辆进行安全监控，如异常驾驶行为、碰撞预警等，从而提高行车安全。

车辆智能化服务：车辆可以与云端进行智能化服务交互，如语音识别、智能导航、智能音乐等，从而提高驾驶体验。

云云通信

云与云之间的通信，包括云计算资源、数据、和服务的实时交换，以及对云之间的协同决策和协作控制。

云资源协同利用：不同云服务提供商之间通过标准化协议和 API 交换计算资源、存储容量、和网络带宽等，以实现云资源的协同利用，如自动分配计算实例、自动存储数据备份等。

数据共享与整合：云服务提供商之间通过数据共享协议和标准化数据格式交换信息，以实现数据的共享和整合，如云上的大数据分析、跨云数据库查询等。

服务协同交付：不同云服务提供商之间通过 API 和标准协议交换服务信息，以实现服务的协同交付，如多云环境下的应用部署、跨云身份验证等。

云计算任务优化：不同云之间通过云间通信技术交换任务执行信息，以实现云计算任务的优化，如选择最适合的云实例执行任务、避免资源争用等。

云协同决策：不同云之间通过标准化协议和通信协议交换信息，以实现云协同决策，如跨云环境下的自动故障恢复、资源分配决策等。

云协作控制：不同云之间通过云间通信技术交换控制指令，以实现云协作控制，如自动调整云资源分配、负载均衡、流量控制等。

云与云之间的协同功能可提高云服务的可用性、性能和灵活性，使不同云服务提供商能够更好地协同工作，为用户提供更强大的云计算体验。

车人通信（V2P）

车辆与行人之间的通信，包括行人安全、交通信号灯控制、行人导航、行人健康监

测和行人社交互动等方面。

行人安全：车辆与行人之间进行通信，实时获取行人的位置、行动轨迹等信息，从而避免行人与车辆的碰撞事故。

交通信号灯控制：车辆和交通信号灯之间的通信可实现更加快速、准确的信息交换。通过实时的交通控制，提高交通效率和安全性。

行人导航：通过车辆与行人之间的交互，车辆可以向行人提供最佳的行进路线和导航信息，帮助行人更加安全地行走。

行人社交互动：车辆和行人之间的通信可以实现更加智能化的社交互动，如车辆向行人提供周边的社交信息和活动信息等。

车物通信（V2I）

车辆和道路基础设施之间的通信，包括交通信号灯、路况监测设备等，通过 DSRC 实现交通流量控制、交通事故预警等功能。

交通拥堵控制：车辆通过 DSRC 向交通信号灯发送信息，实现智能化交通控制，优化路段通行能力，减少交通拥堵。

路况监测和预警：车辆和道路基础设施之间进行信息交换，实现路况监测和预警功能，如道路施工、交通事故等。

自动驾驶辅助：车辆可以获取道路基础设施的信息，如交通信号灯、路标、车道线等，从而实现自动驾驶辅助功能，如自动停车、车道保持、自动超车等。

交通事故预警：车辆和道路基础设施之间进行信息交换，实现交通事故预警功能，如道路拥堵、交通事故等。

道路收费和管理：车辆可以与道路收费设施进行信息交换，实现智能化道路收费和管理，如 ETC 电子收费等。

车车通信（V2V）

车辆之间的通信，包括车辆行驶路线、车速、加速度等信息的实时交换，以及对车辆之间的协同决策和协作控制。

车队协同驾驶：车辆与车辆之间通过 V2V 通讯交换信息，实现车队协同驾驶，如自动跟车、自动超车、自动换道等。

碰撞预警和避免：车辆与车辆之间通过 V2V 通讯交换信息，实现交通预警和避免功能，如自动刹车、自动避让等。

车辆行驶路线优化：车辆与车辆之间通过 V2V 通讯交换信息，实现车辆行驶路线

优化，如避免拥堵路段、选择最优路径等。

车辆协同决策：车辆与车辆之间通过 V2V 通讯交换信息，实现车辆协同决策，如交通事故处理、交通流量控制等。

车辆协作控制：车辆与车辆之间通过 V2V 通讯交换信息，实现车辆协作控制，如自动加速、自动减速、车辆间距控制等。

车内通信

车内通信是车内的各个系统和设备之间的通信，包括车辆信息系统之间、车载娱乐和办公系统之间、人机交互界面和车载系统之间、以及车内传感器和控制器之间的通信。

车辆信息系统之间的通信：发动机控制单元（ECU）、防抱死制动系统（ABS）、空气袋系统等各种系统之间的数据交换与通信。

车载娱乐和办公系统之间的通信：车载娱乐和办公系统包括车载影音、游戏、网络、办公等系统，这些系统进行相互通信，以便实现更好的用户体验和工作效率。

人机交互界面和车载系统之间的通信：人机交互界面包括车载显示屏、语音识别、手势识别、触摸板等，它们需要和车载系统进行通信，以便实现更好的用户体验和控制功能。

车内传感器和控制器之间的通信：车辆通常配备各种传感器，如摄像头、雷达、激光雷达等，它们与控制器之间需要进行数据传输，以支持驾驶辅助系统和自动驾驶功能。

4.1.2 量子密码在汽车信息安全的典型应用

在智能网联汽车领域，安全和隐私问题至关重要。车辆之间的通信（V2V）、车辆与基础设施的通信（V2I）、车辆与云端的通信（V2C）等各种场景都需要强大的密码保护，以确保数据的保密性、完整性和可用性。密码技术在这些场景中起着至关重要的作用，但传统密码技术可能会受到量子计算机攻击的威胁。

在这一背景下，量子密码技术为智能网联汽车安全提供了一种更加强大和具有未来导向的解决方案，包括身份认证和数据加密等关键领域。

身份认证

车联网的普及为人们的驾驶提供了更多的便利和舒适性，但也引入了新的安全挑战。随着外部网络与车联网的融合，攻击者能够通过外部设备远程侵入车辆网络系统，获得车辆隐私数据，甚至恶意控制车辆。在这种情况下，身份认证成为阻止外部入侵的至关重要的手段。

身份认证的主要目标是确保通信参与者的真实身份，并允许合法的用户或设备访问车联网系统，同时拒绝未经授权的用户访问。

然而，传统身份认证协议在面对高级网络攻击时可能存在漏洞，因为攻击者可以窃听协议中的有效身份验证信息，从而伪造身份。通过引入量子密码技术，车联网系统可以更加可靠地进行身份认证，解决了传统协议可能存在的窃听和身份伪造风险，提高了车联网系统的整体安全性。量子密码结合量子密钥分发（QKD）、安全介质、生物特征可以实现更安全的身份认证：

a. 量子密码结合 QKD：针对有线连接场景下，量子密码可与 QKD 结合，使用量子特性确保密钥的安全性。利用量子特性，密钥在传输过程中不容易被窃听或窃取。这确保了身份认证所使用的密钥不会在传输过程中受到黑客攻击。

b. 量子密码结合安全介质：针对无线连接场景下，可以将量子密码存储在本地安全介质，如 SIM 卡，u 盾等，实现无线连接场景下量子密码的预充注密钥的安全性，通过本地存储预制密钥实现安全的身份认证。

c. 量子密码结合结合生物特征识别：量子密码可以与生物特征识别技术结合使用，如指纹识别、虹膜扫描等，这种组合实现了双因素身份验证，要求用户通过密钥认证与生物特征验证，从而提高了身份认证的安全性。

数据加密

随着越来越多的车辆联网，数据泄露的可能性也会增加。数据加密是一种非常有效的安全措施，广泛用于保护车联网免受恶意行为者的侵害。通过加密数据，可以保护数据的保密性，验证数据的完整性，保证只有预期的各方才能访问数据。 已知的大规模商用的 RSA 密码的安全核心在于，基于大素数分解的数学问题是困难的，目前没有行之有效的算法。要想攻破这个密码，就必须攻克这个长久以来困扰数学家的素数分解问题。然而遗憾的是，量子计算机可以有效地解决素数分解问题，这也意味着 RSA 密码体系在量子计算机面前并不安全。

鉴于传统加密方法可能受到量子计算机等新兴威胁的挑战，量子密码技术提供了一种未来导向的解决方案，以应对未来可能出现的加密攻击。该技术最大的优势在于，即使拦截者在传输过程中截获了部分信息，也无法获取整个信息。这是受到量子纠缠和量子不可克隆性原理的保护。与传统密码学不同，量子加密技术不需要在加密时候使用任何算法，而不使用算法是安全性的保障。

4.1.3 保障范围

智能网联汽车量子密码的保障范围包括数据的真实性、新鲜性、完整性、不可抵赖性、保密性、可用性、可授权性。

表 1 智能网联汽车量子密码保障范围

威胁类型	安全属性	定义	举例
仿冒	真实性 新鲜性	仿冒，冒充他人身份	冒充其他组件发送欺骗信息
篡改	完整性	篡改，非法修改数据	修改数据
否认	不可抵赖(审计) 真实性	抵赖，否认做过的事	否认其操作行为
信息泄露	保密性	信息泄露	个人信息被泄露
拒绝服务	可用性	拒绝服务	资源耗尽或服务不可用
提升权限	可授权性	提权，未经授权但执行了操作	普通用户提升到管理员

4.2 量子通信在智能网联汽车中的典型案例

4.2.1 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，以确保云端和车端之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。

量子密钥的分发

1）移动通信场景。

量子密钥需要通过量子密钥分发中心进行分发。量子密钥分发中心通常由量子随机数发生器，密码机和量子密服管理系统组成。

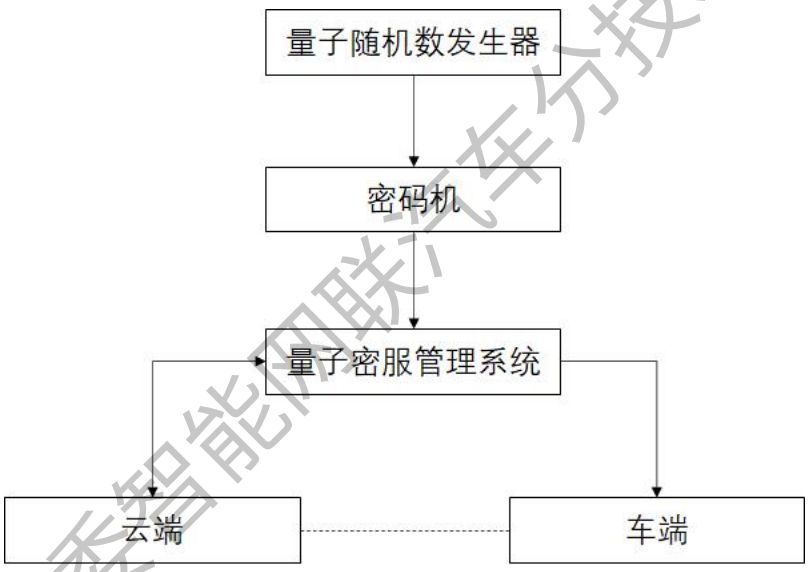


图 18 量子密钥分发中心

该系统允许两个远程方建立共享的会话密钥。下面是具体的过程：

首先，量子随机数发生器生成随机量子比特。生成的随机量子比特需要安全地传输到密码机，用于生成密钥。密码机接收随机量子比特后，使用特定的量子测量来确定每个比特的值,根据测量结果，密码机生成对称加密密钥。量子密服管理系统负责协调整个密钥分发过程。在密钥生成的过程中，量子密钥分发中心利用与车端和云端之间预先共享的量子密钥，对密码机生成的对称加密密钥进行加密。然后，加密后的密钥被传输到车端和云端。车端和云端可以使用他们之间预共享的密钥来解密这个加密的密钥。这种方式确保了在传输过程中密钥的保密性。一旦车端和云端都获得了对称加密密钥，它们可以使用这个密钥进行会话密钥协商，以便建立安全通信。车辆可以使用该对称密钥来

加密自己生成的量子密钥，并将其发送到云端。云端可以解密并获取车辆生成的量子密钥，从而用于加密通信。

量子密钥分发中心作为协调者，负责确保整个过程的正确性和安全性。它生成和分发高度安全的密钥，通过预置量子密钥建立车端与云端的桥梁，从而确保云端和车端之间的通信是加密和安全的。这种系统的安全性建立在量子物理学的原理和传统密码学的双重保护之上，使得任何未经授权的访问或监听都会被检测到并且会导致密钥的重新生成，在理论上是非常安全的。

2）有线通信场景

量子密钥需要通过量子密钥协商中心进行分发。如图 19 所示，量子密钥分发中心由量子密钥分发设备 A、密码机 A、量子密钥分发设备 B、密码机 B 和量子密服管理系统组成。

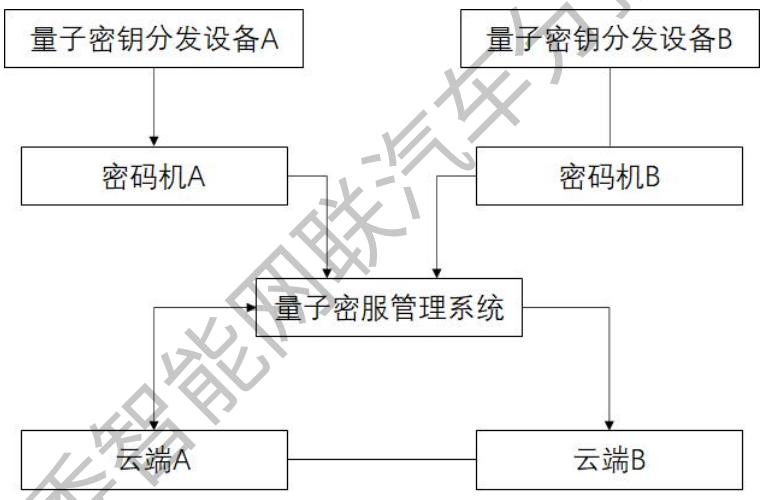


图 19 量子密钥协商中心

两个量子密钥分发设备，各自使用量子密钥生成系统来创建一对相互关联的量子比特并传输到密码机。密码机使用光学设备和量子随机数生成器来生成随机的、不可预测的量子密钥。生成的量子密钥会被传输到一个量子密服管理系统。这个传输可以通过光纤或其他物理通道完成。重要的是确保在传输过程中，量子密钥的安全性不受威胁。量子密服管理系统负责接收来自密码机 A 和密码机 B 的量子密钥片段，并对它们进行验证。验证通常涉及检查量子态是否受到了窥探或中间人攻击的干扰。一旦验证通过，量子密服管理系统会将密码机 A 和密码机 B 的量子密钥片段合并成一个共享的量子密钥。密服管理系统将合并后的量子密钥安全地存储，并将其分发给云端 A 和云端 B。这确保了密钥的保密性。一旦云端 A 和云端 B 都获得了共享的量子密钥，他们可以使用它来加密和解密他们之间的通信。这种加密通信通常使用对称密钥加密算法，其中共享的量

子密钥用作对称密钥。

这个过程涉及生成、传输、验证、合并和分发量子密钥，以确保两个不同的云端拥有相同的安全密钥，可用于加密和解密他们之间的通信。量子密钥协商中心依赖于量子力学的性质，如不可克隆性和量子态的测量，以提供高度安全的密钥分发方式，确保了密钥的安全性和可信度。

量子密钥管理

密钥管理系统由密钥生成、密钥管理、密钥库管理、认证管理、安全审计、密钥恢复和密码服务等模块组成。

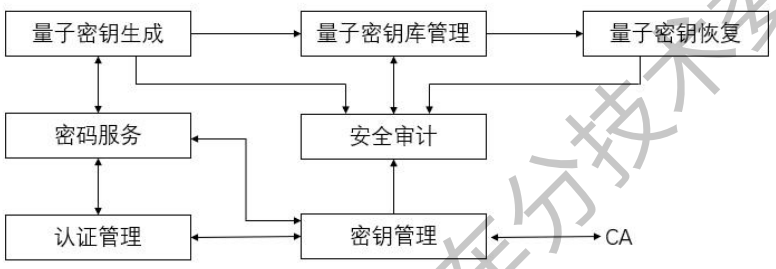


图 20 量子密钥管理系统逻辑架构

量子密钥管理系统提供了对生命周期内的量子密钥对进行全过程管理的功能,包括量子密钥生成、密钥存储、密钥分发、密钥备份、密钥更新、密钥撤销密钥归档、密钥恢复以及安全管理等。

量子密钥生成。通过量子密钥分发中心生成对称加密密钥，该密钥由密钥管理系统进行管理。量子密钥分发中心通常由量子随机数发生器，密码机和量子密服管理系统组成。

量子密钥存储。量子随机数发生器和密码机生成对称加密密钥，在服务端存储在量子密钥分发中心的数据库中；在车端存储在可信的量子安全芯片。

量子密钥分发。在移动网络中，通过量子密钥分发中心生成对称加密密钥，由密钥管理系统进行管理，通过预置量子密钥加密对称量子密钥进行安全分发。在有线网络中，通过量子密钥协商中心进行量子密钥分发。量子密钥协商中心通常有量子密钥分发设备和密码机组成。

量子密钥备份。密钥管理系统采用热备份、冷备份和异地备份等措施实现密钥备份。

量子密钥更新。当证书到期或用户需要时，密钥管理系统根据 CA 请求为用户生成新的量子密钥。

量子密钥撤销。当证书到期、用户需要或管理机构依据合同规定认为必要时，密钥

管理系统根据 CA 请求撤销用户当前使用的密钥。

量子密钥归档。密钥管理系统为到期或撤销的密钥提供安全长期的存储。

密钥恢复。密钥管理系统可为用户提供密钥恢复服务和为司法取证提供特定密钥恢复。密钥恢复需依据相关用户只限于恢复自身密钥。

4.2.2 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：

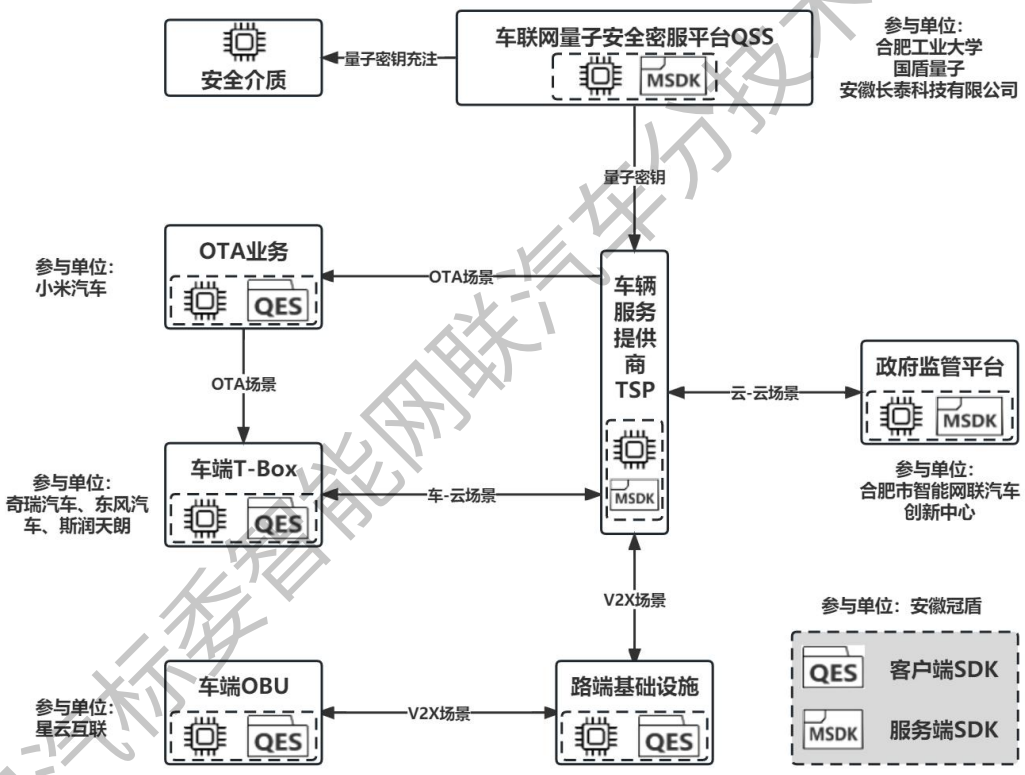


图 21 场景验证架构图

4.2.2.1 场景验证设备信息

应用场景验证主要包含车-云场景，云-云场景，V2X 场景等。实验所用到的相关设备信息如下表所示。

表 2 实验设备信息

设备名称	设备来源	设备图片
奇瑞星途量子通信试验车	奇瑞汽车	
政府监管平台	合肥市智能网联汽车创新中心	
T-BOX	奇瑞汽车	
T-BOX	东风汽车	
T-BOX	斯润天朗	
OBU	星云互联	
QKM	国盾量子	

量子安全网关	安徽冠盾科技	
量子安全接入终端	安徽冠盾科技	
量子密服软件SDK	安徽冠盾科技	/

4.2.2.2 5G 车-云-云应用场景

（一）应用场景

在车云云应用场景下，通过车辆和云端之间建立通信连接，实现车辆与云平台系统之间的数据交换、控制指令传递和信息共享，提供更智能、安全和高效的交通和驾驶体验。通过量子加密通信技术，将车辆与云端之间的交互数据进行加密传输，尤其汽车安全和数据隐私相关的数据。量子密码技术可以应用但不限于以下场景中：

- 车辆识别与授权：验证车辆的身份，并授权其与云系统进行通信，确保车辆合法性；
- 安全通信：保护车辆之间或车辆与云之间的通信，防止窃取或篡改车辆传输的数据，从而确保车辆之间的通信是安全的；
- 车辆位置隐私：保护车辆位置数据的隐私。车辆通常需要共享位置信息，需要保护用户隐私。

车云云系统架构如图 22 所示，主要包括车辆、量子云服务器和汽车服务提供商。量子云服务器主要用于生产、存储和管理量子密钥，同时，将密钥发送给车辆和汽车服务提供商用于量子加密通信。汽车服务提供商主要用于收集车辆数据和隐私数据，同时，根据用户请求提供服务数据以及控制信息。车辆主要使用防篡改设备存储量子密钥，使用量子密钥进行车辆数据和隐私数据的加密传输。

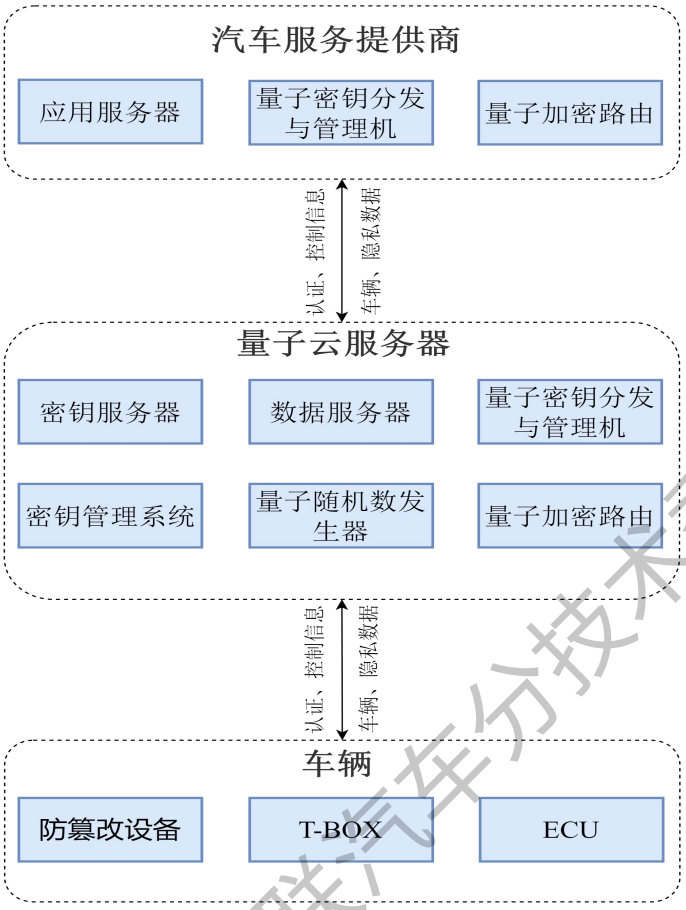


图 22 车云云系统架构

基于上述架构，量子密码技术可以有如下两种应用：

1）车辆识别和授权：

用于车辆与云端通信前的身份识别和授权，采用量子随机数和预置量子密钥，确保车辆身份认证的安全性和高效性。

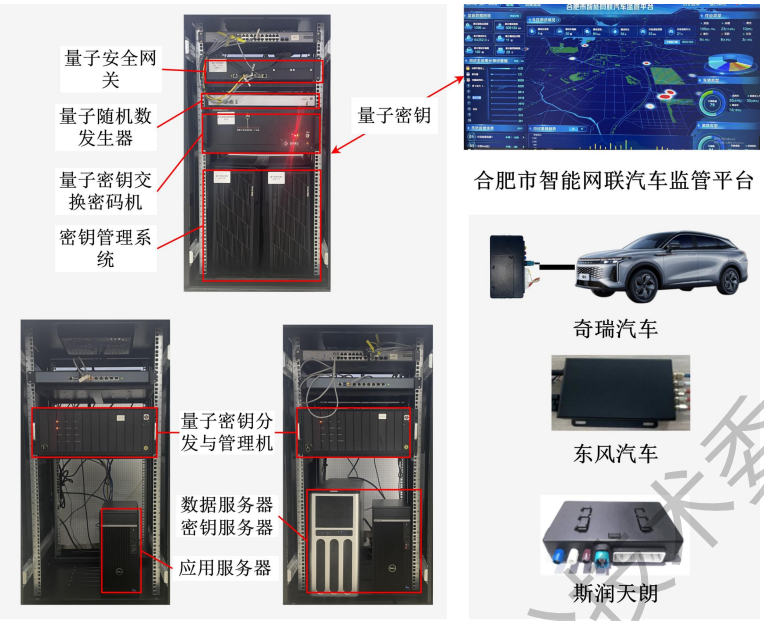
2）车云通信加密：

用于加密传输车辆数据和隐私信息，将量子密钥与国密算法融合，进一步保证车云通信的安全性。

（二）场景验证方案

验证系统如图所示，基于国盾量子的量子密钥分发管理系统 QSS 为基础，搭建具备密钥生成方法管理能力的量子云服务器和汽车服务提供商。将量子密钥充注在各个厂家的 T-BOX（奇瑞汽车，东风汽车，斯润天朗，合肥工大自研量子安全终端等）内，使其具备量子加解密的能力。实现车辆数据加密上传到车企 TSP 平台，并在车企 TSP 平台和政府监管云台（合肥市智能网联汽车创新中心）之间部署 QKD 设备实现云平台之间的量子加密通信。同时，基于仿真测试和实车测试，获取车辆身份授权和加解密通信

的通信开销和计算开销，保证通信的安全性和高效性。



(a) 量子云服务器和汽车服务提供商　　(b) 车辆

图 23 系统验证

（三）实施应用效果对比分析

下面将进行性能分析，性能分析主要从身份授权的计算开销和通信开销两个方面进行分析。在计算开销方面，主要统计云端和车辆计算过程所消耗的时间，并与其他方案进行对比，如图所示。

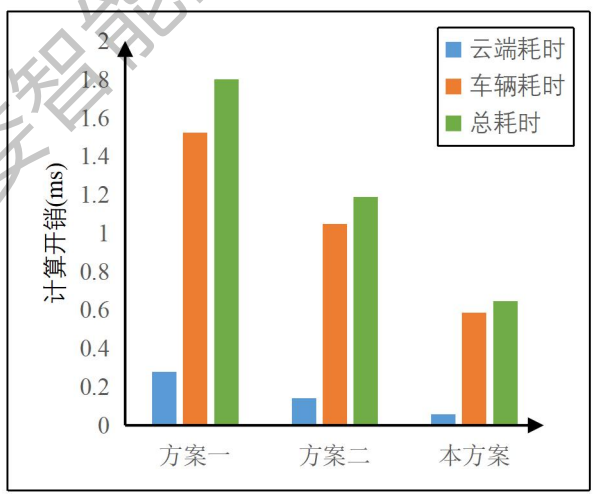


图 24 各方案计算开销对比

在通信开销方面，主要统计通信传输过程中传输数据的大小，数据包越小则通信开销越小，系统更加稳定和高效。通信开销与其他方案对比如下表所示。

表 3 各方案通信开销对比

方案	通信传输消息大小(bytes)	消息大小总和(bytes)
方案一	136+4+136+196+164+32	668
方案二	132+112+164+136	544
本方案	142+114+143+66	465

（四）总结分析

基于量子密码技术的车-云-云通信方案具有更好的通信性能，能够实现车联网数据的保密性、完整性、可用性。智能网联汽车量子通信系统具备良好的可扩展性，能够随着车辆数量的增加而灵活扩展，以适应未来智能网联汽车的发展需求。

4.2.2.3 V2X 应用场景

（一）应用场景

V2X 技术是基于车载自组网络技术实现的车辆之间和车辆与基础设施之间的通信，车载自组网络技术（VANETs）是以车辆为节点构建的移动通信网络，在 V2X 场景下，车辆与车辆之间以及车辆与路端之间会交换包括车辆的位置、速度、行驶轨迹等隐私数据。V2X 技术包括 V2V（车辆与车辆之间的通信）、V2I（车辆与基础设施之间的通信）、V2P（车辆与行人之间的通信）以及 V2N（车辆与网络之间的通信）。这些通信模式通过使用 5G、DSRC（Dedicated Short Range Communications）等通信标准，能实现高速、低延迟的数据传输，可以有效改善道路交通状况。但由于车载自组网络特殊的网络结构，网络拓部结构极易发生变化，及其受到安全攻击。如 DDOS，Sybil 攻击。

1. 交通信号优化控制：V2X 车辆可以与交通信号灯进行通信，提前获取信号灯的状态，从而根据交通流量和优化算法，调整行驶速度以避免红灯等待时间，减少交通拥堵。

2. 危险警告和事故预警：V2X 车辆可以接收到来自其他车辆或道路设施的警告信息，如前方交通意外、施工区域等，从而提前采取避让措施，减少交通事故的发生。

3. 自动驾驶辅助：V2X 车辆可以通过与交通基础设施的通信，获取更准确的位置和地图信息，从而提高自动驾驶系统的定位精度和导航准确性。

4. 智能停车导航：V2X 车辆可以通过与停车场的通信，获取实时的停车位信息和导航指引，提高停车效率和用户体验。

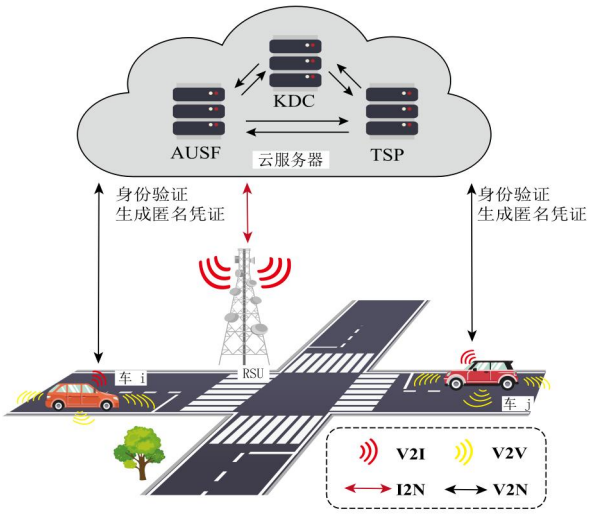


图 25　典型车路协同通讯场景

（二）安全性和隐私要求

• 访问控制：为了确保 V2X 通信的安全性，只有得到明确授权的车辆才能执行密钥协商操作。这意味着在通信之前，必须经过有效的身份验证和授权流程，以防止未经授权的车辆访问通信网络。

• 相互认证：鉴于车载通信信道的开放性和不安全性，消息的接收方需要对发送方的身份进行严格的验证，以确保消息的合法性和完整性。这有助于防止伪造消息和欺骗攻击。

• 保密：在 V2X 通信的过程中，建立的会话密钥必须保持绝对的保密性。这确保了通信的保密性，防止第三方获得敏感信息。

• 身份条件隐私保护：从攻击者的角度来看，通过通信信道传输的消息不应该泄露车辆的真实的身份，从而可以保护车辆的身份隐私。但是，验证应该能够根据车辆发送的消息揭示车辆的真实的身份，从而可以跟踪和发布恶意车辆。

• 前向和后向保密：在会话 S1（或 S2）中建立的会话密钥应该独立于在 S2（或 S1）中建立的密钥。

• 抵抗重放攻击：为了防止重放攻击，接收方必须检查接收到的消息的新鲜度。如果消息已过期，接收方应拒绝处理该消息，以维护通信的完整性和安全性。。

• 抵抗中间人攻击：任何恶意攻击者都不应该成功修改或伪造消息

• 抵抗拒绝服务攻击：所提出的通信协议应具有抵抗拒绝服务攻击的能力，不能破坏 V2X 通信计划。必须采取适当的安全措施，如流量管理和资源分配，以确保通信网络能够抵御拒绝服务攻击，保持可用性和可靠性。

（三）量子通信在 V2X 场景中的应用

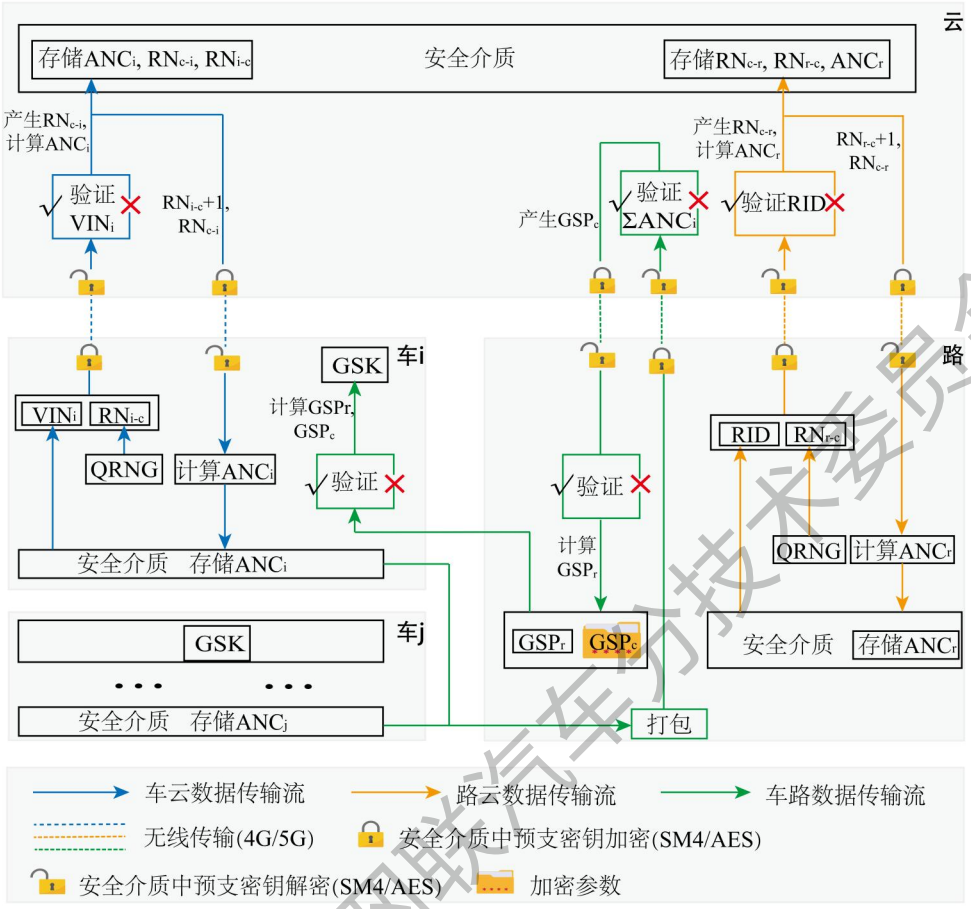


图 26 方案流程图

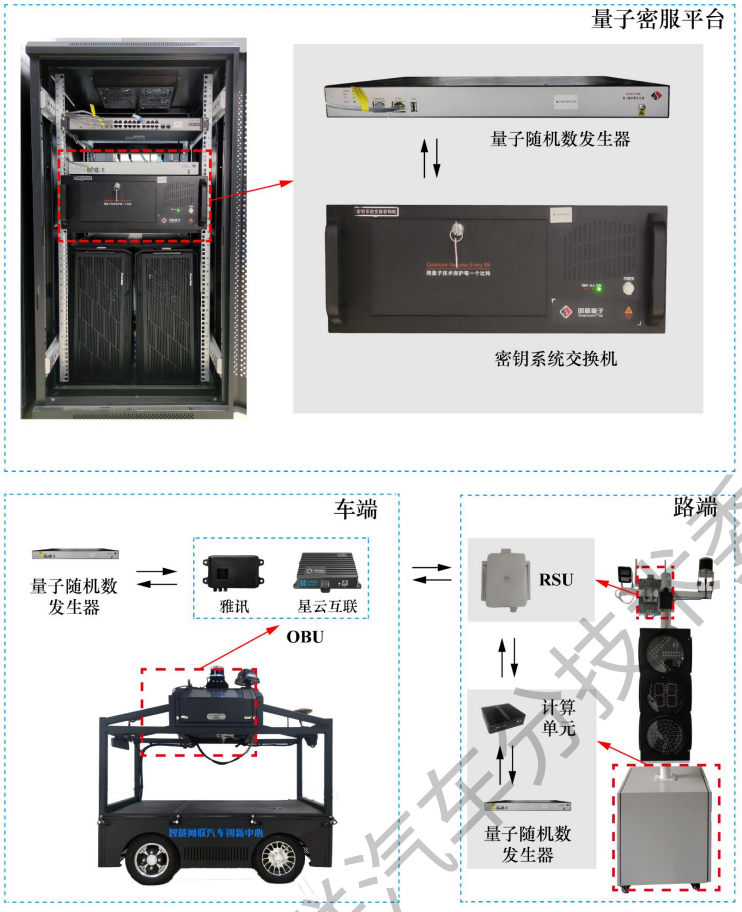


图 27 实验设备示意图

方案包括以下五个阶段：注册阶段，初始化阶段，组通信前密钥下发阶段，组通信阶段，以及组成员变化时组密钥更新阶段。注册阶段主要完成集成 OBU（雅迅、星云互联）的车辆与路端设备 RSU（华为）的量子会话密钥与量子完整性校验密钥的预充注，以及车端唯一标识与路端唯一标识的云端入库操作。初始化阶段负责车辆与路端匿名凭证的生成。车路之间均采用 PC5 广播通信，为了减少了车辆真实身份暴露的风险，车辆与路端交互均使用匿名身份，车路云通过一种两段式的组密钥，即车端分别获得路端和云端的一个关键参数计算得到组密钥，从而减少了组密钥的更新频率。由于路端设备固定，而在一个路端广播通讯范围内，车辆会持续动态更新，即会持续有新的车辆加入或离开。将路端广播通讯范围内的车辆看成一组，一个路端设备管理的组面临的车辆的更新可分为新成员加入与组成员离开两种情况。为了保障前向安全与后向安全，需要及时对组密钥进行更新。

实施应用效果对比分析

表 4 各种方案的计算费用比较(注册+组密钥分发总流程)

方案	车	路	服务器或第三方

Kamil	$5T_h+3T_{add}+3T_{mul}$	（$3T_h+3T_{add}$）*n	$3T_{add}+T_h+$ （$4T_h+4T_{mul}+T_{add}$）*n
Shawky	$2T_{sm}$ $+T_{mul}+T_{veri}+T_{sign}$	$(n+1)T_{sm}$ $+n(T_{mul}+T_{veri})+T_{sign}$	$(n+2)T_{mul}+(n+1)T_{sign}$
本方案	$3T_{sm}$ $+3T_{hamc}+2T_h$	$4T_{sm}+4T_{hamc}+2T_h$	$(3n+4)T_{sm}+(2n+4)\ T_{hamc}+$ $(n+1)T_h$

表 5 组密码更新计算开销（加入）

方案	新加入车辆	原来车辆	路	云
Kamil	$5T_h+3T_{add}+3T_{mul}$	T_h+2T_{add}	$(n+1)(T_h+3T_{add})$	$5T_{add}+4T_h+4T_{mul}$
Shawky	$2T_{sm}$ $+T_{mul}+T_{veri}+T_{sign}$	T_{sm}	$2T_{sm}+T_{mul}+T_{veri}$	$T_{mul}+T_{sign}$
本方案	$3T_{sm}+3T_{hamc}+2T_h$	T_h	$2T_{sm}+2T_{hmac}+Th$	$4T_{sm}+4T_h+4T_{hmac}$

表 6 组密码更新计算开销（离开）

方案	原来车组车辆	路	云
Kamil	T_h+2T_{add}	$n(T_h+3T_{add})$	$(n-1)(4T_{add}+T_h)$
Shawky	T_{as}	$2T_{sm}+T_{mul}+T_{veri}$	$T_{mul}+T_{sign}$
本方案	T_h	$2T_{sm}+2T_{hmac}+T_h$	$(n+1)T_{sm}+2T_h+2T_{hmac}$

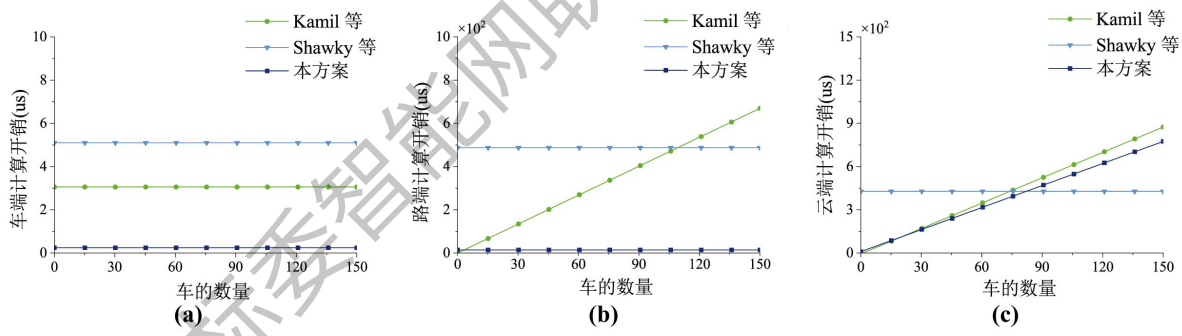


图 28 无车进出时车路云的计算开销

(a)为车端 N 辆车的计算开销;(b)为路端的计算开销;(c)为云端的计算开销

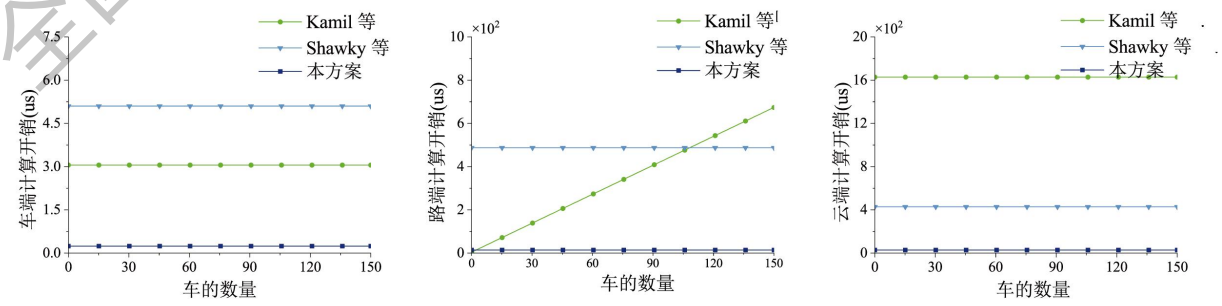


图 29 新车加入时车路云的计算开销

(a)为车端 N+1 辆车的计算开销; (b)为路端的计算开销; (c)为云端的计算开销

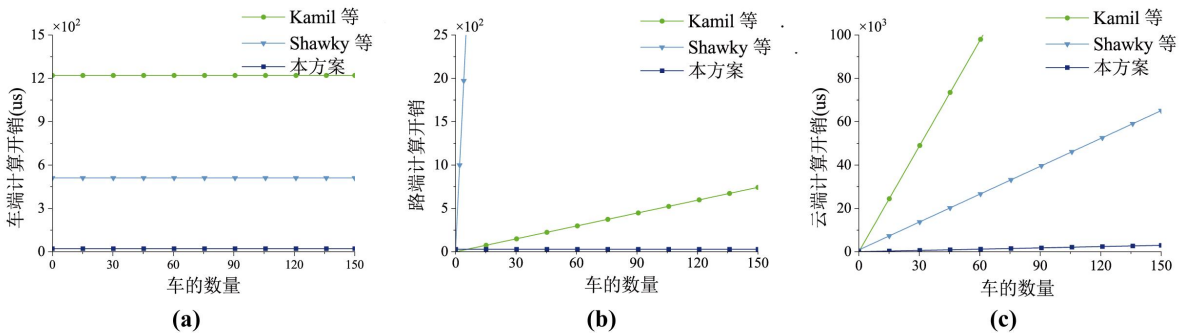


图 30 有车辆离开时车路云的计算开销

(a)为车端 N-1 辆车的计算开销; (b)为路端的计算开销; (c)为云端的计算开销

综上所述，我们可以得到车路云三者在不同状态下执行组密钥更新所需要的时间折线图，如图所示，可以看到我们的方案在多车组密钥分发阶段与组密钥更新阶段有着更大的优势，相比较于区块链的方式，信令开销减少一半。

车联网数据加密后，实现了数据的保密性完整性，由于考虑到车路云三者在不同状态下，并为不同场景设计不同的密钥分发方案，所有实现了可拓展性与实时性。在上述流程中使用密钥为一次一密，可防范重放攻击，中间人攻击，不可服务等多种攻击。

4.2.2.4 OTA 应用场景

通常 OTA 升级场景中，一般会在软件包刷写的基本网络安全防护需求上（如使软件发布服务端用目标 ECU 私钥对包进行签名，车端采用 ECU 公钥进行验签），会增加一下额外的安全付防护。因为在通过 OTA 这种网络传输的方式将升级包、升级信令等数据传入到车端，从而会在 OTA 升级过程中引入更多的网络攻击风险，因此针对 OTA 场景，会提出例如对包的保密性、来源真实性进行防护，升级信令的真实性、完整性进行防护等。

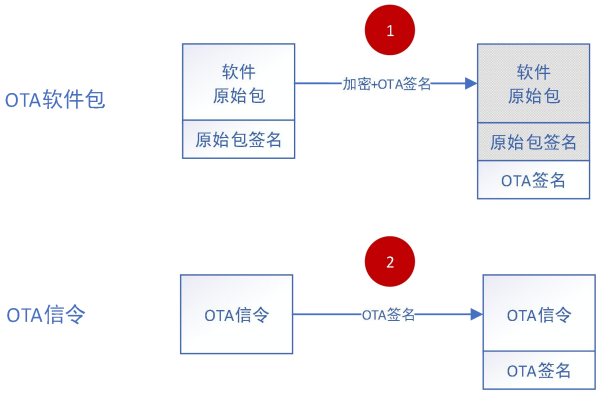


图 31 OTA 加密

OTA 软件包的防护要求

一般会对 OTA 软件包进行加密（防软件包 CDN 服务器、ECU 上被非法获取）、OTA 签名（证明该包来自 OTA 服务器）等保护。

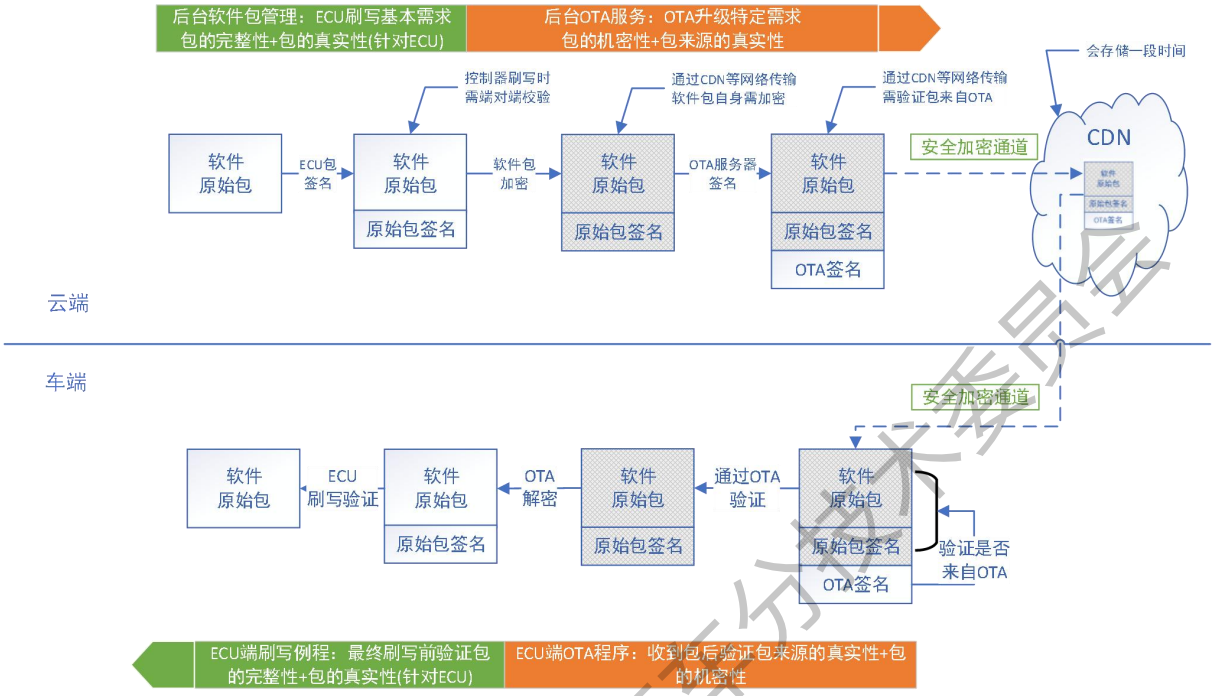


图 32 OTA 软件包加密

OTA 信令的防护要求

一般对 OTA 服务器给车端发出的 OTA 信令增加签名信息，对信令提供完整性（未被篡改）、真实性（来自 OTA）的防护。

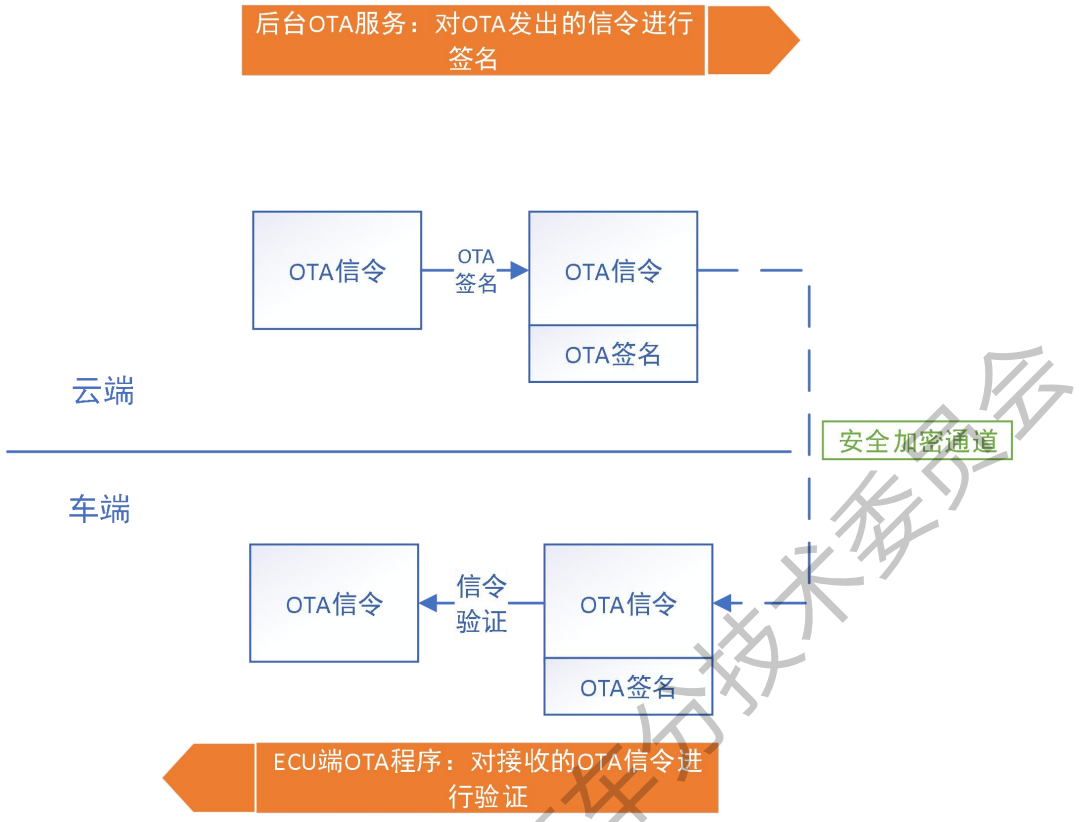


图 33 OTA 信令加密

OTA 场景安全通信防护要点

上述场景中，对 OTA 业务场景的安全通信一般会有三个基本的防护要求：

1) 安全加密通道需求

· 利用标准的 X.509 数字证书，搭建双向 TLS1.2 安全加密通道；

· 通道建立时，会使用双方的证书来验证对方身份的真实性（公钥交换）；

· 所有在该通道传输的数据都会统一加密；

所有在该通道的数据都会加上防重放等防护机制；

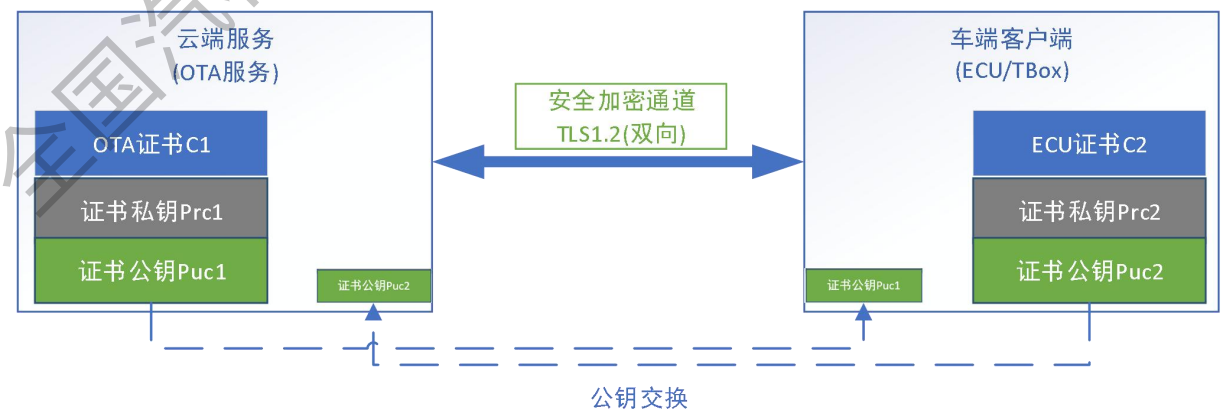


图 34 OTA 安全加密通道

2) 签名验签防护

· 云端：采用 OTA 服务器的公私钥对中的公钥，对 OTA 软件包、或 OTA 信令进行签名；

· 车端：采用 **OTA 服务器的公钥**，利用车端的 OTA 程序，进行验签；

车端获得 OTA 的公钥一般有两种方式：

a) ECU 或整车出厂时预制 OTA 签名公钥；

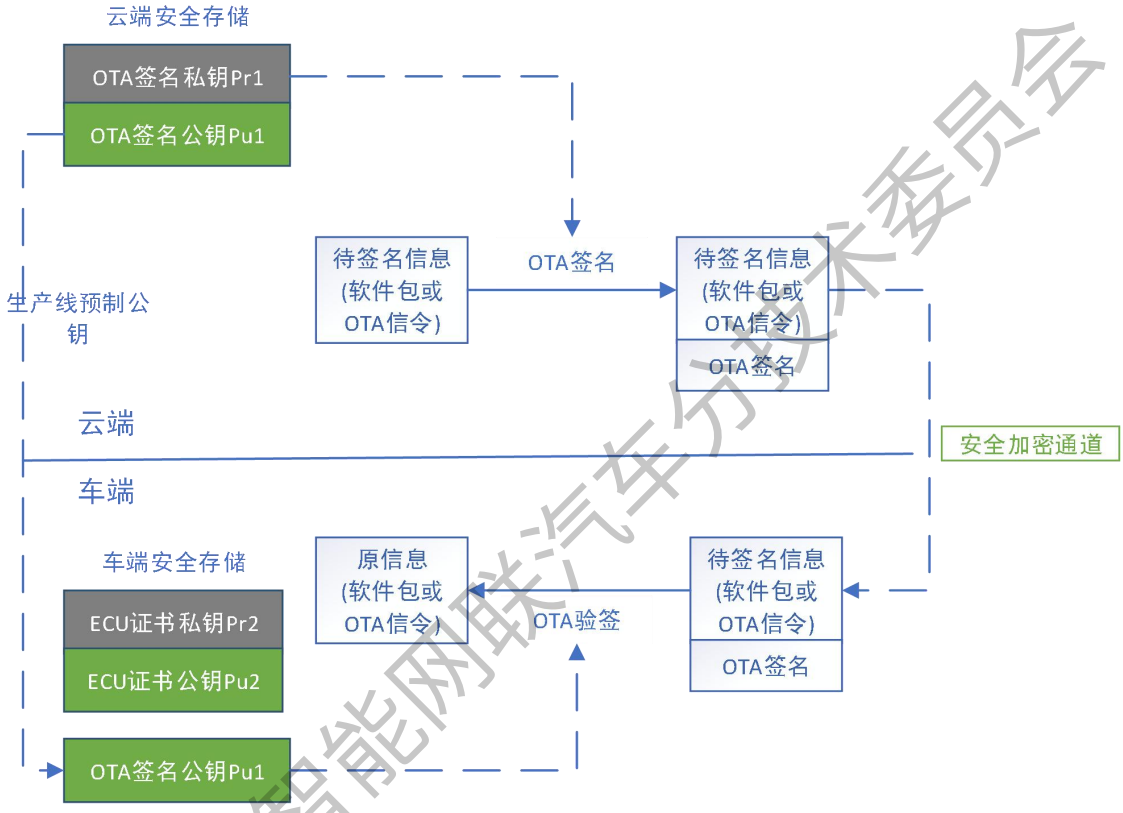


图 35 OTA 公钥

b) 使用期间将 OTA 公钥随着软件包的签名信息一起下发给 ECU（PCKS#7 格式）；

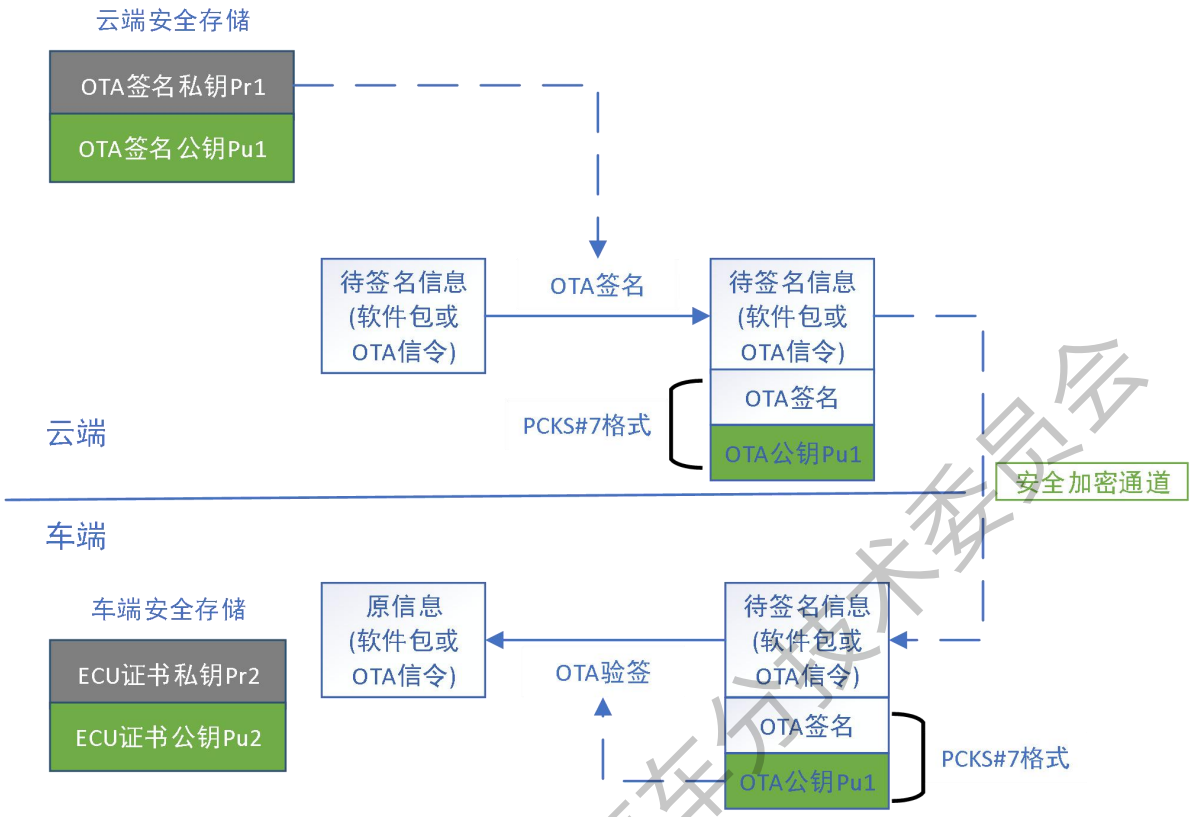


图 36 OTA 签名

3) 加密防护

· 云端：OTA 服务器给每个软件包动态生成一个对称加密密钥（如 K1），对软件包进行加密；

· 车端：ECU 接收到软件包的加密密钥（K1），对软件包进行解密；

车端获取软件包加密密钥（K1）一般也有两种方式：

a) 使用加密信封的方式来传递，如 OTA 服务端使用车端 ECU 的公钥（如 ECU 身份证书），对该软件包加密密钥进行加密，ECU 端使用 ECU 的私钥解密，获取软件包加密密钥（K1）。

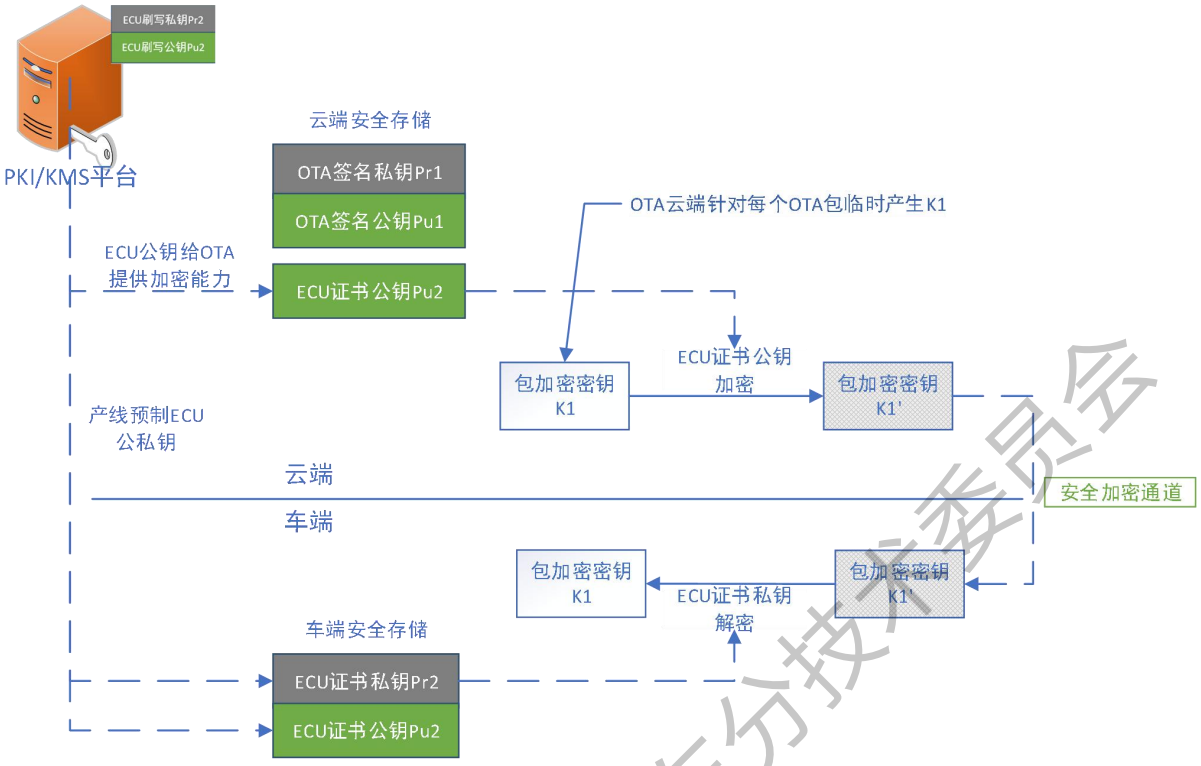


图 37 OTA 私钥

b) 云端通过 OTA 签名私钥+ECU 证书公钥，采用密钥协商算法，如 DH，双方协商出一个对称密钥，用此对称密钥对包加密密钥进行加密传送（车端采用：ECU 证书私钥+OTA 签名公钥）。

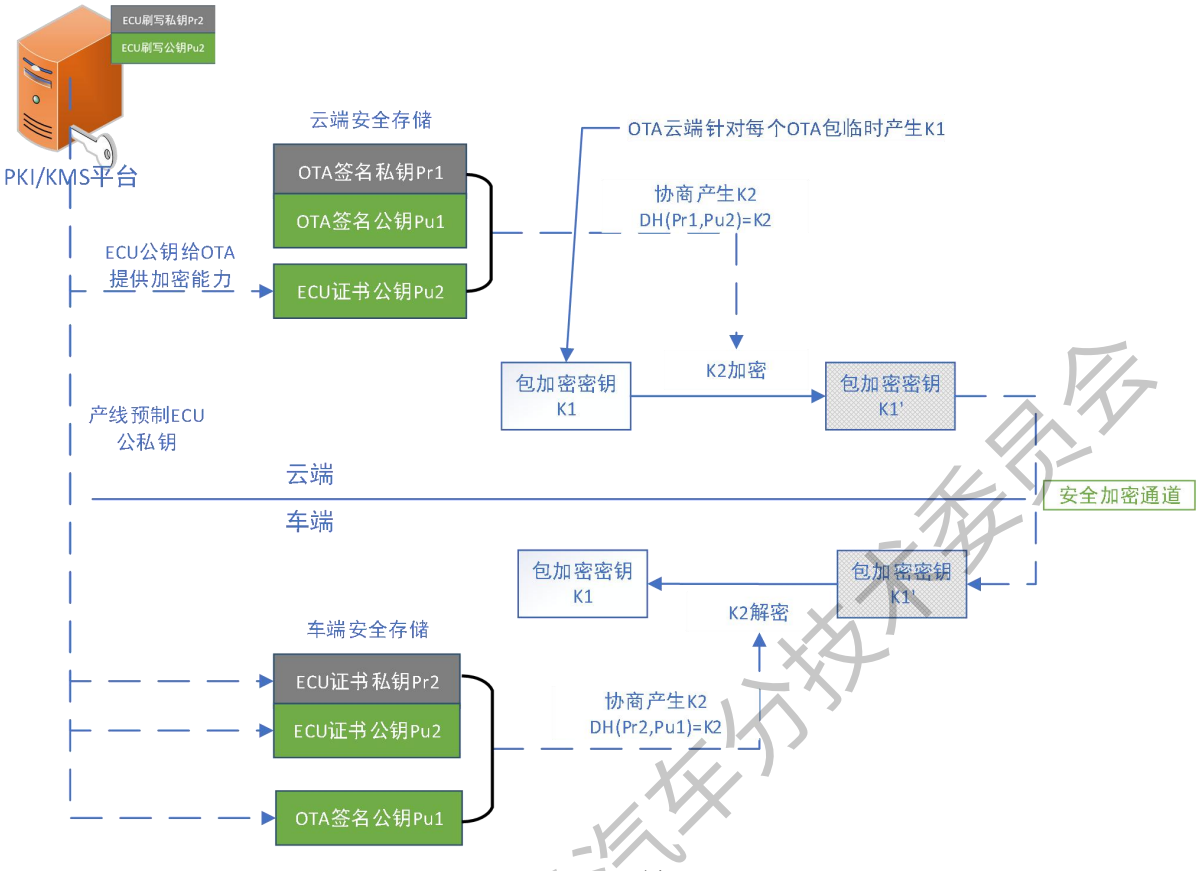


图 38 OTA 公钥

OTA 场景安全通信分析

从上述几种 OTA 的应用场景中对安全通信的实现方式进行进一步分析，都需要将自己的公钥共享给对方，以完成相应的身份认证、加解密、密钥协商等，比如：

- 利用 X.509 搭建的安全加密通道 TLS 时，需要将自己的公钥共享给对方，才能完成身份的验证；
- OTA 服务端使用 ECU 公钥加密对称密钥 K1 实现对称密钥的传送，也是需要提前知道 ECU 证书公钥；
- 在协商产生的密钥 K2 时，则双方都需要交换自己的公钥给对方，才能完成密钥协商；

这些都是基于使用非对称密钥及其算法来提供的网络安全防护手段，如果针对公私钥对的量子攻击商业工具出现在市面时，其工具可以根据公钥就可以轻易的计算得到私钥，就轻而易举的破解了此类基于非对称算法搭建的信任体系，整个智能网络汽车的 OTA 应用场景将变得极度的不安全。因此亟待一种新的抗量子攻击的方案来替换、或完善此类场景的网络安全防护手段。

OTA 场景实施应用效果测试分析

1) 测试方针

在 VCCD 上对量子SDK 相关接口进行单元测试和性能测试，验证 SDK 正确性、稳定性、健壮性。测试流程图如下所示：

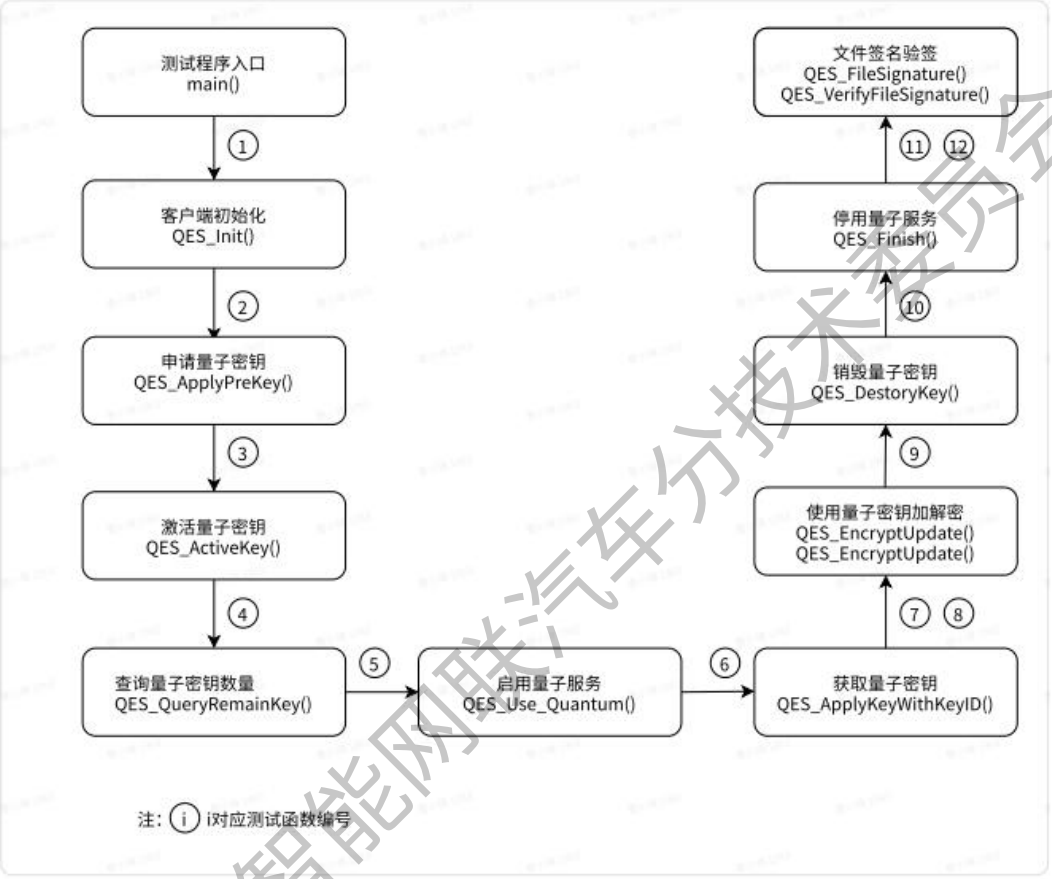


图 39 集成量子密钥的 OTA 业务测试流程图

2) 单元测试结果

表 7 单元测试结果统计

NO	函数名	OK	NG	N/A	分支覆盖率	项目数
1	QES_Init	2	0	0	100%	2
2	QES_ApplyPreKey	1	0	0	100%	1
3	QES_ActiveKey	1	0	0	100%	1
4	QES_QueryRemainKeys	1	0	0	100%	1
5	QES_Use_Quantum	1	0	0	100%	1
6	QES_ApplyKeyWithKeyID	1	0	0	100%	1
7	QES_EncryptUpdate	6	0	0	100%	6
8	QES_DecryptUpdate	6	0	0	100%	6
9	QES_DestoryKey	1	0	0	100%	1

10	QES_Finish	1	0	0	100%	1
11	QES_FileSignature	4	0	0	100%	4
12	QES_VerifyFileSignature	4	0	0	100%	4

3) 性能测试

a) 量子加解密性能测试

对三个文本文件（大小分别为 1KB,1MB,1GB）进行加解密；

```
-rw-rw-r-- 1 xm xm 1.0G Oct  8 07:10 bigFile.txt
-rw-rw-r-- 1 xm xm 1.0M Oct  8 07:22 midFile.txt
-rw-rw-r-- 1 xm xm 1.0K Oct  8 06:45 smallFile.txt
```

对两个域控软件包（大小分别为 11MB,1.2GB）进行加解密。

```
-rw-rw-r-- 1 xm xm  11M Oct  9 10:05  S00                    701.mbf
-rw-rw-r-- 1 xm xm 1.2G Sep  7 02:51  S0                     701.mbf
```

分别进行10轮量子加解密测试，针对函数QES_EncryptUpdate、QES_DecryptUpdate，性能测试结果如图所示。

```
2023-10-08T08:38:00+00:00
Running ./myTest
Run on (8 X 3392.03 MHz CPU s)
CPU Caches:
  L1 Data 32 KiB (x8)
  L1 Instruction 32 KiB (x8)
  L2 Unified 1024 KiB (x8)
  L3 Unified 36608 KiB (x8)
Load Average: 1.04, 0.84, 0.81
-------------------------------------------------------------------------------
Benchmark                      Time       CPU        Iterations      Bytes/Seco
-------------------------------------------------------------------------------
BM_ENCRYPT/1KB/iterations:10  43.1 us     43.1 us         10          22.67 MiB/
BM_ENCRYPT/1MB/iterations:10  42.2 ms     42.2 ms         10          23.72 MiB/
BM_ENCRYPT/1GB/iterations:10  43.9 s      43.9 s          10          23.33 MiB/
BM_DECRYPT/1KB/iterations:10  47.1 us     47.0 us         10          20.77 MiB/
BM_DECRYPT/1MB/iterations:10  45.8 ms     45.8 ms         10          21.85 MiB/
BM_DECRYPT/1GB/iterations:10  46.9 s      46.9 s          10          21.79 MiB/
BM_ENCRYPT/11MB/iterations:10 451.4 ms    451.2ms         10          23.55 MiB/
BM_ENCRYPT/1.2GB/iterations:10 50.6s      50.6 s          10          23.32 MiB/
BM_DECRYPT/11MB/iterations:10 488.3 ms    488.2ms         10          21.77 MiB/
BM_DECRYPT/1.2GB/iterations:10 54.4 s     54.4s           10          21.70 MiB/
注：第一列是程序名称+文件大小+迭代次数，第二列是平均迭代一次的时钟时间，
第三列是平均迭代一次的CPU时间，第四列是循环的迭代次数，第五列是每秒钟处理的字节速率
```

图 40 性能测试结果

获取量子密钥性能测试

向量子密钥服务端获取 10 个 16 字节的量子密钥，针对函数 QES_ApplyKeyWithKeyID，性能测试结果如下：

```
2023-10-08T11:50:31+00:00
Running ./myTest
Run on (8 X 3392.03 MHz CPU s)
CPU Caches:
  L1 Data 32 KiB (x8)
  L1 Instruction 32 KiB (x8)
  L2 Unified 1024 KiB (x8)
  L3 Unified 36608 KiB (x8)
Load Average: 0.76, 0.51, 0.36
-------------------------------------------------------------------------------
Benchmark                        Time             CPU   Iterations   Bytes/Sec
-------------------------------------------------------------------------------
BM_GETKEY/16B/iterations:10     264917 us       80558 us     10       198.614B/

注：第一列是程序名称+文件大小+迭代次数，第二列是平均迭代一次的时钟时间，
第三列是平均迭代一次的CPU时间，第四列是循环的迭代次数，第五列是每秒钟处理的字节速率
```

图 41 获取量子密钥性能测试结果

由以上分析可见，量子密钥相关接口具有正确性、稳定性、健壮性。

4.2.2.5 5G 远控驾驶量子加密应用

（一）应用场景

车路云一体化融合控制系统是利用新一代信息与通信技术，将人、车、路、云的物理层、信息层、应用层连为一体，进行融合感知、决策与控制，可实现车辆行驶和交通运行安全、效率等性能综合提升的一种信息物理系统，也可称为“智能网联汽车云控系统”，或简称“云控系统”。5G 远控驾驶是“云控系统”的一类典型应用，它可应用但不限于以下场景中：

①在灾区、高危路段的远程驾驶，可以提高营救效率和通行效率；

②在矿山、油田等生产区域，远程驾驶代替工人完成作业，减少人员伤亡；

③在无人驾驶车辆出现问题时，驾驶员及时接管，可以消除车辆异常，改变车辆失控状态，避免车辆伤害到行人和其它车辆；

④自动驾驶实车测试中，危险极端工况场景可由远程驾驶代替。

5G 驾驶系统架构如图所示，主要包括远控平台、云控网关和远控台架。远控平台与云控网关以及远控台架交互调度、控制、连接、以及状态信息等，实现车辆调度、系统管理、数据监控、智能监控、报警管理等；远控台架与车辆之间通过 5G 网络交互视频流数据、信令数据、控制指令、监控数据等，在远控平台的统一调度下实现车辆的远程实时控制。

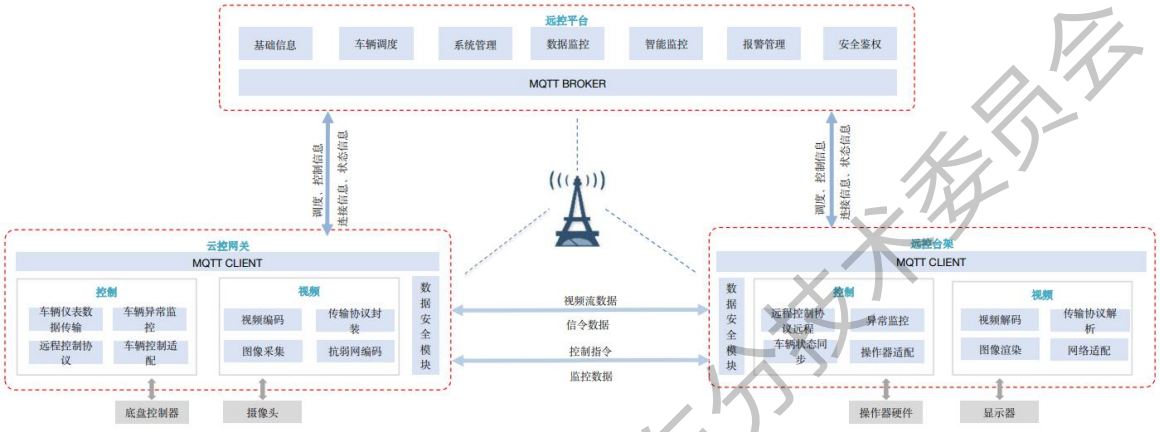


图 42 5G 远程驾驶系统架构

基于上述架构，在 5G 远控驾驶中，量子安全技术可以有如下两种应用：

① 车云通信加密：用于远控平台调度、控制、连接等重要信息以及状态信息等车辆隐私信息的加密传输，采用国密算法加量子密钥，进一步提升信息车云交互的安全性。

② 端端通信加密：用于云控网关（车端）与远控台架之间控制指令以及监控数据的加密传输，进一步保障和提升驾驶安全性。

（二）场景验证方案

验证系统如图所示，基于东风在 2018 年实现的基于 4G 网络的远程驾驶系统搭载及测试系统进行研发。在自研的 L4 级自动驾驶车辆 Sharing-VAN 以及远控台架的基础上搭载 5G 远程驾驶系统，对 T-Box 进行改造，通过内置量子 SD 卡、开发密钥充注系统的方式，实现量子密钥的充注；同时，基于东风技术中心园区的 5G 专网，开展 5G 远程驾驶中的端端加密以及车云交互中的量子加密应用，实现 5G 远控驾驶量子加密示范应用。

图 43 场景验证示意

5. 标准化与产业化建议

5.1 智能网联汽车信息安全标准现状

在《国家车联网产业标准体系建设指南》的指导下，全国汽车标准化技术委员会（TC114）、全国信息技术安全标准化技术委员会（TC260）、中国通信标准化协会（CCSA）、车载信息服务产业应用联盟（TIAA）、中国智能网联汽车产业创新联盟（CAICV）等各标准委员会及行业组织积极开展智能网联汽车共性基础、关键技术以及行业产业急需标准的研究制定，在车联网（智能网联汽车）网络安全标准研制方面已取得阶段性成果。

5.2 全国汽车标准化技术委员会

全国汽车标准化技术委员会下设的智能网联汽车分技术委员会（SAC/TC114/SC34）负责归口管理我国智能网联汽车领域的国家标准和行业标准。2017 年，智能网联汽车分标委秘书处正式设立汽车信息安全标准工作组。我国现有汽车信息安全标准根据应用的范围和对象，划分为强制性标准、推荐性标准及行业标准，汽车信息安全标准体系框架如图所示。

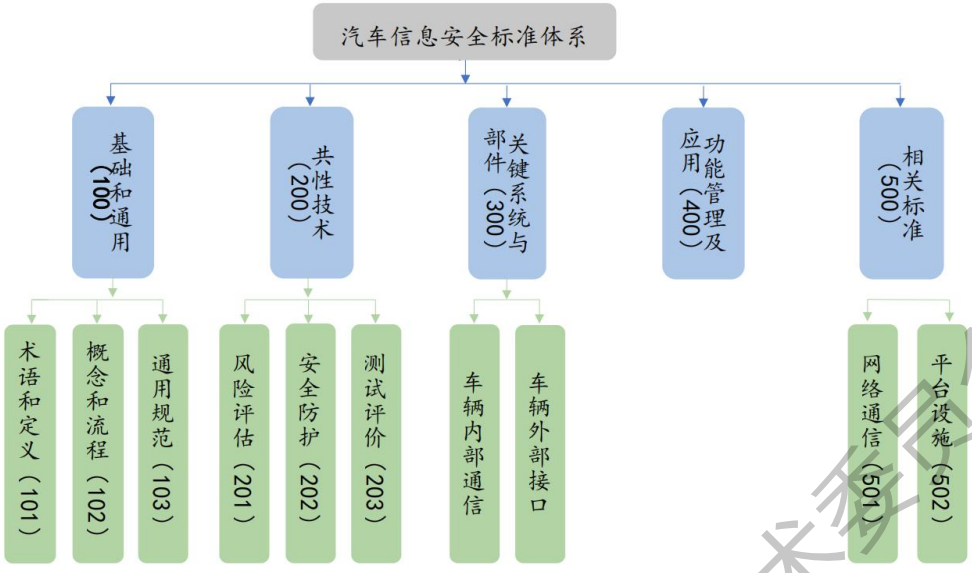


图 44 汽车信息安全标准体系框架

（1）基础和通用类项目

基础类标准主要包括术语和定义、概念和流程及通用规范三部分。术语和定义标准主要用于统一汽车信息安全技术有关的专用术语及其定义；概念与流程标准主要围绕汽车产品全生命周期相关流程管理要求；通用规范主要包括汽车信息安全涉及的共性基础技术规范如数字证书与密码技术等，该类标准研究与制定将为其他的信息安全相关标准提供基础支撑作用。

（2）共性技术类项目

共性技术类标准主要包括涉及汽车整车、系统、部件信息安全防护共性技术的风险评估、安全防护和测试评价三部分，涵盖了汽车信息安全的评、防、测各个关键环节。风险评估标准用于规范汽车专用的信息安全风险评估方法；安全防护标准用于规定包括认证、审计、完整性要求等在内的整车与系统的信息安全防护通用技术条件和汽车在遭受网络攻击时应具备的入侵事件检测能力，以及相应的应急响应措施技术标准，这类标准还包括各种车辆资产均会涉及到的数据、软件方面的通用安全要求；测试评价标准主要用于指导整车、系统及其部件的信息安全测试与评价实施。该类别旨在梳理各不同层级标准项目的共性技术特点，提出通用的共性安全技术要求。

（3）关键系统与部件类项目

关键系统与部件类标准主要针对车辆信息传输通路上采集、处理、通信与交互等各主要节点所涉及的系统和部件信息安全提出防护要求。根据汽车运行过程所涉及到的信息传递节点，将该类标准细分为车辆内部通信及车辆与外部接口两个部分。车辆状态与

环境感知标准包括汽车在驾驶或非驾驶过程中雷达、摄像头、传感器等用于感知人、车、路相关信息的设备所应满足的信息安全防护标准；车辆控制与信息处理标准主要是对具有车辆控制及信息处理功能的一系列中央处理器、整车控制单元、微控制器、远程控制器等车辆专用逻辑部件和设备的信息安全防护要求；车辆内部通信主要是面向包括CAN、LIN、MOST 总线、车辆内部通信协议以及信息交互网关等用于汽车专用部件和设备信息通信的安全防护要求；车辆与外部接口标准主要是对汽车与外界通信的各类接口所应具备的信息安全功能的技术要求。

（4）功能应用与管理类项目

功能应用与管理类标准包括了汽车使用过程中的信息通信应具备的信息安全功能，以及汽车在各类具体应用场景下所应满足的安全防护要求，包括身份认证、软件升级（OTA）、电动汽车充电等具体标准。

（5）相关标准类项目

相关标准类主要包括车辆外部通信过程以及车联网平台和基础设施相应的一系列信息安全防护标准、规范和指南。这部分将与汽车信息安全标准相配合，实现汽车与外界通信的整体网络环境安全。

截止目前，汽标委智能网联汽车分委会基于标准体系规划与行业实际需求，汽车信息安全标准工作组研制的标准进展如表 8 所示。

表 8 汽标委汽车信息安全标准及研究项目进展

序号	项目名称	性质	进度
1	《汽车信息安全通用技术要求》	GB/T	发布
2	《电动汽车远程服务与管理系统信息安全技术要求及试验方法》	GB/T	发布
3	《车载信息交互系统信息安全技术要求及试验方法》	GB/T	发布
4	《汽车网关信息安全技术要求及试验方法》	GB/T	发布
5	《电动汽车充电系统信息安全技术要求》	GB/T	发布
6	《汽车软件升级通用技术要求》	GB/T	报批
7	《汽车诊断接口信息安全技术要求》	GB/T	报批
8	《汽车信息安全应急响应管理指南》	GB/T	报批
9	《道路车辆 信息安全工程》	GB/T	制定中
10	《汽车整车信息安全技术要求》	GB	报批
11	《汽车电子控制单元（ECU）信息安全防护技术要求研究》	研究项目	完成预研
12	《汽车信息安全风险评估规范》	研究项目	完成预研

13	《车载计算平台标准化需求研究》	研究项目	完成预研
14	《智能网联汽车 数字证书应用技术要求研究》	GB/T	提交立项
16	《道路车辆 信息安全工程审核指南》	GB/T	预研
17	《道路车辆 软件升级工程》	GB/T	预研
18	《汽车漏洞分类分级规范》	GB/T	预研

5.2.1 全国信息技术安全标准化技术委员会

全国信息技术安全标准化技术委员会（SAC/TC 260，简称信安标委）着手汽车电子系统本身，建立信息安全标准体系及网络安全指南，如表 9 所示。

表 9 信安标委汽车信息安全相关项目进展

序号	标准名称	性质	进度
1	《信息安全技术 汽车电子系统网络安全指南》	GB/T	已发布
2	《信息安全技术 车载网络设备信息安全技术要求》	GB/T	制定中
3	《信息安全技术 网络产品和服务安全通用要求》	GB/T	已发布
4	《信息安全技术汽车数据处理安全要求》	GB/T	已发布

5.2.2 中国通信标准化协会

中国通信标准化协会（CCSA）积极完善汽车信息安全标准体系。目前，CCSA 研制的车联网安全相关标准进展如表 10 所示。

表 10 CCSA 汽车信息安全相关项目进展

序号	标准名称	性质	进度
1	《基于公众电信网的联网汽车信息安全技术要求》	YD/T	已发布
2	《车联网信息服务 数据安全技术要求》	YD/T	已发布
3	《车联网信息服务 用户个人信息保护要求》	YD/T	已发布
4	《车联网无线通信安全技术指南》	YD/T	已发布
5	《车联网信息服务平台安全防护要求》	YD/T	已发布
6	《车载应用与服务软件的安全要求》	YD/T	已发布
7	《移动智能终端数字车钥匙信息安全技术要求》	YD/T	已发布
8	《基于 LTE 的车联网无线通信技术 基站设备测试方法》	YD/T	已发布
9	《基于 LTE 的车联网无线通信技术 网络层技术要求》	YD/T	已发布
10	《基于 LTE 的车联网无线通信技术 网络层测试方法》	YD/T	已发布
11	《基于 LTE 的车联网无线通信技术 消息层技术要求》	YD/T	已发布
12	《基于 LTE 的车联网无线通信技术 消息层测试方法》	YD/T	已发布

5.2.3 汽车信息安全相关国际标准动态

5.2.3.1 联合国世界车辆法规协调论坛(UN/WP.29)

世界车辆法规协调论坛（UN/WP.29）是联合国下属的一个专门负责制定和协调汽车技术法规的机构。其下属的智能交通与自动驾驶（ITS/AD）非官方工作组根据七国集团（G7）的提议开始关注车辆信息安全问题，牵头制定了《自动驾驶汽车网络安全与数据保护指南》，并成立了车辆信息安全与软件升级（CS/OTA）专项工作组，负责车辆信息安全相关法律法规的研究与制定。

CS/OTA 组以车内信息安全为重点，以制定信息安全技术法规或决议为目标，吸收国际电联和国际标准化组织的相关成果，与国际电信联盟下设的第 17 组（即信息安全）相互融合。此外，还在网络安全、数据保护、汽车软件升级（OTA）等方面进行深入研究，制定相关国际标准和法规。

目前，CS/OTA 小组已经完成了对汽车信息安全风险和威胁的总结和分类，提出了包括术语定义以及威胁分析和安全防护的基本原则和措施的标准草案。相关成果不仅将在联合国层面对相关协议签署国的车辆法律法规、汽车产品认证和准入相关条款产生直接影响，也将成为世界其他国家制定车辆信息安全标准的重要依据和参考。

5.2.3.2 道路与车辆技术委员会国际标准化组织（ISO/TC22）

2016 年 10 月，隶属于道路与车辆技术委员会国际标准化组织（ISO/TC 22）的汽车电子技术委员会（ISO/TC 22/SC 32）正式成立车辆信息安全工作组（ISO/TC 22/SC 32/WG 11），负责制定车辆信息安全的相关标准。该标准的具体运作方式是在 ISO/TC 22 的框架内共同成立 ISO/SAE 车辆信息安全联合工作组（ISO/SAE JWG），参照现有的信息安全国际标准，包括 ISO 27000 系列信息安全标准、ISO/IEC 15408 信息安全评估原则和美国 SAE J3061，并在各国现有基础和经验的基础上，开展车辆信息安全国际标准即 ISO 21434（道路车辆-网络安全工程）的研究和制定。

ISO 21434 主要针对道路车辆的电子和电气系统以及系统之间的接口交互和通信，将规范企业和组织层面的信息安全管理和风险管理的要求，车载电子和电气系统以及系统之间的接口交互的信息安全技术要求，安全生命周期（概念、设计、开发、生产、运营、维护和报废）中系统之间的通信，威胁分析和风险评估方法，安全的策略（预测、预防、探索、响应和恢复等）。威胁分析和风险评估方法，安全策略（预测、预防、探

索、响应和恢复等），信息安全的系统测试评估方法，以及信息安全过程开发控制的要求。并由 4 个工作组组成，具体分工见表 11。

表 11 从属于 ISO/TC 22/SC 32/WG 11 的工作组

工作小组	任务
威胁分析和风险评估管理小组	信息安全相关项目的定义、威胁识别、漏洞识别和风险管理、风险评估和安全级别的定义。
产品开发组	生产发布前的信息安全标准：基于 V 流程的系统化项目、信息安全标准的制定、信息安全技术的控制以及信息安全的验证和确认。
运营/维护组	生产发布后的信息安全标准：应急响应、现场操作、工厂操作、维护/服务、报废、管理控制、售后服务和改造。
过程审查小组	组织层面的信息安全管理，以及信息安全文化；项目层面的信息安全管理，人员的角色和职责，信息安全的工作计划，审查，分布式开发过程中的信息安全开发接口协议；基于 V 模型的信息安全生命周期中各流程之间的互动，如何定制安全生命周期的工作内容；信息安全设计，开发和生产中的配套流程，如变更管理，分配管理，文件管理和工具管理等。

5.2.3.3 欧洲和美国

为了促进对车辆网络空间安全的保护，减少人们对车辆信息安全和个人数据及隐私保护的恐慌，美国国家公路交通安全管理局（NHTSA）于 2016 年 10 月发布了《现代车辆信息安全最佳实践》版本。该文件全面阐述了通用网络的适用范围、背景、定义和安全导向指导、汽车行业网络安全指导、网络安全教育、后装设备和可维护性等内容，部分弥补了美国现行汽车标准中关于信息安全内容的不足。此外，美国各大汽车集团在 2015 年率先成立了旨在共享汽车信息安全漏洞信息的汽车信息安全协会（AUTO-ISAC），成为促进美国汽车生产企业信息安全保护成效的重要合作平台。

欧盟早在 2008 年就开始了第七个框架计划中有关车辆信息安全的研究项目，资助 EVITA（E-security Vehicle Intrusion proTected Applications）项目，开发车载网络结构和硬件安全模块部署策略，以确保车辆的信息安全。欧洲网络信息安全局（ENISA）以欧盟成员国为中心，为各国的信息安全保护提供建议和有效的解决方案。特别是其在 2016 年 12 月发布的《车辆智能信息安全的正确做法和建议及快速修复》，为寻找解决智能汽车信息安全的相关问题提供了参考。此外，英国、德国、荷兰等国家也更多地参与到汽车信息安全的研究中来，成为欧洲相关标准的法律法规制定工作的一部分。

5.3 量子技术相关标准现状

量子计算利用量子纠缠和叠加的物理性质，在数据的存储、特征的表征和计算的高效并行方面具备技术潜力，有望在大数据、人工智能、交通、物理、电信、化学制药等领域取得突破性应用，是目前量子信息技术（Quantum Information Technology，QIT）领域重点关注的发展方向之一。随着量子计算技术的不断进步，学术界与工业界的不断交融，新应用模式的不断探索，商业资本的不断投入，量子计算的标准化工作也在多个标准化发展组织（Standard Development Organization，SDO）逐步展开[15]。

5.3.1 国内标准

我国目前正在积极推动布局量子信息技术标准化方面相关工作。2018 年 8 月，量子计算与测量标准化技术委员会（TC578）成立，主要负责量子计算与测量领域国家标准制修订工作，由国家标准化管理委员会负责业务指导。此外，全国信息技术标准化技术委员会物联网分技术委员会（SAC/TC28/SC41）也成立了先进计算研究组，开展先进计算技术体系梳理和标准化需求研究。

2021 年 5 月，国内首批量子通信相关标准 YD/T 3834.1-2021《量子密钥分发(QKD)系统技术要求 第 1 部分:基于诱骗态 BB84 协议的 QKD 系统》、YD/T 3834.2-2023《量子密钥分发（QKD）系统技术要求 第 2 部分：基于高斯调制相干态协议的 QKD 系统》及 YD/T 3835.1-2021《量子密钥分发(QKD)系统测试方法 第 1 部分:基于诱骗态 BB84 协议的 QKD 系统》经国家工信部批准实施，是国内首批行业标准，以及国内首个量子随机数相关行业标准《基于 BB84 协议的量子密钥分发（QKD）用关键器件和模块第 3 部分：量子随机数发生器（QRNG）》，适用于量子随机数发生器。

国家密码管理局发布的密码行业标准《诱骗态 BB84 量子密钥分配产品技术规范》《诱骗态 BB84 量子密钥分配产品检测规范》于 2022 年 5 月 1 日开始实施。《量子随机数发生器测评规范》《量子密钥分发设备密钥输出接口规范》等行业标准正处于研究和起草过程中。随着相关标准的制定和实施，量子保密通信的前置测评审批等工作将进一步有标准可循，并推动相关技术和产品在有资质要求的高端市场大规模应用。

5.3.2 国际标准

目前，量子计算国际标准研究初步启动，ITU-T、IEEE、IETF、ISO/IEC 等多个 SDO 及 EU Qflagship、NIST 等研究组织正积极开展量子计算标准化布局以及标准化研究的前期工作。国际标准化格局如图所示。

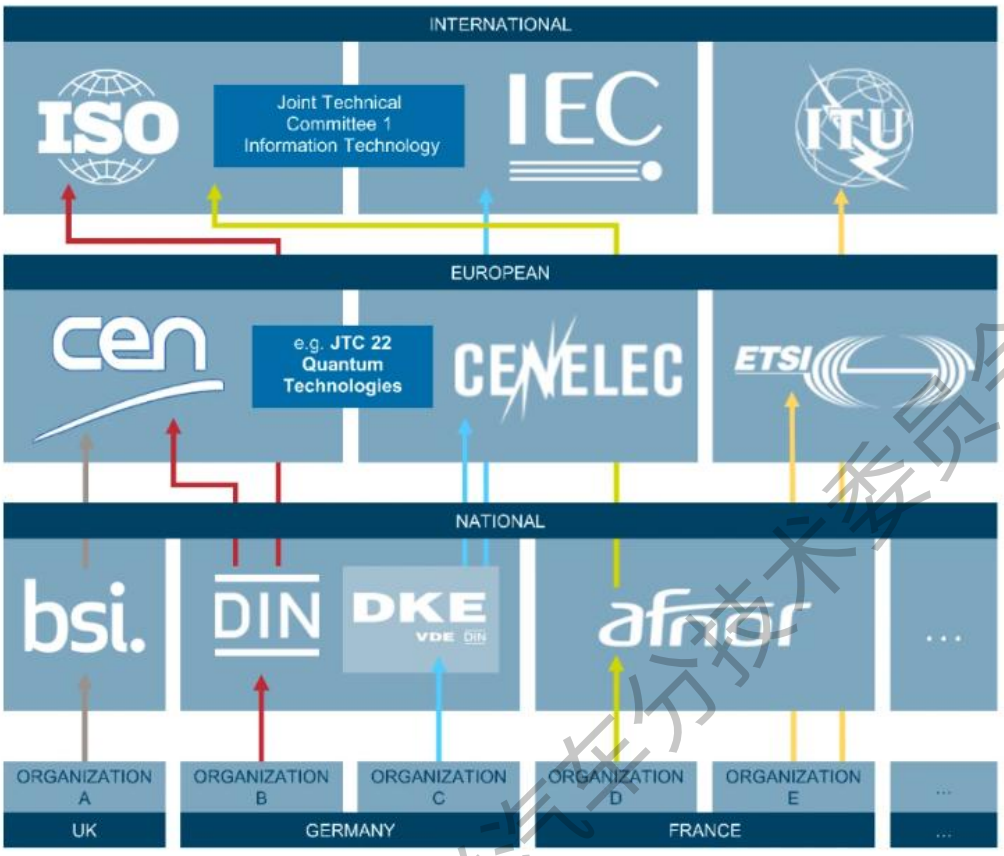


图 45 量子计算国际标准

1.ITU-T

目前，ITU-T 中主要由 FG-QIT4N 量子信息及网络技术焦点组[16]进行量子计算方面的预标准化工作。2019 年 9 月 27 日，在瑞士日内瓦会议上，ITU-T 决定设立 FG-QIT4N 焦点组，计划由来自中国方面的专家担任主席，来自美国、俄罗斯的专家担任联合主席，对量子增强型网络技术、量子信息技术驱动的新型服务及应用开展标准化预研工作。目前，量子计算作为 QIT 的重要技术领域，焦点组的 WG1 工作组对其开展了预标准化研究和套路讨论。

量子计算、量子云计算、分布式量子计算、盲量子计算、量子信息网络、量子互联网等作为 FG-QIT4N 焦点组重要的技术内容，目前正在 WG1 的各工作子组间进行预标准化工作推进。涉及到量子云计算、量子信息网络、量子互联网等标准议题，计划与 ITU-T SG13[17]、IETF[18]等 SDO 开展联络，为推动量子计算相关标准立项，提供相关技术背景信息和标准化工作建议。

2.IEEE

目前，IEEE 主要有如下两个工作项目在进行量子计算的标准化研究，仍处于起步

阶段，旨在澄清概念，定义术语，识别标准化需求并提供性能指标和基准。

（1）IEEE P7130：量子计算技术术语及定义

为了使量子信息技术达成技术共识，该标准定义了量子技术相关的专有名词与特定术语，以在量子计算方面实现兼容性和互操作性，目前该标准通过立项建议（Approved PAR），处于研究周期中。

（2）IEEE P7131：量子计算性能度量指标和基准测试

该标准涵盖量子计算性能度量，用于标准化量子计算硬件和软件的性能基准。这些度量标准和性能测试包括：对量子计算机进行基准测试（独立测试和对比测试），以及对量子计算机与经典计算机进行基准测试所需的一切测试，所用方法考虑了专用解算器等因素。目前，该标准通过立项建议（Approved PAR），处于研究周期中。

3.IETF

IETF 标准组织的互联网技术研究工作任务组 IRTF，设立了量子互联网研究组（Quantum Internet Research Group，QIRG）。该研究组致力研究量子信息网络的架构、使能技术、路由协议、关键器件等方面内容，并依托新一代量子互联网络开展量子计算、量子传感和量子通信等服务应用的标准化工作，其中与量子计算相关的量子信息处理、量子信息互联及组网协议也可能在 QIRG 组开展讨论，目前该研究组的相关标准草案还在讨论之中。

4.ISO/IEC

2018 年，国际电工委员会第一联合技术委员会（ISO/IEC JTC 1）在量子计算方面成立了两个研究工作组，分别是 SG2 和 SC7/SG 1。2019 年，ISO/IEC JTC 1 重新组建了量子计算的咨询工作组（AG），继续开展量子计算在信息技术领域标准化研究和需求分析工作，目前该组已经完成了研究梳理工作并向 JTC 1 提交了研究报告，同时建议 JTC 1 正式成立相应的技术组织，专门开展信息通信技术对量子计算的标准化需求研究，梳理应用场景和案例，开展术语标准的研制。2020 年 4 月，由我国牵头提出的《信息技术 量子计算术语和词汇》国际标准提案在 ISO/ IEC JTC 1 成功立项，对量子计算领域中的常用术语和词汇进行标准化制定，并于 2020 年 6 月下旬召开远程会议进行讨论。中国主导的 ISO/IEC 23837-1《量子密钥分发的安全要求、测试和评估方法 第 1 部分：要求》、ISO/IEC 23837-2《量子密钥分发的安全要求、测试和评估方法 第 2 部分：测试和评估方法》国际标准提案进入国际标准发布阶段，这是首个系统性地规范量子密钥分发(QKD)安全检测技术的国际标准。

5.EU Quantum Flagship

2018 年 10 月，欧盟委员会推出了 10 亿欧元的“量子技术旗舰项目”，为期 10 年。欧盟量子旗舰（EU Quantum Flagship）组织是欧盟委员会成立的面向量子信息技术的研究组织，采用量子信息创新项目征集方式，号召欧盟工业界和学术界开展对量子信息技术的长期研究及发展演进工作。目前，欧盟量子旗舰组织已设立了 20 个量子信息领域的科研项目，这些项目将来有望为量子信息技术的标准化提供基础研究成果和技术支持。

2020 年 6 月，欧盟量子旗舰组织、欧洲标准化委员会和欧洲电工标准化委员会（CEN-CENELEC）成立量子技术标准组，开展量子技术相关的预标准化工作，目标是加强量子技术领域的所有欧洲利益相关方之间的互动交流，沟通正在进行的活动，确定共同的需求和合作机会，并建议采取进一步行动举措，推进量子技术的标准化，支持量子技术的工业部署。

6.NIST

考虑到量子计算的算力提升对现代密码学的挑战，例如 Shor 算法理论上对现有 RSA 加密体系造成巨大的威胁，Grover 算法可降低密钥的强度等，美国国家标准技术研究所（National Institute of Standards and Technology，NIST）已经启动了量子信息对抗情况下的量子公钥密码算法的技术征集和评估标准化项目，该项目的实现目标为在经典计算体系与未来量子计算体系中，采用抗量子密码学（Post Quantum Cryptography）技术升级现有公钥密码体系，在量子计算时代提供网络信息安全保障解决方案。

7.CEN 和 CENELEC 联合发布世界上首个量子技术综合标准化路线图

2023 年 3 月 22 日，欧洲标准化委员会(CEN)和欧洲电工标准化委员会(CENELEC)联合发布了由德国国家标准化组织（DIN）牵头研发的“量子技术综合标准化路线图”。这是迄今世界上第一个量子技术综合标准化路线图，提供了一个全面的视野，对欧洲的量子计算、量子通信与安全、量子精密测量进行了标准化布局——量子领域标准化工作的里程碑。

量子技术已不再是未来的梦想。以量子计算机为代表的新一代量子技术正在迅猛发展。正如我们常见的智能手机，也是使用量子物理的研究结果使半导体的应用成为可能。量子技术将继续对各行各业、商业和研究的应用产生巨大影响。然而，由于缺乏各种技术标准来支持量子技术在欧洲的开发和部署，在一定程度上影响了量子技术的广泛应用。因此，量子技术综合标准化路线图的出台对量子技术的普及和应用具有重要意义。CEN 和 CENELEC 发布的量子技术的标准化路线图是一份指南，为量子技术的所有领域提供

了标准化需求和建议，包括：量子通信与密码学、量子计算与仿真、量子传感器和计量学、量子系统的基本技术。多领域所含丰富的内容使该路线图成为世界上第一份全面解决量子技术标准化问题的文件，而不仅仅局限于量子计算机等单个应用。

作为未来知情决策（如投资）的基础，该路线图旨在促进欧洲新产业的建立以及新设备和基础设施的发展。此外，CEN 和 CENELEC 还发布了一份包含量子技术用例的文件，解释了特定应用场景的标准化要求。由此可以推断出何时何地需要哪些规范和标准。

这些文件由 200 多名量子技术领域的专家组成的量子技术工作组（FGQT）制定。该工作组是在德国标准化组织（DIN）、荷兰应用科学研究组织（TNO）和欧盟委员会的共同倡议下成立的。DIN 是 FGQT 作为国家标准化组织的成员，并在推动路线图方面取得了重大进展。联邦物理技术学院量子技术能力中心 QTZ 负责人、FGQT 副主席和新成立的 CEN/CENELEC JTC 22“量子技术”副主席 Nicolas Spethmann 博士表示：“量子技术的标准化支持量子技术组件的可比性，从而产生信任和可靠性。在仍然年轻的量子技术中，这有助于欧洲经济在量子技术的产业发展中发挥主导作用。”

对于路线图，FGQT 专家已经确定了标准化的需求和可能性，以及引入新标准的具体步骤。在文件中，他们还提出了进一步行动的顺序。毕竟，各种技术的成熟度各不相同。虽然量子计算机等一些设备最近才上市，但量子磁力计等其他设备已经是成熟的产品。标准化路线图在推荐次序中将这些不同的成熟度考虑在内。

路线图推出后将着力推动实施。下一步，将在文件的基础上具体制定标准。为此，CEN 和 CENELEC 于 2023 年 3 月成立了量子技术联合技术委员会 JTC 22 QT(Joint Technical Committee 22 on Quantum Technologies)，这是世界上第一个全面研究量子技术的标准化委员会。它以制定的路线图为基础，全面推进量子计算领域的各类相关标准制定工作。

在研究层面上，量子技术的标准在提高通信的效率性和结果比对的效果方面具有非常重要的意义。标准使协作更加灵活，因为硬件和软件等组件可以相互交换和组合。另一方面，产业需要标准化才能将量子技术推向欧洲和世界各地的市场，而目前的量子技术组件和设备的通用术语、比较测量和性能测试只是其中的一部分。

参考文献

[1]刘志昊.量子安全通信研究——基于纠缠交换的量子密钥分发和量子直接通信[A].2009：全文.

[2]李宏伟，陈巍，黄靖正等.量子密码安全性研究.中国科学：物理学力学天文学，2012，42（11）：1237~1255.

[3]吴华，王向斌，潘建伟.量子通信现状与展望.中国科学：信息科学，2014，44（3）：296~311.

[4]中国通信标准化协会.量子保密通信技术白皮书.2018.12:全文.

[5]中国信息协会量子信息分会.量子安全技术白皮书.2022.1:全文.

[6]中国信息通信研究院.量子信息技术发展与应用研究报告.2022:12~59.

[7]石琴，鲁康源，程腾.基于量子密钥的车-云加密通信架构研究.[J]:汽车工程,2023,45(6):936-943..

[8]石琴，潘廷亮，程腾.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:全文

[9]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：全文.

[10]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：全文.

[11]Cui, X. Zhang, H. Zhong, J. Zhang, and L. Liu, “Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment,” IEEE Trans. Inf. Forensics Security, vol. 15, pp. 1654–1667, 2019:full text.

[12]J. Zhang, H. Zhong, J. Cui, Y. Xu, and L. Liu, “Smaka: Secure many-tomany authentication and key agreement scheme for vehicular networks,” IEEE Trans. Inf. Forensics Security, vol. 16, pp. 1810–1824, 2020：full text.

[13]Shawky M A, Jabbar A, Usman M, et al. Efficient blockchain-based group key distribution for secure authentication in VANETs[J]. IEEE Networking Letters, 2023, 5(1): 64~68.

[14]Kamil I A, Ogundoyin S O. A lightweight certificateless authentication scheme and group key agreement with dynamic updating mechanism for LTE-V-based internet of vehicles

in smart cities[J]. Journal of Information Security and Applications, 2021, 63: 102~994.

[15]QIT4N-I-117. Introduction of QIT4N and relevant standardization activities[C], 2020：full text.

[16]ITU. ITU-T Focus Group on Quantum Information Technology for Networks(FG-QIT4N)[EB/OL].2020：full text.

[17]ITU. ITU-T SG13: Future networks including cloud computing, mobile and next-generation networks[EB/OL]. 2020：full text.

[18]IETF. Internet engineering task force[EB/OL].2020:full text.