量子通信技术应用研究联合实验室
Quantum Communication Technology and Application Research Laboratory of Xiong'an

中国联通
China unicom

量子安全通信技术应用白皮书(2022)

量子通信技术应用研究联合实验室
中国联合网络通信有限公司智能城市研究院

2022年12月

前　言

二十世纪初，人们开始以量子为对象，研究物质世界微观粒子的运动规律，并逐步建立起量子力学理论体系。到了二十世纪中叶，随着量子科技的发展，现代光学、电子学和凝聚态物理等技术不断取得重大突破，推动了激光器、半导体、计算机等经典器件的问世，引发了第一次量子革命。进入二十一世纪后，随着量子调控技术的进步和发展，人们可以对微观体系的量子态进行精确的观测与调控，以量子计算、量子通信、量子测量等技术为代表的第二次量子革命正在到来。

近年来，我国大力实施创新驱动发展战略，在多领域取得重大进展。量子通信技术在实用化和工程化方面得到较快发展，网络建设规模和各类应用示范均处于全球领先水平。数字经济时代，网络安全、数据安全等问题变得日益严峻，这些问题关乎个人利益、企业生存和国家安全。研究表明，量子通信技术是唯一被严格证明的、符合香农无条件安全特性的通信方式，在党政军、能源、金融、交通等领域具有广泛的应用前景和商业价值。

中国联通与雄安新区智能城市创新联合会、中国雄安集团数字城市科技有限公司成立量子通信技术应用研究联合实验室(应用示范中心)，坚持以全球化视角为引领，结合智能城市建设，积极开展产业合作、技术创新，推动科研成果转化，全方位助力国家量子战略落地。

本白皮书以技术研究及应用示范成果为基础，分析了量子安全通信发展机遇，研究了量子安全通信关键技术和产业标准规范，并从典

型行业应用角度，给出了基于端到端量子加密网络内生安全的解决方案，助力打造重点行业量子安全通信应用标杆，促进量子通信技术的发展，支撑数字经济安全、快速发展。

本白皮书在编制过程中，得到了雄安新区智能城市创新联合会、中国雄安集团数字城市科技有限公司、国网雄安新区供电公司、浙江九州量子信息技术股份有限公司、江苏亨通问天量子信息研究院有限公司、上海循态量子科技有限公司、国科量子通信网络有限公司、鼎桥通信技术有限公司等单位的帮助与指导，在此，向以上单位表示诚挚的谢意。

目 录

一、 量子安全通信发展机遇

1.1技术发展概述

在量子通信技术发展方面，19 世纪末到 20 世纪上半叶，伟大的科学家们积极探索，对量子概念的提出和发展做出了巨大贡献。1900 年，普朗克提出黑体辐射量子假说，首次引入能量子的概念；1905 年，爱因斯坦提出光量子假说，运用能量子概念使量子理论得到进一步发展；1913 年，玻尔提出的原子理论为量子理论体系奠定了基础；1923 年，法国物理学家德布罗意提出微观粒子具有波粒二象性的假说；1926 年，薛定谔率先找到了描述粒子运动状态的波函数方程，也就是著名的薛定谔方程；1927 年，海森伯得出的测不准关系，以及玻尔提出的并协原理，对量子力学给出了进一步的阐释；1925 年到 1928 年，物理学界形成了完整的量子力学理论，与爱因斯坦的相对论并肩形成现代物理学的两大理论支柱。量子力学理论的形成是物理学发展中的一场革命，它揭示了微观世界的特殊运动规律，有力地冲击了经典物理理论，使人的认识开始从宏观世界深入到微观世界。1984 年，两名贝尔实验室研究人员提出了国际上第一个量子密钥分发协议 BB84 协议，正是这个协议的诞生，保密通信进入了量子时代。

在密码安全技术发展方面，1917 年，G.Vernam 提出一次性密码（One Time Password，OTP）的思想，即对于明文采用一串与其等长的随机数密钥进行加密，接收方使用相同的随机数密钥进行解密，随机数密钥真正随机且只使用一次,OTP 加密技术已经被证明是安全的。

但在经典通信领域，其所需的密钥很难在不安全的信道上实现无条件安全分发，采用不安全的密钥来实施“一次一密”加密仍然是不安全的。后来，出现了公钥密码体制，接收方有一个公钥和一个私钥，接收方将公钥公开出去，发送方用公钥加密信息后发给接收方，接收方用私钥解密信息。公钥密码体制的优点是不需要经过安全的信道对外传递密钥，但它的安全性是基于难于求解的数学难题，例如大数分解问题，相关资料表明，量子计算机的并行计算能力可以攻破RSA/DSA/ECDSA等密码，现有公钥体系将面临巨大挑战。

量子保密通信是量子信息领域中率先进入实用化的技术方向。量子保密通信基于量子密钥分发（Quantum Key Distribution，QKD）技术，结合适当的密钥管理、安全的密码算法和协议而形成的安全通信解决方案。近年来，量子安全通信已逐步从理论走向实验，并向实用化发展。加拿大Rubenok小组从理论上解决了量子通信网络中的量子中继问题，证明了QKD是现实条件下保障通信保密的有效技术；T. Silva小组在两段8.5公里的光纤链路上，使用弱相干态和偏振编码对MDI-QKD协议进行原理性验证；Nicolas Gisin小组进行了一项关于MDI-QKD实验工作，其传输距离成功达到了307公里；潘建伟小组通过研发高效低噪声单光子探测器，详细展示了能够抵抗所有针对探测器攻击的MDI-QKD实验；罗开广小组则通过MDI-QKD实验演示了一种可以抵抗所有探测器侧信道攻击的偏振编码方案。

2018年以来，我国在量子通信技术领域不断突破新记录。清华大学的研究团队首次实现了25个量子接口之间的量子纠缠，打破了

先前加州理工学院研究组 4 个量子接口之间纠缠的纪录。中国科学技术大学的研究团队在国际上首次实现 18 个光量子比特的纠缠，刷新了所有物理体系中最大纠缠态制备的世界纪录。中国科学技术大学的研究人员还在量子通信研究中取得新进展，创造密集编码量子通信信道容量新纪录。

另外，基于量子力学原理生成真随机数，产生量子密钥，采取云服务方式通过经典网络分发到应用端，适用于有线网、移动网、物联网等各种经典网络环境，形式灵活多样、轻量优质，使得更多的用户享有高安全等级的服务。该两种方案都是基于量子科技的安全通信方案，即使面对量子计算的挑战也能得到安全保障。

1.2 国家政策支持

世界各主要国家和组织均相继建成了各自的实地量子保密通信网络。比如，美国的伯特利量子通信网络(Battelle Quantum Network)、日本东京量子通信网络(Tokyo Network)、欧洲 SECOQC 量子通信网络以及中国京沪量子通信干线工程等。

我国已多次举办研讨会、出台一系列相关政策并成立专业部门，促进我国量子技术发展。自 2006 年发布《国家中长期科学和技术发展规划纲要》开始，提出了重点研究量子通信、量子计算的载体、关联规律和调控原理。2013 年发布《国家重大科技基础设施建设中长期规划》，再次强调“为空间网络、光网络和量子网络研究提供必要的实验验证条件”。

2020 年 10 月 16 日，习近平总书记主持召开中央政治局集体学习，专题学习量子科技研究和应用前景，并就中国量子科技如何抢占国际制高点、构筑发展新形势提出了一系列具体部署和要求。

“十四五”规划提出，强化国家战略科技力量，加强基础研究、注重原始创新，优化学科布局和研发布局，推进学科交叉融合，完善共性基础技术供给体系。瞄准人工智能、量子信息等前沿领域，实施一批具有前瞻性、战略性的国家重大科技项目。量子通信作为量子信息分支受到国家重点扶持，中央和地方均出台了相关的政策，加快布局量子通信产业，相关政策的发布将进一步促进产业发展及应用落地。

表 1-1 主要政策

时间	政策名称	颁布部门	主要内容
2006 年 2 月	《国家中长期科学和技术发展规划纲要（2006-2020 年）》	国务院	重点研究量子通信的载体和调控原理及方法，量子计算，电荷－自旋－相位－轨道等关联规律以及新的量子调控方法，受限小量子体系的新量子效应，人工带隙材料的宏观量子效应，量子调控表征和测量的新原理和新技术基础等。
2006 年 5 月	《2006—2020 年国家信息化发展战略》	中共中央办公厅 国务院办公厅	综合信息基础设施基本普及，信息技术自主创新能力显著增强，信息产业结构全面优化，国家信息安全保障水平大幅提高，国民经济和社会信息化取得明显成效，新型工业化发展模式初步确立，国家信息化发展的制度环境和政策体系基本完善，国民信息技术应用能力显著提高，为迈向信息社会奠定坚实基础。
2011 年 7 月	《国家“十二五”科学和技术发展规划》	科技部	突破光子信息处理、量子通信、量子计算、太赫兹通信、新型计算系统体系等重点技术
2013 年 2 月	国家重大科技基础设施建设中长期规划（2012—2030 年）	国务院	为突破未来网络基础理论和支撑新一代互联网实验，建设未来网络试验设施，主要包括：原创性网络设备系统，资源监控管理系统，涵盖云计算服务、物联网应用、空间信息网络仿真、网络信息安全、高性能集成电路验证以及量子通信网络等开放

时间	政策名称	颁布部门	主要内容
			式网络试验系统。
2015 年 5 月	《中国制造 2025》	国务院	掌握新型计算、高速互联、先进存储、体系化安全保障等核心技术，全面突破第五代移动通信（5G）技术、核心路由交换技术、超高速大容量智能光传输技术、“未来网络”核心技术和体系架构，积极推动量子计算、神经网络等发展。研发高端服务器、大容量存储、新型路由交换、新型智能终端、新一代基站、网络安全等设备，推动核心信息通信设备体系化发展与规模化应用
2015 年 10 月	《国家民用空间基础设施中长期发展规划(2015-2025 年)》	国家发改委、财政部等	超前部署科研任务之（二）通信广播卫星科研任务：开展激光通信、量子通信、卫星信息安全抗干扰等先进技术研究与验证。
2016 年 6 月	《长江三角洲城市群发展规划》	国家发改委	加强智慧城市网络安全管理，积极建设“京沪干线”量子通信工程，推动量子通信技术在上海、合肥、芜湖等城市使用，促进量子通信技术在政府部门、军队和金融机构应用。
2016 年 11 月	《“十三五”国家战略性新兴产业发展规划》	国务院	加强关键技术和产品研发，布局太赫兹通信、可见光通信等技术研发，持续推动量子密钥技术应用
2016 年 12 月	《信息通信行业发展规划{2016-2020 年}》	国家工业和信息化部	发挥互联网企业创新主体地位和主导作用，以技术创新为突破，带动移动互联网、5G、云计算、大数据、物联网、虚拟现实、人工智能、3D 打印、量子通信等领域核心技术的研发和产业化。
2017 年 1 月	《战略性新兴产业重点产品和服务指导目录{2016 年版}》	国家发改委	包括信息安全咨询服务、信息系统安全集成、网络安全维护服务、信息安全风险评估、信息系统等级保护咨询、攻击防护服务、加密保密服务、网络安全应急服务、安全测试服务，以及电子认证、信息安全认证、信息安全培训、电子取证、安全审计、数据备份及灾难恢复服务等。安全态势感知、预警，安全风险评估，安全咨询等面向工业控制系统的信息安全服务。
2017 年 5 月	《“十三五”国家基础研究专项规划》	科技部、教育部、中科院、国家自然科学基金委员会	奠定我国在新一轮信息技术国际竞争中的科技基础和优势方向。量子通信研究面向多用户联网的量子通信关键技术和成套设备，率先突破量子保密通信技术，建设超远距离光纤量子通信网，开展星地量子通信系统研究，构建完整

时间	政策名称	颁布部门	主要内容
			的空地一体广域量子通信网络体系，与经典通信网络实现无缝链接；
2018 年 1 月	《国务院关于全面加强基础科学研究的若干意见》	国务院	优化国家科技计划基础研究支持体系，拓展实施国家重大科技项目，加快实施量子通信与量子计算机、脑科学与类脑研究等“科技创新 2030-重大项目”，推动对其他重大基础前沿和战略必争领域的前瞻部署。
2018 年 7 月	《金融和重要领域密码应用与创新发展工作规划｛2018 年-2022 年｝》	中共中央办公厅、国务院办公厅	大力推动密码科技创新，加强密码基础理论、关键技术和应用研究，促进密码与量子技术、云计算、大数据、物联网、人工智能、区块链等新兴技术融合创新。
2019 年 12 月	《长江三角洲区域一体化发展规划纲要》	中共中央、国务院	统筹规划长三角数据中心，推进区域信息枢纽港建设，实现数据中心和存算资源协同布局。加快量子通信产业发展，统筹布局和规划建设量子保密通信干线网，实现与国家广域量子保密通信骨干网络无缝对接，开展量子通信应用试点。加强长三角现代化测绘基准体系建设，实现卫星导航定位基准服务系统互联互通。
2020 年 3 月	《关于科技创新支撑复工复产和经济平稳运行的若干措施》	科技部	大力推动关键核心技术攻关，加大 5G、人工智能、量子通信、脑科学、工业互联网、重大传染病防治、重大新药、高端医疗器械、新能源、新材料等重大科技项目的实施和支持力度，突破关键核心技术，促进科技成果的转化应用和产业化，培育一批创新型企业和高科技产业，增强经济发展新动能。
2021 年 3 月	《“十四五”规划和 2035 年远景目标纲要》	全国人大	全社会研发经费投入年均增长 7%以上，力争投入强度高于“十三五”时期。瞄准人工智能、量子信息、集成电路、生命健康、脑科学、生物育种、空天科技、深地深海等前沿领域，实施一批具有前瞻性、战略性的国家重大科技项目。
2021 年 11 月	《“十四五”信息通信行业发展规划》	工信部	将加大 6G、量子通信等网络技术研发支持力度，前瞻布局 6G、量子通信等新技术安全，并推动人工智能、先进计算和量子计算等新兴技术应用。
2021 年 12 月	《“十四五”国家信息化规划》	中央网络安全和信息化委员会	要探索建立面向未来的量子信息设施和试验环境；加强人工智能、量子信息等关键前沿领域的战略研究布局和技术融通创新，加强 5G、量子技术等领域知识产权保护。

1.3应对安全挑战

1.3.1 数字化转型背景

1）政府数字化转型是全面推动政府整体智治的有效手段

数字政府建设是落实网络强国、数字中国、智慧社会战略的重要举措，是加快政府职能转变、塑造政府公共服务理念、完善政府治理的全方位、系统性、协同式的一场深刻变革。

政府数字化转型是要把整个政府运作模式进行创造性的数字化改造，注重业务流协同、数据流贯通、技术流集约，推动政府工作过程数字化和工作结果数字化，进而改变政府运作流程、治理方法甚至组织架构。

2）企业数字化转型是整体构建企业高质量发展的重要引擎

人类社会经历了农业社会、工业社会的发展阶段，目前正快速迈向数字社会。相对于以往，数字时代的到来引发了包括技术、经济、思维、生存等各方面的跨越式巨变。农业社会生产要素是土地资源，生产方式为人工劳作；工业社会生产要素是矿藏与石油，生产方式为机械；数字时代生产要素是数据，生产方式为人工智能。这种不同以往的生产环境变化，促使全球各国在调整自己的国家战略。作为数字经济发展的基础，企业数字化是适应数字经济发展的主动选择。

在科技赋能上，随着工业化、信息化、互联网领域科技的发展积累，已经呈现出深度融合，并催生深刻化学反应的趋势。云计算、大

数据、物联网、移动互联网等技术已逐渐成熟，并正以我们以往不可想象的手段，改变我们的生产生活方式，这启发我们以更大的想象力，来借助科技的力量，重新审视企业的发展。

3）政企数字化转型面临重大信息安全挑战

数字化是信息技术发展的产物，是指将我们物理世界的信息转化为计算机能够直接识别处理的“0”和“1”的过程。这个过程就像19世纪人类进入电气时代一样影响深远。数字化是一柄双刃剑，在政企利用信息技术推动数字化转型实现生产力飞跃的同时，信息资产的迅速膨胀，网络连通的更加广泛，伴随而来的是以全新面貌出现的安全问题。

1.3.2 敌手攻击风险

数字经济时代，线上线下融合，病毒、木马、高级持续性攻击等网络威胁和风险从虚拟网络空间向现实物理世界蔓延扩散，严重威胁经济社会安全乃至国家安全。

信息技术的革新导致“网络犯罪”更猛烈也更猖獗，因为其简便性，不受空间、时间等因素的限制。目前威胁的主要形式表现在越来越多的黑客实施“网络犯罪”时不再是单兵作战，而是形成了分工明确的产业链，他们拥有丰富的数据和情报，廉价的网络攻击资源，强大的网络攻击武器，收集信息、挖掘漏洞、实施攻击、盗取数据、出售变现等一系列流程清晰明了，令受攻击者遭受损失且难以追查。

1.3.3 量子霸权威胁

2019 年，IBM 公司在国际消费类电子产品展览会上展出了最新的量子计算机模型，把量子计算成果引入大众视线；同年，谷歌在《自然》杂志上发文，宣告“量子霸权（Quantum Supremacy）”。

这两件事对经典计算机和普通加密领域产生了巨大冲击，量子计算机拥有超大的存储能力和超强的运算能力，能以超过经典计算机指数级倍数的速度执行特定计算任务。这种量子优势将对我国各政企行业产生巨大威胁，传统信息安全手段和技术将被颠覆。

1.3.4 云上数据安全

随着计算机和网络技术的快速发展，云计算将数据资源、存储设备和软件应用成功融合到一起，为众多用户解决了大数据的存储与管理问题。但近年来，不断发生的云数据泄露事件引起了用户的重视。云计算中所有用户的数据都存放在云端，并将计算结果通过网络回传给客户端，用户之间共享计算或存储资源，安全隔离不够或某些用户恶意攻击，从而造成数据保密、数据备份、数据共享等方面面临巨大的安全问题。

1.4 应用前景广阔

信息安全上升到国家高度，量子安全以其不可分割、不可克隆、一次一密等特性，为信息安全保驾护航，有重要的战略价值。当前，无论在技术储备、基础设施、应用领域、国家政策上，量子安全通信

产业化发展箭在弦上。

随着“量子卫星”、“京沪干线”等重大项目的建设，我国量子通信技术已跻身全球领先地位，率先实现了量子传送、加密和分发，理论实力、技术基础和产业应用世界领先。量子保密通信技术凭借其信息论安全特性，在今后的一段时期内将被大范围推广及应用。同时，基于量子力学原理生成真随机数，由云平台存储、分发密钥，通过一次一密或高频率更新的密钥进行加解密，保障数据安全，为用户提供灵活便捷、覆盖广泛的量子真随机加密通信，具有广阔的市场空间和商业价值。

表 1-2 主要应用表

业务名称	产品组合	经典案例	备注
量子骨干网建设	量子密钥分发 QKD（接收、发送）、波分复用、安全中继、量子中继器、量子光交换机、量子安全加密路由器等	“京沪干线”、“武合干线”、“京雄干线”、“宁苏干线”等项目	量子保密通信骨干网具有链路距离长、承载容量大、可靠性与健壮性要求高的需求特点
量子城域网建设	量子密钥分发 QKD（接收、发送）、波分复用、安全中继、量子中继器、量子光交换机、量子安全加密路由器等	“广州量子城域网”、“合肥量子城域网”、“芜湖量子政务网”等项目	城域网负责城市范围内不同区域、不同行业机构的连接，上联骨干网，下联局域网/用户区域，具有链路长度中等、业务容量较大、可拓展性要求高、组网拓扑复杂的需求特征
量子局域网建设	密钥云平台、密钥管理 QKM、量子光交换机、量子安全加密路由器、量子安全 IPSec VPN、量子安全 SSL VPN、量子 Q 盾、密钥充注等	大型央企、集团公司、综合性企业、有竞争力/保密性企业等局域网建设	局域网上联城域网，下联一个小区域（如一个企业的办公楼群）内多个用户终端的接入，具有距离要求不高、下联分支数量大、业务接入多元化等需求特征
数字政务量子保密通信应用融合	密钥云平台、密钥管理 QKM、量子光交换机、量子安全加密路由器、量子安全 IPSec VPN、量子安全 SSL VPN、量子 Q 盾、	省、市、区及各委办局数字政务量子保密通信应用融合项目	用于保护政企专网基础设施及其服务的安全性，企业或政府机构通常要求通信服务提供高度的机密性、完整性和真实性，需要强制性地采用专用的安全系统，结

业务名称	产品组合	经典案例	备注
	密钥充注等		合 QKD 的链路加密，可以与这些技术结合来满足政务网各站点之间信息加密需求。
数字金融量子保密通信应用融合	量子密钥分发 QKD（接收、发送）、波分复用、安全中继、量子中继器、量子光交换机、量子安全加密路由器等	“京沪干线”金融应用示范接入、苏州量子保密金融专线	解决量子密钥资源到移动终端“最后一公里”的配送及使用需求，保障移动终端和业务中心之间能够开展量子通信业务
关键基础设施量子加密融合应用	量子密钥分发 QKD（发送、接收）、量子 CPE 加密组件、量子安全加密路由器、量子光交换机等	国家电网下属灾备中心以及山东、安徽、浙江等省电力公司	可用于保护关键基础设施中的数据采集与监控系统（Supervisory control and data acquisition，SCADA）数据通信安全性
云和数据中心异地灾备量子加密融合应用	量子密钥分发 QKD（发送、接收）、量子光交换机、量子安全加密路由器、波分复用、量子集控站等	政务、金融、保险、证券、电商等行业客户关键数据异地灾备量子加密传输	针对云和数据中心对海量数据存储安全、异地备份传输安全以及用户核心数据上云安全进行量子加密融合应用
国家、省级、教育领域量子实验室建设	密钥分配系统、红外单光子探测仪、高速激光器等量子信息教育与科研仪器	国家、省级、大学、重点实验室项目	

二、 关键技术研究进展

2.1量子密钥分发 QKD

基于量子密钥分发的量子通信技术是现阶段发展相对成熟并具备产业化潜力的典型技术，能够与现有的光通信、大数据、云计算等新型技术进行融合互补，打造服务多种行业，开放灵活、智能互联的量子生态体系。

和现有的密码技术不同，量子密钥分发技术基于量子力学原理，

使用量子态来编码信息，通过对量子态的制备、传输和检测实现安全分发量子随机数，其核心思想是利用非正交单量子态的不可克隆性来完成安全分发。所以量子密钥分发协议，指的是量子态编码、传输和测量方法的规定。1984 年，物理学家 Bennett 和密码学家 Brassard 提出了世界上第一个具有里程碑意义的 QKD 协议，也就是著名的 BB84 协议。此后，物理学家和密码学家又相继提出了其他量子密钥分发协议，如 E91、B92、BBM92、SARG04、COW、DPS、GG02、测量设备无关量子密钥分发（MDI-QKD）等协议，而各种量子密钥分发协议又可以按照编码量子态的特点分为离散变量（DV）、连续变量（CV）等类别。

2.1.1 离散变量量子密钥分发

DV-QKD 作为最早出现的密钥分发技术，无论是在理论还是在实践领域都取得了一定的成果和进展，主要的量子密钥分发协议有 BB84 协议、E91 协议和 B92 协议等。到目前为止，BB84 协议应用最广泛，该协议通过将信息调制到光子的偏振态上，并随机从四种偏振态中选择一种发送，实现无条件安全的密钥分发。另外，还存在其他一些改进协议，如六态协议、正交态协议等。

2.1.2 连续变量量子密钥分发

2002 年，物理学家 Grosshans 和物理学家 Grangie 提出了一个全新的基于相干态的 CV-QKD 方案，即 GG02 协议，该协议使用弱相干态进行高斯调制实现量子密钥分发，使得之后可以完全使用标准化光

通信器件实现量子密钥分发。随着 GGO2 协议的提出，各种改进性的协议不断出现，如 no-switching 协议、四态调制协议、相干态双相位调制协议等。

2.2高速量子随机数发生器

量子随机数发生器是利用量子随机过程产生真随机数的一种装置，其随机性由量子力学的基本原理保证，传统的量子随机数发生器是根据光子经过分束器后的路径选择来生成随机数，其生成速率较低，无法满足行业应用的多元化需求。为了提高生成速率，后续相继出现多种改进型的高速量子随机数发生器。

此外，量子随机数发生器具备机架式、USB 型、板卡型等多种形态。在具体场景中，采用量子随机数发生器产生的真随机量子密钥结合对称加密模式进行加密，首先利用量子的物理特性解决了对称加密模式中密钥的安全传输问题，保证了密钥不可被克隆、窃听、篡改，其次保留了对称加密方式的高效性特点。从而推动了高速量子随机数发生器及量子密钥云产品的研发和应用落地。

2.3量子密钥云平台

量子密钥云平台是融合 ICT 基础设施和量子随机数发生器、QKD 量子密钥分发技术，形成了基于量子安全的云底座。其基于量子安全云计算技术把各业务分散部署的计算、存储、网络等物理资源融合在一起，结合量子安全能力，实现统一的资源池化，统一为上层业务按需提供服务，提升整体资源利用率，为各类业务应用的数据安全保驾

护航。

量子密钥云平台可实现从基础软硬件到应用软件的整个产业链的自主可控，将量子安全能力赋能数字经济基础设施以及助力产业数字化转型。

2.4量子可信中继增强技术

由于光纤传输的信号损耗，量子密钥分发 QKD 产品通过光纤直接传输有一定的距离上限，而量子可信中继增强技术是量子保密通信的关键技术，可拓展量子通信应用范围。相邻的中继节点间进行量子密钥分发，从而通过各对相邻中继节点达成量子密钥加密传输。其中通过“一次一密”的加密传输方式，实现节点可信中继，保障量子密钥传输的安全。

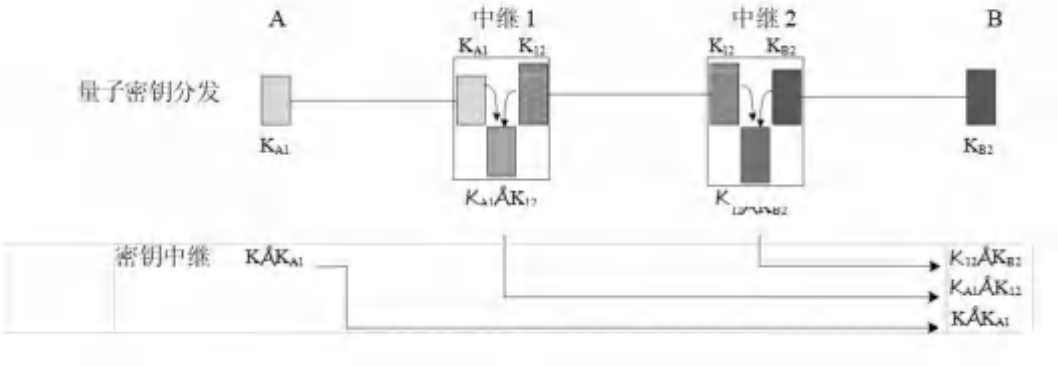

图 2-1 量子可信中继增强原理图

量子可信中继安全的方案根据具体需求制定。对于安全等级较高的场景，可以把可信中继节点设在对应机房里，结合人员管理和技术手段来保障中继可信。对于通用场景应用，可以采用安全技术手段保障无人值守中继节点的安全可信，如密钥落地即密技术、密钥分拆中

继技术，中继密钥迭代变换技术等，从而避免中继节点造成的密钥泄露风险。综上所述，对于各类应用场景，量子可信中继增强技术都可以高效可靠的保障量子密钥安全。

2.5量子加密路由组网技术

量子加密路由组网技术是支撑量子通信网络灵活组网的关键。量子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。

量子加密路由组网是量子通信与经典通信的融合组网，实现了路由交换与安全应用的无缝融合。该技术支持在线获取量子密钥，支持完备的路由和 MPLS 业务特性，满足灵活组网和端到端服务保证的要求，满足量子广域网互联、VPN 网关、融合网关等多种应用场景的组网需求。对于大规模的量子通信网络，一般通过分域和分层管理来减低路由表维护的难度，提高路由收敛速度，从而实现灵活组网，提高网络的兼容性和可扩展性。

2.6共纤传输技术

在量子密钥分发 QKD 的场景应用中，需要一根单独的光纤传输量子信号，另一根独立的光纤传输同步信号，而目前的裸光缆资源相对紧张，在量子保密通信建设的现网没有多余裸光缆时，就需要新增光缆，将导致建设成本高、工程实施困难等难点。为此，探索量子信号

与经典信号在现有的光纤中共同传输就显得比较关键。量子密钥分发信道和经典光通信共纤传输技术就是将经典信号与量子信号融合在一根光纤中进行传输，实现量子信道和经典信道的融合传输。

共纤传输最典型的方法是运用波分复用技术，将量子密钥分发与经典光通信共纤传输。对于原始噪声、四波混频、拉曼散射等的共纤传输干扰，可以采用多种方法抑制干扰，如增大合波器和分波器的隔离度、增大与经典信道的波长间隔、降低经典光的入纤光功率、降低合波器和分波器的插入损耗等。量子密钥分发信道和经典光通信共纤传输技术的应用，便于量子密钥分发与经典通信网络更好地融合，满足量子城域网建设、业务专线接入等需求，为行业场景提供融合的量子安全服务，更好的赋能各行各业。

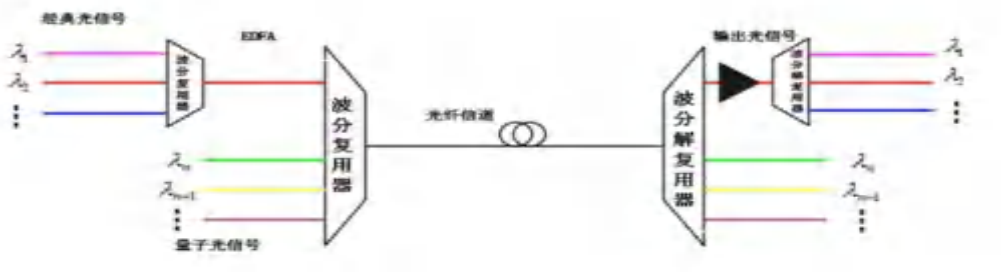

图 2-2 量子密钥分发信道和经典光通信共纤传输原理图

三、 产业化标准化进展

3.1 产业化路线

（1）技术逐渐走向成熟

近年来，我国在量子通信领域成绩斐然，取得了多项世界领先研究成果，并且已经将科研成果逐渐转化到实用状态。

在长距离量子通信方面，“墨子号”实现了洲际量子密钥分发和量子隐形传态，并利用共享密钥实现加密数据传输和视频通信，为构建全球化量子通信网络奠定了坚实基础。

在新型量子比特编码方面，首次在砷化镓半导体量子芯片中成功实现量子相干特性好、操控速度快、可控性强的电控新型编码量子比特。

在关键器件制造方面，成功实现了世界上最快的 68Gbps 的量子随机数发生器，为未来超高速量子密码系统的量子随机数需求提供了可行的解决方案；1.25GHz InGaAs/InP 单光子探测器单片集成读出电路技术的实现，可使高速量子通信终端设备中体积占比最大的探测器模块尺寸减小一个数量级以上，为研制小型化量子通信系统奠定了重要的器件基础。

（2）产业链逐步形成

随着量子通信应用的陆续开展，越来越多企业看到量子通信广阔的市场前景，纷纷涉足该领域。多种形式的合作也陆续展开，共建实验室、产业联盟，加强产学研用合作。

我国已经初步形成了涵盖终端和元器件供应商、量子设备与解决方案提供商、网络建设与系统集成商、网络运营与业务提供商的量子通信产业链条。上游主要包括芯片、光量子探测仪等器件。中游主要包括量子密钥收发器、量子随机数发生器收发端等核心设备以及量子堡垒机、量子交换机、量子路由器、量子集控站、量子网关等网络设备。下游主要包括各类量子通信应用产品和专用网络。

3.2标准化路线

量子保密通信从实用化走向产业化规模应用之路仍然面临不少挑战。标准化是其中十分重要的一环，对于未来产业健康发展具有奠基石的意义和作用。目前已有不少国内外标准化组织开展相关标准工作，国际上有国际标准化组织（ISO）、国际电信联盟（ITU）、欧洲电信标准化协会（ETSI）、电气电子工程师学会（IEEE）、云安全联盟（CSA）等，国内有中国通信标准化协会（CCSA）、中国密码行业标准化技术委员会（CSTC）、中国信息安全标准化技术委员会等。量子通信作为跨学科、跨领域的系统工程，标准化工作仍处于发展初期，需要多领域、不同标准组织之间合作推进，以尽快形成支撑大规模组网、运营、应用、认证的完整标准体系。

3.2.1 国际标准组织积极开展标准化工作

目前量子通信正在形成国际标准，相关标准组织正在加速开展相关标准化工作，一些主要成果如下:

（1）ISO/IEC 标准化进展

2022 年 10 月，由我国主导的《量子密钥分发的安全要求、测试和评估方法》国际标准提案进入发布阶段，预计在 2023 年正式发布，这是首个系统性地规范 QKD 安全检测技术的国际标准。该国际标准为 QKD 模块定义了一套严格和通用的安全规范，分为 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》。该标准将为 QKD 产品的设计和安全测评提供国际权威标准的指导，助力量子通信领域产业化结构的优化升级，对于完善商用密码体系具有积极作用。

（2）ITU 标准化进展

国际电信联盟（ITU）的工作主要集中在量子通信领域，QKD 网络和后期安全方面的工作由 ITU-T 未来网络研究组（ITU SG13）和 ITU-T 网络安全研究组（ITU SG17）领导。核心内容是 QKD 网络标准大纲，包括提供基本概念（ITU-T Y.3800）、解决功能要求（ITU-T Y.3801）、架构（ITU-T Y.3802）、密钥管理（ITU-T Y.3803）以及控制和管理（ITU-T Y.3804）。ITU 还为 QKD 网络(ITU-T X.1710)、密钥组合方法(ITU-T X.1714)和量子噪声随机数发生器的架构(ITU-T X.1702)提供了安全框架。

此外，我国还推动在 ITU-T 成立面向网络的量子信息技术研究焦点组（FG-QIT4N），全面开展量子信息技术标准化研究工作。这是 ITU 大力推动量子密钥分发国际标准化工作以来的进一步举措，是国际标准化组织中第一个量子信息技术焦点组。焦点组将组织和协调 ITU-T 内量子通信、计算等技术的标准化研究工作，并协调其他标准化组织，旨在构建全球量子信息标准化开放工作平台。

（3）欧洲电信标准化协会（ETSI）进展

ETSI 早在 2008 年 9 月即成立了 QKD 工作组，针对量子通信系统的技术规范、测试方法、安全认证和网络应用等方面开展标准化，发布了 QKD 应用场景、QKD 组件和内部接口、QKD 应用服务接口、QKD

系统光学模块的特性、QKD 安全证明、QKD 模块安全等规范。

3.2.2 我国加速标准体系建设

（1）量子通信与信息技术特设任务组（CCSA-ST7）

为推动量子通信关键技术研发、应用推广和产业化，CCSA 于 2017 年 6 月成立了量子通信与信息技术特设任务组（The 7th Special Task Group, ST7），目标是建立我国自主知识产权的量子保密通信标准体系，支撑量子保密通信网络的建设及应用，推动 QKD 相关国际标准化进展。ST7 下设量子通信工作组（WG1）和量子信息处理工作组（WG2）两个子工作组，该组织已汇聚国内量子通信产业链的主要企业及科研院所，现有 51 家会员单位。

（2）量子密码标准制订工作组

国家密码管理局密码行业标准化技术委员会（密标委）在 2012 年设立了量子密码标准制订工作组。2021 年 10 月，密标委正式发布量子密码标准《诱骗态 BB84 量子密钥分配产品技术规范》和《诱骗态 BB84 量子密钥分配产品检测规范》，并于 2022 年 5 月开始实施。这两项标准作为我国密码行业量子技术的首批标准，对基于弱相干态光源的诱骗态 BB84 协议各阶段的技术实现进行了规范，并对采用该协议的 QKD 产品设计提出了基本要求和检测方法。

3.3与其他安全体系之间的关系

3.3.1 量子安全与OSI安全体系

OSI协议模型是为实现系统互连所建立的通信功能分层模型，是TCP/IP协议的基础,OSI安全体系是根据OSI七层协议模型来建立的，其针对网络通信的7个层次，在每个层次上都定义了相关的安全技术，可与量子通信技术深度融合。

1)在数据链路层，OSI协议定义了一种在链路层对多协议分组进行点到点传输的方法，但不提供对其所封装的数据进行完整性和机密性保护。针对此安全隐患，可运用基于量子加密技术的PPTP/L2TP隧道封装技术，对链路中的数据进行量子加密，并采用链路层隧道封装技术传输，实现信息数据的加密保护。

2)在网络层，传统的IPV4协议未考虑到安全问题，无法防范网络层的攻击，可以应用量子IPSec增强其安全性，实现报文的机密性、完整性、源地址认证以及抗伪地址、抗量子计算的攻击能力。量子IPSec能够保障在所有支持IP的传输介质加密通信，保障主机间运行于网络层上的所有协议安全加密传输。其可以应用于各类组网场景，如量子路由器组网、量子防火墙防护等。

3)在传输层，为了达成端到端的加密安全，可应用传输层安全协议(TLS）和安全套接字层(SSL)。量子SSL一般采用公开密钥技术，保证端到端通信的保密性和可靠性，使客户端侧与服务器侧之间的通信不被攻击者窃听，目前Web浏览器普遍将HTTP和SSL相结合为

HTTPS，从而实现安全通信。TLS 是确保网络上通信应用和其用户隐私的协议，使服务器端和客户端在数据交换之前进行相互认证，并协商加密算法和量子密钥。

4)在会话层，量子 SOCKS 代理是最灵活的网络代理标准协议，主要应用于客户端与外部服务器之间的通讯连接。当防火墙后的客户端要访问外部的服务器时，就跟量子 SOCKS 代理服务器连接，对客户端提供可信授权和身份认证。此外，使用 SOCKS 代理，应用层不需要做任何的改变，但是客户端需要专用的 SOCKS 化程序。

5)在应用层，量子应用程序代理工作在应用层之上，位于客户端与应用服务器之间，为应用程序提供网络代理服务。当客户端需要调用应用服务器上的数据时，首先将数据请求发给代理服务器，代理服务器再根据这一请求向应用服务器索取数据，然后再由代理服务器将数据传输给客户端。应用层代理服务器可支持多种类型的应用层协议，如：HTTP、HTTPS、FTP、TELNET 等，与量子加密技术的无缝融合，实现应用数据的安全。

3.3.2 量子安全与等级保护安全体系

信息安全等级保护是国家信息安全保障工作的基本制度、基本国策，是开展信息安全工作的基本方法，是促进信息化发展、维护国家信息安全的根本保障。量子通信技术可以纳入到等级保护管理策略中，更好的实现“明确等级、增强保护、常态监督”。量子安全与等级保护安全体系建设，可以围绕以下几个方面开展:

1)网络信任体系方面，建设基于量子加密技术的CA认证系统，为相关业务系统提供身份认证、密码服务以及安全可信的支撑服务，实现业务用户信息的统一管控，为网络接入、系统访问提供统一的身份认证和鉴权管理。

2)安全技术体系方面，量子安全设备可结合入侵检测、安全审计、SSL VPN等网络安全设备构建安全防护体系，实现数据全生命周期的管理。进一步搭配云平台和态势感知，对未知威胁与入侵攻击进行主动安全监测以及态势感知预判，实现统一的全面监测监管。

3)安全管理体系方面，根据具体安全管理现状，建立相关安全策略、安全管理制度、操作流程规范等安全管理规范，加强对安全管理人员的安全技能培训，定期开展安全事件应急处置演练，提高突发事件的应急处置能力。

4)风险管理体系方面，可针对内部的业务系统，委托专业测评机构进行等级测评和风险评估，定期对信息系统等级安全保护体系的合规性要求进行测试评估，发现信息系统面临的安全风险，积极采取风险应对措施，并对残留风险持续监控防控。

3.3.3 量子安全与工业互联网安全体系

量子安全与工业互联网安全体系，涉及设备、控制、网络、应用、数据五个层次的安全，也是量子通信与工业互联网深度融合的应用体系。设备安全是指工业智能设备的安全，融合量子加密技术实现无条件安全的接入防护；控制安全主要包括控制软件安全和控制协议安全

两方面，实现各种通用或专用程序的安全，以及控制过程的通信协议安全；网络安全涵盖全链路的网络安全，通过量子加密技术的赋能，达成工业内网与外网的组网安全，标识解析安全；应用安全是工业互联网各类场景的平台安全、本地应用安全、云化应用安全，量子通信技术可助力应用系统安全合规建设；数据安全覆盖数据全生命周期各环节的安全，量子安全技术可结合传统安全技术构建安全可信的安全管理体系。

四、 重点行业应用

4.1行业方案

4.1.1 党政军

（一） 行业应用场景

随着信息技术的快速发展和广泛应用，信息安全牵涉到国家安全和社会稳定，我国已将信息安全提升为国家安全战略。在信息化建设过程中，基础信息网络、信息系统、信息资源以及个人信息等安全方面的问题与日俱增，安全威胁日益严峻。

信息安全本身包括的范围很广，大到国家军事政治等机密安全，小到商业企业机密、个人信息安全。网络环境下的信息安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（数字签名、信息认证、数据加密等）直至安全系统，其中任何一个安全漏洞便可以威胁全局安全。

（二） 量子加密解决方案

依托于量子保密通信系统，主动获取或自动接收量子密钥分发 A 点或 B 点自动产生的高效、高可用的量子密钥，经过量子安全路由器传输至各应用系统或网络安全设备，为其提供加密所需的密钥源。

各类智能终端、应用系统、数据链路采用量子密钥进行整体加密，可安全、稳定运行在电子政务外网链路，为数字政府、数字化改革提供量子保密通信技术支撑，创新政府数字化改革思路，构建数字政府立体化网络安全空间，推动数字政府密码基础设施建设。

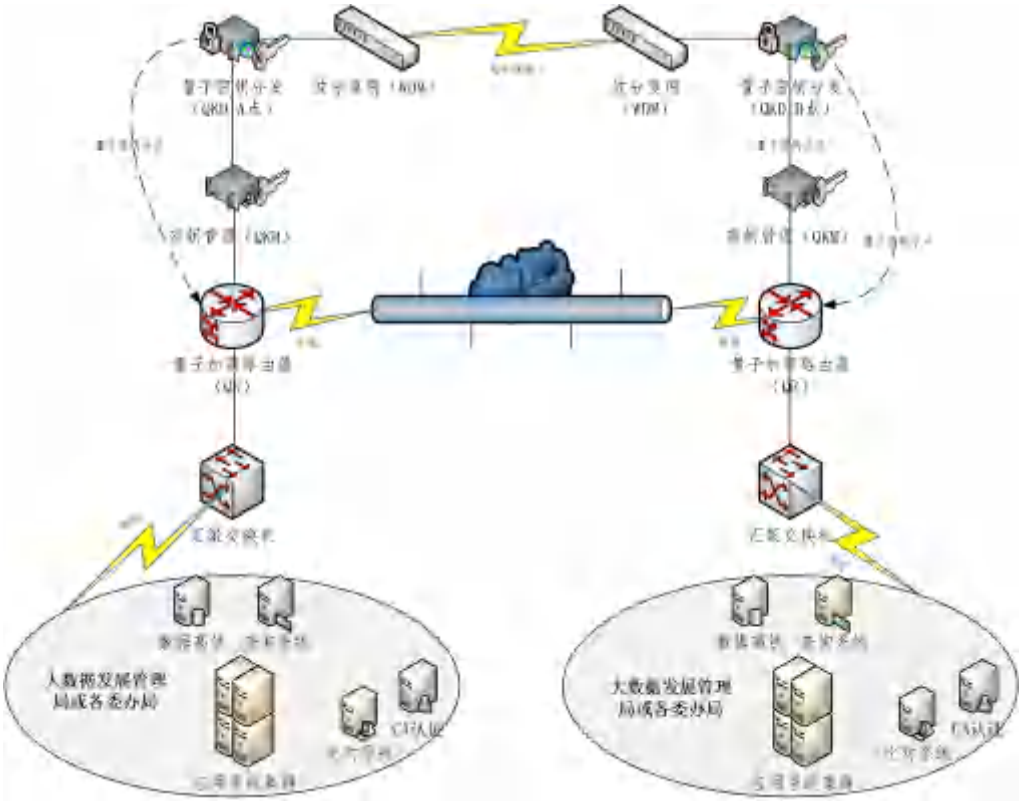

图 4-1 政务量子加密解决方案

4.1.2 能源

（一） 行业应用场景

随着泛在电力物联网发展，智慧能源信息系统中存有大量暴露在公共环境或使用公网通信的测控设备，这些设备存在被黑客入侵破解后群控的安全隐患。若采用传统加密方法，在庞大数据量的支撑下几乎无法满足信息安全需求，但是若以量子加密技术对数据进行保护，以目前技术发展来看，完全可以满足信息安全需求。

（二） 量子加密解决方案

以能源电力自动化系统为例，基于量子技术对配电自动化终端设备防护体系进行加固，技术机理为通过光子探测器观测光量子生成的量子真随机数，替代原有电网固定密钥，对电力系统关键信令进行加密，从网络层提高设备的安全等级。融合无线通信资源，有效降低有线专网建设成本，盘活公司海量测控设备，在保证安全前提下，强化电力对电网、设备、业务的精准掌控度。

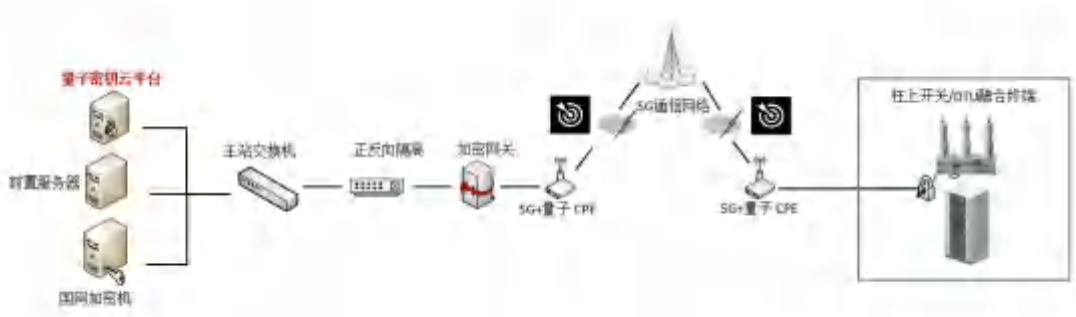

图 4-2 电力配电自动化量子加密解决方案

4.1.3 金融

（一） 行业应用场景

当前金融业务管理系统的规模不断扩大，各系统在提升管理水平、协同业务拓展等环节发挥重要作用，但信息防护体系不够完备，存在

数据泄露和被非法利用的风险。在日常业务中，银行产生海量用户信息、交易数据、日志数据等，对具有复用价值的数据如何安全存储和有效传输成为了银行一项重要挑战。

（二） 量子加密解决方案

银行信息化程度越来越高，数据越来越集中，根据“两地三中心”体系（同城灾备中心、异地备份中心），银行可利用量子保密通信技术，对同城和异地之间的通讯链路进行加密，确保数据传输的安全。

基于量子密钥分发技术 QKD 的金融安全解决方案包括组建量子保密通信网络以及配备量子安全路由器进行经典信道安全组网，提供金融数据端到端的量子安全加解密功能。

图 4-3 金融系统量子加密解决方案

4.1.4 交通

（一） 行业应用场景

交通运输是国民经济的基础产业和关系国计民生的服务性行业，在国家经济、文化等建设中发挥着重要作用。随着交通行业信息化程

度逐渐提高，云计算、大数据、物联网、移动应用、人工智能等新一代技术的应用，以及“互联网+”促进交通运输行业的转型升级，智慧交通已成为交通运输信息化发展的方向和目标。目前，各省市都在推进智慧交通建设，其中数据安全是智慧交通发展建设中的关键因素。

（二） 量子加密解决方案

省交通厅中心到站级服务器通过 QKD 网络分发量子密钥，站级服务器和车路站及车辆通过公私钥体系分发量子密钥。省中心密钥云服务器完成车路协同系统所需要的所有密码的全生命周期管理；车路站和车辆设备的密钥采用三层密钥管理体系，密钥源是真随机数芯片。

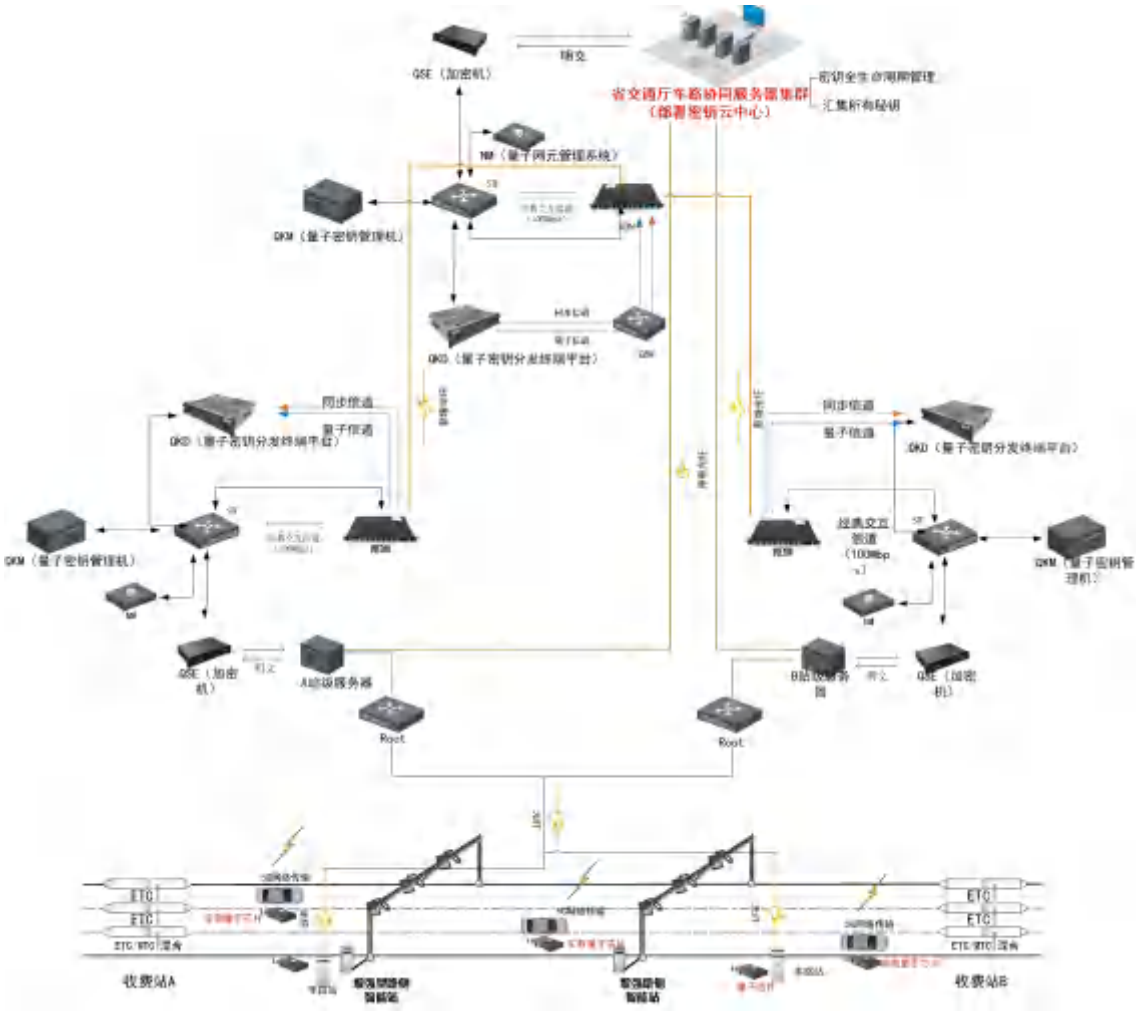

图 4-4 智慧交通量子加密解决方案

4.1.5 工业互联网

（一） 行业应用场景

工业互联网安全是实现我国工业互联网产业高质量发展的重要前提和保障，也是建设网络强国和制造强国战略的重要支撑。目前，我国工业互联网发展迅速，已广泛应用于能源、交通、制造、国防等行业领域，对经济社会发展的带动效应日益显著。工业互联网在构建全新生产制造和服务体系，为高质量发展和供给侧改革提供支撑的同时，也打破了传统工业环境相对封闭可信的状态，增加了遭受网络攻击的可能性，为此，亟需加快构建工业互联网安全保障体系，提升工业互联网安全保障能力。

（二） 量子加密解决方案

在工业互联网安全产品方面，防护类产品中的边界、终端安全防护是当前的主要分布形态，发展相对成熟，市场占有率较大。随着网络安全等级保护 2.0 的正式实施，防护类产品将成为工业互联网安全整体解决方案中必备的基础安全设施，市场规模将继续稳定增长。对此，量子加密将对工业互联网终端数据链路防护起到关键作用，量子密钥云平台与终端进行身份认证并在线分发量子密钥，终端采集数据经过量子加密后传输到服务端进行解密。

图 4-5 工业互联网量子加密解决方案

4.1.6 医疗卫生

（一） 行业应用场景

随着移动医疗、AI 医疗影像、电子病历等数字化应用的普及，医疗数据泄露事件频发。因此，强化我国健康医疗大数据安全管控和个人隐私保护，持续推进健康医疗大数据安全规范和法规建设显得尤为重要。国家卫健委印发《关于落实卫生健康行业网络信息与数据安全责任的通知》，明确网络信息与数据安全责任，不断提高安全防护能力。

（二） 量子加密解决方案

利用量子密钥云平台服务系统对网络通信数据进行加密。如下图所示，根据医联体的业务需求，在二级医院、县级医院、乡镇卫生间的各个终端设备配备密钥终端盒或 SDK；监控摄像头、门诊 pc、一体机（SDK 加密）、支付管理系统（SDK 加密）等设备终端数据通过终

端盒或 SDK 将加密好的数据通过专网或公网上传，在医联体数据处理中心（三级医院）前串接密钥云平台。其中量子密钥云平台提供量子密钥分发、数据加解密功能，监控摄像头、门诊 pc、一体机、支付管理系统等设备终端通过密钥云终端盒、SDK 方式接收量子密钥并进行数据加解密。

图 4-6 医疗系统量子加密解决方案

4.1.7 文化旅游

（一） 行业应用场景

现代旅游业的兴起与发展，始终离不开技术的赋能。自数字技术

兴起以来，旅游业是数字技术应用的重点领域，推动“互联网+旅游”深化发展，提升旅游产业数字化水平，能够助力数字中国建设。同时，伴随着互联网+旅游的发展，数据泄露事件也常有发生，旅客信息安全成为影响旅客满意度的重要因素。2020 年底，文旅部等联合印发的《关于深化“互联网+旅游”推动旅游业高质量发展的意见》中明确指出要落实旅游数据安全管理责任，保障旅游数据收集、传输、存储、共享、使用、销毁等全生命周期的安全，防止数据丢失、毁损、泄露和篡改。

（二） 量子加密解决方案

充分利用现有网络环境和政务云平台资源，包括与景区的通讯链路及与横向部门、涉旅企业、运营商等数据整合的链路进行整体安全设计。

1）横向部门

横向部门的信息化系统运行环境包括自建机房和电子政务云。量子密钥云平台对接部署在自建机房的信息化系统走外网通道，对接部署在电子政务云的系统走政务云内部网络。针对公安、交警等部门，通过量子安全路由器 VPN 专网的方式来接入智慧旅游大数据中心平台。

2）第三方系统平台

若涉及第三方系统平台数据，通过量子密钥云平台接口开发，以外网的方式通过量子密钥云平台接入点接入智慧旅游大数据中心。

3）景区

一般情况下景区内部管理数据不接入政务云平台，景区通过设置前置机，通过外网通道实现与政务云的对接。

4）涉旅企业

通过外网通道实现与涉旅企业对接。

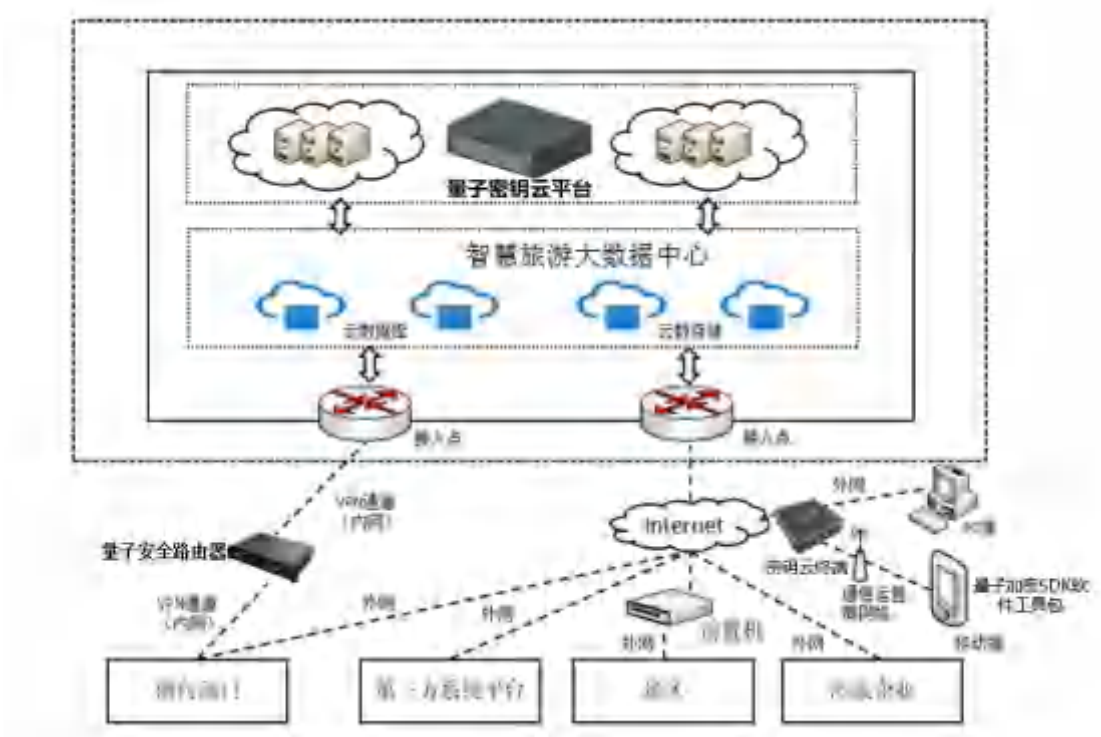

图 4-7 智慧旅游量子加密解决方案

4.1.8 教育

（一） 行业应用场景

随着高校信息化建设的不断发展，高校对信息资源的依赖程度越来越高，所以信息资源的安全问题日益成为高校不可忽视的问题。以“人防+物防+技防”提升教育互联网安全防护水平，筑牢教育互联网健康发展的安全“底座"。强化安全防护意识，善事前预警、事中控制和事后处置的全周期安全防护体系;形成合力提升技术保障水平，

切实保障设备安全、控制安全、网络安全、应用安全和数据安全;加强高新技术的开发应用，完善教育互联网安全技术体系。

（二） 量子加密解决方案

在不改变已部署的设备网络架构基础上，添加量子密钥云平台。采用透明加密，用户无感知，不影响用户使用习惯。针对智慧教育大数据应用模式，量子密钥云平台需要构建相应的服务模型，以有效支撑其服务系统优化设计，使构建的密钥分发服务系统能够更加贴近实际应用与高效运行。

图 4-8 智慧教育量子加密解决方案

4.1.9 电商物流

（一） 行业应用场景

伴随着《数据安全法》的出台，我国数据活动的监管将迎来一个新的时代，个人信息安全也将会得到愈发全面的保护，个人用户的数据安全问题将更加受到监管部门的重点关注。电商行业近些年迅猛发展，不论是交易数据还是用户数据都爆炸式增长。在电商的生态链中，电商企业、境内外消费者、平台企业、支付机构、物流企业等主体在

线上及线下场景深度交织，形成诸多主体之间的数据交互关系，信息流、物流、资金流交叉频繁，这个行业也天然要受到重点监管。

（二） 量子加密解决方案

电商远程支付服务业务系统包含支付客户端和支付平台两部分，该系统的密码应用主要解决支付交易资金转移相关的安全问题，用户通过移动终端上的支付客户端应用软件发起支付交易请求，支付平台响应和处理支付客户端的交易请求，之后与清算机构系统进行资金结算。

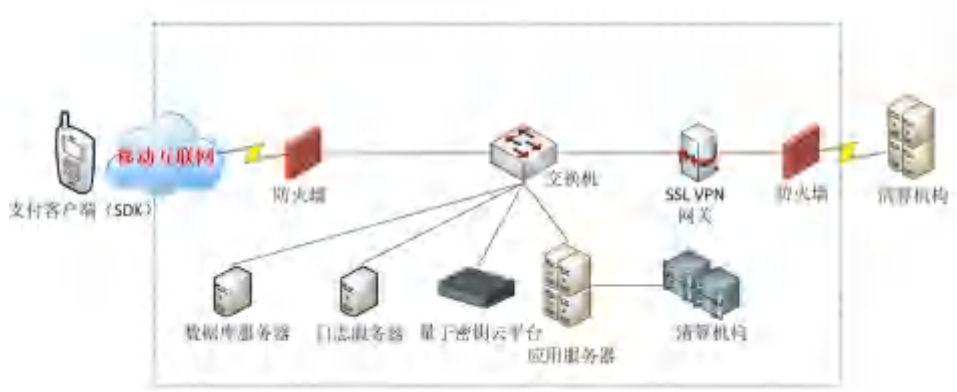

图 4-9 电商量子加密解决方案

4.2 典型场景

4.2.1 无人机巡检

无人机产业蓬勃发展，但是安全问题也在逐渐爆发。无人机、控制平台、机槽等无人机系统各主要环节存在网络安全管理问题。其中包括缺乏安全检测认证、缺乏有效的安全防护技术等诸多问题。基于量子加密技术的无人机巡检，采用量子物理真随机产生的量子密钥作为身份认证及会话密钥，实现一次一密，为无人机系统控制平台到机

槽、无人机到控制平台、无人机到机槽提供全方位的量子安全防护。量子加密无人机巡检可应用于电网巡检、铁塔巡检、生态环境检测等无人机巡检场景。

图 4-10 量子加密无人机系统解决方案

4.2.2 集群对讲

在公网集群对讲指挥调度系统中，指挥调度功能是最为重要的功能之一，也是衡量一个集群指挥调度系统是否具备强大控制能力的重要指标。基于量子加密技术的集群对讲应用如下图所示，在前端各个对讲终端上集成 SDK，从量子密钥云平台获取密钥，发端对数据进行加密，通过运营商公网进行传输，收端使用对称密钥解密。量子加密集群对讲系统可以应用在电网、政府等重保任务中，确保重大活动安全可靠。

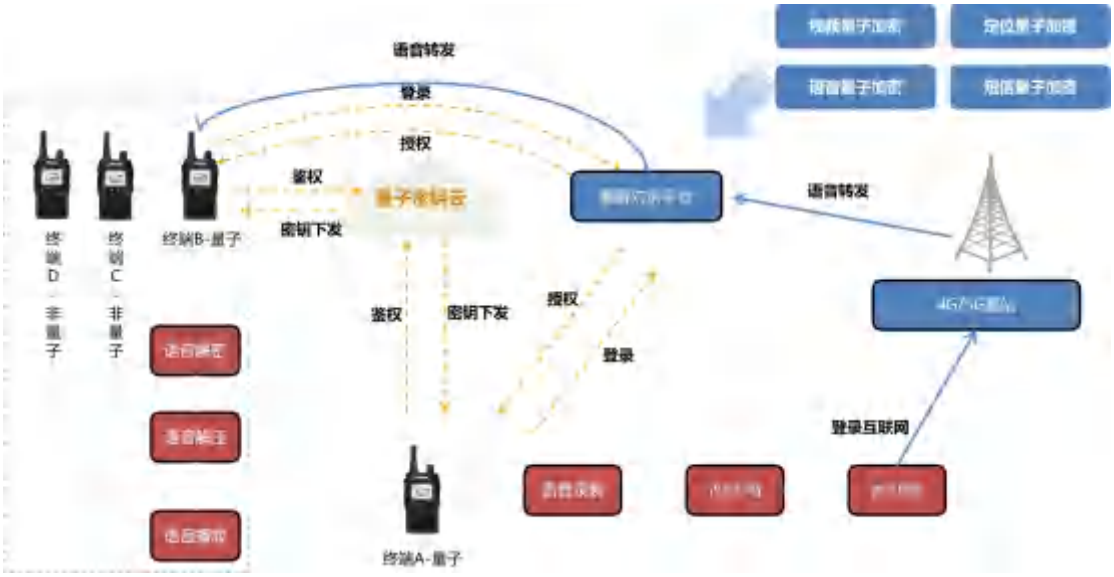

图 4-11 集群对讲系统量子加密解决方案

4.2.3 视频会议

近年来，随着通信技术和互联网技术的不断发展，视频会议技术的应用范围也在不断的扩大，视频会议系统的建设高潮也随之来临，这给用户带来便利的同时，也带来了一定的安全问题。随着视频会议系统安全性问题的不断曝光，用户对视频会议系统的网络安全问题更加重视。通过对视频会议系统的网络安全问题进行分析和探究，完成基于量子加密技术的视频会议系统数据加密业务。如下图所示，在两个视频会议终端前分别串接量子密钥终端，量子密钥云平台提供量子密钥，保证视频会议身份认证和两端数据安全传输。量子加密视频会议系统可应用于各个行业，乃至个人用户。

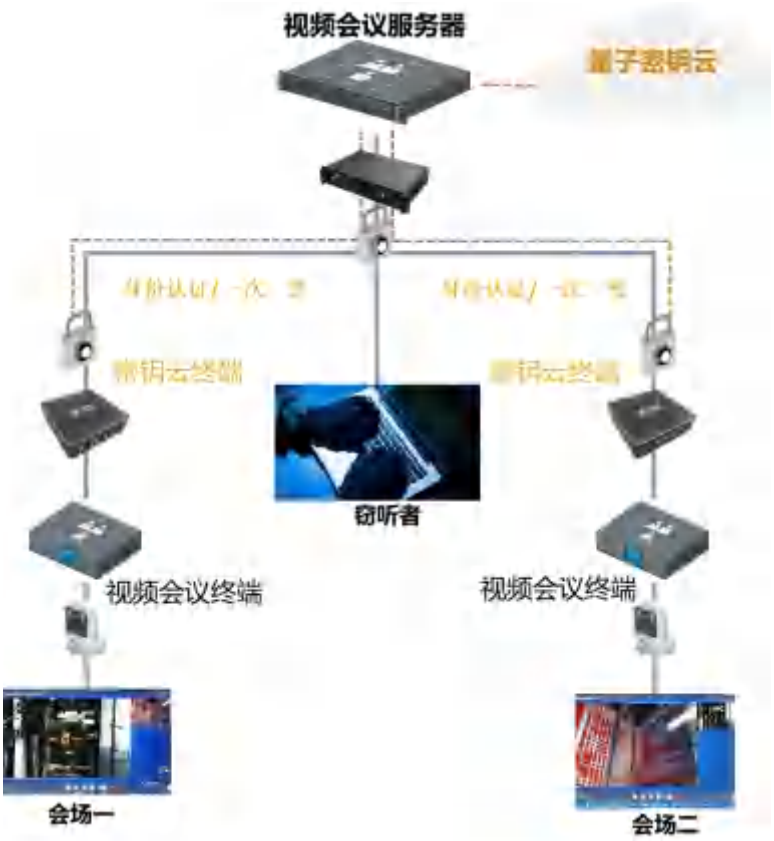

图 4-12 视频会议系统量子加密解决方案

4.2.4 车联网

随着网络世界的不断拓展和信息技术的快速升级，车联网成为了人们的研究热点。车联网又称车载自组织网络，它以智能网联汽车终端、移动智能终端和车联网云端业务平台为主体，以路侧单元为补充，其通信场景分为车内通信、车与车通信、车与人通信、车与云通信和车与路通信。将 5G 技术运用于车联网被认为是实现未来智能城市和智能交通的有效途径。不同于传统的蜂窝通信网络，由于车联网涉及到人身安全问题，车联网中车辆发出的车联网消息需要以极低的传输时延以及极高的传输可靠性进行传输，这一需求使得车联网必须是一种具有超低时延超高可靠性的网络。因此如何设计一个新的网络结构

来满足未来车联网对消息时延以及可靠性的需求成为了目前车联网研究领域的重点。基于此，我们通过在车联网云平台部署量子密钥云服务，建立面向车辆端、路侧单元、移动终端及其各网络边界的接入鉴权服务，确认用户的访问权限。此外，量子密钥云服务向车侧和路侧分发量子密钥，当车侧和路侧单元通过 4/5G 网络与边缘云进行通信时，利用量子密钥加密数据，减少数据在无线网络的空中暴露风险。

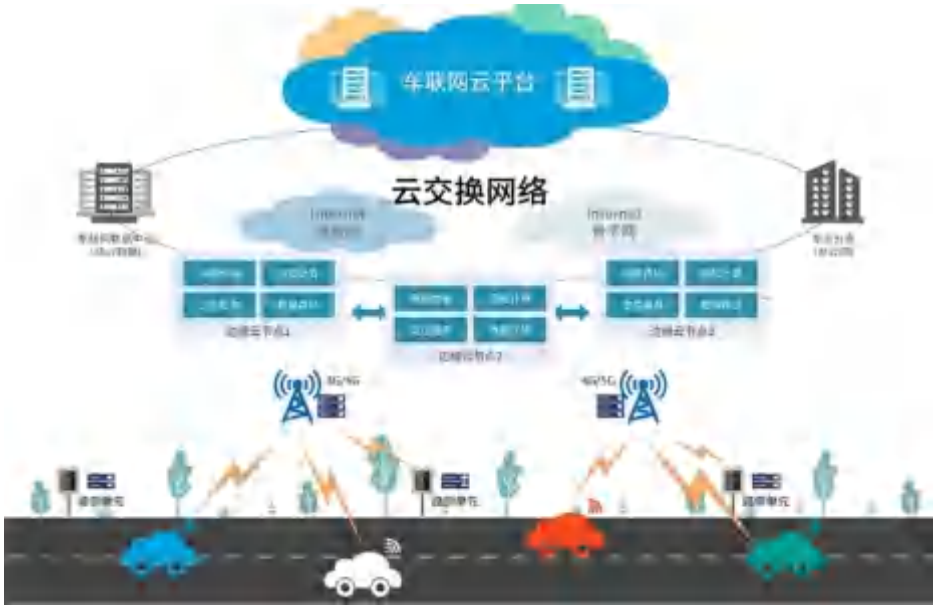

图 4-13 量子安全车联网解决方案

4.2.5 量子密话

保密移动通信是利用加密算法对传输的移动通信信息进行加密封装并发送给指定的对象。随着现代信息技术和互联网的发展，为移动保密通信的安全性提出了很多新的题目。身处数字化社会，保密移动通信不仅可以用于军事、国防等领域，还可以用于涉及保密数据传输的各类组织和机构，包括政府、金融、电信、保险、财政等领域和部门，应用前景非常广阔。利用传统加密算法进行保密移动通信的方

式，在实际应用中由于语音信号数据量大、且在传输的过程中实时性要求高，并且网络丢包情况时有发生，会耗费时间造成网络堵塞，导致大量时延，难以实现实时加密语音。为了解决这些问题，我们提出了基于内生安全体系的量子密话方案，如下图所示，用户接入管控平台时完成双向身份认证，在安全环境下，在线往用户手机终端建立密钥池，实现密钥的安全分发与用户隐私安全保障。当需要加密通话时直接从用户终端实时获取密钥加密即可，保障通话安全无时延。

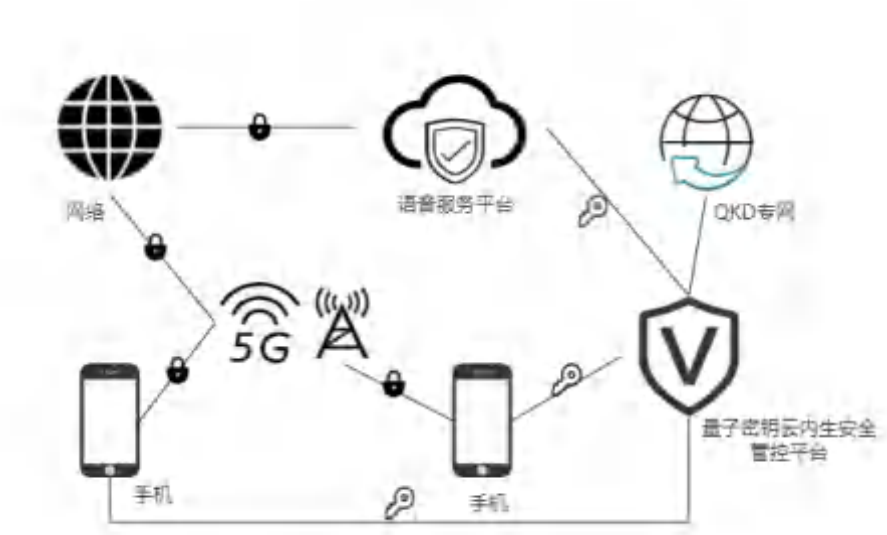

图 4-14 量子密话解决方案

4.2.6 数据确权

随着以大数据、云计算和人工智能等为代表的新型工业革命的到来，数据已成为当下具有重要经济价值的资源，并且已经成为一种新时代的生产要素。海量的数据给人们的生活带来了便捷，也为企业带来了巨大的商机，促进了社会的发展。由于数据不仅涉及个人信息隐私和保护，也涉及企业竞争和商业机密，甚至国家、社会公共安全和

利益，因此如何用好数据成为了亟待解决的重大课题。这其中数据确权是一个不可避免又极具挑战性的问题。在数据确权过程中，需要既保护数据所有人的权利和隐私，同时要有利于数据的高效流通和利用，让社会分享大数据价值增值的益处。基于此，我们提出利用量子密钥的量子安全数据确权解决方案。如下图所示，量子密钥云平台提供量子密钥池作为数据确权的钥匙，原始数据产生后按照数据所有权分配所属的加密密钥进行加密存储。在数据流通过程中，实现密文流通，保证数据不被泄露。在数据使用过程中，按照使用权和时效对数据以可用不可见的方式进行使用，从而保证数据在全生命周期过程中的产权边界清晰安全。

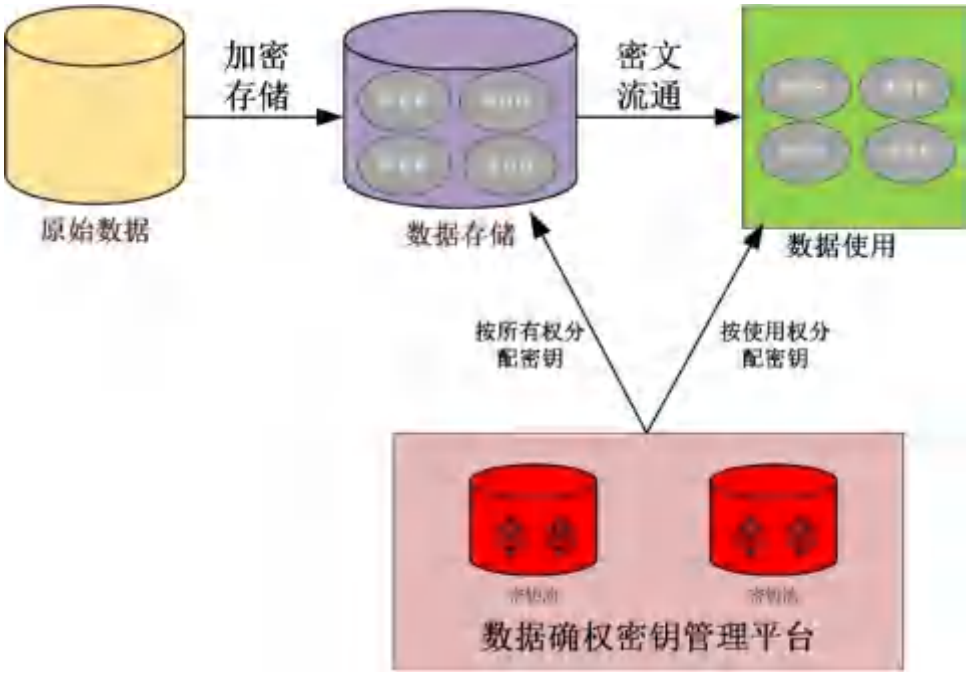

图 4-15 量子安全数据确权解决方案

4.2.7 数据隔离

传统数据资产面临着数据产生来源复杂，数据标准不一致，维护

复杂，数据容易形成孤岛，无法有效挖掘利用的问题。随着大数据、云存储技术的发展，数据上云逐渐成为未来发展的趋势。在云数据库里，如何保证用户只能调取具有访问权限的数据，而无法获取没有权限的数据，实现数据的精确访问，对数据按获取权限进行隔离，是保证数据不被滥用和安全访问的关键。基于此，我们提出基于量子密钥的量子安全数据隔离解决方案。如下图所示，量子密钥云平台提供量子密钥池作为数据隔离存储和按授权解密访问的钥匙。用户在调取数据湖中所需的数据时，首先需要通过数据湖的接入认证，然后利用获得的授权量子密钥对待访问的数据进行解密，从而即保证只有合法用户能够进入到数据湖中，也能够保证用户只能够调取具有访问权限的数据，而无法获取到数据湖中的其他数据。

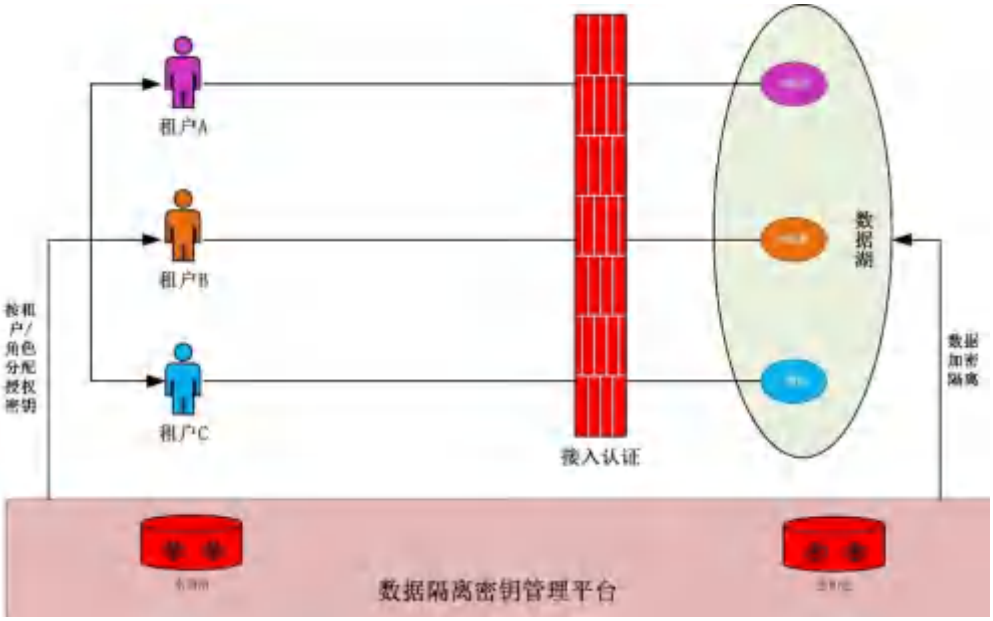

图 4-16 量子安全数据隔离解决方案

五、 总结与展望

随着移动互联网、智能终端、大数据、人工智能等新一代信息技

术的快速发展，数字经济已成为推动国家高质量发展的重要引擎。如何通过新技术手段保障大数据、云计算平台，工业控制系统，物联网等关键信息基础设施安全，是数字经济首要面临和需要解决的问题。

量子科技作为推动数字经济的核心力量，在经济高质量发展及国家安全保障中将起到至关重要的作用，量子通信技术应用研究联合实验室积极响应国家号召，携手产业合作伙伴，进一步推动量子通信与现网应用深度融合。未来，在技术领域深化量子安全通信技术尤其是QKD设备的研究，解决现有网络在传输距离、成码率以及共享现有光电通信网络等技术方向存在的问题，完善量子技术标准体系，针对体系架构、协议算法、组网方案等多个技术方向，建立统一的量子技术应用化平台。尤其是当前较为成熟的量子安全通信技术与现有行业应用进行深度融合，可提供全新的安全解决方案，以高可靠安全传输，赋能各行业的安全发展。

量子赋能•守护未来