中国移动量子“Q 波”技术白皮书

（2022 年）

中国移动

前　言

习近平总书记在2020年10月举行的中央政治局第二十四次集体学习中强调，要充分认识推动量子科技发展的重要性和紧迫性，加强量子科技发展战略谋划和系统布局。国家在“十四五”规划和2035年远景目标纲要中提到，强化国家战略科技力量，加强量子信息等原创性引领性科技攻关。

本白皮书在分析量子技术发展情况、量子技术对移动通信网安全影响的基础上，提出量子信息技术与移动通信网的融合创新方案，即量子“Q波”，Q是量子英文Quantum的首字母，波代表无线电波，寓意量子技术与移动通信网的融合。通过构建量子密钥服务体系，提供一体化新型信息安全服务能力，满足高安全通信应用的需要。期望运营商、设备商、科研院所共同探讨和推进量子技术的产业落地，实现安全可靠的网络、灵活通用的安全服务。

参与单位：中国移动通信有限公司研究院、中移系统集成有限公司、中国移动通信集团终端有限公司、信通数智量子科技有限公司、东南大学、卫士通信息产业股份有限公司。

目 录

1 量子信息技术发展概况

1.1 发展方向

量子信息技术是量子物理与信息科学交叉的新生学科，其物理基础是量子力学。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 世纪最重要的科学发现之一。进入 21 世纪，量子科技革命的第二次浪潮正在来临，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、提升测量精度等方面突破经典技术的瓶颈，将极大地改变和提升人类获取、传输和处理信息的方式和能力。

当前，量子技术主要包括量子通信、量子计算和量子测量，三大技术领域的成熟度存在一定差异。基于量子密钥分发的量子保密通信已进入产业化初期，是国内外运营商在量子科技领域的主要投入方向。

1.1.1 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。其安全性由量子力学基本原理保证，在量子密钥传输过程中，窃听者无法做到既窃听又不留下痕迹。量子通信有两种最典型的应用方式：量子密钥分发（QKD）和量子隐形传态。量子密钥分发可以提供原理上无条件安全的通信手段，是首个从实验室走向实际应用的量子信息技术。量子隐形传态可以用来传输任意未知的量子态，同时也是远距离量子密钥分发所需的量子中继的重要环节。

量子通信不是要替代经典通信方式，而是通过在经典通信中使用量子密钥以提升通信安全性，同时量子通信的规模化应用也需要与经典通信技术相融合。发展量子通信技术的终极目标是构建广域量子通信网络体系，广泛认可的发展路线是：通过光纤实现城域范围内的量子通信网络；通过中继分段传输实现城际量子通信网络；通过卫星中转实现数千公里甚至是全球化的量子通信网络。

1.1.2 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。

量子计算研究可分为三个阶段。第一个阶段是实现“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；第二个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；第三个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。

1.1.3 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。

1.2 国内外发展现状

1.2.1 主要国家政策

作为事关国家信息安全的战略新兴领域，世界各国纷纷启动国家级量子科技战略行动计划，支持量子通信技术的研发和产业化。如，美国在 2018 年发布《国家量子计划法案》的基础上，2020 年再次发布《量子网络战略愿景》、《“量

子互联网”国家战略蓝图报告》，将量子互联网建设提上日程；2022 年 5 月签署两项总统政令《关于加强国家量子计划咨询委员会的行政命令》和《国家安全备忘录：在提升美国在量子计算领域的领导力的同时缓解密码系统面临的风险》，加快推动美国量子信息科学发展。英国在 2018 年启动了第二阶段国家量子技术计划，强调要以行业为主导，加快量子通信等技术的商业化。欧盟在《量子技术旗舰计划》的支持下，正在全力推进建设量子通信基础设施（QCI）。德国政府在“量子技术：从基础到市场”的量子技术研究国家计划中，提出重点研究量子卫星、量子计算和用于高性能高安全数据网络的测量技术等领域。此外俄罗斯、日本、韩国等国家也进行了战略部署。

1.2.2 量子通信设施部署概况

我国在 2016 年建成了世界首条远距离量子通信“京沪干线”，并已实现与世界首颗量子试验卫星“墨子号”的对接。现在正在国家发改委的支持下，面向国家战略需求和可持续运营要求，建设覆盖京津冀、长江经济带、粤港澳等重点区域的国家广域量子保密通信网络。受此影响，主要发达国家也在量子通信基础设施领域加快部署。如，美国 Quantum Xchange 公司正在建设沿东海岸的连接华盛顿特区和波士顿的总长约 800 公里的美国首个州际、商用量子密钥分发网络；欧盟量子通信基础设施项目的先导工程 OPENQKD 项目已经启动，通过部署测试平台，提升电信、医疗、电力供应和政府服务领域关键应用的安全性；英国分别在 2019 年和 2021 年完成了国家量子保密通信网络和伦敦量子城域网的建设，正在医疗、国防、银行和物流等领域开展试点应用；德国的 QuNET 大型量子通信项目，将建立德国量子通信基础设施的中心平台，为政府等关键领域服务，并为建设量子互联网奠定基础；韩国国家量子密钥分发网络将连接全国 48 个关键政府部门并保障其通信安全；俄罗斯铁路公司已经在莫斯科和圣彼得堡之间建成了总长 700 公里的量子通信干线等。

在加紧布局远距离光纤量子通信网络的同时，全球主要国家和地区也在大力推进天基 QKD 基础设施建设。如，欧空局于 2018 年 5 月启动了空间量子加密通信系统项目（QUARTZ）；英国联合新加坡在 2018 年 9 月启动了量子卫星 QKD Qubesat 项目；加拿大空间局正在部署为加拿大政府、金融交易等提供安全服务

的量子卫星 QEYSSat 项目；德国在量子技术研究框架计划中将基于立方卫星的量子保密通信作为重点研究内容等。

1.2.3 电信运营商量子产业化现状

近年来，世界主流电信运营商纷纷加大对量子保密通信产业的投入。英国电信 BT、北美的 Verizon 和东芝联合研发量子密钥分发技术。Verizon、BT、西班牙 Telefonica 和韩国 SKT 等主流运营商联合产业界，正在建设量子保密通信网络。SKT 于 2020 年推出了首款量子加密手机 Galaxy A Quantum，并于 2022 年 4 月发售了第三代量子加密手机。中国移动、中国电信于 2022 年 5 月分别发布了基于 VoLTE 的量子加密通话产品。

2 中国移动量子密钥服务体系

2.1 量子计算对密码算法的影响

在移动通信网中，安全保密通信一般可分为密钥协商阶段和加密通信阶段，其中密钥协商阶段的目标是计算出通信双方共享的会话密钥，该会话密钥用于对后续通信进行加密保护。两个阶段涉及到对称密码算法和非对称密码算法。量子计算将对传统的密码算法带来较大的冲击。

（1）对非对称密码体系的影响

目前常用的非对称密码算法包括 RSA、椭圆曲线、DH 密钥交换算法等。其中 RSA 算法依赖于对大整数进行质数分解的困难性；椭圆曲线算法依赖于有限域上求离散对数的困难性。Shor 算法及其变种能够在多项式时间内解决这些数学上的难题。

（2）对对称密码体系的影响

Grover算法本质上是一种针对无结构数据的搜索算法，理论上Grover搜索算法能够对非结构化的搜索问题提供二次方的加速，可以有效地攻破轻量级算法等密钥长度较短的对称密码。目前，业界普遍认为256bit的对称密码算法可以抵抗量子计算机的攻击。

（3）对散列算法的影响

Grover算法对散列算法的安全也产生威胁。对于对称算法，理论上具有平方级加速，但是在现实应用中难以评估。对SHA256算法的单一原像攻击需要大约2^{166}次操作，而不是理论上的2^{128}次。寻找碰撞作为散列算法的另一安全度量，目前尚未有比经典算法更加有效的量子算法。可以认为，目前常用的SHA256、SHA512、SM3等散列算法仍是安全的。MD5、SHA1等散列算法由于自身问题在经典计算体系中已经不再安全，因此应禁止使用。

综合上述分析可知，对称密码算法通过增加密钥长度即可抵抗量子计算攻击，因此，量子计算对网络安全影响的关键在于非对称密码算法。美国已经启动抗量子密码算法的征集，美国国家标准局NIST将于近日公布第四轮征集的全球抗量子公钥算法候选者，并准备在2024年完成抗量子密码标准制定，从而取代现有非对称密码算法。

2.2 量子技术对通信网的使能作用

国家层面为加速形成移动互联网尤其是 5G 生态，占领新一代移动通信技术的制高点，加快了政府、军警、金融、先进制造等行业的数字化、智能化业务转型，这些行业都是涉及国家安全、社会稳定的关键行业，要求自主可控、安全可靠。量子技术最成熟的应用是量子随机数生成（QRNG）和量子密钥分发（QKD），将量子技术与移动通信网结合以增强安全性已成为热门话题。

量子随机数是利用量子状态随机性的特点提取得到的随机数，与从经典物理噪声源（如热噪声）中提取的随机数相比具有“真随机”的特性，更加难以模拟和预测，安全性更高。采用量子随机数发生器升级替代传统软件算法生成的随机数，可广泛应用于通信网络中身份认证、密钥产生、加密传输等场景，进一步提升通信系统的基础安全性。

利用量子物理体系的内禀随机性，如量子态坍缩等，进行随机数生成制备，称为量子随机数发生器，由量子力学理论模型保证其真随机性，随机数生成速率可达更高水平。因此，量子密钥具有真随机性。

QKD与基于计算复杂度的经典密码体制不同，其安全性是基于量子力学的基本原理，具备信息论安全性。所谓“信息论安全”（也可称为“无条件安全”）

是指拥有严格数学证明的与计算复杂度无关的安全性，不论敌手拥有多大的计算能力，其安全性都不会受到影响。QKD的这种“信息论安全性”有下列假设前提：敌手（窃听者）不掌握攻入合法用户设备内部的侧信道；敌手不能拥有违反量子物理学原理的技术。因此，敌手即使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，也不会对QKD的安全性造成影响。

基本的QKD系统通常由具备量子密钥分发能力的一对节点设备组成，它们通过量子信道和经典信道连接，可以在点对点链路上实现信息论安全的对称密钥分发，并且利用此对称密钥可以对经典信道上传输的数据进行加密保护。通过QKD组网技术可以在多个节点设备间实现信息论安全的对称密钥分发，并对数据信息进行安全保护。

2.3 量子密钥服务体系方案

中国移动基于量子技术与移动通信网络技术，提出量子密钥服务体系方案，构建量子密钥安全能力，提供集中一体化信息安全服务，满足高安全通信应用的需要。量子密钥服务体系由量子密钥无线分发系统、量子保密通信系统、量子密钥服务中心、量子密钥服务应用构成。其中，量子保密通信系统当前主要基于量子密钥分发网络实现，鉴于量子密钥分发网络已有白皮书进行介绍，此处不再进行赘述。

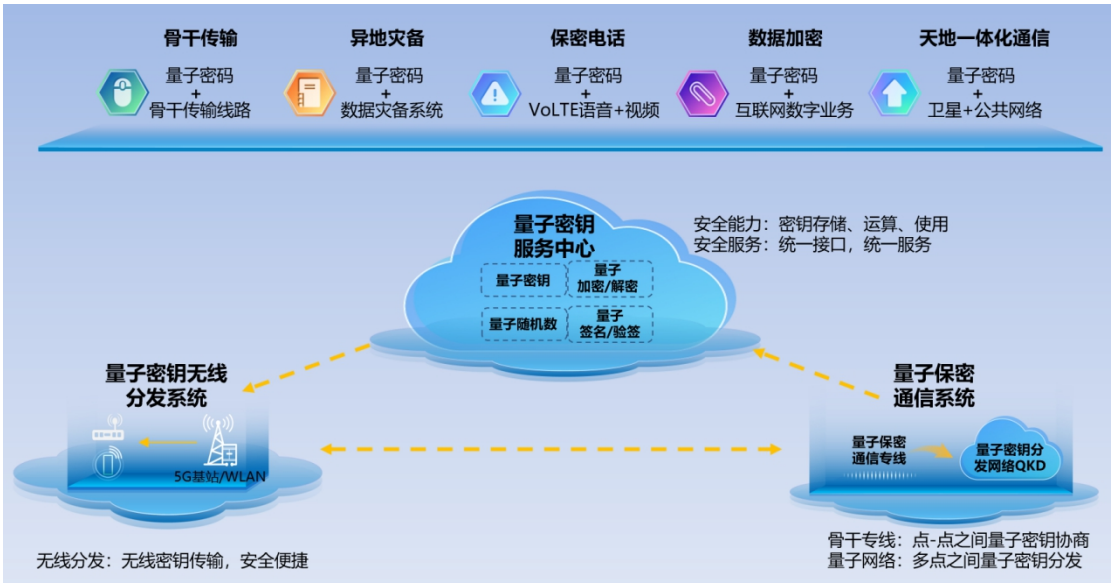

图1 量子密钥服务体系

（1）量子密钥无线分发系统

量子密钥分无线发系统接受量子密钥服务中心和量子密钥分发网络的量子密钥，通过无线分发的方式进行密钥的分发。无线分发是指通过无线信道进行密钥分发，即利用无线信道随机性、互易性、去相关性等特点在终端和基站/Wi-Fi热点等无线通信信道中产生具有信息论安全性的密钥对所传输的量子密钥进行密钥分发。

（2）量子密钥服务中心

量子密钥服务中心是量子密钥服务体系的核心。通过建设集中统一的量子密钥服务中心，将量子密钥分发网络、保密通信网络形成的量子密钥与通过移动通信网络及业务服务网络连接的用户联系起来。以量子保密通信系统分发的量子密钥、量子随机数等关键安全要素为基础，对现有加/解密、签名/验签技术进行抗量子计算安全增强；同时通过统一接口、统一服务的方式将这些量子安全能力向内外部用户开放，形成量子通信安全业务，完成对信息系统的机密性、完整性、可认证性、不可否认性等安全属性的保护。

（3）量子密钥服务应用

量子密钥服务应用基于量子密钥安全服务可通过与骨干传输、数据异地灾备、保密电话、互联网数据加密、天地一体化通信等应用场景结合实现量子赋能，从而提升通信系统整体安全性。

基于此，中国移动提出了量子“Q波”，实现量子技术与移动通信网的融合，主要包括：实现终端量子密钥安全分发，解决量子密钥“最后一公里”传输难题；构建量子密钥安全服务中心，满足用户多应用多业务的密钥和密码需求；最终实现量子赋能，服务千行百业，为信息服务保驾护航。

3 量子“Q 波”密钥无线分发系统

3.1 量子密钥分发问题

为了满足移动终端对量子密钥的应用需求，当前主要采用离线灌装的方式将预先生成的一定量量子密钥充注入USIM卡、TF密码卡、SoftKey等终端安全介质，

并配发给移动终端用户使用。整个密钥离线灌装操作在具有安全保障的物理环境中进行，确保量子密钥分发过程的安全性。

由于终端安全介质留给量子相关业务的存储空间有限，一次灌装所能充注的密钥量也是有限的，通常为几百Kbit。因此，在预装密钥消耗完之后，通常要求量子移动端用户携带终端安全介质到业务运营商的指定网点与量子密钥充注设备对接，补充充注量子密钥。这种离线充注的方案虽然满足了量子密钥终端用户的使用需求，但是要求用户在量子密钥不足时，携带设备前往特定服务站点加注。频繁的加注给用户带来使用上的不便，也给量子密钥运营服务商提出了较高的系统建设要求。因此，离线安全灌装的方法只能作为小规模、短期性的解决方案使用。

从量子密钥应用产业长远发展及大规模应用来看，通过无线通信网络实现量子密钥安全分发是解决量子密钥移动端部署问题的有效途径，因此在当前量子密钥技术发展应用的早期阶段，研究并探索高安全性的无线物理层安全技术实现量子密钥无线分发，推动量子“Q波”密钥分发技术的落地实施具有重要的理论价值及实践意义。

3.2 量子密钥无线分发技术

量子密钥无线分发的核心关键是无线物理层密钥生成。近年来，全球无线通信领域的专家、学者从信息论安全理论出发，提出了利用无线信道内在的安全特性在无线通信系统的物理层实现达到信息论安全水平的安全通信方法。该方法利用无线信道使收发双方从无线信道中提取出特征相似的信道状态信息并基于此生成一致的对称密钥，从而在物理层实现安全通信。由于无线物理层密钥生成技术产生的密钥具有较高的安全性，因此被视为未来通过无线环境实现移动端量子密钥分发的有效技术手段，也就是量子密钥无线分发。

无线信道在相干时间内具有短时互易性。通信双方互相发送的导频信号会经历相同的信道衰落，所以测量得到的信道特征极为相似，因此从信道特征中提取信道状态信息，进而生成会话密钥具备可行性。在另一方面，处于同样无线环境下的第三方窃听者虽然也能够监测到合法通信双方交互的导频信号，但由于无线信道在空间上具有去相关性，在一定距离（半波长）间隔以上接收到的信号将经

历不同的信道衰落，因此窃听者无法提取与合法接收者相同的信道特征来产生密钥，这就确保了合法用户间所生成密钥的安全性。

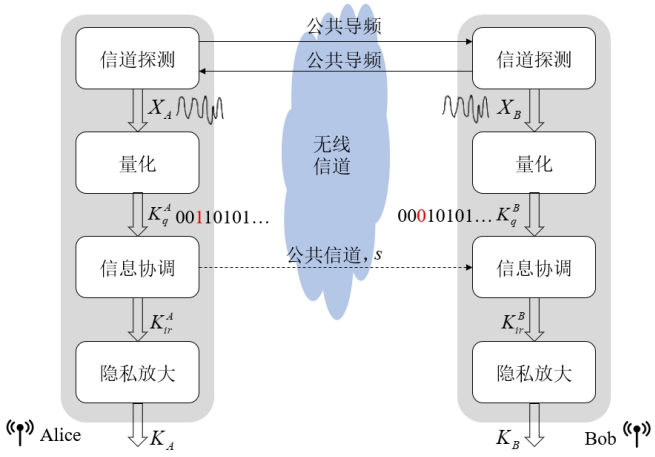

图2　无线物理层密钥生成原理

基于上述原理，无线物理层密钥生成技术通常包括信道探测、量化、信息协调和隐私放大四个阶段。

- 信道探测：合法用户Alice和Bob互相发送已知的导频信号帧进行信道探测。在相干时间内，双方发送的信号经过相同的信道衰落到达对方。接收方用接收到的信号与已知的导频信号进行计算，估计获取这段时间内的信道状态信息。由于信道探测的过程是双向的，通过信道估计可分别获得信道测量结果X^A和X^B。
- 量化：Alice和Bob将测量结果X^A和X^B转换成二进制数字，即K_q^A和K_q^B，对信道状态的测量值完成量化。
- 信息协调：由于无线信道在上下行方向上的随机波动，Alice和Bob的测量量化结果可能存在差异，因此对于K_q^A和K_q^B之间不一致的比特值，需要采用信息协调的方法来消除，通常可通过在公共信道上交互一些校验信息最终使Alice和Bob获得匹配一致的原始密钥K_{ir}^A与K_{ir}^B。
- 隐私放大：上一步在无线信道上公开传输了一定量的数据信息用于信息协调，因此有可能被窃听者获取来做密钥分析。为了消除部分信息泄露可能带来的负面影响，通常需要对K_{ir}^A与K_{ir}^B做哈希计算以确保所生成密钥的安全性。最终，经过隐私放大，Alice和Bob获得密钥K^A与K^B。

利用K^A与K^B，Alice和Bob可以基于“一次一密”的方法对双方无线空口上传输的数据进行加密保护，实现用户信息的高安全传输。

基于量子密钥无线分发方案，终端用户便可不必再前往充注网点离线灌装量子密钥。终端可根据本地量子密钥的剩余量的多少，随时随地发起量子密钥在线申请过程补充新的量子密钥。对于量子密钥新鲜性要求高的用户应用，终端甚至可以通过无线网络从量子密钥中心实时获取量子密钥，从而确保用户业务高安全性需求得到满足。

3.3 研究进展及关键问题

为验证量子密钥无线分发方案，中国移动联合东南大学科研团队开展合作，将南京江宁无线谷接入国家量子保密通信骨干网，为江宁无线谷用户节点提供量子密钥分发和密钥管理与中继等功能。

通过在雨花台区软件园范围新建汇聚站，汇聚站节点部署量子密钥生成设备、量子密钥管理设备和光交换设备等，实现与其它汇聚站节点及用户节点量子密钥分发和密钥管理与中继等功能。江宁无线谷用户节点部署量子密钥生成与管理终端，实现与集控站或汇聚站量子密钥生成设备进行量子密钥分发，并实现量子密钥管理和中继等功能。

同时，基于USRP软件无线电平台和Wi-Fi信号帧进行了物理层密钥生成技术的原型验证。原型系统主要由软件无线电平台配合工作主机进行基于无线信道特征的密钥生成，其中的信息交互由无线路由器来沟通协调。原型系统的用户端界面可以实时显示信道状态信息和密钥生成情况。系统在室内、走廊、室外三种不同的实验环境进行了连续多次的数据采集，测试了系统生成密钥的有效性和安全性，密钥生成速率不低于256比特每分钟。

为有效实现融合物理层密钥的量子密钥无线分发网络，还需要解决以下关键问题：

（1）如何实现低开销、低复杂度的无线物理层密钥信息协调

信息协调用于确保通信双方提取物理层密钥的一致性，消除由无线信道波动造成的量化结果差异。信息协调的实现需要额外的协议和通信双方之间的信息交换，因此又被称为交互信息协调机制。该机制通常使用校验码或纠错码来纠正密

钥的不一致比特，但这也意味着更多的信息被泄露和需要更高的算法复杂度。因此，信息协调之后往往需要隐私放大步骤以获得“随机的”密钥。复杂的信息协调与隐私放大过程将会极大的增加系统复杂度和通信开销，降低密钥的更新效率。因此，如何进行高效且轻量级地信息协商机制是量子“Q波”在落地应用中面临的关键问题之一。

（2）如何在准静态环境下生成高熵物理层密钥

由于无线信道特征在信道相干时间内保持不变，物理层密钥的随机性因此受到信道变化速度的限制，影响了量子密钥分发的速率。在现实应用场景中，室内用户设备并不一定时时处于运动状态，信道的变化速度受周围环境的影响较大。此外室内环境也可能出现因为各传播径之间延迟时间差别不大而导致的多径衰落不明显、信道特征随机性不足的情况。物理层密钥的安全性取决于信道特征本身的随机性，因此，如何在准静态室内环境下生成高熵物理层密钥是量子“Q波”技术中一个亟需解决的问题。

（3）量子“Q波”技术如何兼容现有常用无线通信体制

室内无线覆盖常用的通信体制有Wi-Fi、LTE、5G等，如何设计融合现有通信体制的量子密钥无线分发方法是一个影响实用化的重要问题。量子密钥无线分发网络需要兼容现有体制，即本网络的加入不应显著影响现有网络的运行效率。因此需要设计与现有体制相似的帧结构、参数设置和传输协议控制，并评估量子“Q波”系统在实际中的运行效率。

（4）如何构造可信的密钥管理系统

量子“Q波”系统通过量子密钥服务中心将量子密钥以数据方式发送至终端，因此量子密钥服务中心承担着量子密钥的存储、转发与管理功能，其安全性的保障尤为重要。为了确保量子密钥服务中心不被病毒和恶意软件侵害，需要基于国产安全芯片，构建安全可信的软硬件平台和量子密钥管理系统。

4 量子“Q 波”密钥服务中心

量子密钥服务中心是量子密钥服务体系的核心，是基于量子密钥源建立对称密钥管理与应用支撑系统，主要用于保护密钥的保密性、完整性和可用性，并满足用户多应用多业务的密钥和密码需求。

量子密钥服务中心既支持利用无线信道特性产生具有信息论安全的密钥对所传输的量子密钥进行安全保护，也支持通过量子安全介质（例如USB key、TF卡等方式）对量子密钥进行安全保护，将量子密钥的使用场景拓展到量子密钥分发网络以外，扩展了量子密钥的应用范围和场景。

量子密钥服务中心遵循国家商用密码及密钥管理相关标准，通过相关密码服务设备和标准接口向应用系统提供基于量子密钥的密码安全服务。

4.1 系统架构

量子密钥服务中心系统架构主要分为三层：资源层、管理应用层和服务层，通过密码设备、安全介质等对应用层提供量子密钥和量子密码服务能力。

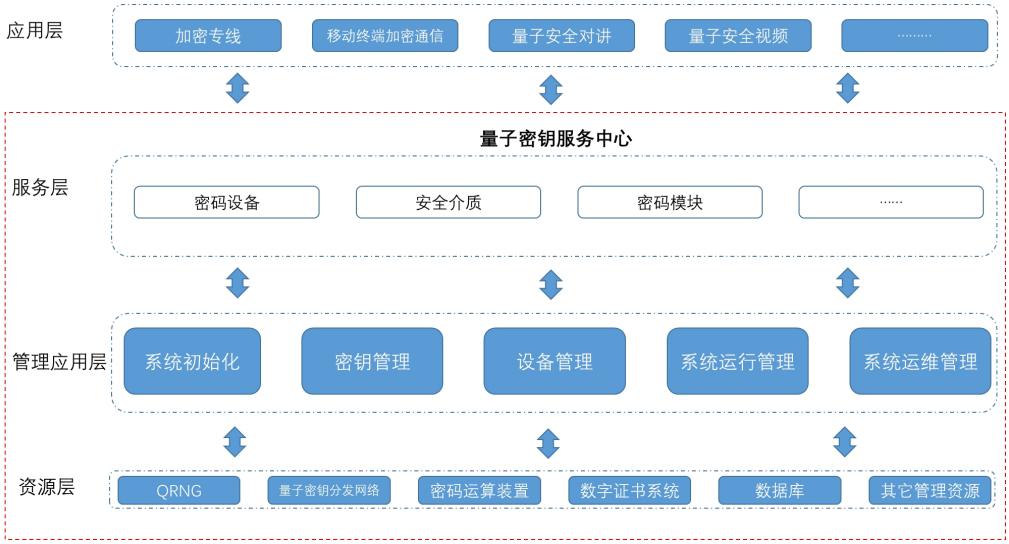

图3 量子密钥服务中心系统架构

资源层主要包括QRNG、量子密钥分发网络、密码运算装置、数字证书系统、数据库和其它管理资源。其中QRNG和量子密钥分发网络提供量子密钥源；密码运算装置提供对称密码算法加解密运算、数据摘要运算等密码服务；数字证书系

统提供证书管理，包括证书签发等服务；数据库提供设备管理信息、密钥管理信息等信息的管理能力。

管理应用层主要为量子密钥服务中心提供密钥管理、设备管理等能力。其中系统初始化为初始化工作提供能力支撑，包括系统权限管理、系统管理密钥生成等；密钥管理主要对量子密钥进行全生命周期管理，包括密钥生成、销毁、恢复等；设备管理主要包括密码设备管理、设备量子密钥融合增强等；运营和运维管理提供分级管理、设备维护等能力。

服务层主要为量子密钥服务中心提供对外服务能力。量子密钥服务中心通过密码设备、安全介质等向上层应用系统提供量子密钥和密码服务能力。

4.2 主要功能

量子密钥服务中心为用户提供量子密钥全生命周期管理、量子安全设备管理、设备与用户身份鉴别、量子会话密钥分发/协商、量子增强基础密码服务等功能和服务。

（1）量子密钥全生命周期管理

量子密钥服务中心支持量子通信网络、量子随机数发生器等多种量子密钥生成系统接入应用，具备量子密钥生成、量子密钥存储、量子密钥分发等全生命周期管理功能。

（2）量子安全设备管理

量子密钥服务中心对所辖系统用户使用的密码设备（例如服务器密码机、PCIE密码卡等）和量子安全介质（例如SD卡、U盾、安全芯片等）进行统一管理。

（3）设备与用户身份鉴别

量子密钥服务中心融合应用量子密钥，对访问系统的终端设备与用户进行接入认证。

（4）量子会话密钥分发和协商

量子密钥服务中心根据密钥分发/协商策略，为通过身份鉴别的设备与用户提供量子会话密钥分发和协商服务。

（5）量子密钥增强基础密码服务

量子密钥服务中心融合运用量子密钥，对经典密码算法进行密钥安全增强，向应用系统提供基于量子密钥融合增强的安全认证、密钥分发、加解密等服务。

5 量子“Q 波”在通信行业应用场景

5.1 关键信息基础设施安全

通信服务系统、供水服务系统、电力生产与分配服务系统、天然气服务系统、石油服务系统、金融服务系统、卫生服务系统、运输系统、粮食生产与分配系统等关键基础设施，在社会经济的正常运行中发挥着重要作用。对于这些关键信息基础设施而言，系统的安全性和可靠性至关重要，通信过程中的信息真实性、完整性、机密性将直接影响整个体系的安全。

利用QKD网络为各通信节点以信息论安全方式分发的密钥，可以实现高安全性的鉴权、加密和完整性保护功能，增强对关键信息基础设施的保护。

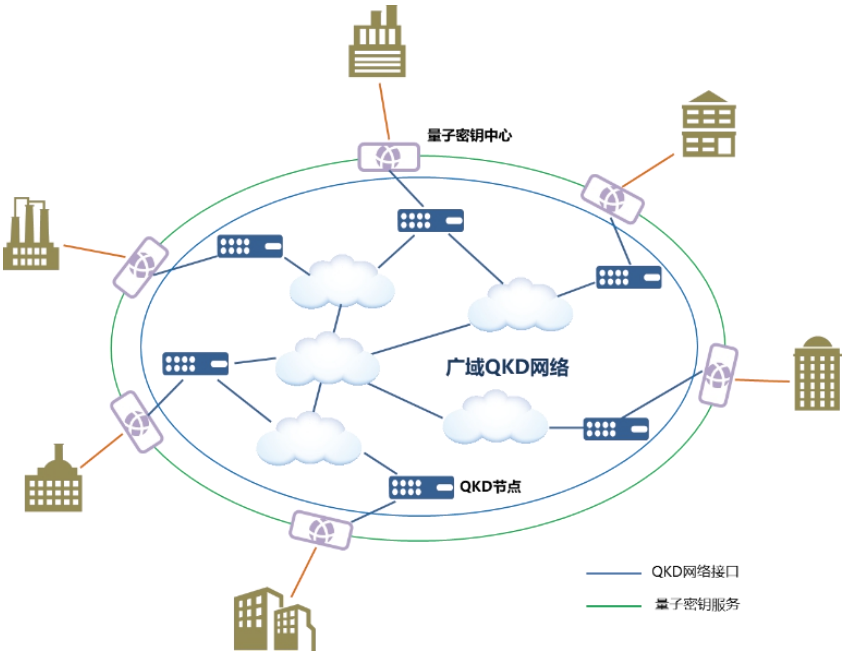

图4 关键信息基础设施通信安全场景

通过构建专用的广域QKD网络，提供多节点的密钥分发管理、密钥中继转发等功能。业务使用方通过专用接口访问QKD网络，利用QKD网络为通信双方分发的密钥进行数据加解密操作。

5.2 移动终端加密通信

量子保密通信技术可以实现加密语音电话、视频电话以及数据通信，满足党政军等具有高安全等级机构的要求。通过将QKD系统产生的量子密钥配置于移动终端，能够使终端用户使用达到信息论安全的量子密钥，从而确保移动终端保密通信达到更高等级的安全性，防止敏感信息泄露。

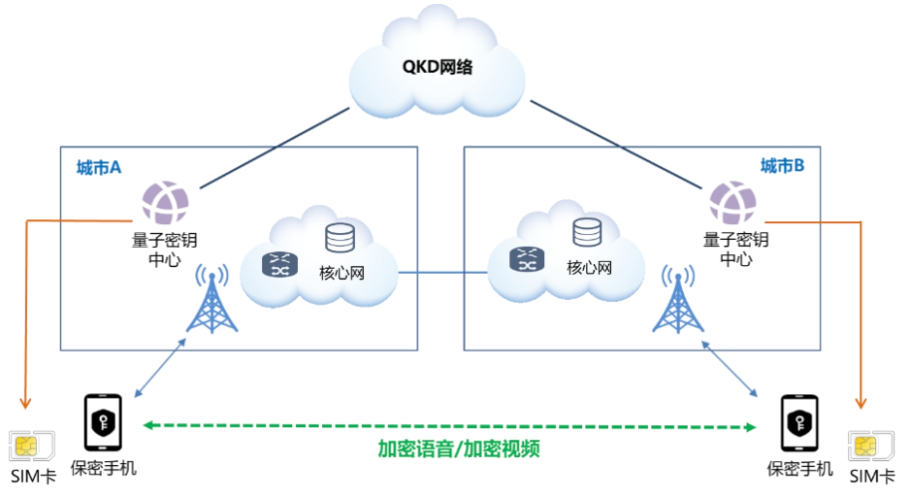

图5 移动终端加密通信应用场景

量子加密通信终端将依托移动通信网络，通过4G/5G网络接入，面向政企等行业用户提供全面、广泛网络覆盖的量子加密通信服务。基于用户通信终端量子安全SIM卡，实现终端认证，语音、短信、多媒体等数据通信加解密服务。量子密钥中心为量子密话业务系统平台、终端用户提供全天候量子密钥综合保障；量子密钥来源于量子通信网络、量子随机数发生器等。

以量子VoLTE加密通话为例，其主要由量子密码服务中心与VoLTE加密通信系统两部分组成。其中量子密码服务中心以量子随机数发生器为基础构建，依托安全能力平台提供量子密码的集中服务。VoLTE加密通信系统为通话主被叫双方使用量子密钥对语音信息进行加密保护，具有直接入密、带内密钥协商、一话一密、端到端加密、量子密话显性、国密SM2/SM3/SM4/ZUC算法等技术优势。

量子VoLTE加密手机终端含贴芯密码卡、量子密管家APP等模块。贴芯密码卡支持量子密钥安全存储、密码算法安全运算等功能，确保密码本地安全；量子密管家APP软件实现密码卡在线管理，支持用户-密卡绑定、远程销毁等功能，确保密码应用安全。

5.3 量子安全对讲

量子安全对讲是融合集群调度、多媒体视频实时对讲能力，全网统一运营管理的公网加密对讲产品。依托移动通信网络，面向用户提供无距离限制、安全可靠、低时延的高清视频对讲服务。量子安全对讲系统具备灵活组织架构管理、地图可视化调度、深度融合用户工作流程等优势，采用量子密钥分发技术与对讲终端、业务系统深度融合，满足特殊用户及业务场景在网络安全、数据安全等方面的加密与认证需求。

图6 量子安全对讲应用场景

量子加密对讲可应用于4G/5G网络环境，支持对讲群组语音、视频等数据加密与认证，采用主管部门认证的密码算法及产品，提供商密级的加解密与远程管理安全服务。

5.4 量子安全视频

量子安全视频是指将基于量子密钥的密码技术广泛应用于视频数据的加解密，如保密视频会议、视频监控加密、保密视频指挥等场景。通过量子密钥服务中心，将量子密钥向视频终端延伸，利用基于量子密钥的密码技术，保障终端的接入安全和视频数据的传输安全。

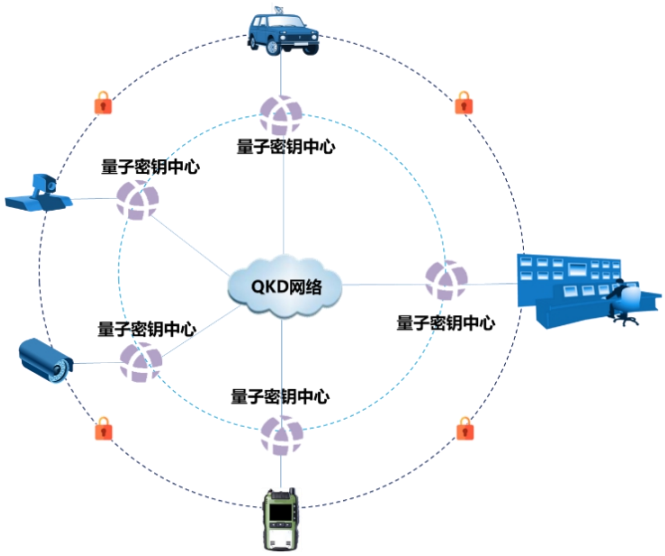

图7　量子安全视频应用场景

5.5 量子安全物联网

量子安全物联网是指将基于量子密钥的密码技术与物联网芯片融合形成量子安全物联网芯片。量子安全物联网芯片支持e-SIM功能提供NB-IoT通信服务，并且支持国密算法，结合量子密钥形成量子加密通信能力，为物联网终端和应用提供量子安全保护。

量子安全物联网芯片可以广泛应用于物联网燃气表终端、物联网水表终端、物联网电表终端等各行业应用的物联网终端中，通过量子密钥管理平台为量子安全物联网芯片提供量子密钥管理以及充注更新服务，物联网终端向物联网应用系统传输的数据通过量子安全物联网芯片实现数据的量子加密，使得传输的用户数据得到更加安全的保障。

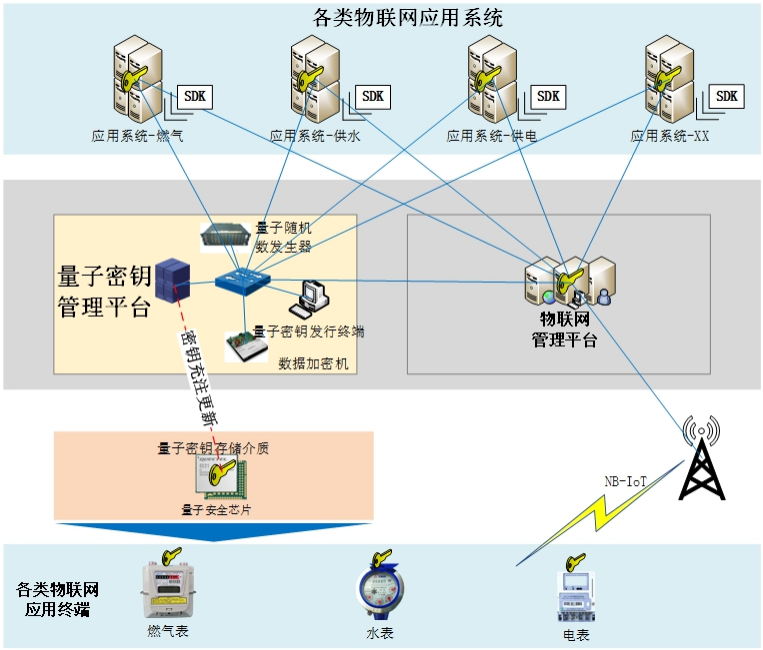

图 8　量子安全物联网应用场景

5.6 数据容灾备份

在相隔较远的两地建立两套或多套功能相同的IT系统并对重要的数据信息进行安全存储及备份，实现系统及数据的灾备是保障信息系统安全的重要手段。数据容灾备份过程中，主站点与备份站点之间的通信要求严格的数据保密性，可使用量子保密通信技术建立加密通信链路，并通过QKD技术按需更换密钥，保证数据备份传输时的安全性。

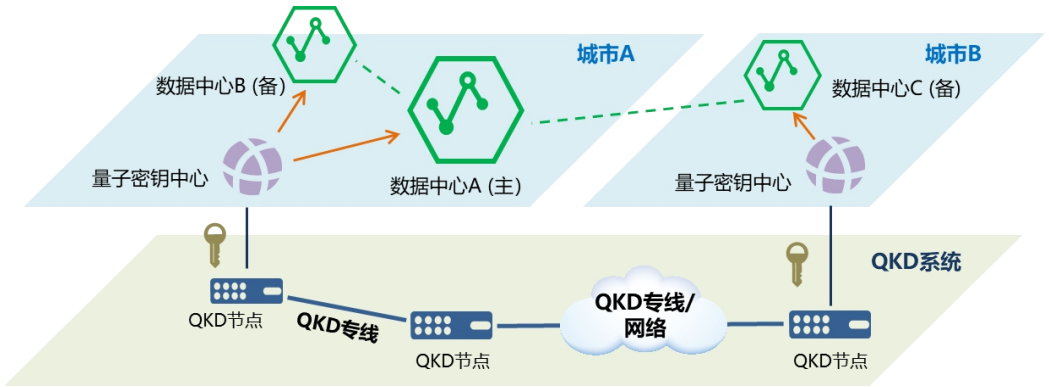

图9　数据容灾备份应用场景

6 推进建议

面向国家“十四五”量子信息重点科技战略布局，探索量子技术典型应用场景、产业发展趋势、核心关键技术，开展测试验证及应用实践，促进量子信息技术与移动通信网的融合创新，量子“Q波”推进如下：

2022年：开展关键技术及应用试点

结合政策引导，与产业各方合作，探索量子密钥分发技术在传统通信基础设施的应用，开展试验网建设，探索产品化能力。联合科研院所进行原型系统的研发、测试和验证，促成物理层密钥生成技术有效落地。

2023年：推进专用芯片研发、完善标准体系

加快推进量子密钥分发技术专用芯片和模组的研发，支持量子“Q波”的产业化发展。同时，积极推动量子保密通信全产业链基础共性、互联互通、行业应用等方面标准制定，以标准化促发展，为量子保密通信产业规模化发展提供支撑。

2024年：加强市场推广、打造融合创新应用

发挥运营商平台优势，通过技术、产品、测评、服务等能力，推动量子保密通信做深做细，扩大市场应用规模，为客户提供量子安全保障。打造“量子+ICT”融合的创新应用，打通跨领域、跨行业应用，提升量子安全能力覆盖与服务范围。

缩略语列表

缩略语	英文全名	中文解释
4G	4th Generation mobile network	第 4 代移动通信网
5G	5th Generation mobile network	第 5 代移动通信网
AES	Advanced Encryption Standard	高级加密标准
DH	Diffie-Hellmen	迪菲-赫尔曼密钥交换算法
ICT	Information and Communications Technology	信息通信领域技术
LTE	Long Term Evolution	长期演进
MD5	Message Digest Algorithm 5	消息摘要算法 5
NB-IoT	Narrow Band Internet of Things	窄带物联网
QCI	Quantum Communication Infrastructure	量子通信基础设施
QKD	Quantum key distribution	量子密钥分发
QRNG	Quantum Random Number Generators	量子随机数发生器
RSA	Rivest- Shamir- Adleman	李维斯特-萨莫尔-阿德曼
SHA1	Secure Hash Algorithm 1	安全散列算法 1
SHA256	Secure Hash Algorithm 256	安全散列算法 256
SHA512	Secure Hash Algorithm 512	安全散列算法 512
SIM	Subscriber Identity Module	用户识别卡
SM2/3/4	Shang Mi 2/3/4	商用密钥
TF	TransFlash	闪存
USB	Universal Serial Bus	通用串行总线
USIM	Universal Subscriber Identity Module	全球用户身份模块
VoLTE	Voice over Long-Term Evolution	长期演进语音承载
Wi-Fi	Wireless Fidelity	无线联盟
WLAN	Wireless Local Area Network	无线本地网络
ZUC	Zu Chongzhi	祖冲之算法