量子城域网网络架构及应用研究

朱雁平
中电信量子信息科技集团有限公司　安徽　合肥　233000

摘　要：量子信息技术将在多个领域产生基础性甚至颠覆性的重大影响，成为未来科技产业发展和关注的焦点。我国对量子信息技术发展与应用高度重视，已在多个城市完成量子城域网建设并投入使用。文章解读了量子城域网中应用到的量子密钥分发技术，分析了量子城域网运用的组网架构，比较了量子通信与经典通信的工程建设，介绍了量子城域网典型的项目案例应用，并对量子城域网及量子信息技术发展做出总结和展望。

关键词：量子城域网；量子通信；网络架构；量子密钥分发

1 引言

信息化时代网络安全关乎国计民生，网络空间成为陆、海、空、天之外的第五疆域，保密通信技术的发展对网络安全保障意义重大。随着现代计算能力的不断演进，特别是未来量子计算机的发展，通过数学加密保证信息安全的经典通信保密安全性受到了极大威胁。研究表明，如今广泛使用的公钥密码系统（如RSA和椭圆函数法）在面对量子计算机时完全行不通，而对称式密码的安全性则有所降低，例如高级加密标准（AES）需要延长密码的长度，以便在同等程度上获得安全保障。安全传输技术已经成为科学家们在对抗量子计算攻击方面的重要课题。

以量子力学为主要特征的量子保密通信为信息的安全传输打开新局面，通过量子态进行密钥的协商和信息传输，并且可以利用量子原理及时发现窃听行为，从而使窃听者不能获取信息，确保信息安全。量子密钥分发技术已经实现了阶段性的实用化和产业化，典型应用可大致分为量子骨干网和量子城域网。本文将重点讨论量子城域网网络架构及应用研究。

2 量子密钥分发技术介绍

与传统的通信和加密技术不同，量子密钥分发的基础是量子力学基本原理，同时需要借助量子态实现信息的表示、传输、测量等操作，这使得它能够抵御物理上窃听者的任何破译技术和计算能力的攻击，具有理论上可证明的安全性，且与计算复杂度无关。因此，量子密钥分发可承受包括量子算法在内的任何通道攻击，同时量子态的测量塌缩、不可克隆等特性使得量子密码也具有窃听可侦性，其物理特性预示着量子密码的应用前景十分广阔。

量子密钥分发的安全性基于物理原理，其基本方法是通过制备、传输和检测量子状态，利用量子态对信息进行编码，从而实现随机数字的安全分发（即密钥）的目的。对于量子态编码、传输和测量方法的规定，称为量子密钥分发协议。

量子密钥分配协议有很多，大体都是依据以下量子物理学原理来保障安全：

（1）单量子不可再分。量子（Quantum）是物理量变化的最小单元，单个量子是不可分割的。量子密钥分发如果采用单个量子（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（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。如果攻击者将一个量子重新制备后，按照测量结果发送给接收方，那么单量子状态必然会发生改变，这就会导致解码结果与编码不一致。量子密钥分发双方通过检测误码率以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，任何未知的单个量子中，不存在获得精确一致拷贝的方法。当量子密钥分发双方随机调制单量子态时，如果攻击者在侦听到量子信号后试图复制多个拷贝， 必然会造成复制态与初始态之间的偏差，进而导致解码结果与编码不符，量子密钥分发双方可通过侦测发现和后处理上进行消除。

3 量子城域网架构分析

量子城域网从整体架构上分为业务平面、承载平面、管理平面、安全平面四个平面。

（1）业务层面：该层为量子网络的核心，负责量子密钥的分发业务，主要包括量子密钥管理系统和量子密

钥分发系统两个部分。

图1 量子城域网系统架构示意图

（2）承载层面：该层主要包含IP承载网和传输网，其中，量子城域网站点较少、业务量小，可不涉及传输网，后期量子城域网随着站点规模的增加和网络覆盖的扩展，可根据需要引入传输系统。

（3）管理层面：该层主要包含对承载层面、业务层面、安全层面的管理，具体包含传输网管系统、数通网管系统、安全管理系统、量子网管系统等各类管理系统。实现对业务、系统、网元的统一管理。

（4）安全层面：该层主要涉及安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心五方面的内容。

4 量子城域网组网及应用分析

量子城域网以量子密钥分发技术为核心，与传统通信网络相结合，构建面向政务业、金融、交通、工业等需求客户的城市级量子通信基础设施，实现敏感信息传输、关键数据存储等业务安全服务。量子城域网实际上是通过构建覆盖全城的量子密钥分发网和传输通信网，实现基于量子安全技术的高等级安全通信服务。针对政务、国防、金融企业、驻外机构实际业务需求，提供敏感信息加密传输、关键数据加密存储等服务。

量子城域网根据网络划分可分为量子城域接入网和量子城域核心网。量子城域接入网主要由靠近用户的用户站组成，可实现与上联的接入站协商生成量子密钥，提供量子密钥给量子安全加密设备，实现业务数据加解密。量子城域核心网分为接入站、中继站和集控站，其中接入站是用户站的接入节点，可连接城域集控站、中继站或接入站节点；中继站作为量子城域网环路扩大的功能站点，连接集控站和接入站，实现城域网的密钥中继功能；用户站可实现与上联的接入站协商生成量子密钥，提供量子密钥给量子安全加密设备，实现业务数据加解密的节点。

在量子保密通信的实际城域网络应用中，要想实现量子加密，需要建立量子密钥分发网络，解决不同规模、不同用户的应用需求。根据不同的量子城域网需求场景和服务对象，其组网方式会有对应的解决方案。

4.1 小型量子城域网

小型量子城域网以点对点组网方式为主。典型的应用场景是在不同数据中心之间进行同城灾备、数据备份和业务连续性等业务，利用量子保密通信保障数据中心之间的数据传输安全。

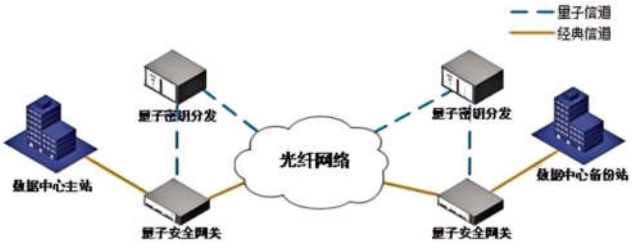

图2 小型量子城域网组网方式

4.2 大/中型量子城域网

大/中型量子城域网适用于多用户的行业组网，典型应用是政企专网，政府机构为了提供高度的机密性、完整性和真实性，通常要求通信服务必须强制采用专用安全系统。目前一般采用基于IPSec或TLS的安全虚拟专用网络（VPN）技术来对数据中心与分支机构之间的流量进行鉴权和加密，QKD系统可采用星形的组网方式，QKD链路加密机可结合这些技术，满足各站点间的信息加密需求。当然，结合城市间通信距离的需求，也可以分区域采用混合组网方案。

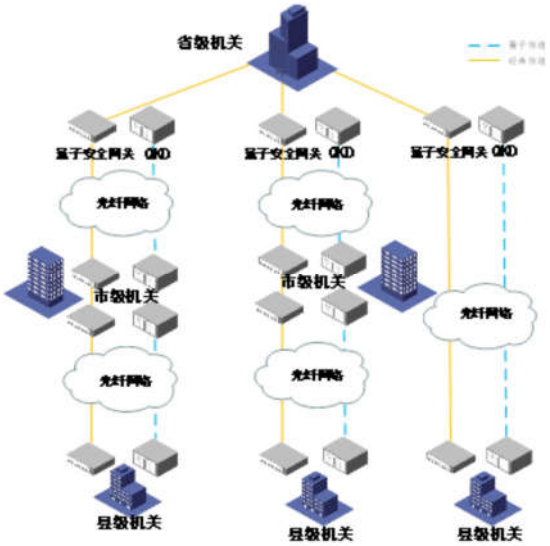

图3 大/中型量子城域网组网方式

4.3 基于QKD+OTN的量子城域网

基于传统OTN光网，融合量子密钥分发技术，构建安全可信的新型抗量子计算信息基础设施，打造超高安全的OTN专线增值业务和新型量子城域网解决方案。该

方案将OTN光网与量子密钥加密机制和算法相融合，进一步增强OTN精品专线的安全性能，不仅使其成为业务专线市场上高品质OTN光网加持量子加密通信的重要尝试，而且大大降低为开通量子专线而单独建设网络路由的投资。

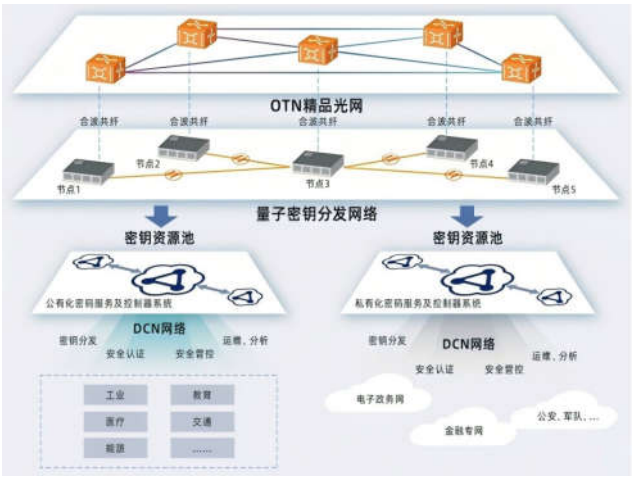

图4 基于QKD+OTN的新型量子城域网解决方案

4.4 量子城域网的典型案例

作为率先部署量子保密通信网络的国家，我国主要由专业的量子保密通信网络运营商为各行业的客户提供稳定、可靠的量子安全服务，以促进量子保密通信网络发展和产业链成熟。依托国家广域量子保密通信骨干网，我国在合肥、上海、武汉等多个城市部署了量子城域网，推动量子密钥分发网络技术在多用户组网、实际应用、经典光网络融合等方面不断发展，为大规模应用打下良好基础。未来我国量子城域网将会以骨干网沿线为主，逐步向西南、中西部地区城市建设量子通信城域网。

（1）合肥量子城域网。由中国电信承建的合肥量子城域网是目前国内量子保密通信城域网中规模最大、用户最多、应用最全的城域网。合肥量子城域网包含8个核心环网站点和159个接入环网站点，网络光纤全长1147公里，为市区两级近500家单位提供了量子安全接入服务。该网络成为实用化量子保密通信网络的标杆案例，提升了城市整体信息安全，形成量子通信应用的“合肥模式”。

（2）上海量子城域网。上海量子保密通信应用示范网包括8个汇聚节点、29个接入节点，覆盖工商银行、中国银行等17家金融用户单位，实现量子保密通信的同城数据灾备和安全传输、企业网银量子保密通信安全传输应用以及多点高清量子保密通信视频会议通话等应用，为金融机构提供高安全等级的数据服务。

（3）武汉量子城域网。武汉量子保密通信城域网包括1个可扩展的展示中心、1个大型集控站、1个大型可信中继站、9个可信中继站和60个用户节点。该网络覆盖全市重要数据中心和核心部门，以量子政务为抓手，确保武汉智慧城市应用核心数据传输安全。

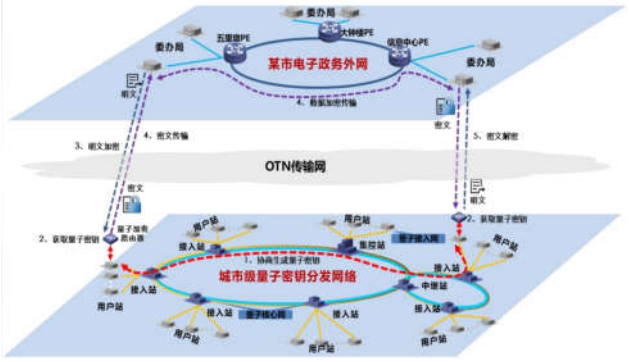

图5 合肥量子保密通信城域网

5 总结与展望

对于事关国计民生的各行业各领域信息安全而言，量子保密通信网络的建设和应用，能够为广大用户提供量子安全服务，抵御经典破译和未来量子计算的挑战，具有极大的现实意义和极高的战略价值。尽管量子城域网方面已经进入实用化阶段，但其基于量子密钥分发和量子保密通信技术的应用范围和技术影响力仍然受到限制。面对后量子安全加密技术的竞争，量子保密通信城域网和长距离传输工程组网的应用仍有待进一步探索和提升，其大规模商业化应用价值仍需进一步挖掘。未来，量子信息技术的发展和应用需要在国家顶层规划上制定量子信息技术领域的整体发展战略，推出总体发展规划，有效引导和推动相关研究与应用的发展，将政策支持优势转化成为核心工程技术优势，实现量子通信技术创新和可持续发展。

参考文献

[1]龙桂鲁,潘栋.量子直接通信研究进展[J].电信网技术,2021,000(007):1-7.

[2]崔智.量子通信技术发展现状及应用研究[C].北京通信学会,2016.

[3]唐建军,李俊杰,张成良,等.开放型量子保密通信系统架构及共纤传输技术研究与实验[J].电信科学,2018,34(9):28-36.

[4]王向斌,尹浩,马怀新,等.量子保密通信的技术现状及安全性[J].物理,2006,35(2):125-129.

[5]罗俊,刘驰,王丙磊.融合量子密钥分配的电信运营商密码应用体系[J].电信科学,2023,39(01):136-145.

[6]王天琪.量子安全技术[M].中山大学出版室,2023,5.