量子保密通信关键技术及组网应用探讨

Discussion on Key Technologies of Quantum Secure Communication and Networking Application

李文华[1]，袁夕征[1]，熊晓然[2]（1. 北京电信规划设计院有限公司，北京 100048；2. 北京邮电大学，北京 100876）
Li Wenhua[1], Yuan Xizheng[1], Xiong Xiaoran[2]（1. Beijing Telecom Planning & Designing Institute Co., Ltd., Beijing 100048, China; 2. Beijing University of Posts and Telecommunications, Beijing 100876, China）

摘　要：
基于量子密钥分发（QKD——Quantum Key Distribution）的量子保密通信为信息通信和安全领域提供了新的发展方向，获得了广泛的关注和显著的成效。以量子保密通信的关键技术为基础，结合量子保密通信组网架构的设计及应用实例，对量子保密通信组网应用进行探讨，为进一步拓展量子保密通信的组网应用提供重要的参考价值。

关键词：
量子密钥分发；量子保密通信；组网应用
doi：10.12045/j.issn.1007-3043.2019.02.013
中图分类号：TN914
文献标识码：A
文章编号：1007-3043（2019）02-0069-07

Abstract：
Quantum secure communication based on quantum key distribution（QKD） provides a new development direction for information communication and security, and has gained wide attention and remarkable results. Based on the key technologies of quantum secure communication and the design of quantum secure communication network architecture, it discusses the application examples of quantum secure communication networking, and provides important reference for expanding the application of quantum secure communication.

Keywords：
Quantum key distribution; Quantum secure communication; Network application

引用格式：李文华，袁夕征，熊晓然. 量子保密通信关键技术及组网应用探讨[J]. 邮电设计技术，2019(2)：69-75.

0 引言

量子保密通信在保障通信安全方面具有巨大的优势，在国防、政务、金融等部门中具有极其重要的应用价值。量子保密通信技术主要是基于量子密钥分发技术（QKD），为传统信息安全技术的发展提供新的发展方向。不同于经典信息，量子通信的基本信息单元是量子比特，对量子比特的处理过程遵从量子力学的规律。将量子密钥分发与当代信息通信技术相结合的量子保密通信是一种实现数据高安全传输的新兴信息安全技术。

量子密钥分发技术以量子物理基本原理做保障，可以在公开信道上无条件安全地分发密钥，从原理上保证了一旦存在窃听就必然被发现。一旦在通信双方成功建立了密钥，这组密钥就是安全的，而且这种具有绝对随机性的密钥从原理上是无法被破解的。因此，量子保密通信被认为是保障未来通信安全最重要的技术手段之一，具有十分重要的经济价值和战略意义[1]。

量子保密通信网络组网是量子通信技术中的重要支撑，随着该项技术的成熟发展和在我国网络应用规模上的不断扩大，也为我国抢占国际信息安全技术

收稿日期：2018-12-02

的制高点打下坚实的基础；量子保密通信网络对保障我国通信安全具有十分重要的意义。这里将对量子保密通信的原理技术及实际应用进行详细讨论，通过将量子密钥分发应用于量子保密通信组网中，进一步分析量子保密通信的组网应用，并为其提供更多参考价值，从而使之适用于更广泛的应用场景。

1 量子保密通信的技术原理

1.1 基本原理

量子保密通信是基于量子密钥分发的密码通信解决方案。量子密钥分发就是用量子信息给经典信息加密后，用经典信道传递加密后的信息，再用量子信道传递密钥。只要因果律成立（无法超光速通信），量子密钥分发的安全性就可以得到严格证明，其安全性原理如下。

a）单光子不可再分原理：量子密钥分发采用单个量子（通常为单光子）作为信息载体。由于单光子是构成物质的基本单元，是能量和动量的最小单元，不可再分，因此窃听者无法通过窃取半个光子并测量其状态的方法来获得密钥信息。窃听者可以在截取单光子后，测量其状态，然后根据测量结果发送一个新光子给接收方。但根据量子力学中的海森堡测不准原理，这个过程一定会引起光子状态的扰动，发送方和接收方可以通过一定的方法检测到窃听者对光子的测量，从而检验他们之间所建立的密钥的安全性。

b）量子不可克隆原理：窃听者也试图在截取单光子后，通过复制单光子量子态来窃取信息。但量子力学中的不可克隆原理保证了未知的量子态不可能被精确复制，量子一经测量便会改变它原有的形态。采用光子偏振或者相位进行编解码，均可以实现BB84协议。

c）“一次一密”安全传输：按照BB84协议，每一个光子随机选择调制的基矢，接收端也采用随机的基矢进行监测。当发送与接收端选择的基矢一致时，接受到的信号被认为是有效的而被纪录，如果选择的基矢不一致，则数据被丢弃。这样就可以保证发送与接收方获得了一致的随机数序列，从而可以实现“一次一密”的绝对安全通信。

1984年，Benett与Brassard提出的首个量子密钥分发协议（BB84协议）是目前最重要的量子保密通信协议[2]。BB84协议中使用光子的水平偏振态、垂直偏振态和±45°偏振态来实现编码。如图1所示，发送端

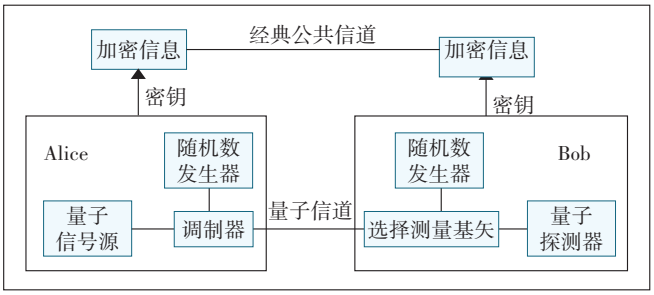

图1 BB84协议示意图[4]

Alice主要由量子信号源、调制器、随机数发生器等部件构成，根据随机生成的二进制数串，生成不同的偏振态单光子作为发送的量子比特。接收端Bob通过量子信道接收单光子信号，随机选择基矢对光子进行测量，并将测量基矢通过经典信道告知Alice，双方保留基矢相同的部分；最后，双方再通过公开一段量子密钥，来估计误码率和可能的窃听者Eve的存在，最终Alice和Bob共同产生量子密钥[3]。

原始BB84协议要求使用单光子源进行量子保密通信才能实现无条件安全性[5]。然而目前单光子源技术还不够成熟，无法大规模应用。在实际应用中，一般采用常见的激光光源等含有多光子的光源进行密钥分发，存在严重的安全性隐患。窃听者可以采用光子数分离攻击（PNS——Photo-Number-Splitting Attack）得到具体的密码。

PNS过程的原理如图2所示，窃听者Eve对于Alice所发射的脉冲进行光子数测量。如果是1个光子，那么Eve则吸收该光子；如果光子数大于1，那么Eve从中分离一个光子给自己，其余的光子通过一个低损耗或者无损耗通道发射给Bob。那么Eve和Bob手中所具有的光子将完全一致。并且对于目前技术，Alice传递一个弱相干态，通道往往是大损耗的。Eve完全可以将他的光子数分离攻击伪装成通道的损耗，而使得Bob完全无法发现有Eve的存在，此时双方通信则完全不安全[6]。

为了避免这种攻击，在正常通信的光信号中随机

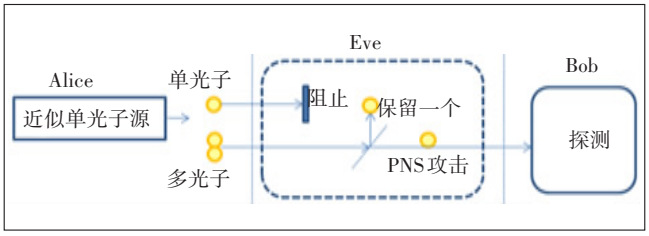

图2 PNS攻击原理示意图

掺入部分强度不同的光信号（即诱骗态信号），通过分别测量不同强度光信号的错误率实现对于窃听者（Eve）的检测，从而保证量子保密通信的安全性。目前，诱骗态BB84协议是各量子密钥分发协议中实用化程度最高、性能最好、安全性分析最深入全面的协议[7-9]。

1.2 关键技术

为了在实际应用中可以达到量子密钥分发系统功能与性能的指标，一般通过以下关键技术来实现。

a）高性能诱骗态光源产生技术。高速诱骗态光源是目前实用化的无条件安全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。为了实现诱骗态方法，光源随机地改变输出脉冲强度[10-12]，同时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。

b）高性能近红外单光子探测技术。单光子探测系统是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，其性能提升可以提高通信网络的容量，扩展通信网络的通信速率。当前，国际上通用的通信波段单光子探测器有3类：超导探测器、铟镓砷雪崩二极管单光子探测器和上转换探测器。

c）高性能偏振反馈补偿技术。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。高速偏振反馈补偿技术可以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。目前已研发的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。

d）高性能时间相位编码技术。相比偏振编码而言，相位编码量子保密通信系统能够容忍更大的信道扰动，但不足的是，相位编码系统较低的成码率严重限制了量子保密通信网络的性能。时间相位编码量子保密通信系统，可以有效结合传输效率高和信道扰动容忍高的优势，提升量子保密通信系统的综合性能。

e）量子信道的波分复用技术。波分复用是提升系统传输速率的有效手段，并在经典光通信中广泛应用。波分复用过程中，额外的插入损耗是限制系统最终性能的重要指标。使用波长通道数越多，插入损耗越大，量子保密通信具有明显差异。为了保证通信安全，量子保密通信要求出射光脉冲强度为单光子量级，不能通过提高发射功率抵消波分复用器件的插入损耗，系统的密钥成码率将受此影响有所下降。

f）城域网共纤技术。城域网的量子密钥分发系统采用共纤传输方式，用于量子保密通信和经典通信的复用，信号传输方向为二者同向。量子通信网络对信道的要求包括量子信道要求、协商信道要求、共纤传输时的信道要求。量子信道的基本原则要求是退相干效应很小，能保持量子态的远距离相干传输；协商信道主要要求满足QKD设备的带宽和延时的需求；共纤传输时的信道一般利用波分复用技术实现共纤传输。

2 量子保密通信的组网架构

目前尚无标准化、统一化的QKD网络架构，业内通常采用的架构一般包括物理层、传输层、网络层、密钥管理层和应用层，其组网架构如图3所示。

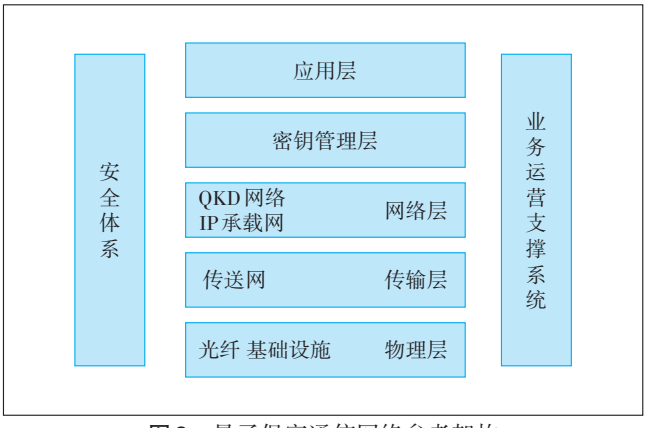

图3 量子保密通信网络参考架构

其中，网络层主要包括QKD网络和经典数据通信网络。QKD网络是利用量子密钥分发技术，实现2台量子保密通信终端间的安全、高效的密钥共享的网络；经典网络即传统的数据通信网络，实现设备间的数据传输。密钥管理层是利用可信中继技术、经典网络通信技术和网络管理技术等实现大规模、跨地域的安全、高效的密钥分发与管理，实现在不同区域的2台量子保密通信终端间的安全、高效的密钥共享。应用层是使用支持采用量子密钥对数据传输进行安全保护操作的量子加密终端或模块实现数据的安全传输。业务运营支撑体系是围绕量子保密通信网络运营特征及需求，建设由业务支撑系统（BSS）及运营支撑系统（OSS）组成的一体化业务运营支撑系统，实现对网

络设备的配置和运维、业务的开通和运营。安全体系主要包括与量子保密通信相关制度体系和安全体系建设。

2.1 组网的功能模型

综合目前量子保密通信网络的现状，并考虑网络架构的设计需求以及未来的发展，可以建立如图4所示的网络功能模型。

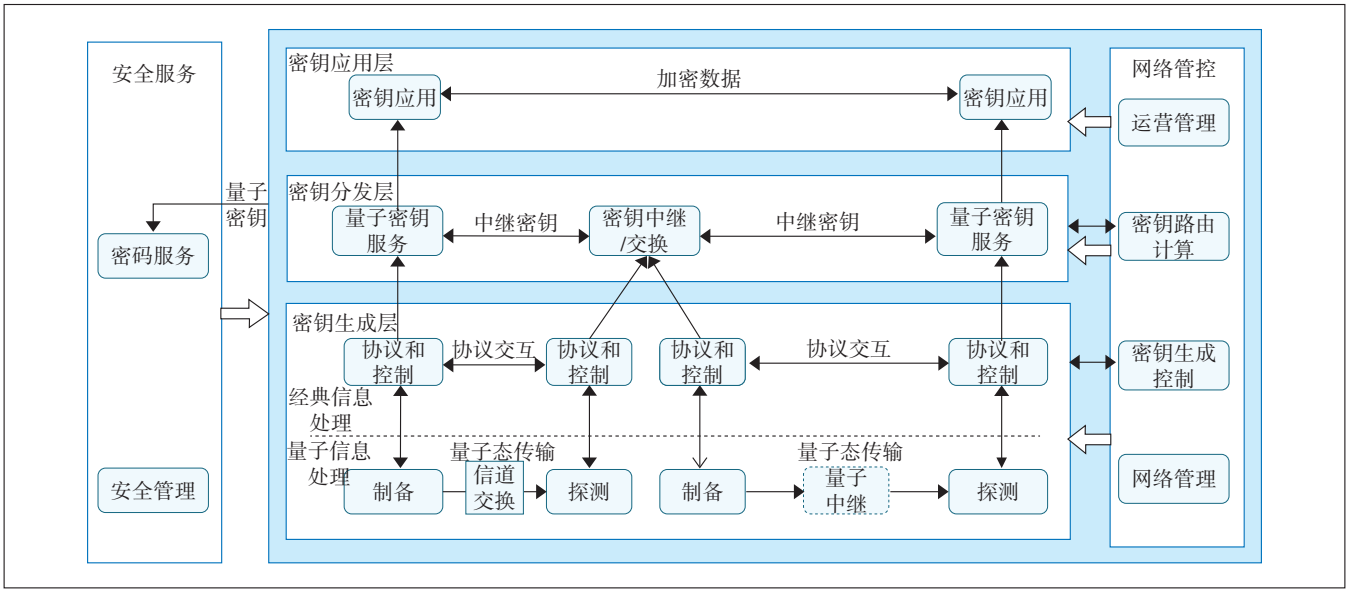

图4 量子保密通信网络功能模型

最底层，是量子保密通信网络的技术基础。密钥生成层既进行量子信息的处理也进行经典信息的处理。

量子信息的处理包括：量子态制备、量子态探测、量子信道交换、量子中继等功能。

a）量子态“制备”模块依据量子密钥分发协议（如BB84协议）完成光量子制备及发送。

b）量子态“探测”模块接收对端发送的光量子，依据量子密钥分发协议完成量子态解码及光子的探测。

c）量子“信道交换”模块，接收网络管控的控制，实现量子信道的切换。

d）“量子中继”模块，负责量子态的中继传输，基于纠缠交换的量子中继技术，通过多次纠缠交换实现远距离的纠缠分发，从而为量子密钥分发建立量子信道。量子中继技术在未来可以广泛应用，从而协助或者部分替代量子密钥分发层中的密钥中继功能。

密钥分发层处于量子保密通信网络三层结构的中间层，密钥生成层和密钥分发层的交互主要作用是将密钥生成层产生的量子密钥安全保密地传输给密钥分发层。其主要功能包括密钥中继、密钥转发（交换、路由）功能以及密钥存储和密钥输出等量子密钥服务等。密钥中继是指在网络中，通过直接中继站为2个远距离节点之间进行量子密钥的中继，将一端节点的量子密钥分发到对端节点的过程；密钥转发是指在量子保密通信网络的复杂拓扑中，将量子密钥数据有路由选择的分发到远端，形成点对点量子密钥。密钥存储是对接收到的密钥生成层上传的量子密钥，以及密钥中继和密钥转发的量子密钥，进行两端量子密钥管理设备的信息同步，并安全地存储到设备内部的存储器。密钥输出主要是面向密钥应用层输出安全一致的量子密钥，供应用业务使用量子密钥为用户提供安全服务。

密钥应用层处于量子保密通信网络三层结构的最上层，是量子密钥最终应用的位置。密钥应用层包含用户的密钥管理系统、各种量子密钥应用设备以及相关的数据传输网络。

网络管控平台主要包括运营管理、网络管理、密钥路由、密钥生成控制等功能。其中运营管理、网络管理等功能和经典网络的相关功能类似。安全服务平台包括密码服务和安全管理两大系统。密码服务为量子保密通信网络需要使用密码的功能如认证、加密、签名等提供密码服务；安全管理主要负责入侵检测、访问控制、病毒防护、安全态势等安全管理功能。

2.2 组网应用的相关技术

量子保密通信网络的组网技术的主要目标将量

子密钥分发设备的链路密钥分发能力扩展为可以覆盖广域地区的密钥分发能力，实现整个量子保密通信网络中任意两设备之间都可以获取量子密钥，并用于业务数据加密或者数据鉴权、身份认证等应用。在实际的量子保密通信组网中应用的关键技术主要包括：

a）动态密钥中继路由技术。该技术通过中心路由服务器实时收集网络中设备的运行状态、密钥量状态以及设备间链路的状态，对全网的密钥中继过程的传输路径进行规划，按照路由计算策略找到最优的可用路径，并下发到各节点的密钥管理机，由密钥管理机按密钥中继路由指引进行密钥中继业务。

b）分层次和分区域管理的组网技术。集中规划式动态路由可以实现同一网络中的路径保护功能。大规模网络将采用分区域建网、独立控制的方案，将量子保密通信网络的组网层次划分为国家级干线、省级干线、市级接入3级。量子保密通信网络中密钥中继业务依照设备的ID进行路由寻址，在环网组网方案中依照区域划分来规划设备ID。

c）高性能路由规划。量子密钥中继路由变化频率快，密钥中继路由要求随着密钥量的变化实时更新，更新频率相对较高，导致对路由计算的实时性要求比较高。量子保密通信网络建设成为环网链路拓扑后，随着网络规模扩大以及干线沿线更多接入网的建设，全网密钥路由的计算压力成倍增加，需要在支持大数据量密钥路由计算的同时，也能给出快速的路由变更响应速度。

d）跨域组网认证技术。为实现在广域网络中节点间的密钥中继分发，在应用层设备和密钥生成设备之间需要添加密钥管理系统。密钥管理系统位于量子保密通信体系中的中间层，主要实现密钥中继分发流程、控制密钥生成设备的密钥生成流程、接收量子密钥进行存储，以及向应用层设备输出量子密钥。密钥管理系统由密钥管理机和密钥管理服务系统组成。实现与密钥管理服务系统的灵活组网，可以形成大中规模的城域网也可以满足小微型网络的部署要求。应用层设备与量子层设备通过密钥管理机接入，密钥管理机受辅助系统的管理和控制。

3 量子保密通信的组网应用实例

近年来，国内外已经建设了一系列的量子保密通信技术验证及商用网络，也先后开展多项重大技术研究[13-14]，下面分别从干线与城域的角度列举一些典型应用实例。

3.1 量子干线组网

3.1.1 京沪干线

“京沪干线”是连接北京、上海，贯穿济南和合肥全长2 000余千米的量子通信骨干网络，并通过北京接入点实现与“墨子号”的连接，是实现覆盖全球的量子保密通信网络的重要基础。

量子骨干网络由量子系统、平台系统、传输系统以及基础设施四大部分构成，其中量子系统主要由量子密钥分发子系统与量子密钥管理子系统构成；平台系统由数据通信系统、备份容灾系统、网络管理系统、安全体系、IP承载网以及业务运营支撑系统构成；传输系统采用100G光传输进行建设；基础设施主要由光纤信道、机房等构成。其中，承载经典网络信息流量光纤通道为全线贯通模式；承载量子信道的光纤只承载相邻两站点的量子信号，不会全线贯通。骨干系统物理架构及相互关系如图5所示。

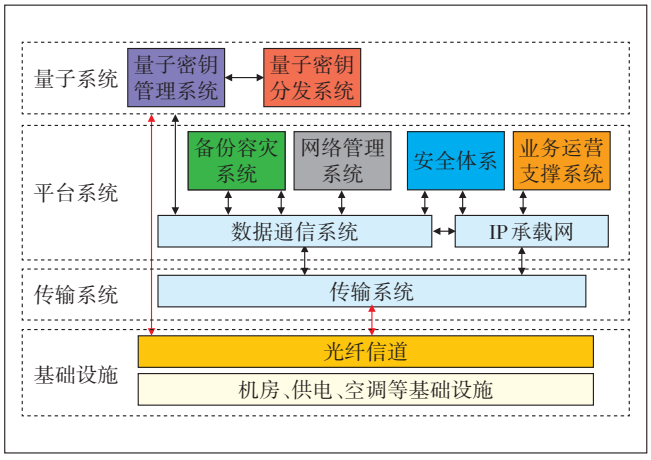

图5　骨干系统网络结构示意图

其中，量子密钥分发子系统由量子密钥分发设备发射端、量子密钥分发设备接收端、量子波分复用终端等设备及配套光纤资源构成。量子密钥分发设备按照包含诱骗态的BB84量子密钥分发协议，实现相邻两点间的量子密钥分发；量子密钥分发设备的发射端和接收端通过量子波分复用终端进行光路复用和解复用处理，实现量子信道同步光和信号光复用在同一根光纤中；量子密钥分发过程所需经典交互数据传输信道，由站点间的数据通信子系统提供；量子密钥分发设备由量子密钥管理子系统管理和控制。

量子密钥管理子系统由密钥管理机、密钥生成控制/中继路由系统构成。采取分区控制的方式，量子密

钥分发设备通过局域网与所属密钥管理机互联，进行密钥和信息的交互；量子密钥分发设备根据密钥管理子系统的密钥生成策略指令进行相应的量子密钥分发流程，并将生成的量子密钥输出到密钥管理子系统相应的密钥管理机设备进行管理和使用。

3.1.2 沪杭干线

全球首条量子商用干线——“沪杭干线”如图6所示，北起上海南至杭州，全长260 km，连接了长三角经济最为活跃的两大地区，它的开通标志着量子通信技术真正走向了产业化。这条绵亘于上海与杭州之间的城市保密通信动脉，其商业化应用主要体现在量子加密通话、异地灾备、政务公文传输等方面，通过量子技术给信息传输加上保密钥匙，为行业、企业等用户的信息安全保驾护航。

图6 “沪杭干线”路线示意图

随着“沪杭干线”应用的不断增多，应用过程中的反馈也将进一步促进“沪杭干线”服务的提升，在量子政务、量子金融、量子商务等领域更多的应用服务，为沿线地区的政府部门、金融机构或大中型企业提供基于量子安全的专网通信服务。

在我国，量子通信产业发展已逐步构建起长距离卫星传输、城市间干线传输、城市内部的城域网的“三位一体”量子通信网络大格局，在“沪杭干线”已全线贯通的背景下，量子通信干线和量子通信城域网以点线结合的方式，实现信息长距离和短距离传输的超安全保障，将成为全国量子信息骨干网络的重要组成部分。以“沪杭干线”为开端，在各行各业有志之士的努力下，量子通信产业化之花将开满神州大地。

3.2 城域网组网

2013年，东芝欧洲实验室完成了利用分光器件实现时分复用的1点对多点的量子密钥分发试验。实验原理如图7所示，多路发射端通过一个1×N的无源分光器件连接到探测接收端。每一路发射端发射量子信号周期为1/N GHz，通过调节不同发射端发射信号的时间延迟，使得N路发射端的信号耦合后正好形成1 GHz的脉冲信号，可以由门控频率为1 GHz的单光子探测器探测。不同发射端发射的量子信号由时间位置可以区分，因此可以分别按时间位置探测，完成相应的密钥协商后处理过程，从而实现1对N的量子密钥分发。该实验展示了量子密钥分发和PON融合的潜力。

此外，由于当前量子设备的组网技术限制，国内目前一般采用如图8所示的城域网接入方案。当骨干站点与城域网相应集控站/汇聚站点位于不同物理机房，城域网接入需要在相应骨干站点增配量子密钥分发设备接收端，与城域网相应集控站/汇聚站新增的量子密钥分发设备发射端构建量子密钥分发双链路，实

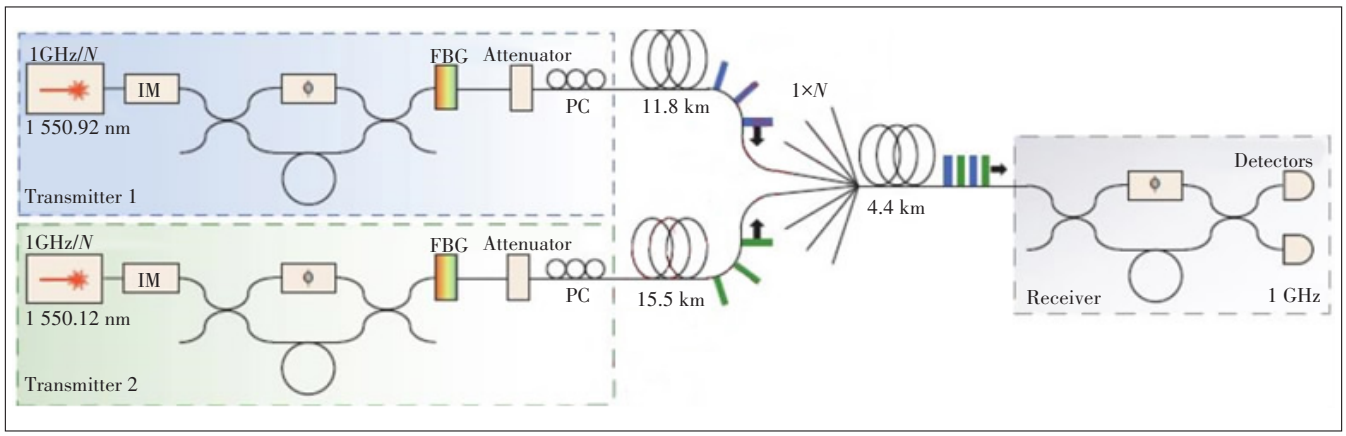

图7 东芝量子接入网实验原理图

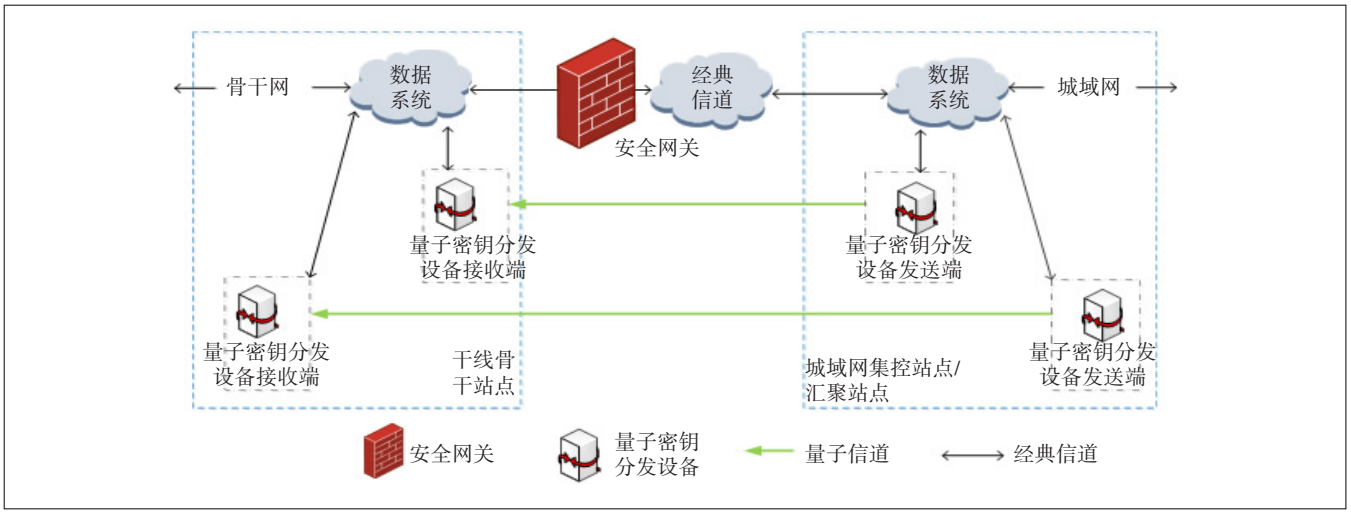

图8　城域网扩展接入

现城域网和干线的量子信道互联互通。经典信息的交互通过经典信道完成，经典信道通过部署安全网关进行网络边界安全管控。同步配置光纤资源。此种接入方案需要增配量子密钥分发设备，但城域网和干线网络的边界清晰，便于实行安全管控。

4 结束语

在未来的信息通信行业，量子保密通信将作为一个有望与国际高新技术领域发展同步的富有战略意义的制高点，成为未来的国家综合科技实力的主战场之一。基于量子保密通信技术的研究和应用将会受到越来越多的重视和关注。近年来我国量子保密通信技术的研究和发展较为迅速，进一步为量子保密通信组网奠定基础。量子保密通信作为从理论上保证信息传输绝对安全性的通信技术，是未来保障网络信息安全的有效解决方案之一。

本文详细探讨了量子保密通信的原理与组网技术，而后对量子保密通信组网应用进行了详细的分析，为量子保密通信网络的部署和应用提供重要的参考。量子保密通信技术有着广阔的应用前景，为未来信息通信行业提供更加安全的保障，将成为通信发展进程中一颗备受瞩目的新星。

参考文献：

[1] LAI JS, WU BB, LI SH, et al. Progress and security analysis of quantum cryptography communication [J]. Telecommunications Science, 2015, 31(6): 39-45.

[2] 艾祎，杜壮. 量子通信应用产业范围广泛[J]. 中国战略新兴产业，2016(19): 66-68.

[3] GISIN N, RIBORDY G, TITTEL W, et al . Quantum cryptography [J]. Reviews of Modern Physics, 2002(74): 145-195.

[4] 王磊，赵广怀，范晓楠，等. 量子保密通信在电网业务应用的方案研究与设计[J]. 电力信息与通信技术，2018, 16(3): 34-38.

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

[6] HU J. Quantum key distribution with the decoy-state method[J]. Scientia Sinica, 2011, 41(4): 459.

[7] HWANG WY. Quantum key distribution with high loss: toward global secure communication[J]. Physical Review Letters, 2003, 91(5): 057901.

[8] WANG XB. Beating the photon-number-splitting attack in pratical quantum cryptography[J]. Phys Rev Lett, 2005(94): 230503.

[9] HOI-KWONG LO. Decoy state quantum key distribution [J]. International Journal of Quantum Information, 2008, 3(supp01): 143-143.

[10] WANG XB, PENG CZ, ZHANG J, et al. General theory of decoy-state quantum cryptography with source errors [J]. Physical Review A, 2008, 77(4): 1912-1917.

[11] ZHAO Y, QI B, LO HK . Quantum key distribution with an unknown and untrusted source[J]. Physical Review A, 2008, 77(5): 052327.

[12] WANG XB. Decoy-state quantum key distribution with large errors of light intensity[J]. Phys Rev A, 2007(75): 052301.

[13] ALLEAUME R, DEGIOVANNI I, MINK A, et al. Worldwide standardization activity for quantum key distribution [C]// Globecom Workshops. IEEE, 2015.

[14] JUNSEN L, BINGBING W U, RUI T, et al. Analysis on the application and development of quantum communication [J]. Telecommunications Science, 2016.

作者简介：
李文华，毕业于北京邮电大学，高级工程师，主要从事通信网络、技术研究和技术管理工作；袁夕征，毕业于北京邮电大学，高级工程师，主要研究方向为传送网和政企ICT；熊晓然，北京邮电大学在读硕士研究生，研究方向为量子光学与量子信息。