



专题：量子保密通信技术与应用

开放型量子保密通信系统架构及共纤传输技术与实验

唐建军¹, 李俊杰¹, 张成良¹, 丛煜华², 龚浩敏³

- (1. 中国电信股份有限公司北京研究院, 北京 102209;
2. 科大国盾量子技术股份有限公司, 安徽 合肥 230088;
3. 烽火通信科技股份有限公司, 湖北 武汉 430205)

摘 要: 量子保密通信因其具有理论上的无条件安全性, 在国防、金融、政务、商业等领域的应用潜力巨大, 同时也对通信网络提出了一定的要求。在研究量子保密通信的基础上, 提出了开放型量子保密通信的系统架构; 同时为了更好地与现有通信系统融合, 提出了一种量子密钥分发 (QKD) 系统与大容量光通信系统共纤传输方案, 并通过实验验证了 QKD 系统和 80×100 Gbit/s DWDM 系统共纤传输的可行性, 在超过 100 km 共纤 (G.654 超低损光纤) 传输条件下同时实现了 QKD 成码率超 1 kbit/s 和 8 Tbit/s DWDM 系统无误码传输。

关键词: 量子保密通信; 共纤传输; 波分复用

中图分类号: TN913

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018253

Research and experiment of open quantum cryptography communication system architecture and co-fiber transmission technology

TANG Jianjun¹, LI Junjie¹, ZHANG Chengliang¹, CONG Yuhua², GONG Haomin³

1. Beijing Research Institute of China Telecom Co., Ltd., Beijing 102209, China
2. QuantumCTek Co., Ltd., Hefei 230088, China
3. FiberHome Telecommunication Technologies Co., Ltd., Wuhan 430205, China

Abstract: Based on the study of the mechanism of quantum encryption system, the system architecture of open quantum cryptographic communication was proposed. In order to better integrate with the existing communication system, a quantum key distribution (QKD) system and a large capacity optical communication co-fiber transmission scheme were proposed, and the QKD system and 80×100 Gbit/s DWDM were verified through experiments. The feasibility of the system common fiber transmission was realized under the condition of ultra 100 km common fiber transmission, the QKD bit rate >1.0 kbit/s and 8 Tbit/s DWDM system without error bit and the practical threshold of the commercial encryption device key rate >1.0 kbit/s was achieved.

Key words: quantum secure communication, co-fiber transmission, wavelength division multiplexing

1 引言

随着云计算、雾计算等技术的发展以及量子计算机和量子并行算法的出现,传统以复杂数学算法为基础的密钥协商通信系统面临巨大的安全威胁。随着社会信息化水平的日益提高,通信和信息网络已经深入影响到国民经济和人民生活的方方面面。然而,网络和信息的安全威胁却像一把“达摩克利斯之剑”时刻高悬。

作为对抗安全威胁的利器,加密通信近年来越来越被人们所重视。但是信息技术发展日新月异,基于算法复杂性的经典加密通信技术受到分布式计算和量子计算等新技术的挑战,未来量子计算技术有可能成为传统加密算法的终结者。进一步提高算法复杂度和密钥长度等手段不能解决根本问题,因此,人们迫切需要一种全新的加密通信技术彻底解决安全性问题,量子保密通信技术应运而生。

我国面临的信息安全形势日益复杂,在政务、金融和关键基础设施等领域需要进一步提高网络信息安全的保障能力,量子保密通信的试点应用和产业推广呈现较快发展趋势^[1]。2017年,量子保密通信“京沪干线”项目建成并通过验收,“沪杭干线”“宁苏干线”和“武合干线”等项目也相继开始建设,全球首颗量子科学实验卫星“墨子号”实验研究同步推进^[2]。量子保密通信初步形成集技术研究、系统集成、建设运维和安全应用为一体的产业链,相关器件商、设备商、运营商、最终用户单位等上下游企事业单位积极探索基于量子保密通信的安全通信应用。总体而言,我国量子保密通信技术的研究与应用发展处于世界领先水平,有效保障未来网络的信息传输安全。

但是,量子保密通信的应用与产业化发展同样面临一些困难和瓶颈,包括量子保密通信系统的协议、器件、设备和网络缺乏相应的技术规范

和标准体系等^[3]。基于QKD (quantum key distribution, 量子密钥分发)的量子保密通信的主要功能是完成量子密钥的安全分发,它不是现有通信系统的替代,而是有益补充。那么量子保密通信系统与现有大容量OTN/WDM等传送系统的有机融合,对于量子保密通信的规模商业化应用极其关键。本文就开放型量子保密通信系统及其架构以及共纤技术等相关问题进行研究与探讨,以便可平滑升级现有通信网络。

2 量子密钥分发原理及其发展

2.1 量子密钥分发原理

1984年美国IBM公司科学家Bennett等人^[4]提出了首个量子密钥分发协议——BB84协议,使量子密钥分发的研究从理论走向了实践。2005年美国学者Lo等人^[5-7]提出了多强度诱骗态调制方案,解决了量子密钥分发系统中的弱相干光源多光子的安全漏洞,为量子保密通信的实用化打开了大门。

量子保密通信是量子论和信息论相结合的新兴研究领域,它利用量子态或纠缠效应等进行信息传输或密钥分发,由量子力学原理保证信息传输的绝对安全性,主要包括量子隐形传态(quantum teleportation, QT)和QKD两类^[8-9],其中量子隐形传态技术尚不成熟^[10],而量子密钥分发是发展最为迅速、有望最早实现商用化的技术,本文聚焦于QKD进行研讨。量子密钥分发可以建立安全的通信密码,通过一次一密的加密方式可以实现点对点方式的安全经典通信,这里的安全性是在数学上已经获得严格证明的安全性^[11],这是经典通信迄今为止做不到的。

QKD是基于量子态传输实现的。为便于传输,现有的QKD实验和设备一般以光子为量子态载体,其表现形式即光子态传输。量子信息的编码空间以光偏振为主,如图1所示。

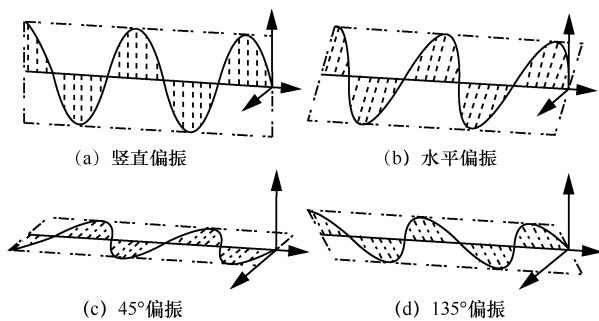


图1 单光子偏振

最经典的 QKD 协议为 BB84 协议^[4]。在 BB84 密钥分发方案中，以量子态对应于经典二进制码 (bit)。为简单起见，考虑一种最简单的量子态：光子偏振 (如图 2 所示)。水平或 45°偏振对应于经典比特 0；竖直或 135°偏振对应于经典比特 1。Alice 向 Bob 发射一系列单光子偏振态。每个光子的偏振从水平、竖直、45°或 135°中随机选出。或者说，Alice 随机使用了两组基，称为直角基 (水平偏振或竖直偏振) 及斜角基 (45°偏振或 135°偏振)。对每个飞入光子，Bob 随机选用直角或斜角基测量其偏振 (对每个飞入光子 Bob 只能选用一组基测量)。这样，在 BB84 方案中，对每个飞入光子，有一半概率 Bob 使用错误基测量，即 Bob 的测量基与 Alice 的制备基不一样。他们通过经典公开通道比较每个光子的制备基与测量基。Bob 丢弃那些使用了错误基得到的测量结果。对于剩下的测量记录，Bob 随机抽取一部分与 Alice 对照，检验每组基下各态的误码率并丢弃这些公开宣布的用作检验的测量结果。若误码率过大，他们放弃所有数据。否则，他们再对剩余数据 (初始码，即 raw key)，通过纠错 (error correction)、隐私放大 (privacy amplification) 而提炼出最终码 (final key)。

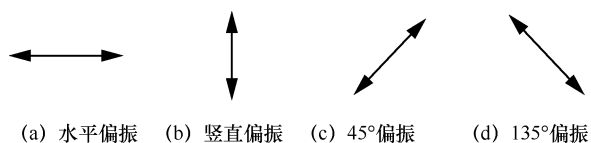


图2 光子的4个偏振态可以用作量子密码

基于 BB84 协议的量子密钥分发无需共享纠缠对资源，只需要单光子态传输。目前真实系统没有理想单光子源，采用的是近似单光子源，即强度为单光子量级的弱激光源，后简称弱光。由于传输损耗，基于弱光传输的量子密钥分发安全距离受到严重限制。另一方面，窃听者可以冒充通道损耗进行光子分数 (photon number splitting, PNS) 攻击，一个行之有效的办法是采用近年发展起来的诱骗态方法 (decoy-state method)^[5-7]，它虽然继续采用现有光源，但安全性等价于理想单光子源，距离与理想单光子源距离基本相同。

2.2 量子保密通信原理

量子保密通信是基于 QKD 产生的密钥，对业务通信进行加密，从而实现保密通信。点对点传输量子加密通信系统原理如图 3 所示，通过单光子量子态的制备、传输、测量和经典通信协议后处理，实现通信双方之间的量子密钥共享，再结合一次一密的对称加密体制 (即通信双方均使用与信息等长的密码进行逐比特的加解密操作)，理论上可实现绝对安全的量子保密通信。

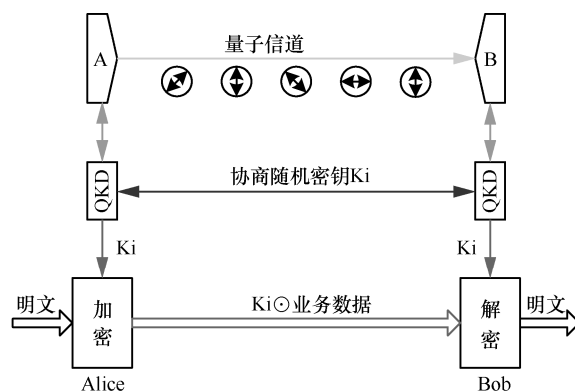


图3 点对点传输量子保密通信系统原理

由于光纤损耗导致大量光子丢失，要达到一定成码率，QKD 的距离受限，一般 80~100 km 需要可信中继，广域传输量子保密通信系统原理如图 4 所示。每一中继段需利用协商出的随机密码 K_i 对端到端密钥 K_{ab_i} 进行加密和解密，经多段中继后，即可实现密码 K_{ab_i} 的分发，从而实

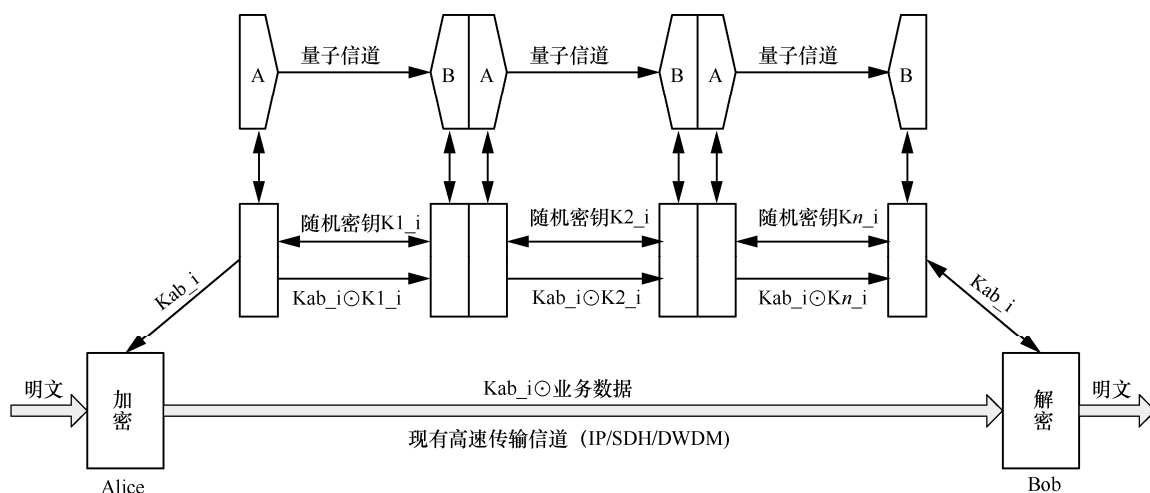


图4 广域传输量子保密通信系统原理

现端到端的加密。由于量子信道协商产生的随机密码成码率远低于业务通信，所以一般情况下，密钥定期更新，重复使用。

2.3 量子保密通信研究现状与标准进展

早在20世纪90年代，由美国研究者谢尔（Shor）提出的谢尔量子算法就被证明可以大幅降低破解公钥的计算复杂度。这预示着将来有一天一旦有了大规模的量子计算机，那么基于计算时间复杂度的加密学将面临失效的危险。正由于量子计算机的潜在威胁，量子保密通信的研究得到美国、英国、日本和欧盟等国家和地区的高度重视。

随着QKD及相关技术的发展和逐步成熟，量子保密通信在国内外已有不同规模的试点应用，尤其是近几年呈现快速发展趋势。美国、欧盟、英国、法国、奥地利、瑞士、日本等国家和地区积极投入巨资研究量子保密通信及相关实验和试点。我国量子保密通信的试点应用起步稍晚但发展迅速。2017年建成的“京沪干线”，连接北京、济南、合肥、上海等城域网，全长2000多千米。“墨子号”量子卫星于2016年8月成功发射，由此点燃全球量子热潮。

目前，世界各国已经开展了量子保密通信技术的标准化研究工作，以欧洲电信标准化协会

（ETSI）、美国云安全联盟（CSA）和电气与电子工程师学会（IEEE）等为代表的国外研究机构在该领域率先布局，并已取得一定研究成果^[1]。中国通信标准化协会（CCSA）也于2017年6月成立了量子通信与信息技术特设任务组，开始启动量子保密通信技术标准的研究工作^[3]。但目前的标准成果较少，难以促进量子保密通信的规模化应用。

3 开放型量子保密通信系统架构与接口

3.1 开放型量子保密通信系统的必要性

当前的量子保密通信系统，由集成业务系统的量子网关设备同时完成量子密钥的分发与业务提供，一般只支持语音电话、可视电话等基本的通信业务，无法满足互联网和云计算时代的业务多样性需求。

由于采用量子设备厂商的私有协议，量子密钥的分发与业务提供没有解耦。单独依靠少数几家量子保密通信设备商，无法支撑量子保密通信产业，且由于产业链严重受限，很难满足金融、政府等客户的业务基本需求。故亟需将量子保密通信与多种多样的业务传输设备解耦，实现它们之间的开放互联，为量子保密通信大规模应用奠定基础。因此中国电信作为我国最大的政企通信



业务提供商，率先在量子保密通信的实用化方面开展了大量工作，提出了开放型量子保密通信系统的概念，并联合合作伙伴进行了研究探索。

3.2 开放型量子保密通信系统架构

量子保密通信的绝对安全性可以用于密钥的产生和发放，但是无法实现高速率大容量通信。为了解决这个问题，本文提出了开放型量子加密通信系统（如图 5 所示），其中量子密钥服务器（QKS）设备是量子密钥分发网络（QKDN）的组件，主要功能是向量子加密通信设备（QCCD）提供量子密钥（QK）服务；量子加密通信设备（QCCD）利用量子密钥，通过经典通信网络（CCN）完成量子加密通信服务；QKS 设备与 QCCD 设备之间的接口称为量子密钥应用接口（QK_API）。

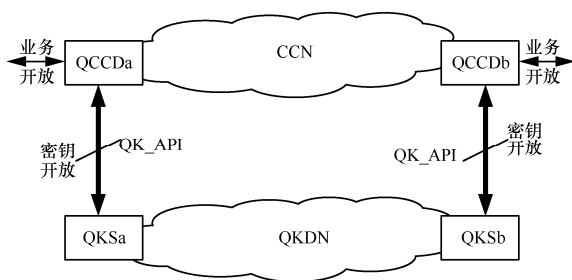


图 5 量子保密通信网络与系统结构示意图

此处“开放”的含义并不是将量子密钥或者量子保密通信技术开放出来，并不影响量子保密通信的安全性。“开放”的含义是通过标准化的接口兼容更多的业务类型和设备形态，具体包括“业务开放”和“密钥开放”：“业务开放”指的是量子加密系统只在信息传输层提供基于量子密钥的保密通信，上层业务系统可以是现有或者未来发展的任何新型业务，“密钥开放”指的是量子密钥网关设备提供标准化的 API，任何厂商的量子加密传输设备均可通过标准化接口提供量子加密通信服务。通过这种接口开放的方式，极大扩展了产业链，为未来量子保密通信的产业化规模发展铺平了道路。

采用这种开放式架构，优势明显。

- 量子保密通信设备商可专注于 QKDN 设备与系统的研发。
- 业务提供及业务加密等多样性功能的需求交给传统通信设备商，可快速利用现有成熟的传输与数据通信的产业链，实现业务的开放。
- 不同厂商的量子保密设备与通信设备均可互通，快速形成可规模应用的产业链。
- 业务透明传输，可平滑升级现有业务，客户的网络与系统无需改造。

3.3 开放型量子保密通信接口

经研究，提出量子保密通信接口，包括量子密钥分发生命周期的全生命周期，量子密钥 QK 由 QKDN 产生，分发给 QCCD，关键步骤如下。

步骤 1 加密通信初始化

在加密通信之前，加密通信两端 QCCD 在对应的 QKS 注册，分别获得 QKS_ID，并告知对方。

步骤 2 启动服务

在发起加密通信前，QCCD 需向 QKS 请求密钥量的需求，QKS 可及时准备好量子密钥。

步骤 3 获取密钥与同步更新

在加密通信时，密钥成对使用，两端加密密钥建议不一致，两端分别需要获取密钥和同步更新，加密密钥序号由 QKS 分配，解密密钥由对端 QCCD 回复的密钥序列号指定。

步骤 4 密码需求变更

当加密通信的需求发生变更时，比如通信会话需求变化。

步骤 5 结束加密通信

当加密通信会话全部结束暂不需要密钥时，QCCD 通信设备需要向 QKS 设备发起会话结束请求，停止密钥生成。

4 QKD 与传统通信共纤传输

4.1 共纤传输的需求与技术发展现状

由于量子信号光非常微弱，通常只有单光子水平，等效光功率约为 -70 dBm，量子密钥分发

(QKD)在实际应用中,需要一根单独的光纤传输量子信号,另一根光纤传输同步信息和协同通道。而目前运营的光缆纤芯资源相对紧张,尤其是大客户的接入光缆纤芯更加匮乏。在实际部署量子保密通信升级而现网又没有多余纤芯时,就需要新增部署光缆,将导致部署周期长、升级成本高、工程实施困难等问题。为此,探讨量子信号与业务信号在现有的光纤中共同传输就很有必要。

第一个 QKD 与经典光通信的波分复用实验是由 Townsend 小组^[12]在 1997 年实现的。2010 年, Eraerds 等人^[13]实现了 QKD 与传输数据速率为 1 Gbit/s 的经典光通信的共纤传输。Choi 等人^[14]将这一指标提高到 10 Gbit/s,该实验是基于 PON 的。2017 年, Wang 等人^[15]实现了一根光纤传输 QKD 和 1 Tbit/s 经典相干光通信,最远传输距离达到 80 km。

4.2 共纤传输面临的挑战

共纤传输最直接的方法是采用波分复用技术,将 QKD 与经典光通信共纤传输,如图 6 所示。事实上, QKD 与经典通信波分复用最大的挑战来自经典强光产生的自发拉曼散射以及四波混频效应对量子信号光造成的影响。在短距离光纤传输并且存在多个经典光通信信道时,非线性的四波混频效应占主导,而在长距离光纤传输时,线性拉曼散射效应占主导。

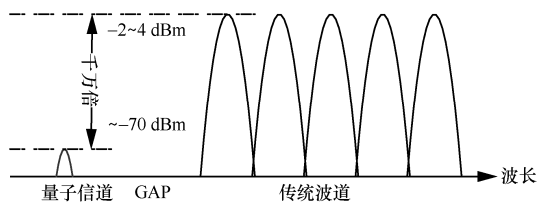


图6 量子波道与经典波道共纤波分复用示意图

光纤中的拉曼散射主要来自自发拉曼散射,是一种线性效应,散射强度与光功率成正比。实现大容量百公里共纤传输,传统光通信需采用密集波分复用,而且传统 DWDM 信号光功率较强,

如何隔离强经典光所产生的拉曼散射噪声是实现大容量百公里共纤传输的挑战之处。

共纤传输时,还需要考虑量子信号与 DWDM 信号是同向还是背向、量子信号的承载波长选择等,这些都是共纤传输研究面临的挑战。

4.3 共纤传输应对策略

对于共纤的干扰(如原始噪声、四波混频、拉曼散射等),经研究可以通过多种方法共同抑制其产生。

(1) 增大合波器和分波器的隔离度

增大量子波道和 DWDM 波道的隔离度,在共纤的源头控制 DWDM 合波信号在量子信号波长上的噪声,一般要求隔离度在 100 dB 以上(噪声光功率要远低于信号光功率)。

(2) 降低合波器和分波器的插入损耗

量子波道和 DWDM 波道的合波器和分波器的插入损耗,直接影响 DWDM 和量子信号的传输距离,每降低 1 dB 插入损耗(合波器和分波器共 2 dB),共纤传输的距离可增加约 10 km。

(3) 增大与经典信道的波长间隔

QKD 的波长可分配传统 C 波段(与业务波长保持适当的间隔)、L 波段或 O 波段。由于光信号传输时存在红移的现象(短波长对长波长的影响与长波长对短波长的影响都偏大),且 O 波段与 C 波段(业务波长所在的波段)的间隔更大,故选 O 波段更合适。

(4) 降低经典光的入纤光功率

传统 80 波 DWDM 系统的合波后入纤功率约为 20 dBm,这样的功率产生的噪声对量子波道的干扰是致命的。经测试,需将 80 波 DWDM 总功率调整至 0~7 dBm。

(5) 量子信号与 DWDM 信号同向共纤

同向传输时, DWDM 信号对量子信号的串扰也将随着光纤的传输衰减,接收端的噪声在可控的范围之内;而反向传输时, DWDM 信号对量子信号的串扰几乎没有衰减,量子信号接收机的噪

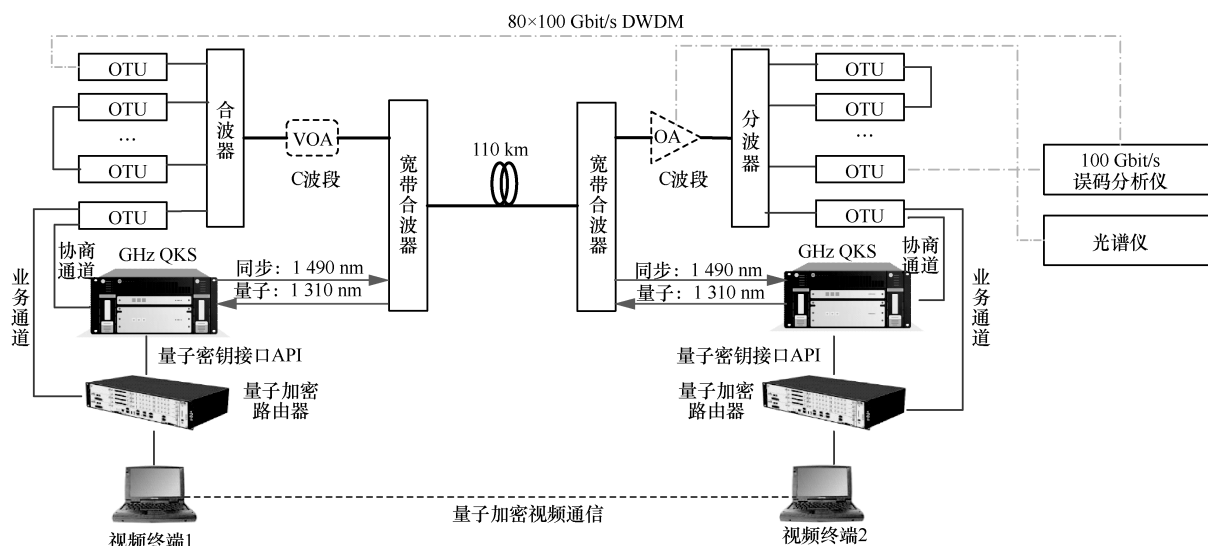


图7 量子信号与 DWDM 共纤传输系统方案

声将最大。经测试验证，量子信号与 DWDM 信号同向共纤传输时，串扰最小。

5 实验验证

5.1 实验方案

根据本文上述提出的开放型量子保密通信系统架构与接口方案及共纤传输方案，进行研发与实验验证，验证测试系统架构如图7所示，由 A、B 共 2 个节点构成，每个节点的构成如下。

(1) DWDM 设备

采用烽火通信的 80×100 Gbit/s 商用系统，信道间隔为 50 GHz，其光谱图如图8所示，总传输带宽为 8 Tbit/s。

(2) QKD 设备

采用国盾量子的 GHz QKD 商用设备，A 节点为发送端，B 节点为接收端。量子信号波长为 1310 nm，光脉冲频率为 625 MHz，采用诱骗态 BB84 协议编码。同步信号波长 1490 nm，同步脉冲频率 100 kHz，功率为 -33.5 dBm。

(3) 经典量子波分复用终端

根据上述研究结果定制器件，为上述 80 波 DWDM 信号、量子信号和同步信号提供复用和解

复用功能，插入损耗 < 2 dB，DWDM 对量子信号的串扰值 < -150 dB（确保 DWDM 信号噪声与量子信号隔离）。

(4) 量子密钥管理设备

采用国盾量子 QKM-T500 商用设备，其功能是从 QKD 设备获取密钥，并通过上述的量子密钥接口 API 协议，分发两端的量子加密路由器。

(5) 量子加密路由器

通过上述的量子密钥接口 API 协议接收量子密钥，利用量子密钥为业务提供加解密服务。

(6) 光纤

采用康宁和长飞 G.654 超低损光纤，本实验中光纤长度分别 80 km、90 km、100 km、110 km、115 km。

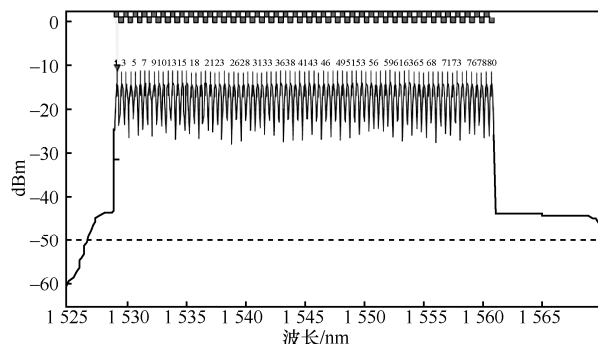


图8 80×100 Gbit/s DWDM 系统光谱图

5.2 实验结果与分析

为减少经典 DWDM 信号对量子信号的串扰, 将经典 80 波 DWDM 合波后的入纤光功率衰减至 1.5 dBm (此功率是 DWDM 系统可以无误码工作的最小功率, 对量子信号的干扰也最小)。测试结果如下。

- 100 Gbit/s 无误码: 利用 OUT UNI 将 79 波串接, 通过 100 Gbit/s 误码仪验证测试, 16 h 无误码。
- QKD 可成码: 每 5 min 统计 QKD 成码率, 在不同长度时的成码率见表 1, 115 km 极限共纤超长距离时, 16 h 平均成码率达 0.41 kbit/s, 如表 1 和图 9 所示。

表 1 不同共纤光纤距离时成码率测试结果

光纤距离/km	光纤损耗/@1 310/dB	成码率/(kbit·s ⁻¹)
80	22.44	8.1
90	25.84	2.9
100	27.31	1.6
110	30.90	0.5
115	31.52	0.41

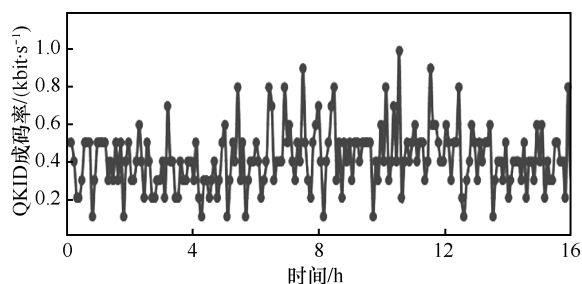


图 9 115 km 超长距共纤传输时 QKD 成码率

- 加密视频业务正常: 超清视频 (1080P) 通信流畅, 无卡顿 (与协商信道共同占用 1 波 100 Gbit/s 信道)。

通过上述实验, 验证了量子密钥接口 API 协议的可行性以及 10 km 级的超长距共纤的可行性, 共纤传输容量和距离在业界均领先, 对于标准的 80 km 共纤时, 有较大的余量和较高的成码率。

6 结束语

本文在提出开放型量子加密通信系统架构的基础上, 提出了实用的量子密钥接口协议, 便于量子密钥分发与业务通信更好地融合, 为用户提供融合的安全通信服务。

本文提出的共纤传输方案及验证系统模型证明了该共纤方案的可实施性和可部署性, 共纤传输的距离 (115 km) 与容量 (8 Tbit/s, 80 个波长, 单波长 100 Gbit/s) 在业界均领先, 能够满足用户业务的平滑升级需求, 而不需要额外部署光纤, 特别适用于大客户的专线接入等场景, 为量子保密通信的规模化应用奠定基础。

参考文献:

- [1] 赖俊森, 吴冰冰, 李少晖, 等. 量子保密通信研究进展与安全性分析[J]. 电信科学, 2015, 31(6): 39-45.
LAI J S, WU B B, LI S H, et al. Progress and security analysis of quantum cryptography communication[J]. Telecommunications Science, 2015, 31(6): 39-45.
- [2] 赖俊森, 吴冰冰, 汤瑞, 等. 量子通信应用现状及发展分析[J]. 电信科学, 2016, 32(3): 123-129.
LAI J S, WU B B, TANG R, et al. Analysis on the application and development of quantum communication[J]. Telecommunications Science, 2016, 32(3): 123-129.
- [3] 赖俊森, 吴冰冰, 汤瑞, 等. 量子保密通信标准化现状与发展分析[J]. 电信科学, 2018, 34(1): 1-7.
LAI J S, WU B B, TANG R, et al. Analysis on the status and development of quantum secure communication standardization[J]. Telecommunications Science, 2018, 34(1): 1-7.
- [4] BENNETT C H, BRASSARD G. Quantum cryptography: public key distribution and coin tossing[C]//International Conference on Computers, Systems, and Signal Processing, December 10-12, 1984, Bangalore, India. [S.l.:s.n.], 1984: 175-179.
- [5] LO H K, CURTY M, TAMAKI K, et al. Secure quantum key distribution[J]. Nature Photonics, 2014, 8(8): 595-604.
- [6] DISTRIBUTION D S Q K. Decoy state quantum key distribution[J]. IIUM Engineering Journal, 2010, 23(4): 86-90.
- [7] LIU Y, CHEN T Y, WANG J, et al. Decoy-state quantum key distribution with polarized photons over 200 km[J]. Opt Express, 2010(18): 8587-8594.
- [8] 周正威, 陈巍, 孙方稳, 等. 量子信息技术纵览[J]. 科学通报, 2012, 57(17): 1498-1525.
ZHOU Z W, CHEN W, SUN F W, et al. A survey on quantum information technology[J]. Chinese Science Bulletin, 2012, 57(17): 1498-1525.
- [9] 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): 296-311.

WU H, WANG X B, PAN J W. Quantum communication: status and prospects[J]. Scientia Sinica (Informationis), 2014(44): 296-311.

- [10] BENNETT C H, BRASSARD G, CREACUTE C, et al. Teleporting an unknown quantum state via dual classical and Einstein Podolsky-Rosen channels[J]. Physical Review Letters, 1993, 70(13): 1895.
- [11] SHOR P, PRESKILL W J. Simple proof of security of the BB84 quantum key distribution protocol[J]. Physical Review Letters, 2000(85): 441-444.
- [12] TOWNSEND P D. Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing[J]. Electronics Letters, 1997, 33(3): 188-190.
- [13] ERAERDS P. Quantum key distribution and 1 Gbit/s data encryption over a single fibre[J]. New Journal of Physics, 2010, 12(6): 063027.
- [14] CHOI I, YOUNG R J, TOWNSEND P D. Quantum key distribution on a 10 Gbit/s WDM-PON[J]. Optical Fiber Communication, 2010, 18(9): 9600-9612.
- [15] WANG L J, ZOU K H, SUN W. Long distance co-propagation of quantum key distribution and terabit classical optical data channels[J]. Physical Review A, 2017, 95(1).

[作者简介]



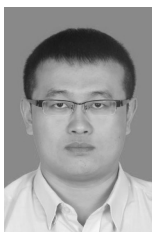
唐建军（1977-），男，博士，中国电信股份有限公司北京研究院光通信研究中心高级工程师，主要研究方向为量子保密通信、大容量光传输系统。



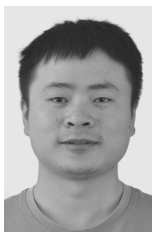
李俊杰（1977-），男，博士，中国电信股份有限公司北京研究院网络研发与运营支持部副主任、教授级高级工程师，主要研究方向为光通信网络与系统。



张成良（1970-），男，中国电信股份有限公司北京研究院副院长、教授级高级工程师，中国通信标准化协会传送与接入网技术委员会副主席，中国通信学会光通信委员会副主任，主要研究方向为光通信技术。



丛煜华（1978-），男，科大国盾量子技术股份有限公司 QKD 产品线信道产品团队负责人、高级工程师，主要研究方向为量子保密通信与经典通信信道融合技术、量子保密通信信道共享技术。



龚浩敏（1985-），男，烽火通信科技股份有限公司高级工程师，主要研究方向为光线路与传输系统技术。