



综述

量子通信应用现状及发展分析

赖俊森, 吴冰冰, 汤瑞, 赵文玉, 张海懿

(中国信息通信研究院技术与标准研究所, 北京 100191)

摘要:量子通信是一种具备无条件安全性的物理层安全解决方案,其技术现状、实用化水平和发展面临的瓶颈是业界关注的焦点。首先分析了量子通信的试点应用情况及其存在的主要问题,然后梳理了量子通信产业化推广的现状和国内外标准化研究工作的进展,在此基础上探讨了量子通信系统性能测试评价技术,最后提出了量子通信未来发展的策略建议。

关键词:量子通信;产业化;评价;前景

中图分类号: TN915

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2016085

Analysis on the application and development of quantum communication

LAI Junsen, WU Bingbing, TANG Rui, ZHAO Wenyu, ZHANG Haiyi

Technology and Standards Research Institute, China Academy of Information and Communication Technology (CAICT), Beijing 100191, China

Abstract: Quantum communication, which can provide unconditional security, is a physical layer solutions for information security. The status and challenge of its technology development and application are the focus of the industry. The field trials of quantum communication and main problem were analyzed. Driving force and bottleneck of its commercialization were clarified and worldwide standardization research were reviewed. System performance test and evaluation were discussed and future development recommendations were also provided.

Key words: quantum communication, industrialization, evaluation, prospect

1 引言

量子力学和量子信息技术的发展使人类能够对光子和原子等微观粒子进行精确的人工操控,并以革命性的全新方式实现了对信息的编码、存储、调制、传输和运算处理。量子通信是利用量子态和量子纠缠效应进行信息或密

钥传输的新型通信方式^[1],基于量子力学原理能够在理论和协议层面提供无法被监控和窃听的绝对安全性保证,在当前复杂多变的信息安全形势下其重要性日益突显,成为重要的科技发展方向之一。

量子通信中的量子隐形传态、量子安全直接通信和量子秘密共享等分支一直是前沿基础理论研究领域和

收稿日期:2016-01-05;修回日期:2016-02-29

基金项目:国家自然科学基金资助项目(No.61171076, No.61201260, No. 61471128);国家高技术研究发展计划(“863”计划)基金资助项目(No.2013AA013402, No.2015AA015502)

Foundation Items: The National Natural Science Foundation of China (No.61171076, No.61201260, No.61471128), The National High Technology Research and Development Program of China (863 Program) (No.2013AA013402, No.2015AA015502)



科学实验探索方面的热点,但限于实用化发展水平,距离产业应用尚有一定距离^[2,3]。作为量子通信技术中最具实用化前景的一个分支,基于量子密钥分发(quantum key distribution, QKD)的量子通信经过 30 余年的研究和发展,在协议技术、系统器件和组网架构等各方面初步成熟并进入推广试用阶段,近年来呈现出加速发展的趋势^[4-7],也是本文分析讨论的重点。

作为新型的安全保障技术,量子通信的技术现状、实用化水平和面临的发展瓶颈等已成为业界关注的焦点。鉴于此,本文首先分析量子通信试点应用的基本情况及其中存在的主要问题,之后梳理了产业化推广的发展现状和面临的瓶颈,同时介绍了国内外该领域标准化研究取得的工作进展,并对如何评价 QKD 系统的性能测试进行了探讨,最后提出了未来发展的策略建议。

2 应用现状与问题

基于量子密钥分发的量子通信原理如图 1 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通信^[8-10]。1984 年美国 IBM 公司科学家 Bennett 等人^[11]提出了首个量子密钥分发协议——BB84 协议,使量子通信的研究从理论走向了现实。2005 年美国学者 Lo 等人^[12]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,为量子通信的实用化打开

了大门。

目前,量子通信在国外已有小规模试点应用。随着量子密钥分发技术的发展和逐步成熟,世界各国试点应用呈现快速发展趋势,2003 年美国 DARPA 资助哈佛大学建立了世界首个量子密钥分发保密通信网络。此后,欧美日等多个地区和国家相继建成了瑞士量子、东京 QKD 和维也纳 SECOQC 等多个量子通信实验网络,演示和验证了城域组网、量子电话、基础设备保密通信等应用^[13-16]。2013 年美国知名研究机构 Battelle 公布了环量量子通信骨干网络项目,计划采用瑞士 IDQ 公司设备,基于分段量子密钥分发结合安全可信节点密码中继的组网方式,为谷歌、微软、亚马逊等互联网巨头的数据中心提供具备量子安全性的通信保障服务。

国内量子通信的试点应用起步稍晚但发展迅速。2007 年中国科学技术大学在北京实现了国内首个光纤量子电话,之后相继在北京、济南、芜湖和合肥等地建立了多个城域量子通信示范网、金融信息量子通信技术验证专线以及关键部门间的量子通信热线。2014 年,量子通信“京沪干线”项目通过评审并开始建设,计划建成北京和上海之间的基于安全授信节点密码中继的距离超 2 000 km 的国际首个长距离光纤量子通信骨干线路。中国科学院牵头的战略先导专项“量子科学实验卫星”计划,由中国科学技术大学、中国科学院研究所和中国航天科技集团第八研究院合作,计划于 2016 年发射全球首个量子通信卫星^[17-20]。

量子通信的应用近年来呈现加速发展的趋势,但在应用推广过程中也暴露出了一些问题,主要包括以下 3 个

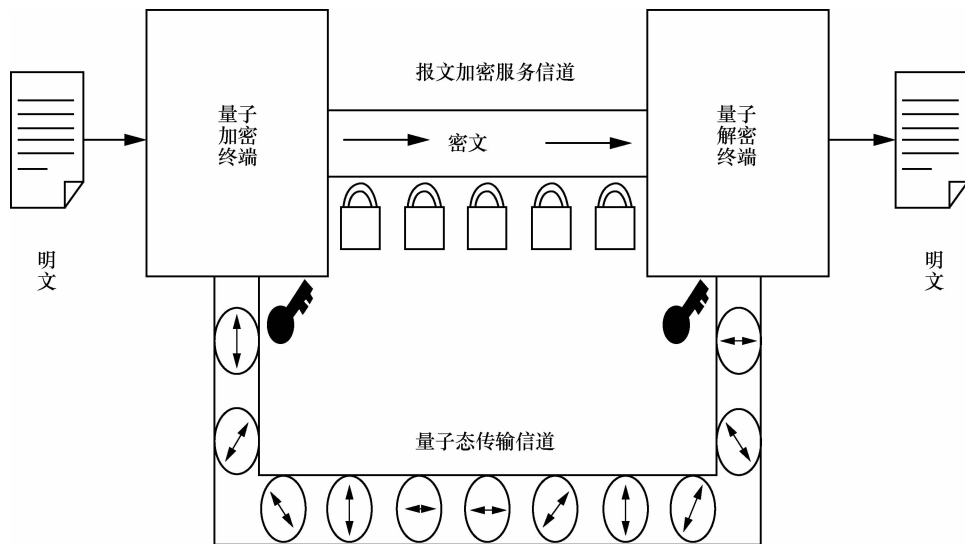


图 1 量子通信系统原理

方面。

(1) 系统性能待提高, 技术瓶颈待突破

在典型的光纤传输 QKD 系统中, 百公里长距离传输条件下, 其系统可用的安全码率约为 10 kbit/s 量级, 相对于现有光传送网基于波分复用和相干传输技术实现的 Tbit/s 量级的信息传输差距很大, 难以实现对信号的一次一密加密; 而在数十公里量级的短距离传输中, 由于 QKD 系统协议处理机制和器件性能的限制, 能够实现的安全码率约为 2 Mbit/s 量级。QKD 系统通过协议改进和发展新型器件进行性能提升的难度较大, 其核心器件, 如单光子源、高品质纠缠光源、高性能光子探测器等器件的研发进展相对缓慢。

在广域量子通信组网方面, 由于量子态存储和纠缠操控技术目前尚不成熟, 所以基于纠缠交换和量子存储的量子中继方案目前难以使用, 现有报道的量子通信长距离传输和组网均为基于可信中继节点量子密钥管理器的密钥中继方案。星地量子通信是未来实现广域组网的一个可选方案, 但目前尚无量子通信卫星平台的实验验证, 其中涉及的关键技术和系统性能仍需进一步验证。

(2) 系统的现实安全性存在一定风险

在实际的 QKD 系统中, 光源、信道节点和接收机的不理想特性使其难以满足理论协议模型的安全性证明要求, 成为可能被窃听者利用的安全漏洞, 所以针对实际 QKD 系统进行攻防测试和安全性升级将是其运营维护面临的一个问题。在现有的长距离量子通信传输中, 基于可信中继节点的密钥存储和转发不满足无条件安全性证明的要求, 可能成为整个系统的安全风险点。现阶段由于 QKD 系统的密钥生成码率较低, 在对高速业务信号进行加密处理时难以满足一次一密的要求, 必须借助 AES 等对称加密算法对密钥进行重复使用和算法处理, 难以满足无条件安全性证明的严格要求。

(3) 目前应用场景有限, 前期投入偏高

现阶段量子通信主要面向政务、国防、金融等长期安全性要求很高的特定应用场景, 市场规模有限且较为分散, 传统通信业界对于量子通信的应用目前仍然持观望态度, 参与程度和热情较低。对现有系统进行量子通信升级的前期软硬件改造投入要求较高, 而且 QKD 系统包含大量精密光学器件, 对于日常使用和运营维护也有一定要求。此外, 由于单光子量子态信号与传统光信号同光纤混合传输时将引入性能劣化, 所以量子通信系统组网时通常

需要使用额外的独立光纤链路资源, 也是其推广应用所面临的一项挑战。

3 产业化推广情况

量子通信的战略意义吸引了西方各国科研机构的关注, IBM、NIST、Battelle、NTT、东芝、西门子等著名公司和机构一直密切关注其发展并投资相关研究^[21-24]。其中东芝欧洲研究所一直是国际上最活跃的量子通信研究团队之一, NTT 和 NIST 的联合团队在量子隐形传态和量子密钥分发实验等方面也取得一系列研究成果。英国政府在 2013 年发布了为期 5 年的量子信息技术专项, 投入 2.7 亿英镑用于量子通信和量子计算等方面的研究成果转化, 促进新应用和新产业的形成。国外成立了多个专门从事量子通信技术成果转化和商业推广的实体公司。例如美国的 MagiQ 公司和瑞士日内瓦大学成立的 idQuantique 公司等, 能够提供 QKD 量子通信的商用化器件、系统和解决方案。法国电信研究院成立的 SeQureNet 公司从事连续变量量子密钥分发产品的开发。美国洛斯阿拉莫斯国家实验室成立了 Qubittek 公司, 主攻智能电网安全通信领域。国内开展量子通信相关研究的代表性机构包括中国科学技术大学、清华大学、山西大学、南京大学、中国科学院微系统所和技术物理所等。以中国科学技术大学相关研究团队为核心发起成立了科大国盾量子、安徽问天量子 and 山东量子等产业化实体, 进行量子通信前沿研究成果向应用技术和商用化产品的转化, 国家对量子通信领域持续的专项投入和政策扶持为其发展提供了强劲动力。2015 年 12 月, 中国科学院、中国科学技术大学和科大国盾量子等机构在北京共同发起组建了“中国量子通信产业联盟”。

虽然基于量子密钥分发的量子通信产业化目前已经取得了一定进展, 但是大规模的应用推广仍然面临一系列的困难和挑战^[25], 主要包括以下 4 个方面。

(1) 初期市场规模和用户群体有限

QKD 系统前期投入和改造要求较高, 主要面向的是有高安全性要求的部分高端客户, 开发其需求并且保持可持续发展和盈利能力是重大的挑战。在产业化初期, 由于目标市场和用户群体有限并且分散, 给市场推广、检测认证和售后服务带来了较高的门槛和投入要求。

(2) 产业化供应链的建立尚需时日

QKD 系统采用的单光子源和光子探测器等核心器件



与传统光学器件完全不同,其性能参数、生产水平和供货能力等问题都会对产业的发展和推广应用产生影响,新产业链的培育也需要较长的时间。

(3) 技术验证与标准规范研发滞后

对于任何高新技术而言,测试认证和标准化是商用化推广的必备条件,而新型测试认证技术的开发通常是非常复杂、昂贵和耗时的,而且需要计量和标准化组织的协调与合作。目前测评技术和标准化研究已经成为量子通信应用的一项瓶颈。

(4) 系统应用需基础设施资源的支持

目前难以实现 QKD 系统的量子态信号和传统强光信号的混传,所以大规模量子通信组网需要额外的光纤资源进行支持,将对量子通信系统的应用造成限制。此外,量子通信无法共享传统光通信设备等基础设施,需要进行全新部署,造成前期大量软硬件升级改造的高投入要求。

4 标准化研究进展

在量子通信的标准化研究方面,目前欧洲处于领先地位。2008年,奥地利维也纳的 SECOQC 量子通信网络演示项目完成后,欧洲电信标准化协会(ETSI)成立了包括16家成员单位在内的 ISG-QKD 小组,展开前瞻性的标准化工作。2010年起陆续发布了与 QKD 量子通信系统与网络相关的5项规范建议,涉及应用案例(GS 002)、物理接口(GS 003)、应用接口(GS 004)、安全验证(GS 005)、模块安规(GS 008)等内容。2015年6月发布了量子安全白皮书^[26-31]。ETSI 对于 QKD 量子通信标准化的主要目标包括:技术规范,即 QKD 系统的实现方法和原理、主要器件的性能参数范围、工作环境要求以及内部和外部的接口定义等;测试方法,对 QKD 光学子系统工作状态的光层性能参数以及系统协议的密钥性能参数进行可溯源的校准和测试评价;安全认证,对 QKD 器件和系统进行包括侧信道分析、攻防测试、安规特性、安全性证明等内容的安全认证体系;网络应用,进行 QKD 技术应用场景分析、现有网络基础设施集成化分析、应用接口规范以及需求、前景和问题分析。

在国内,清华大学、中国科学技术大学和中国密码学会等研究机构与相关企业等也启动了量子通信技术规范和密码标准的初步研究工作。科技部“863”计划项目《光纤量子通信综合应用演示网络》设立了专门的子课题进行量

子通信技术标准和规范研究。在“京沪干线”项目中,由中国科学技术大学联合解放军信息工程大学开展量子通信的安全性测评研究,并探索制定相关的规范和标准。量子通信作为量子物理学和信息科学的前沿交叉学科,涉及众多技术领域,标准化工作的难度较大。目前我国量子通信领域标准化研究相对滞后,尚未形成可以充分体现和总结技术研究最新进展以及试点应用经验的标准化成果,造成这一情况的主要问题在于对标准化研究的重视程度不足,研究机构和企业各自为战,缺乏有效的沟通和协作机制,难以形成合力。

5 系统测评技术

对于任何新兴技术而言,提供一套完善和准确的系统性能测试评价方法以及配套的指标参数规范和标准体系,是保证供应商之间产品的一致性与互操作性以及用户获得产品质量和性能保证的重要前提。基于 QKD 的量子通信系统的性能参数包括两个方面:一是协议性能参数,如安全码率、可用传输距离、量子信道误码率(QBER)等;二是光学子系统参数,如单光子源性能参数和光子探测器性能参数等。为了开发具有明确定义的 QKD 系统组件性能参数表征方法,欧盟委员会成立了工业量子通信计量(MIQC)项目组,集合了英国 NPL、意大利 INRIM 和德国 PTB 等多个国家级测试计量研究机构,共同开展 QKD 器件性能参数和系统安全性的测试评价方法研究^[32,33]。目前,针对 QKD 光学子系统的性能参数测试方法研究已取得一定的进展,能够提供描述 QKD 光学子系统性能的重要参数,具体见表1,其中既包含宏观

表1 KD 光学子系统主要性能参数

类别	弱相干脉冲源	光子探测器
单光子 (微观)	平均光子数	暗计数率
	单光子发射率	后脉冲概率
	光子定时抖动	光子探测概率
	光谱线宽	死区时间
	频谱一致性	恢复时间
	时域包络	部分恢复时间
	时域一致性	最大计数率
光信号 (宏观)	时钟频率	时钟频率
	光脉冲重复频率	门控频率
	光源功率	门控时域包络
	功率稳定性	探测效率线性度
	光源波长	频谱响应度
	光信号偏振态	定时抖动

层面的性能参数,如光功率、波长、偏振态等,也包含了单光子量级的微观性能参数,如光源平均光子数、探测器暗计数率和恢复时间等,这些性能参数是QKD系统性能的重要瓶颈。

对于宏观性能参数,可以采用现有的可溯源的时域和频域检测测量方法和仪表,例如光功率计、光谱分析仪和高速示波器等。对于单光子量级的微观性能参数,需要采用新的检测仪表和测试方法,如对于弱相干光源输出脉冲包含的平均光子数,可以采用单光子探测器进行计数检测;对于光子定时抖动,可以采用超导纳米线探测器(其自身的时域不确定性小于100 ps)进行事件检测并观察时域统计直方图进行测量;对于光子探测器的暗计数率,可以通过统计无光入射时探测器的响应数来进行测量,通过暗记数事件与门控触发自相关,可以得到暗记数事件时域直方分布,进行归一化处理计算。探测器的死区时间是在一次光子检测事件之后,无法再对单光子输入光信号进行探测的持续时间。可以采用两个与探测器门控信号保持同步的单光子脉冲光源作为输入,调整两个脉冲源之间的时延,对于超过探测器死区恢复时间的时延值,探测器会输出多光子的检测结果,而死区时间就是探测器获得多光子检测结果所需的最小时间间隔。由于量子通信技术仍处于研究和发展之中,新的物理效应、协议技术和器件都可能出现和引入,需要对其性能测试评价方法和标准化规范进行升级和更新。此外,对于QKD系统侧信道和现实安全性进行测试评价的方法和标准规范尚待研究。总体而言,量子通信系统的性能和安全性测试评价技术以及标准规范目前尚不完善,将会对其商用推广和产业发展形成一定的制约和影响。

6 发展策略建议

对于下一步量子通信技术和产业发展的策略建议包括技术、产业和标准3个方面。首先,加大政策支持和专项投入,突破关键技术形成竞争优势。加强国家政策支持和专项资金投入,通过科学研究基金、重大科技专项和试点应用工程等多种形式,从长期战略高度推动量子通信基础科研、技术攻关、设备研制和产业应用等工作。其次,结合信息安全需求,稳步推进战略布局与产业应用。关注政务、金融和国防等领域的信息安全威胁和保障需求,稳步分阶段开展量子通信产业化的战略布局和示范推广应用。制定相关产业政策,适当鼓励和引导业务运营商及设备制造商

的参与。最后,协调产学研合作,加强测评技术的研究与标准规范的制定。结合我国信息安全保障的紧迫需求,加强通信、密码和安全等领域研究机构和标准化组织的沟通协调,推动量子通信整体架构、性能指标、安全技术要求及测试评价技术等方面的标准化研究。

7 结束语

量子通信作为未来信息通信行业的一个新兴战略性制高点,已经成为国家科技实力竞争的主战场之一,同时也是我国在高新技术研究与应用领域为数不多的与国际发展保持同步并且有望实现跨越引领的突破口。基于量子密钥分发的量子通信技术近年来在研究和应用方面发展明显加速,获得越来越多的关注和重视。但仍需清醒地认识到,量子通信的应用发展仍然面临从技术产业到测评标准等多方面的瓶颈和局限,现阶段尚不具备大规模应用推广的条件。今后,在技术、产业和标准等方面取得进展和突破的前提下,量子通信在国家信息安全领域和ICT产业中将发挥重要作用,具有广阔的应用前景。

参考文献:

- [1] LO H K, CURTY M, TAMAKI K. Secure quantum key distribution[J]. *Nature Photonics*, 2014, 8(8): 595-604.
- [2] PIRANDOLA S, EISERT J, WEEDBKOOK C, et al. Advances in quantum teleportation [J]. *Cancer Research*, 2015, 9(10): 5439-5439.
- [3] 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.
- [4] STINSON D R. *Cryptography: theory and practice* [M]. Florida: CRC Press, 2006.
- [5] 龙桂鲁. 量子计算算法介绍[J]. *物理*, 2010, 39(12): 803-810.
LONG G L. Introduction to quantum algorithms [J]. *Physics*, 2010, 39(12): 803-810.
- [6] SHANNON C E. Communication theory of secrecy systems[J]. *Bell System Technology Journal*, 1949, 28(4): 656-715.
- [7] 吴华, 王向斌, 潘建伟, 等. 量子通信现状与展望[J]. *中国科学: 信息科学*, 2014, 44(3): 296-311.
WU H, WANG X B, FAN J W, et al. Quantum communication: status and prospects[J]. *Scientia Sinica (Informationis)*, 2014, 44(3): 296-311.
- [8] 李宏伟, 陈巍, 黄靖正, 等. 量子密码安全性研究 [J]. *中国科学: 物理学 力学 天文学*, 2012, 42(11): 1237-1255.



- LI H W, CHEN W, HUANG J Z, et al. Security of quantum key distribution [J]. *Scientia Sinica(Physica, Mechanica & Astronomica)*, 2012, 42(11): 1237-1255.
- [9] 王金东, 张智明. 量子密钥分发系统的现实无条件安全性[J]. *量子电子学报*, 2014, 31(4): 449-458.
- WANG J D, ZHANG Z M. Unconditional security of quantum key distribution based on practical devices [J]. *Chinese Journal of Quantum Electronics*, 2014, 31(4): 449-458.
- [10] 黄靖正. 量子密钥分配系统实际安全性研究[D]. 合肥: 中国科学技术大学, 2014.
- HUANG J Z. Practical security analysis of quantum key distribution system [D]. Hefei: University of Science and Technology of China, 2014.
- [11] BENNETT C H, BRASSARD G. WITHDRAWN: quantum cryptography: public key distribution and coin tossing [J]. *Theoretical Computer Science*, 1984(560): 175-179.
- [12] DISTRIBUTION D S Q K. Decoy state quantum key distribution[J]. *Iium Engineering Journal*, 2010, 23(4): 86-90.
- [13] PEEV M, LANGER T, LORUNSER T, et al. The SECOQC quantum key distribution network in Vienna [C]//Conference on Optical Fiber Communication-Includes Post Deadline Papers, March 22-26, 2009, San Diego, CA, USA. New Jersey: IEEE Press, 2009: 1-3.
- [14] TENG-YUN C, JIAN W, HAO L, et al. Metropolitan all-pass and inter-city quantum communication network [J]. *Optics Express*, 2010, 18(26): 27217.
- [15] STUCKI D, LEGRE M, BUNTSCHU F, et al. Long-term performance of the SwissQuantum quantum key distribution network in a field environment [J]. *Neuroscience Letters*, 2012, 13(12): 123001-123018.
- [16] SASAKI M, FUJIWARA M, ISHIZUKA H, et al. Field test of quantum key distribution in the Tokyo QKD network [J]. *Optics Express*, 2011, 19(11): 10387-10409.
- [17] 陈巍. 光纤量子密钥分配的实验研究[D]. 合肥: 中国科学技术大学, 2008.
- CHEN W. Experimental research on fiber quantum key distribution [D]. Hefei: University of Science and Technology of China, 2008.
- [18] 王双. 光纤量子密钥分配关键技术研究[D]. 合肥: 中国科学技术大学, 2011.
- WANG S. Research on the key technologies of fiber quantum key distribution[D]. Hefei: University of Science and Technology of China, 2011.
- [19] 刘洋. 远距离量子密钥分发系统的相关研究[D]. 合肥: 中国科学技术大学, 2012.
- LIU Y. The experimental study of long range Quantum key distribution system [D]. Hefei: University of Science and Technology of China, 2012.
- [20] 亓波. 量子通信光学地面站 ATP 关键技术研究[D]. 北京: 中国科学院光电技术研究所, 2014.
- QI B. Study on acquisition, tracking and pointing key technology of optical ground station for quantum communication [D]. Beijing: the Institute of Optics and Electronics, Chinese Academy of Sciences, 2014.
- [21] CHOI I, ZHOU Y R, DYNES J, et al. First quantum secured 10-Gb/s DWDM transmission over the same installed fibre[C]//2014 European Conference on Optical Communication (ECOC), September 21-25, 2014, Cannes, France. New Jersey: IEEE Press, 2014: 1-3.
- [22] ALAKSIC S. Perspectives and limitations of QKD integration in metropolitan area networks [J]. *Optics Express*, 2015, 23(8): #232520.
- [23] DAMIEN S, CLAUDIO B, SYLVAIN F, et al. Continuous high speed coherent one-way quantum key distribution [J]. *Optics Express*, 2009, 17(16): 13326-13334.
- [24] TAKWSUE H, DYER S D, STEVENS M J, et al. Quantum teleportation over 100 km of fiber using highly efficient superconducting nanowire single-photon detectors [J]. *Optica*, 2015, 2(10): 832-836.
- [25] NATSHEH A, GBADEGESHIN S, RIMPILAINEN A, et al. Identifying the challenges in commercializing high technology: a case study of quantum key distribution technology [J]. *Technology Innovation Management Review*, 2015, 5(1): 26-36.
- [26] ETSI-GS-QKD-002: quantum key distribution use cases [EB/OL]. [2015-12-23]. http://www.etsi.org/deliver/etsi_gs/qkd/001_099/002/01.01.01_60/gs_qkd002v010101p.pdf.
- [27] ETSI-GS-QKD-003: quantum key distribution components and internal interfaces[EB/OL].[2015-12-23]. http://www.etsi.org/deliver/etsi_gs/QKD/001_099/003/01.01.01_60/gs_QKD003v010101p.pdf.
- [28] ETSI-GS-QKD-004: quantum key distribution application interface [EB/OL].[2015-12-23]. http://www.etsi.org/deliver/etsi_gs/QKD/001_099/004/01.01.01_60/gs_QKD004v010101p.pdf.
- [29] ETSI-GS-QKD-005: quantum key distribution security proofs [EB/OL].[2015-12-23]. http://www.etsi.org/deliver/etsi_gs/QKD/001_099/005/01.01.01_60/gs_QKD005v010101p.pdf.
- [30] ETSI-GS-QKD-008: quantum key distribution QKD module security specification [EB/OL]. [2015-12-23]. http://www.etsi.org/deliver/etsi_gs/QKD/001_099/008/01.01.01_60/gs_QKD008v010101p.pdf.
- [31] ETSI white paper No.8. quantum safe cryptography and security [EB/OL].[2015-12-23]. <http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf>.
- [32] ALLEAUME R, CHAPURAN T E, CHUNNILALL C J, et al. Worldwide standardization activity for quantum key distribution [C]//Globecom Workshops (GC Wkshps), December 8-12,

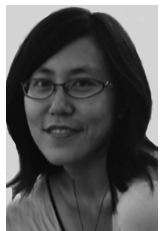
2014, Austin, TX, England. New Jersey: IEEE Press, 2014: 656-661.

- [33] Characterisation of optical components of weak coherent pulse quantum key distribution systems [EB/OL].[2015-12-23]. <http://projects.npl.co.uk/MIQC/publications.html>.

[作者简介]



赖俊森(1983-),男,博士,中国信息通信研究院技术与标准研究所高级工程师,主要研究方向为高速光传输与光网络技术。



吴冰冰(1984-),女,博士,中国信息通信研究院技术与标准研究所高级工程师,主要研究方向为光电子器件、高速光传输与光网络、光信号处理技术。



汤瑞(1984-),男,中国信息通信研究院技术与标准研究所工程师,主要研究方向为高速光传输与光网络技术。



赵文玉(1974-),男,博士,中国信息通信研究院技术与标准研究所主任工程师,主要研究方向为40 Gbit/s、100 Gbit/s WDM, OTN等光传送网新技术研究、标准制定以及系统测试评估。



张海懿(1972-),女,中国信息通信研究院技术与标准研究所高级工程师、部门主任,主要研究方向为光传输系统、OTN、PTN、WDM系统、SDH系统、MSTP、自动交换光网络以及电信传送网络体制标准、运营商技术咨询。