



专题：量子保密通信技术与应用

量子保密通信测评与标准化发展分析

赖俊森¹, 吴冰冰¹, 汤瑞¹, 丁梦宇², 赵文玉¹, 张海懿¹

(1. 中国信息通信研究院技术与标准研究所, 北京 100191;

2. 工业和信息化部电信设备认证中心, 北京 100088)

摘要: 基于量子密钥分发 (QKD) 的量子保密通信 (QSC) 是未来提升信息安全保障能力的有效解决方案之一。随着量子保密通信实验网络建设和试点应用的发展, 相关测试评估和标准化的需求日益明显。在介绍量子保密通信技术原理和系统架构的基础上, 探讨量子保密通信系统的测试评估方法和标准化研究最新进展, 进一步分析了量子保密通信测评与标准化目前存在的典型问题, 最后对其未来发展前景进行了展望。

关键词: 量子密钥分发; 量子保密通信; 测试评估; 标准化

中图分类号: TN915

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018245

Analysis on the progress of quantum secure communication test evaluation and standardization

LAI Junsen¹, WU Bingbing¹, TANG Rui¹, Ding Mengyu², ZHAO Wenyu¹, ZHANG Haiyi¹

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

2. Telecommunications Equipment Certification Center, Ministry of Industry and Information Technology of China, Beijing 100088, China

Abstract: Quantum key distribution (QKD) based quantum secure communication (QSC) is one of the promising solutions for improving information security. With the development of experimental network construction and demonstrational application, the demand of QSC test evaluation and standardization is becoming more urgent. Based on the introduction of technology and architecture of QSC system, the latest progress of QSC test evaluation and standardization was reviewed, typical questions in test evaluation and standardization were analyzed, and development trends and prospects were also discussed.

Key words: quantum key distribution, quantum secure communication, test evaluation, standardization

1 引言

量子通信是利用微观粒子 (如光子) 的量子

叠加态或量子纠缠效应等进行信息或密钥传输的新型通信方式, 主要分为量子隐形传态 (quantum teleportation, QT) 和量子密钥分发 (quantum key

收稿日期: 2018-08-01; 修回日期: 2018-09-07

基金项目: 国家自然科学基金资助项目 (No.61471128, No.61671159)

Foundation Items: The National Natural Science Foundation of China (No.61471128, No.61671159)

distribution, QKD) 两类^[1]。量子隐形传态基于量子纠缠对分发测量实现收发双方的信息直接传输,但是受制于高品质纠缠源制备和分发测量等技术瓶颈,目前尚未进入实用化,是量子信息领域前沿研究的热点方向之一^[2]。量子密钥分发基于量子叠加态的制备、传输和测量,实现收发双方之间的共享密钥生成,之后再通过对称加密方式完成信息的加密传输和解密接收,基于量子密钥分发的保密通信称为量子保密通信(quantum secure communication, QSC)^[3]。量子保密通信是量子信息领域中率先进入实用化的技术方向,是未来提升信息安全保障能力的解决方案之一^[4]。有部分媒体和业者常将量子通信、量子密钥分发和量子保密通信等概念混为一谈,容易引发误解和不必要的争论,需要进行明确区分。

近年来,我国量子保密通信技术研究和试点应用发展较为迅速,已初步形成集技术研究、设备制造、建设运维和安全应用为一体的产业链。以“墨子号”量子科学实验卫星为代表的科研成果具备先进水平;多家量子保密通信设备厂商具备提供商用化解决方案能力;以量子保密通信“京沪干线”为代表的示范应用线路和济南、合肥、北京、上海等地的城域网示范应用项目在数量和规模方面处于领先;政务、金融和关键基础设施等高安全需求领域也开始探索基于量子保密通信的信息安全应用。

随着量子保密通信技术和应用的发展,相关测评与标准化的需求也日益明显。由于量子保密通信属于量子物理、光通信和信息安全等多学科交叉的新兴技术领域,用户对于其技术原理、工作机制和指标参数以及系统设备可靠性和安全性等方面都存在一个认识理解和信任的过程。此外,量子保密通信目前应用场景主要面向高安全性需求的重要通信领域,对于技术和设备的测试评估和检测认证都有很高要求。在缺少相应的测评规范和标准体系的情况下,现有的试点示范应用向

规模化商用和产业化应用的推广和转化将面临困难。通过积极研究和构建量子保密通信测评机制和标准体系,才能充分验证量子保密通信系统的功能、性能和安全性等核心价值,同时也能够对技术研究和产品研发形成有效的引导,促进技术演进、成本优化和产业发展。研究和建立量子保密通信测评机制和标准体系已经成为推动其商用化发展和产业化应用的必要条件之一。

本文在介绍量子保密通信技术原理和系统架构的基础上,提出系统测评整体方案,分析关键测评项目和方法,分析相关标准化研究进展,讨论测评与标准化面临的主要问题,并对其发展前景进行展望。

2 系统原理架构

量子密钥分发(QKD)根据物理机制和协议类型不同,可以分为基于单光子调制的离散变量协议,如BB84、B92、DPS、COW;基于多光子调制的连续变量协议,如GG02;基于纠缠光子对的纠缠协议,如E91。其中,BB84是最早提出并获得广泛应用的QKD协议,在理论安全性证明方面也更加完备。由于单光子源技术尚不成熟,弱相干脉冲(WCP)光源结合诱骗态强度调制是目前BB84协议的实用化解决方案。根据量子态的制备和测量方式的不同,诱骗态BB84协议QKD的系统实现还可以进一步分为偏振调制、相位调制和时间相位调制等不同技术方案。诱骗态BB84协议QKD技术发展成熟应用广泛,系统设备的多厂商商用化水平较高,也是目前系统测评和标准化研究的主要关注对象。

诱骗态BB84协议QKD系统架构和主要测试点如图1所示。QKD发射机中的弱相干脉冲(WCP)光源经过诱骗态强度调制之后,进行随机控制的量子态制备调制,在经过衰减器之后,将量子态光信号输出光强控制到平均光子数小于1光子/脉冲的单光子水平。同时,QKD发射机

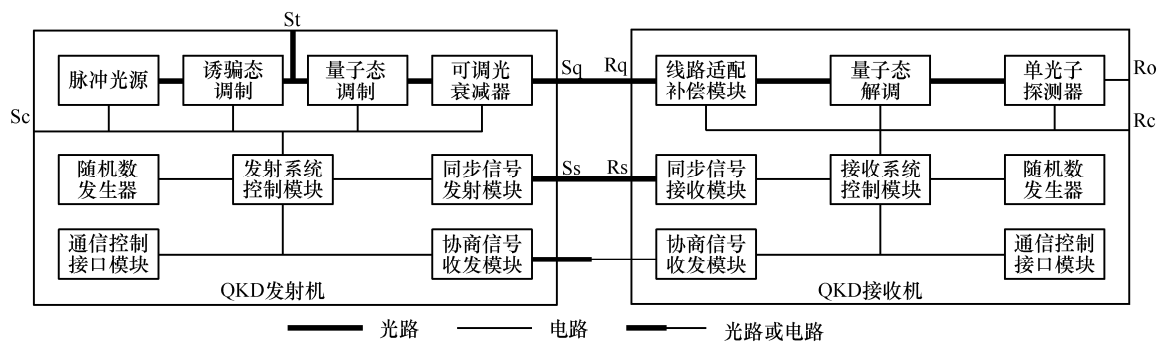


图 1 诱骗态 BB84 协议 QKD 系统架构和主要测试点

输出同步光信号，作为接收机进行量子态光信号检测接收的触发源信号。QKD 接收机对经过光纤线路传输之后的量子态光信号进行线路适配补偿和量子态解调，在基于随机控制的单光子探测器（SPD）完成光子检测和接收计数。QKD 发射机和接收机之间通过光纤或以太网协商信道进行身份认证、协议流程交互和算法后处理，协议算法处理的主要步骤包括基矢比对、密钥筛选、误码估计、纠错校验和保密增强等步骤，最终实现 QKD 发射机和接收机之间的共享随机密钥的生成和提取。其中 Sc、St 和 Sq 是量子光信号测试参考点，分别对应发射机时钟信号、测试光信号和量子光输出信号；Ss 和 Rs 是同步光信号测试参考点，分别对应同步光输出信号和同步光接收信号；Rc、Rq 和 Ro 是单光子探测器测试参考点，分别对应接收机时钟信号、量子光接收信号和 SPD 输出信号。

QSC 使用量子密钥并采用对称加密体制实现业务信息的保密通信。在信息论层面具备可证明无条件安全性的量子保密通信需要同时满足使用量子密钥、一次一密加密算法和散列函数校验算法的 3 个基本条件。QSC 和传统的对称加密式保密通信在加密算法、校验算法和整体功能方面基本一致，主要区别在于使用了量子密钥替换了传统保密通信中收发双方通过协商得到的加密密钥。

QSC 系统的主要构成如图 2 所示，主要设备类型包括量子密钥分发（QKD）设备、量子密钥管理（QKM）设备和量子加密应用（QEA）设备。其中，QKD 设备和链路传输辅助设备（例如波分复用器和光路交换机）属于密钥分发的物理传输层，负责完成点到点的量子态光信号传输和共享量子密钥生成。管控层的 QKM 设备结合网管系统实现网元管理、组网管理和密钥管理等功能，

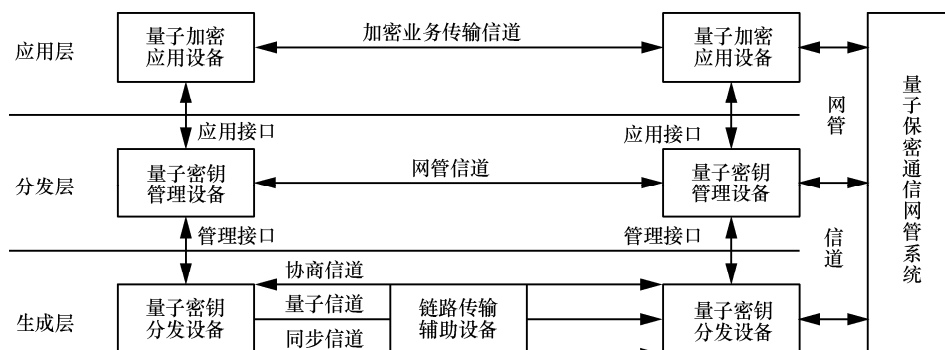


图 2 量子保密通信系统结构原理

QKM 设备间的组网实现端到端的共享密钥生成, 通过管理接口对 QKD 设备进行配置管理, 通过应用接口为上层加密业务传输提供量子密钥服务。QEA 设备使用量子密钥对业务信号进行加密处理, 通过业务信道传输后进行密文接收和解密还原。常见的 QEA 设备包括量子加密 VPN、量子加密路由器和量子安全密码机等。QEA 设备通常可以保留传统密钥协商功能作为量子密钥的备份, 并且具备在量子密钥和传统协商密钥之间进行密钥源切换的功能。

3 测评方案及方法

量子保密通信系统测评方案和主要内容如图 3 所示, 针对 QKD 设备系统, 主要进行设备接口测试和系统功能性能测试。其中, QKD 设备接口测试包括发射机信号接口测试、发射机同步接口测试和接收机 SPD 模块测试。QKD 系统功能性能测试主要涉及协议一致性、密钥成码能力和质量以及设备可靠性。针对 QKM 设备和网管系统, 主要进行网管功能和性能测试, 其中主要包括设备网元管理功能和性能测试、系统组网管理功能和性能测试以及系统密钥管理功能和性能测试。针对 QEA 设备, 则主要进行业务加密的功能和性能测试, 主要涉及加密密钥质量测试、业务加密功

能测试和加密业务信道性能测试。

在 QKD 设备测试中, 发射机信号接口测试的主要关注对象是信号光脉冲重复频率、脉冲宽度、脉冲时域抖动 (Jitter)、中心波长及偏移量、光谱特性、信号光输出功率和平均光子数 (单光子特性)。发射机量子态光信号的输出接口光功率通常小于 -70 dBm, 无法进行常规光信号参数的仪表测试, 所以 QKD 发射机可以在光脉冲信号衰减至单光子水平之前, 提供测试光信号接口 St, 基于高带宽示波器 (OSC) 和高分辨率光谱仪 (OSA) 对光信号脉冲信号进行重复频率、脉冲宽度、脉冲抖动、中心波长和光谱特性等参数测量。对于信号输出光功率和平均光子数参数测试, 在 QKD 发射机量子态光信号的输出接口 Sq, 使用高灵敏度光功率计, 直接进行信号输出光功率的测量, 再通过结合信号输出光功率 (P_{mean})、脉冲重复频率 (f_{pulse}) 和信号中心波长 (λ_{pulse}) 的测试结果, 计算得到量子态光信号的平均光子数统计值, 计算式如下:

$$\mu = \frac{P_{\text{mean}} \times \lambda_{\text{pulse}}}{f_{\text{pulse}} \times h \times c} \quad (1)$$

其中, h 为普朗克常量, c 为光速。QKD 发射机同步光接口测试的主要参数为同步脉冲光重复频率、脉宽、抖动、中心波长和光谱特性以及输出

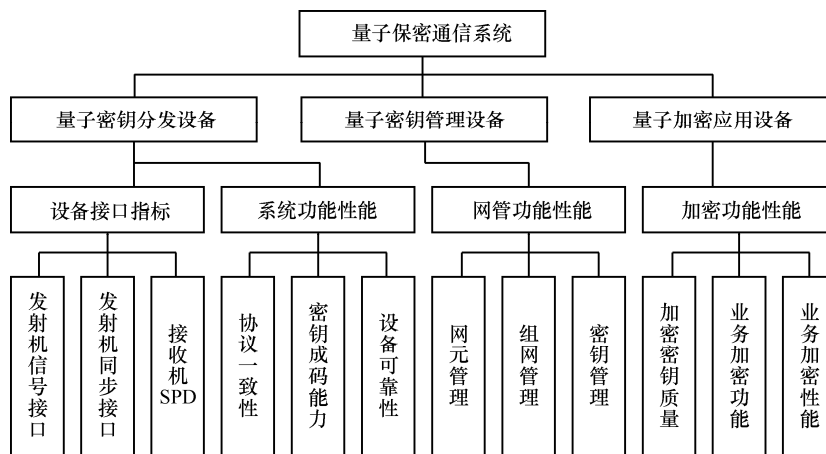


图3 量子保密通信系统的测评方案和主要内容



光功率和接收灵敏度。同步光灵敏度测试可用 OSC 监测 Rc 点的锁相恢复时钟信号，或者 QKD 系统网管的同步光丢失告警，测试同步光信道衰减增大导致同步光接收失效的临界点，从而确定其接收灵敏度。

QKD 设备的 SPD 模块测试，主要关注门控重复频率、检测响应宽度、暗计数概率、后脉冲概率、探测效率和死时间等参数。主要测试环境包括参考 WCP 光源、同步时钟源、检测事件分析仪 (TDC) 等配套仪表和器件。其中，门控重复频率、暗计数率和死时间参数通过仪表测量直接读取，SPD 模块光子检测响应的有效门宽，可以通过同步时钟源调节输入脉冲和 SPD 模块的门控时延，得到不同时延位置的 TDC 探测事件计数，计数分布直方图的 -3 dB 宽度即 SPD 模块的有效门宽。对于后脉冲概率和探测效率，可通过式 (2)、式 (3) 统计计算：

$$\eta = \frac{C_{\text{peak}}}{\mu \times f_{\text{pulse}} \times (1 - C_{\text{all}} \times T_{\text{dead}})} \quad (2)$$

$$P_{\text{after}} = \frac{C_{\text{all}} \times C_{\text{peak}} - C_{\text{dark}}}{C_{\text{peak}}} \quad (3)$$

其中， η 是探测效率， C_{peak} 是 TDC 探测事件计数峰值点， C_{all} 是 TDC 的光子探测事件计数总和， T_{dead} 是死时间， P_{after} 是后脉冲概率，而 C_{dark} 是暗计数率。

QKD 系统测试中的密钥成码速率测试可以通过网管或上位机软件查询实时密钥成码率（最小时间间隔的密钥速率统计，例如 10 s），或者统计一定时间段（例如 1 h）内生成的密钥总量。同时可以结合 SPD 光子探测输出计数和量子信道误码率等参数统计，并根据信道衰减变化条件下的成码速率变化进行验证。对于 QKD 系统传输能力测试，可以使用标准单模光纤环境模拟不同损耗信道情况，例如 25 km、50 km、75 km 和 100 km 光纤，分别对应 5 dB、10 dB、15 dB 和 20 dB 损耗，测试不同信道状态下的 QKD 设备传输与成码

能力。QKD 设备的承诺密钥速率（例如 1 kbit/s），也可以通过在适合的光纤跨段加额外可调衰减器方式进行标定和测量。QKD 系统协商信道抓取分组分析可确定交互信息类型和主要流程步骤，验证系统主要工作流程与诱骗态 BB84 协议要求的符合程度。协商信道通常基于私有协议进行编码或数据压缩，协议一致性分析需要提供协商通信协议机制和编码方式。

QKD 设备长期稳定性测试验证系统长期稳定成码能力，包括实时成码率和小时平均成码率等，测试周期根据具体需求确定，可以为 24 h 或更长。环境可靠性主要验证 QKD 系统在不同温度和湿度环境下保持正常工作的能力，测试环境为温度循环实验室。测试环境的温度和湿度要求根据具体需求确定。

QKM 设备和网管系统通过管理接口实现对 QKD 设备和 QEA 设备的网元管理功能，是正确配置和合理使用 QKD 和 QEA 设备的基本保证。QKM 管理设备的网管功能和性能测试主要通过网管系统或上位机软件进行配置和管理功能验证，并测试其主要性能参数。网元管理功能主要包含 QKD 设备、链路传输辅助设备和 QEA 设备的入网、离网配置、管理和查询。密钥管理功能主要包含 QKM 设备从 QKD 设备输入并存储密钥，量子密钥备份、恢复和销毁管理，QKM 设备向 QEA 设备输出密钥以及密钥管理存储空间容量和密钥输入输出速率等。组网管理功能主要包括 QKM 设备组网同步配置和工作状态查询，量子密钥生成策略和组网路由策略配置管理以及量子密钥中继的配置、管理和工作状态查询。其中，密钥中继组网测试指定包含中继的 QSC 系统节点，进行 QKM 设备同步配置、密钥路由策略配置和密钥中继配置，通过 QSC 网管验证端到端密钥成码功能，并统计端到端密钥成码速率，包含实时成码率和小时平均成码率。现阶段，由于密钥管控分层的 QKM 设备和组网技术均为各厂

商私有的技术解决方案, QKM 功能性测试首先关注基本的配置和管理功能, 同时通过将密钥管理架构、密钥中继方案、中继路由策略和端到端密钥成码方案等方面的共同点和差异性进行呈现和分析, 对后续的 QKM 标准化提供功能和性能需求的认知共识以及实现方案等方面的研究基础。

QEA 设备属于 QSC 系统中的业务应用层, 包括量子加密 VPN、量子加密路由器和量子密码机等设备形态。QEA 设备和传统对称加密式保密通信设备的主要区别在于使用量子密钥取代协商密钥, 由此带来的功能和性能差异是测试研究的关注点。QEA 设备使用量子密钥进行业务加密, 使用密钥一致性测试软件工具和密钥随机性分析测试工具可以进行密钥质量测试。通过读取和存储满足随机性检测要求的密钥文件, 例如单个密钥样本长度 10^6 bit, 1 000 组密钥样本, 之后进行测试软件工具的离线分析和验证。其中, 密钥随机性测试则需要满足 GM/T 0005-2012《随机性检测规范》的测试要求。采用业务分析仪进行业务加密性能、密钥源切换时间和系统长期稳定性测试, 通过业务分析仪设置不同类型、分组长和带宽的双向测试业务, 检测加密业务信道的吞吐量、分组丢失率和业务传输时延, 密钥源切换过程导致的加密业务受损时间以及加密业务长期稳定性, 例如 24 h 加密业务正常传输、无告警和丢失分组等。通过网管系统对 QEA 设备的量子密钥加密的具体配置和状态管理、备份用传统密钥协商和密钥源切换等功能进行验证。

4 标准化新进展

量子密钥分发系统是量子保密通信的核心, 也是量子保密通信标准化研究的重点。近年来, 以 ETSI-QKD/ISG 和 CCSA-ST7 为代表的标准组织, 在量子密钥分发的标准化研究工作方面均取得了一定进展^[5]。

2018 年 3 月, ETSI-QKD/ISG 完成了 ETSI GR

QKD 003 V2.1.1 的修订和发布, 其中在协议技术部分增加了相干单向 (COW) 协议和 CV-QKD 协议技术描述, 在光源和探测器部分增加了 SPD 自由运转模式和超导纳米线单光子探测器 (SNSPD) 描述, 增加了对相位相干 WCP 光源和纠缠光子源的描述, 去除了和其他标准中重叠的测试参数和测评方法的描述。2018 年 6 月, ETSI-QKD/ISG 完成了 ETSI GR QKD 007 V0.0.3 的批准并将发布, 其中结合量子物理学和经典加密理论的定义和描述, 给出了 QKD 技术涉及的术语、定义和缩略语的参考规范, 可以对 QKD 技术描述的相关用语进行统一, 同时为不熟悉 QKD 技术的标准阅读者提供相关技术参考。此外, 对 QKD-004 的 QKD 设备应用接口定义、QKD-012 的 QKD 应用部署器件和通信信道参数、QKD-013 的发射机模块光输出接口特性和测试、QKD-014 的加密应用 API 密钥传输协议与数据格式定义以及 QKD-015 的软件定义网络 QKD 应用接口方案 5 项标准草案文稿也进行了进一步的讨论和更新。

2018 年 4 月, CCSA-ST7 完成了《量子保密通信系统测试评估》研究课题, 成为该标准组织完成的首个量子保密通信标准化研究成果。该研究报告介绍了量子保密通信系统的基本原理、典型设备和功能特性, 梳理量子保密通信系统测评的发展现状、存在的问题以及目前的研究进展, 在深入分析量子保密通信系统的测评内容及测试环境要求的基础上, 重点研究了量子保密通信系统设备的主要测试项目和对应的测试方法, 主要包括诱骗态 BB84 协议量子密钥分发设备接口和系统特性、量子密钥管理功能和性能以及量子加密应用功能和性能等。2018 年 7 月,《量子密钥分发 (QKD) 系统技术要求 第 1 部分: 基于 BB84 协议的 QKD 系统》《量子密钥分发 (QKD) 系统测试方法》和《量子密钥分发 (QKD) 系统应用接口》3 项通信行业标准完成正式立项并开始进行技术文稿讨论和研究, 后续将为量子



保密通信的规模应用部署提供有效的标准参考引导和测评规范支持。

5 问题与前景

QKD 系统的现实安全性研究和测评是量子保密通信测评和标准化关注的一项重要内容。由于实际 QKD 系统器件无法完全满足理论协议安全性证明的假设要求，可能存在被用于恶意攻击和密钥窃听的系统漏洞，即存在 QKD 系统的现实安全性问题。关于 QKD 系统现实安全性问题的研究分析可以参见 ETSI-ISG-QKD 工作组发布的 GS-QKD-005《QKD 安全性证明》、GS-QKD-008《QKD 模块安全性规范》以及 CCSA-ST7 正在开展的研究课题 2017B67《量子密钥分发安全性研究》。QKD 系统现实安全性涉及器件特性分析、漏洞攻击研究和安全防护证明等方面的持续发展演进的学术性研究，例如对时移攻击、探测器控制攻击、信道校准攻击和相位重映射攻击等方式的鉴别和防范以及可以消除所有接收机相关侧信道风险的新型测量设备无关量子密钥分发（MDI-QKD）协议等新型协议和系统方案也都处于研究之中。目前，对于 QKD 系统安全性的体系框架和相关要求尚未完全建立和明确，开展 QKD 系统现实安全性测评的基础条件尚不成熟。在 QKD 设备及器件的安全性要求以及针对不同威胁的 QKD 系统安全要求等标准规范明确之后，可适时开展 QKD 系统的现实安全性标准化和相关测评的研究。2017 年 11 月，由中国代表提议在 IEC/ISO JTC1/SC27 工作组立项了 QKD 系统安全性要求和测试评估方法的研究项目（SP N1502），将为推动 QKD 现实安全性研究和相关标准和测评工作的开展奠定基础。

不同设备厂商之间和不同运维管理域之间的量子保密通信系统的互联互通和互操作是量子保密通信测评和标准化关注的另一项重要内容。QKD 在原理上属于点到点之间的传输技术，未来

QSC 网络中多个 QKD 厂商之间的设备互联互通或多个 QSC 运营商之间的跨管理域组网等场景和需求更有可能出现在基于 QKM 设备和网管系统的量子密钥管控层，而非基于 QKD 设备的量子密钥分发物理层。目前已经开展的针对 QKM 设备和 QSC 网管系统的初步测试，主要验证设备配置管理、密钥中继组网和系统监控功能等方面功能和性能，以推动业界对 QKM 和网管形成趋于一致的理解和共识。同时，CCSA-ST7 也正在开展量子密钥管控层的网络架构、主要接口和协议等方面的研究。随着量子密钥管控层架构、接口和协议等方面的场景需求、技术研究和标准化的逐步明确，未来可以适时开展多厂商间或跨管理域的 QSC 系统互联互通技术研究和相关测试评估。

随着量子保密通信设备研发、网络建设和标准化工作的推进，相关测试评估工作近年来也在逐步开展。随着相关测评和标准化工作的开展，量子密钥分发设备和量子保密通信设备的工程化水平、环境适应性和网管运维功能和性能等多方面技术特性和功能性能得到有效的验证和一定程度的提升，同时也为设备厂商、建设运维单位和用户提供了客观中立的量子保密通信技术、产品和网络的验证评估服务。随着量子保密通信系统测评工作的进一步开展和完善，将对相关设备技术指标、网络建设方案和应用发展情况进行有效验证和规范引导，有助于促进量子保密通信前沿技术发展、设备研究迭代和保障网络建设与应用运维质量，从而进一步推动量子保密通信产业的成熟和发展。

6 结束语

基于量子密钥分发的量子保密通信技术是未来提升信息安全防护能力的有效技术方案之一，近年来的技术研究、设备研制、网络建设和示范应用发展较为迅速。随着量子保密通信技术和产

业的发展,相关测试评估和标准化的需求也日益明显。本文在介绍量子保密通信技术原理和系统架构的基础上,提出量子保密通信系统的整体测评方案,并对关键测试项目和测试方法进行分析,对近来的标准化研究最新进展进行了讨论,同时探讨了量子保密通信未来安全性和互联互通测评与标准化面临的问题和前景。我国量子保密通信技术和产业整体发展态势良好,相信未来在业界各方的共同努力下,随着相关标准化和测评工作等进一步推动和开展,有望进一步促进技术和产业发展与规模化商业应用。

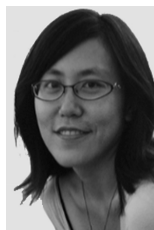
参考文献:

- [1] LO H K, CURTY M, TAMAKI K. Secure quantum key distribution[J]. Nature Photonics, 2014, 8(8): 595-604.
- [2] DIAMANTI E, LO H K, QI B, et al. Practical challenges in quantum key distribution[J]. NPJ Quantum Information, 2016(2): 16025.
- [3] 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): 46-52.
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): 46-52.
- [4] 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, 37(3): 123-129.
- [5] 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.

[作者简介]



赖俊森 (1983-), 男, 博士, 中国信息通信研究院高级工程师, 主要研究方向为高速光传输、WDM/OTN、物理层监测、量子通信新技术。



吴冰冰 (1984-), 女, 博士, 中国信息通信研究院高级工程师, 主要研究方向为光传输系统、高速光传输与光网络、量子通信与量子信息技术。



汤瑞 (1984-), 男, 中国信息通信研究院高级工程师, 主要研究方向为高速光传输、WDM/OTN、光网络技术等。

丁梦宇 (1989-), 女, 工业和信息化部电信设备认证中心助理工程师, 主要从事电信设备进网管理政策等方面研究工作。

赵文玉 (1973-), 男, 博士, 中国信息通信研究院主任工程师, 主要研究方向为高速光纤通信网、WDM/OTN、量子通信等光网络新技术、标准制订和系统测试评估等。

张海懿 (1972-), 女, 中国信息通信研究院高级工程师、宽带网络研究部主任, 主要研究方向为高速光纤通信网、自动交换光网络、SDN 和量子通信等新技术、体制标准制订、运营商技术咨询等。