

量子密钥分发城域光组网技术前瞻

王华, 赵永利

(北京邮电大学信息光子学与光通信国家重点实验室, 北京 100876)

摘 要: 量子密钥分发是量子通信的基本实现技术, 能够提供安全的密钥分发方式。随着点到点量子密钥分发技术的成熟与发展, 多点到多点的量子密钥分发组网成为未来发展的趋势, 如何构建多点到多点的量子密钥分发网络是当前面临的迫切问题。提出了量子密钥分发城域光网络架构, 研究了量子密钥分发城域光组网中的关键问题及解决策略, 探讨了量子密钥分发城域光网络在相关场景的应用, 最后总结分析了量子密钥分发组网未来的发展方向及面临的挑战。所提出的量子密钥分发网络架构能够高效进行多点间的量子密钥分发, 从而为业务灵活地提供密钥资源。

关键词: 量子密钥分发; 城域光组网; 安全

中图分类号: TP303

文献标识码: A

doi: 10.11959/j.issn.1000-436x.2019210

Overview of quantum key distribution metropolitan optical networking technology

WANG Hua, ZHAO Yongli

State Key Laboratory of Information Photonics and Optical Communications,
Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract: Quantum key distribution is a basic implementation technology of quantum communication, which provides a secure key distribution method. With the maturity and development of point-to-point quantum key distribution technology, multi-point to multi-point quantum key distribution networking has become a trend of development in the future. How to construct a multi-point to multi-point quantum key distribution network is currently urgent problem. The architecture of QKD-MON was proposed, the key problems and corresponding strategies in QKD-MON were discussed, the applications of QKD-MON in various scenes were studied, and finally the future development direction and challenges were discussed. The QKD network architecture proposed can efficiently implement QKD between multiple points and provide key resources for the customer flexibly.

Key words: quantum key distribution, metropolitan optical networking, security

1 引言

近年来, 信息网络相关技术的创新、变革突破、融合应用已渗透到政治、经济等领域, 信息交互资源与关键基础设施已成为国家发展重要的“战略资产”。相应地, 信息网络也面临着越来越严重的安全隐患^[1-4]。作为一种安全密钥分发技术, 量子密钥

分发技术可以为信息网络提供密钥, 其安全性和理论完备性由“不确定性原理”“海森堡测不准原理”“量子不可克隆定律”等量子力学基本定律保证, 借助于理论上“无条件安全”“一次一密”的优势^[5-9], 量子密钥分发技术近年来成为世界各国在网络信息安全方面的研究热点。

经过几十年的发展, 量子密钥分发技术从设备

收稿日期: 2019-07-08; 修回日期: 2019-08-20

通信作者: 赵永利, yonglizhao@bupt.edu.cn

基金项目: 国家自然科学基金资助项目 (No.61822105)

Foundation Item: The National Natural Science Foundation of China (No.61822105)

研发、协议设计到网络部署都取得了长足进步并逐步成熟应用。目前，量子密钥分发组网技术^[10-13]在国际上刚刚起步，具有极大的研究空间。作为重要的信息基础设施，光城域网可以为量子密钥分发提供可靠的管道资源，其中，信道资源可以连接网络中的量子密钥分发设备^[14-24]。量子密钥分发光网络利用波分复用技术实现量子通道与经典光通道的共纤传输以降低成本^[25-28]。然而，将点对点的量子密钥分发扩展为面向多点互联的量子密钥分发，实现城域网内多用户任意两点间端到端的量子保密通信，才能充分发挥量子密钥分发的应用潜力。

随着量子密钥分发城域网在实际中的不断部署与试用^[29-37]，其组网过程已成为目前亟待解决的热点问题。面向多点互联的量子密钥分发城域网虽然具备与点到点量子密钥分发类似的特征，即由大量的信号调制、发射、接收、检测、后处理等通信功能模块组成^[38-41]，但必须满足组网功能所带来的一系列基础功能：任意两节点间安全密钥分发、灵活高效地部署和配置、无中继密钥传输路由选择、高效故障密钥服务保护等。量子密钥分发城域网不仅支持多用户间的安全通信，还具有城域距离范围内的无中继传输等优势。

围绕量子密钥分发城域网光组网，本文将详细介绍量子密钥分发城域网各个组成部分、组网关键技术、典型应用场景，并对未来可能面临的挑战进行探讨。深入研究分析量子密钥分发城域网相关技术，这对于设备的合理部署、资源的高效利用、运行的可靠性和稳定性具有重要的理论和现实意义。

2 量子密钥分发城域网光网络架构

针对量子密钥分发城域网光网络中网络开放化和管道弹性化的需求，结合端到端密钥分发的特点，提出了一种量子密钥分发城域网光网络架构，具体如图1所示。量子密钥分发城域网光网络架构从上到下可以分为四层：应用层、控制层、QKD(quantum key distribution)层和数据层。应用层主要生成业务的数据连接请求(包括业务安全等级)。针对应用层请求，控制层主要负责在QKD层和数据层上的量子密钥分发路径计算、量子密钥及频谱资源按需分配、信令交互、设备配置等功能。QKD层可为数据层和控制层分发量子密钥，以建立安全的光网络物理层及控制通道环境。数据层和QKD层可共享光传送通道资源，并利用波分复用技术构建数据通

道、密钥通道和测量通道，以提高资源利用率，减少量子密钥独立运行成本。量子密钥分发城域网光网络架构利用软件定义的优势，将光传送网络频谱资源与量子密钥资源统一抽象并通过南向接口提供给控制器，实现对这两类资源的统一控制，完成密钥与业务的高效适配，实现密钥全网分发的目的。在该架构下，QKD层提供的密钥资源除了能对数据通道进行加密之外，还能用于控制通道中控制信息的加密，“双重加密”的方式进一步增强了该架构的安全性。

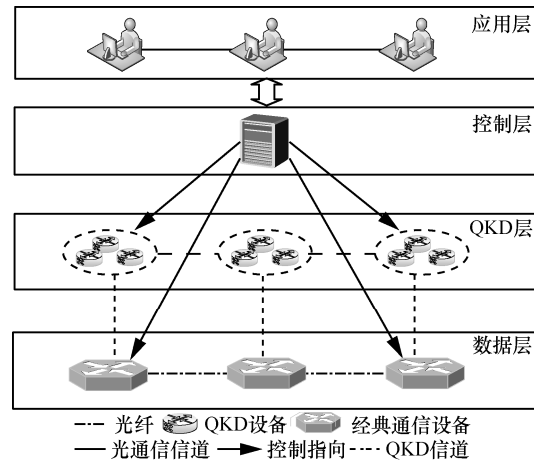


图1 量子密钥分发城域网光网络架构

3 量子密钥分发城域网光组网关键技术

3.1 量子密钥分发城域网光网络节点约束

在量子密钥分发城域网光网络中，量子密钥分发与经典光通信设备所形成的共纤传输节点将成为必然的发展趋势。对于量子密钥分发与经典光通信共纤系统而言，量子信号与经典光信号间的较大光强差异将会导致量子信号的解调出现较高误码，会降低量子密钥分发的传输距离和成码率。由共纤产生的噪声干扰来源主要分为两类，第一类主要由波分器件产生的带外噪声^[42-45]，这是因为通道之间的较小隔离度将会导致经典光漏至量子光波段；第二类主要由拉曼散射和四波混频效应产生^[46-51]，这是因为光纤中传输时的非线性效应会产生新的频率成分，使其频谱延伸至量子光波长。相较于四波混频，自发拉曼散射对量子光信号影响更大。自发拉曼散射源于拉曼效应，当经典光与光纤介质相互作用时，会产生拉曼噪声光子，而拉曼噪声光子的频域分布范围较广，需要在噪声源波长一定范围内延展，且拉曼效应随着光纤长度的增加而变得明显^[52-53]。

为了缓解上述两类噪声干扰对量子密钥分发城

域光组网所带来的影响，通过提出三点基本约束，以实现混合交叉节点结构模型中经典光信道与量子信道间的安全隔离，如图 2 所示。具体约束如下。

约束 1 在量子光与经典光共纤传输时的理想情况下，两者资源消耗之和不超过物理链路上的最大频谱资源数量。

约束 2 在考虑量子光与经典光收发方向相同情况下，信道中拉曼散射、四波混频及波分器件产生的隔离度所带来的影响，可保证量子光在该情况下的最优部署。

约束 3 在考虑量子光与经典光收发方向相反情况下，信道中拉曼散射、四波混频及波分器件产生的隔离度所带来的影响，可保证量子光在这种情况下最优部署。

此外，在保证经典/量子双信道之间安全传输的同时，设置连接量子密钥分发组件与光网络节点内部组件的多类型接口，降低网络建设成本，提高网络性能，优化混合节点内部多维性能参数之间的关联程度，实现量子密钥分发光网络混合节点内部的安全隔离与高效共享。

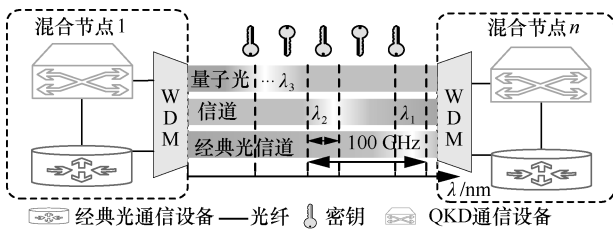


图 2 支持经典光/量子信号共纤传输的节点通信示意

3.2 量子密钥分发城域光网络无中继路由机制

量子密钥分发城域光网络无中继路由机制可以实现量子密钥分发城域光网络中的端到端密钥分发，满足城域光网络范围内的无中继传输。网络中一对节点之间的距离随着路由路径的长度变化而变化，这将导致每对请求节点对之间的密钥生成性能处于可调状态。考虑量子密钥分发在不同距离下的性能参数，将所需服务参数（如密钥量等）视为固定目标，计算合适的路径来生成满足需求的密钥。同时，将量子密钥分发信道切分为许多时隙，这些时隙的灵活分配可以作为满足需求过程中的可调因子。具体路由机制如图 3 所示，需要根据到达时间顺序将请求划分为两类。对于不同时间下到达的安全请求，在获取请求原宿节点及所需密钥数量之后，综合网络中不同路径或链路上的密钥分发性能参数

计算出合适的路由。对于同一时间到达的多个安全请求，需要考虑多个请求来计算并分配合适路由，以优化网络全局服务质量。无中继密钥分发路由技术是支撑量子密钥分发城域光网络灵活组网的关键。一般使用密钥生成速率、密钥缓存量、密钥中继消耗速率等参数描述光网络量子链路的状态，评价链路的质量，所有链路的状态和连接关系构成一个动态的网络拓扑数据库，量子密钥分发城域光网络中的路由表可根据这个数据库，按照距离优先、链路质量优先或者综合评定策略来决定，动态给出密钥中继路由。各个节点实时地更新网络拓扑数据库，共同维护路由表，或者由核心节点或网络来维护路由表。对于大规模的量子密钥分发光网络，一般可通过分域或分层管理来降低路由表维护的难度，提高密钥分发路由收敛的速度，从而实现灵活组网。

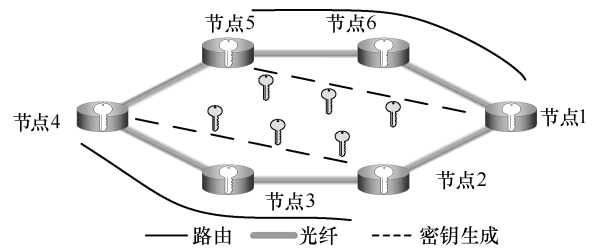


图 3 量子密钥分发城域光网络无中继路由机制

3.3 量子密钥分发城域光网络资源池化方法

量子密钥分发城域光网络中密钥池的构建可以实现业务的安全传输及密钥资源的高效利用，保证密钥的理论上无条件安全，解决现有技术中密钥分发不安全的问题。如图 4 所示，将密钥看成一种池化资源，解耦密钥生成与密钥使用过程。量子通信节点和光节点集成在同一混合量子密钥分发光节点，通过经典光信道和量子信道相互连接，密钥池可以用于存储该节点与相邻节点之间生成的密钥对。基于上述场景，提出了一种量子密钥分发光网络密钥资源池化方法。该方法首先将量子节点与链路资源整合在一个密钥池中，通过量子通信节点产生量子密钥，将量子密钥存储在量子密钥池中，分割量子密钥池为多个密钥空间；然后利用光时分复用技术将密钥空间切分成多个周期性的时间片，这些时间片可以为多个业务提供周期性的密钥并进行密钥更新，可以实现密钥池与业务的“一对多”关系按需分配密钥，大大提升密钥资源的利用率。密钥池的构建主要用于将部分实体密钥池中的资源调度到指定的密钥池中，用来满足特定用户的需求，实现资源的高效利用。

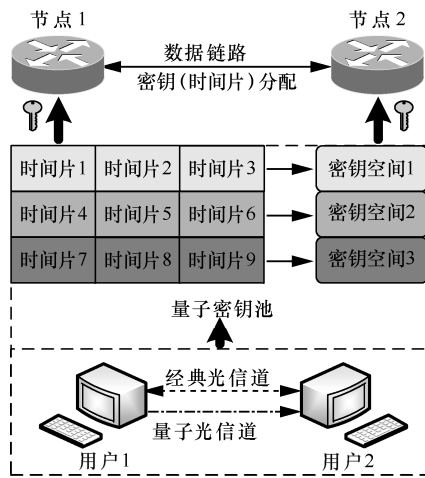


图 4 量子密钥分发网络资源池化示意图

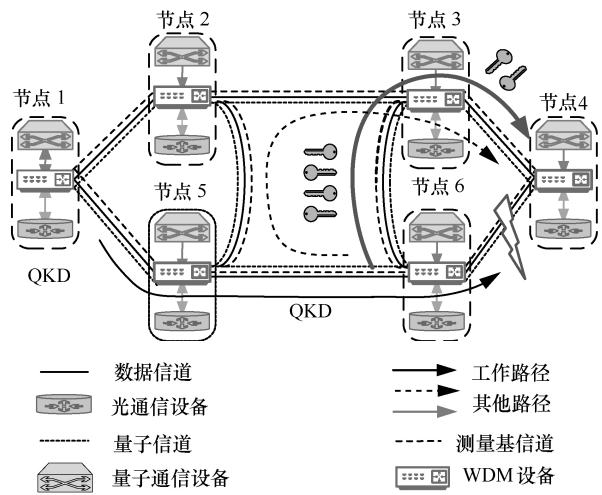


图 5 具备故障容忍特性的多径量子密钥分发示意图

3.4 量子密钥分发城域网多径密钥分发方法

量子密钥分发城域网多径密钥分发可以为网络中的密钥供给服务提供保护恢复机制。结合多径技术，通过多条备用路径的启动可以增强功能的实现效率。密钥供给多径保护方案的核心思想是为每个密钥业务在工作路径上分配多条光纤资源，一条作为工作路径，其他多条作为保护路径。当量子密钥分发网络出现故障后，通过对网络资源进行高效、合理利用来为密钥服务提供保护，为密钥服务工作路径上的每条链路设置共享保护线路，有效提高对量子网络资源的利用。当网络中出现复杂链路故障时，需要将受故障密钥切换到提前设置好的保护资源上，实现对密钥服务的有效保护。本文设计了 2 种方法，即基于专用保护的多径保护方案和基于共享保护的多径保护方案。这 2 种方案确保了密钥供给在工作路径中断时的及时恢复，节省了重路由所消耗的时间。基于专用保护和共享保护的多径方案分别对波长资源进行专用或共享保护设置，设计了不同的密钥保护阈值，以简化由更新密钥引起的资源利用。具体地，如图 5 所示，当存在安全业务请求密钥池为节点 1 和节点 4 分配密钥资源时，可计算 3 条路径：一条工作路径为 1—5—6—4，2 条保护路径分别为 1—2—3—4 和 1—2—5—6—4。当工作光纤收到光纤切断等故障时，将切换到多条保护路径进行密钥重传。

4 典型应用场景

量子密钥分发城域网具有前文所述的优势及基本功能，未来在一些基础网络场景中的作用将会日益突显。具体地，如图 6 所示，量子密钥

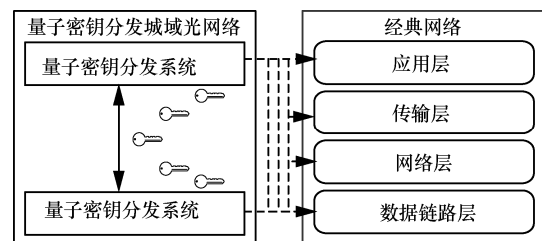


图 6 量子密钥分发网络与经典网络相结合

分发网络可以分别与经典网络中 OSI 模型四层（应用层、传输层、网络层和数据链路层）相结合，以提供安全密钥。相应地，量子密钥分发城域网在一些经典场景中的运用将在下面进行介绍。

4.1 量子密钥分发专用网络

量子保密通信可用于保护企业专网基础设施及其服务的安全性。所谓企业专用网络，即企业或政府机构通过自有网络或从运营商租用的光纤网络，将其总部及所属一个或多个分支机构、数据中心连接组成的专有网络。通过企业专网可为各分支机构提供各种应用服务，例如电子邮件、电话、视频、数据存储、计算等信息服务。在专网中，各分支机构之间通常不需要直接联系，而是通过各数据中心提供的路由进行通信。企业或政府机构通常要求通信服务提供高度的机密性、完整性和真实性，需要强制性地采用专用的安全系统。当前通常采用基于 Internet 协议安全性 (IPSec, Internet protocol security) 或安全传输层协议 (TLS, transport layer security) 的安全虚拟专用网络 (VPN, virtual private network) 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，而密钥链路加密机正好可以与这些技术结合来满足企业网各站点之间信息加密，如图 7 所示。

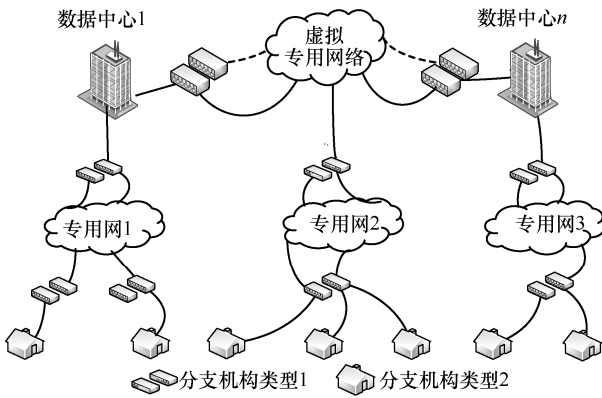


图7 量子密钥分发专用网络

4.2 量子保密接入网络

QKD 有望融入电信接入网的无源光网络(PON, passive optical network)中, 保证 PON 网络中的通信安全。电信接入网使用的 PON 网络结构通常由一个光线路终端 (OLT, optical line terminal) 与多个光网络单元 (ONU, optical network unit) 连接组成。OLT 通常安装在电信网接入机房中, 而 ONU 安装在终端用户附近。目前一台 OLT 可服务于 32~128 个 ONU, 下行业务信息从 OLT 向下游广播到所有 ONU, 而上行业务则采用波分复用方案实现。如图 8 所示, PON 使用无源光器件, 每个 ONU 都可接收到 OLT 的所有下行链路信号。因此, 必须使用加密措施来防止 ONU 对不适合接收的内容进行窃听。当前的解决方案是使用共享对称密钥进行加密/解密, 密钥可以使用智能卡进行分发, 或者采用非对称方法与公钥证书方案进行分发。不难看出, QKD 可以很好地为电信接入网提供新的解决方案。通过 QKD 系统, 可在 OLT 和 ONU 终端用户之间进行安全的密钥分发, 以实现 ONU 用户数据的加密传输, 这对于目前已在中国普遍部署的光纤到户场景具有很大的应用价值。另外, 还可利用 OLT 到 ONU 之间的光纤信道, 用于进行基于单光子或弱光脉冲的量子信号传输, 有望实现 QKD 系统

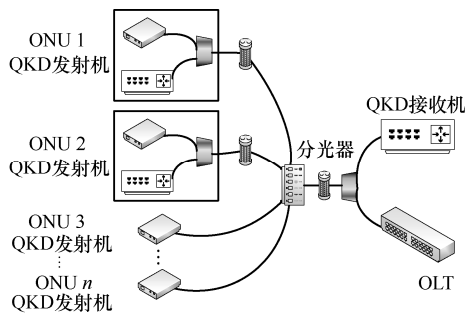


图8 量子密钥分发接入网示意

与 PON 网络在接入网层面的融合。与点对点 QKD 系统不同, PON 中的 QKD 系统需要实现一对多 QKD, 目前已有文献对该场景下的多用户 QKD 技术进行研究及试验。

4.3 量子密钥分发移动终端通信网络

各类移动终端用户的网络安全防护已成为当前关注的热点问题之一^[54]。利用 QKD 自身的独特优势, 同时结合密钥分发中心, 可以将量子密钥分发生成的量子密钥应用于移动终端侧, 保护端到端及端到服务器的通信安全性, 可在移动办公、金融支付、移动作业等多种场景进行应用。如图 9 所示, 量子密钥分发网络结合用于管理量子密钥分发网络产生的量子密钥的密钥分发中心, 以及靠近用户的量子密钥更新终端设备, 可将量子密钥分发网络产生的对称量子密钥充注到终端的安全存储介质 (例如 SD 卡、SIM 卡、U 盾、安全芯片等), 用于其通信过程中的鉴权和会话加密。该方案相比传统的密钥分发中心方案, 可保证会话密钥的前向安全性; 相比传统的公钥基础设施方案, 则可保证身份认证和会话密钥协商过程能够抵抗量子计算攻击。

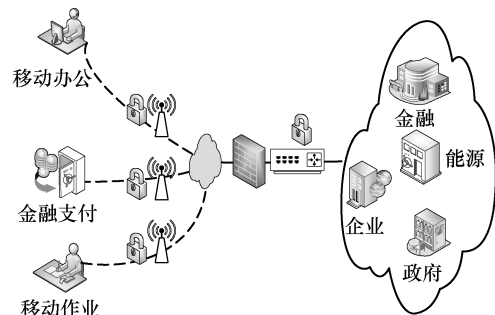


图9 量子密钥分发移动终端通信网络

5 发展趋势及面临挑战

综上所述, 量子密钥分发城域光组网的研究还处于起步阶段, 在组网关键技术方面还有待进一步的研究。目前现有文献也只是针对某一个方面的解决方案, 还没有形成真正应用于多用户间的量子密钥分发城域光网络, 因此, 量子密钥分发城域光组网技术在未来存在着很大的研究空间。与现有技术相比, 未来在网络稳定性、高效性和可靠性 3 个方面还需发展。

在网络稳定性方面, 量子密钥分发城域光网络的搭建依赖于经典光网络的已有光纤设施, 如何在现有光网络中无缝集成量子密钥分发设备变得尤为重要。

在网络高效性方面,城域网内实时且密集的安全请求会导致较低的资源利用率,如何提高网络资源利用率是一个问题。

在网络可靠性方面,网络设施面临着自然因素如地震、飓风、海啸等因素的影响,网络中由节点链路导致故障如何恢复也是一个问题。

6 结束语

自量子密钥分发技术提出以来,各国政府给予了高度重视并已形成一些试点应用。然而,如何将点到点量子密钥分发形成适用于多用户的量子密钥分发网络是学术界和产业界所迫切关注的课题。尤其将理论上的量子密钥分发技术下降于实际的城域光网络中安全需求的满足,仍需要进行大量研究。本文围绕量子密钥分发城域光网络,从网络架构、关键技术、典型场景和未来展望几个方面进行了综述性介绍,以期能为未来量子密钥分发城域光网络的发展提供参考。

参考文献:

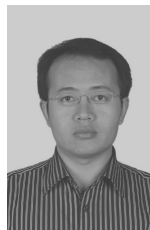
- [1] FOK M P, WANG Z, DENG Y, et al. Optical layer security in fiber-optic networks[J]. *IEEE Transactions on Information Forensics and Security*, 2011, 6(3): 725-736.
- [2] RIVEST R, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. *Communications of the ACM*, 1978, 21(2): 120-126.
- [3] FAUSTO M, WALTER F, JOSÉ S, et al. RSA encryption algorithm optimization to improve performance and security level of network messages[J]. *International Journal of Computer Science and Network Security*, 2016, 16(8): 55-62.
- [4] NINA S, MARIJA F, SZILARD Z, et al. Physical-layer security in evolving optical networks[J]. *IEEE Communication Magazine*, 2016, 54(8): 110-117.
- [5] PAUL A M D. *The principles of quantum mechanics*[M] 3rd ed. Oxford: Clarendon Press, 1947.
- [6] ISLAM N T, LIM C W, CAHALL C, et al. Provably secure and high-rate quantum key distribution with time-bin qudits[J]. *Science Advances*, 2017, 3(11): 1-6.
- [7] LO H, CURTY M, TAMAKI K. Secure quantum key distribution[J]. *Nature photonics*, 2014(8): 595-604.
- [8] DANNA R, JIM W H, PATRICK R R, et al. Long-distance decoy-state quantum key distribution in optical fiber[J]. *Physic Review Letter*, 2007, 98(1): 1-4.
- [9] SHOR P W, PRESKILL J. Simple proof of security of the BB84 quantum key distribution protocol[J]. *Physical review letters*, 2000, 85(2): 441-444.
- [10] MOMTCHIL P, ANDREAS P, OLIVER M, et al. The SECOQC quantum key distribution network in Vienna[J]. *New Journal of Physics*, 2009, 11(7): 1-37.
- [11] PEEV M, PACHER C, ALLEAUME R, et al. Long-term performance of the SwissQuantum quantum key distribution network in a field environment[J]. *New Journal of Physics*, 2011(13): 1-19.
- [12] HUGHES R J, MORGAN G L, PETERSON C G. Quantum key distribution over a 48 km optical fibre network[J]. *Journal of Modern Optics*, 2000, 47(2-3): 533-547.
- [13] WANG S, CHEN W, YIN Z, et al. Field and long-term demonstration of a wide area quantum key distribution network[J]. *Optics express*, 2014, 22(18): 21739-21756.
- [14] CAO Y, ZHAO Y L, YU X S, et al. Experimental demonstration of end-to-end key on demand service provisioning over quantum key distribution networks with software defined networking[C]// *In Proceedings of the OFC. IEEE/OSA*, 2019: 1-3.
- [15] CAO Y, ZHAO Y L, COLMAN-MEIXNER C, et al. Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD)[J]. *Optics Express*, 2017, 25(22): 26453-26467.
- [16] ZHAO Y L, CAO Y, WANG W, et al. Resource allocation in optical networks secured by quantum key distribution[J]. *IEEE Communication Magazine*, 2018, 56(8): 130-137.
- [17] CAO Y, ZHAO Y L, YU X S, et al. Resource assignment strategy in optical networks integrated with quantum key distribution[J]. *Journal of Optical Communications and Networking*, 2017, 9(11): 995-1004.
- [18] WANG H, ZHAO Y, YU X, et al. Protection schemes for key services in optical networks secured by quantum key distribution (QKD)[J]. *Journal of Optical Communications and Networking*, 2018, 11(3): 67-78.
- [19] CAO Y, ZHAO Y L, WU Y, et al. Time-scheduled quantum key distribution (QKD) over WDM networks[J]. *Journal of Lightwave Technology*, 2018, 36(16): 3382-3395.
- [20] WANG H, ZHAO Y, YU X, et al. Resilient quantum key distribution (QKD)-integrated optical networks with secret-key recovery strategy[J]. *IEEE ACCESS*, 2019(05): 60079-60090.
- [21] CAO Y, ZHAO Y, WANG J, et al. SDQaaS: software defined networking for quantum key distribution as a service[J]. *Optics Express*, 2019, 27(5): 6892-6909.
- [22] ALEJANDRO A, VICTOR L, JESUS M M, et al. Virtual network function deployment and service automation to provide end-to-end quantum encryption[J]. *IEEE/OSA Journal of Optical Communications and Networking*, 2018, 10(4): 421-430.
- [23] ALEJANDRO A, EMILIO H, PAUL ANTHONY H, et al. Secure NFV orchestration over an SDN-Controlled optical network with time-shared quantum key distribution resources[J]. *Journal of Lightwave Technology*, 2017, 35(8): 1357-1362.
- [24] AGUADO A, LOPEZ V, LOPEZ D, et al. The engineering of software-defined quantum key distribution networks[J]. *IEEE Communications Magazine*, 2019, 57(7): 20-26.
- [25] CHOI I, YOUNG R J, TOWNSEND P D. Quantum key distribution on a 10Gb/s WDM-PON[J]. *Optics express*, 2010, 18(9): 9600-9612.
- [26] YOSHINO K, OCHI T, FUJIWARA M, et al. Maintenance-free operation of WDM quantum key distribution system through a field fiber over 30 days[J]. *Optics express*, 2013, 21(25): 31395-31401.
- [27] YOSHINO K, FUJIWARA M, TANAKA A, et al. High-speed wavelength-division multiplexing quantum key distribution system[J]. *Optics letters*, 2012, 37(2): 223-225.
- [28] GILLES B, FELIX B, NICOLAS G, et al. Multiuser quantum key distribution using wavelength division multiplexing[J]. *Applications of Photonic Technology*, 2003(5260):149-153.
- [29] BORIS K, CHARLES C L, RAPHAEL H, et al. Provably secure and practical quantum key distribution over 307 km of optical fibre[J]. *Nature Photonics*, 2015(9): 163-168.
- [30] TANAKA A, SASAKI M, FUJIWARA M, et al. Field test of quantum key distribution in the Tokyo QKD Network[J]. *Optics Express*, 2011, 19(11): 10387-10409.
- [31] YIN H, CHEN T, YU Z, et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber[J]. *Physical Review Letters*, 2016(117): 1-5.
- [32] CHEN W, HAN Z, ZHANG T, et al. Field experiment on a "star type" metropolitan quantum key distribution network[J]. *IEEE Photonics*

- Technology Letters, 2009, 21(9): 575-577.
- [33] STUCKI D, GISIN N, GUINNARD O, et al. Quantum key distribution over 67 km with a plug&play system[J]. New Journal of Physics, 2002, 4(41): 1-8.
- [34] DIXON A, DYNES J, LUCAMARINI M, et al. High speed prototype quantum key distribution system and long term field trial[J]. Optics express, 2015, 23(6): 7583-7592.
- [35] CHEN T Y, WANG J, LIANG H, et al. Metropolitan all-pass and inter-city quantum communication network[J]. Optics express, 2010, 18(26): 27217-27225.
- [36] GREEN P E, COLDREN L A, JOHNSON K M, et al. All-optical packet-switched metropolitan-area network proposal[J]. Journal of Lightwave Technology, 1993, 11(5/6): 754-763.
- [37] KAORU S, TOSHIMORI H, MIKIO F, et al. Performance of long-distance quantum key distribution over 90-km optical links installed in a field environment of Tokyo metropolitan area[J]. Journal of Lightwave Technology, 2013, 32(1): 141-151.
- [38] STEFANO P, CARLO O, GAETANA S, et al. High-rate measurement-device-independent quantum cryptography[J]. Nature Photonics, 2015(9): 397-402.
- [39] LI C, ZHOU H, WANG Y, et al. Secure quantum key distribution network with Bell states and local unitary operations[J]. Chinese Physics Letters, 2005, 57(12): 1049-1052.
- [40] TOLIVER P, RUNSER R, CHAPURAN T, et al. Experimental investigation of quantum key distribution through transparent optical switch elements[J]. IEEE Photonics Technology Letters, 2003, 15(11): 1669-1671.
- [41] TAKEOKA M, GUHA S, WILDE M M. Fundamental rate-loss tradeoff for optical quantum key distribution[J]. Nature Communications, 2014, (5): 1-7.
- [42] PATEL K, DYNES J, CHOI I, et al. Coexistence of high-bit-rate quantum key distribution and data on optical fiber[J]. Physical Review X, 2012(2): 1-8.
- [43] XIA T, CHEN D, WELLBROCK G, et al. In-band quantum key distribution (QKD) on fiber populated by high-speed classical data channels[C]//Optical Fiber Communication Conference. IEEE/OSA, 2006: 1-3.
- [44] PATEL K, DYNES J, LUCAMARINI M, et al. Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks[J]. Applied Physics Letters, 2014, 22(19): 1-4.
- [45] QI B, ZHU W, QIAN L, et al. Feasibility of quantum key distribution through a dense wavelength division multiplexing network[J]. New Journal of Physics, 2010(12): 1-18.
- [46] RUNSER R, CHAPURAN T, TOLIVER P, et al. Demonstration of 1.3 μm quantum key distribution (QKD) compatibility with 1.5 μm metropolitan wavelength division multiplexed (WDM) systems[C]// Optical Fiber Communication Conference. IEEE/OSA, 2005: 1-3.
- [47] THIAGO F, GUILHERME B, GUILHERME P, et al. Impact of Raman scattered noise from multiple telecom channels on fiber-optic quantum key distribution systems[J]. Journal of Lightwave Technology, 2014, 32(13): 2332-2339.
- [48] WANG L, HONG C, FRIBERG S. Generation of correlated photons via four-wave mixing in optical fibres[J]. Journal of optics B: Quantum and semiclassical optics, 2001, 3(5): 346-352.
- [50] TURITSYN S K, ANIA-CASTAÑÓN J D, BABIN S A, et al. 270-km ultralong Raman fiber laser. Physical review letters, 2009, 103(13): 1-4.
- [51] HARALD R, SYLVIA S, ANDREAS P, et al. Quantum key distribution integrated into commercial WDM systems[C]// Optical Fiber Communication Conference. IEEE/OSA, 2008: 1-3.
- [52] MCCORMICK C F, MARINO A M, BOYER V, et al. Strong low-frequency quantum correlations from a four-wave-mixing amplifier[J]. Physical Review A, 2008(78): 1-5.
- [53] ZHU W, CROZIER K B. Quantum mechanical limit to plasmonic enhancement as observed by surface-enhanced Raman scattering[J]. Nature Communications, 2014(5): 1-8.
- [54] NEJABATI R, WANG R, BRAVALHERI A, et al. First demonstration of quantum-secured, inter-domain 5G service orchestration and on-demand NFV chaining over flexi-WDM optical networks[C]// Optical Fiber Communication Conference. IEEE/OSA, 2019: 1-3.

[作者简介]



王华 (1994-), 女, 甘肃酒泉人, 北京邮电大学博士生, 主要研究方向为量子密钥分发网络。



赵永利 (1981-), 男, 河北唐山人, 博士, 北京邮电大学教授, 主要研究方向为光通信网络、量子密钥分发网络、人工智能与光联网和弹性卫星光网络。

优青人物介绍

赵永利, 教授, 国家优秀青年科学基金获得者。2018年, 以“弹性光网络控制技术”成果获得国家优秀青年科学基金资助。2014年至今, 发表SCI检索论文108篇, 其中作为第一作者27篇, 通信作者66篇; 二区及以上SCI论文40篇, Google学术引用累计2800余次; 国际会议特邀报告18次, 获得国际学术会议最佳论文6篇; 出版学术著作10部, 授权国家发明专利42项, 提交国际标准提案10篇, 以第一editor牵头一项ITU标准, 完成国家通信行业标准2项。获得国家性和省部级科技奖励9次, 其中以第二完成人成果获得2019年国家科技进步二等奖(已通过初评); 获得2018年中国通信学会青年科技奖, 2018年中国产学研合作创新成果奖个人奖。