引用本文：陆旭，刘世民，刘翔，等：量子密钥分发光网络体系结构与接口机制[J]. 光通信技术，2019，43(10)：36-40.

量子密钥分发光网络体系结构与接口机制

陆 旭[1]，刘世民[1]，刘 翔[2]，曹 原[2]，朱继阳[1]，郁小松[2]，赵永利[2]，张梓平[3*]

（1. 国网内蒙古东部电力有限公司 信息通信分公司，呼和浩特 010020；2. 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；3. 全球能源互联网研究院有限公司 电力通信网络技术实验室，北京 102209）

摘要：为了给将来量子密钥分发(QKD)网络的实际建设提供理论支持，依据 QKD 网络的实际功能组成重点分析了其功能模型，借助分层网络的思想规范了其接口机制，进而通过引入软件定义网络技术提出了一种集中管控的 QKD 发网络体系结构并给出了它的工作流程，最后通过实际搭建 QKD 网络模型实现了 QKD 网络上节点间的 QKD 功能，验证了提出的 QKD 网络体系结构与接口机制的可行性。

关键词：量子密钥分发；网络结构；集中控制；网络接口

中图分类号：TN915　**文献标识码**：A　**文章编号**：1002-5561(2019)09-0036-05

DOI：10.13921/j.cnki.issn1002-5561.2019.10.008　**开放科学(资源服务)标识码(OSID)**：

Quantum key distribution network architecture and interface mechanism

LU Xu[1], LIU Shimin[1], LIU Xiang[2], CAO Yuan[2],
ZHU Jiyang[1], YU Xiaosong[2], ZHAO Yongli[2], ZHANG Ziping[3*]

(1. Information Communication Branch, State Grid Eastern Inner Mongolia Electric Power Co., Ltd., Hohhot 010020, China; 2. State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Optical Communications, Beijing 100876, China; 3. State Grid Laboratory of Electric Power Communication Network Technology, Global Energy Interconnection Research Institute Co., Ltd., Beijing 102209, China)

Abstract: In order to provide theoretical support for the practical construction of quantum key distribution(QKD) network in the future, this paper focuses on the analysis of its functional model according to the actual functional composition of QKD network, standardizes its interface mechanism with the idea of hierarchical network, and then proposes a centrally controlled QKD network architecture by introducing software defined network technology, and gives its working process. After that, this paper realizes the function of QKD between nodes in QKD network by building the model of QKD network, and verifies the feasibility of the architecture and interface mechanism of QKD network proposed in this paper.

Key words: quantum key distribution; network architecture; centralized control; network interface

0 引言

针对量子保密通信的网络化应用进行相关技术研究已经成为量子保密通信领域的研究热点。国内外许多学者对此提出了各种量子密钥分发(QKD)[1]网络模型，例如英国 Bristol 大学的 A. Aguado 等人[2]从电信运营商、设备制造商和应用研究与开发的角度探讨了软件定义网络(SDN)对 QKD 实际部署的影响，提出了一种通用的量子感知 SDN 架构，将其分成应用层、控制管理层和基础设备层[3]。国防科技大学的 Wanrong Yu 等人也针对于 QKD 网络中网络层协议面临资源消耗过高导致的随机路由和复杂网络管理的双重困难，提出了一种三层网络模型，并介绍了每一层次中的关键功能模块[4,5]。

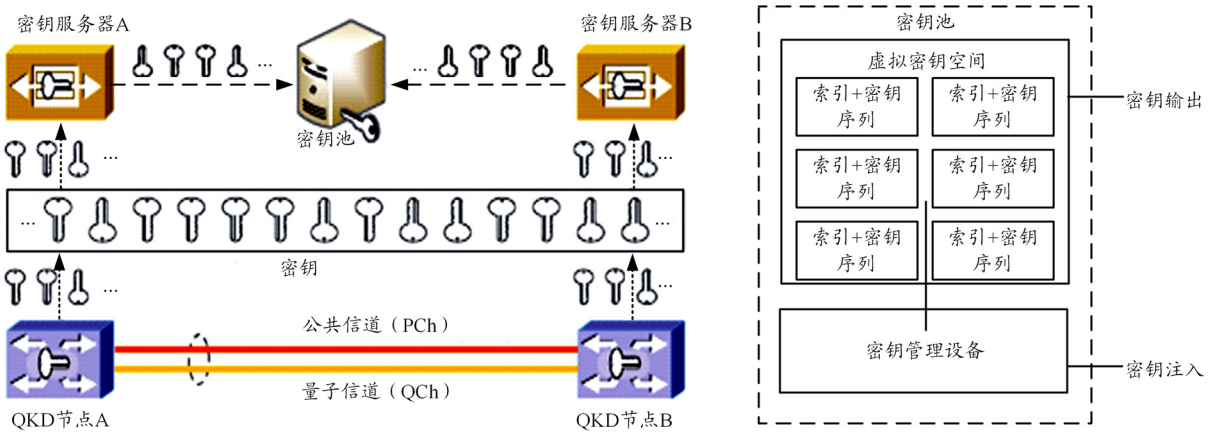
本研究重点探究 QKD 功能网络化给传统网络体

收稿日期：2019-03-13。

基金项目：国网内蒙古东部电力有限公司科技项目(52660319002P)资助。

作者简介：陆旭(1970-)，男，辽宁锦州人，工程硕士，高级工程师。从事电力系统通信、信息运行及管理工作。研究方向为电力系统光纤通信、量子通信、数据通信和人工智能等。获省部级科技进步三等奖 1 项。

*** 通信作者**：张梓平（E-mail: zhangziping@geiri.sgcc.com.cn）。



（a）点到点 QKD 密钥池构建　　（b）密钥池结构

图 1　QKD 网络密钥池概念

系所带来的逻辑上的改变,提出一种集中管控的 QKD 网络体系结构。

1 QKD 网络基本原理

1.1　QKD 网络密钥池

QKD 网络中的关键问题是密钥资源分配与疏导,与传统光网络资源不同,密钥资源具有“逐渐生成并累积、消耗瞬时发生”特点,这使得 QKD 网络状态多变,对密钥资源的高效利用造成了许多困难。借鉴传统的密钥学理论，有人提出了 QKD 网络密钥池的概念[6],如图 1 所示。在由众多点到点 QKD 系统聚合而成的 QKD 网络中，密钥池是存在于网络中量子通信节点内部的一种存储设备,密钥以成对的方式存储在网络中相邻节点对的密钥池中。每个密钥池可分为多个虚拟的密钥空间,称为虚拟密钥池(用索引进行表示)，用于存储其它节点与该节点经密钥中继而来的密钥对。因为密钥资源易消耗且难补充,从而使 QKD 网络对于网络状态更加敏感,复杂网络中的众多密钥管理类设备需要统一管控,协同工作。

1.2 QKD 光网络的功能模型

借助 SDN 的设计思想,在 QKD 网络中,通过将控制功能和 QKD 设备分离,监控网络状态,对网络中的密钥资源、波长资源等进行逻辑上的集中控制,以及通过统一开发的接口将抽象后的 QKD 网络资源提供给需要加密的业务用户，实现统一管控的 QKD 网络体系结构。网络结构可分为 4 层:应用层、控制层、密钥分发层和物理层,如图 2 所示。

物理层处于 QKD 网络结构的底层,是 QKD 网络的技术基础。物理层既要进行量子信息处理,同时也

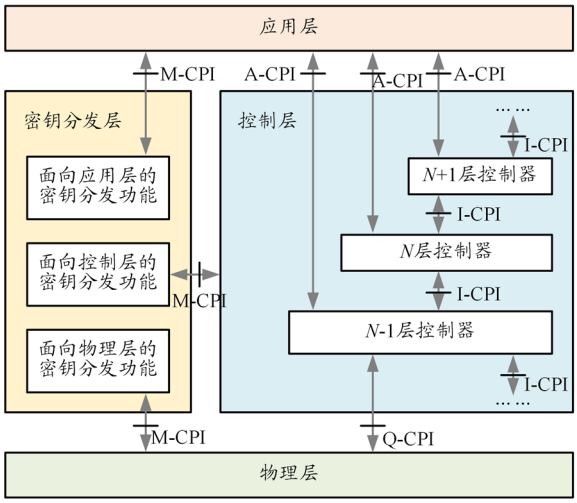


图 2　集中控制的 QKD 网络功能模型

要进行经典信息处理。密钥分发层主要功能包括:设备管理、密钥中继、密钥转发、密钥存储和密钥输出等。密钥分发层主要设备形态有量子密钥管理服务系统、量子密钥管理机和密钥池等。控制层的主要功能是通过南向接口控制物理层 QKD 的行为，并通过北向接口向应用层开放网络能力。最上层是 QKD 网络结构的应用层,包含各类使用量子保密协议的应用或设备。应用层提供包括运营管理、网络管理、密钥路由和密钥生成控制等功能。应用层主要是 QKD 设备,如密钥管理机、密钥管理系统等设备。

1.3 QKD 网络相关接口

如图 2 所示，从功能上来看,QKD 网络中相关的主要接口包括:

①QKD 控制接口(Q-CPI):控制器与 QKD 设备之间的接口(Q-CPI)。SDN 控制器通过此接口控制 QKD 物理层资源。SDN 控制器应支持多个 Q-CPI 的接口,

与多个 QKD 设备相连。

②控制器层间接口(I-CPI):高层控制器与低层控制器件的接口(I-CPI 接口)。根据 SD-QKDN 的控制器分层部署情况,一个控制器可提供多个 I-CPI,允许同时接受多个高层控制器的控制。

③应用控制接口(A-CPI):应用层与控制层之间的接口,应用程序通过此接口从 SDN 控制器接收服务。控制器应支持多个 A-CPI,为多个业务应用提供服务。

④密钥分发接口(M-CPI):密钥分发层与控制层、物理层以及应用层之间的接口,通过与不同层次的接口,实现对密钥分发层中密钥池的管理,分别配置控制层内的资源和策略,配置物理层密钥资源的分发与在密钥池中的存储,配置业务应用层面的业务信息及策略。

2 分析与讨论

2.1 量子密钥分发网络体系结构与工作流程

依据前文中介绍的 QKD 网络功能模型与接口机制,现给出一种集中管控的 QKD 网络体系结构示意图及工作流程,如图 3 所示。

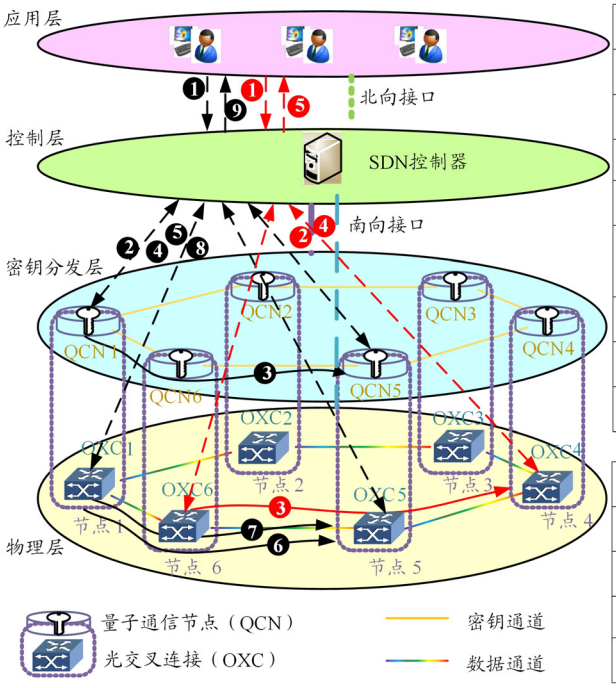
纵向来看,QKD 网络体系结构分为应用层、控制层、密钥分发层和物理层。其中,Restful API 和 OpenFlow 协议(OF)分别作为控制层北向接口和南向接口协议应用和开发。

物理层包括通过 QKD 链路互连的若干 QKD 节点,其中在每个节点上开发和部署 OF 代理(OFA)。QKD 链路由量子信道和使用光纤的公共信道组成。每个节点用作连接到高安全性需求用户的端点,该用户聚合多个 QKD 组件,例如 QKD 发送器、QKD 接收器、可信中继器和密钥服务器。

密钥分发层中密钥服务器可以存储物理层所产生的密钥。每一个物理层 QKD 节点虚拟化为一个量子通信节点(QCN)。现阶段产业可用的点到点的 QKD 距离已经达到 400 km[7]。可信中继器用于扩展端到端 QKD 的物理距离,由于 SDN 控制器决策网络信息灵活高效的特点,所以结合 SDN 技术和可信中继扩展的 QKD 网络理论上没有最大建网规模限制。

控制层由 SDN 控制器组成。除传统 SDN 控制器中的基本网络服务功能外,专门开发的 QKD 功能模块可分为以下 5 个模块:①服务模块用于存储和更新服务信息,以及实现动态端到端 QKD 服务的创建、修改和删除。②拓扑模块收集、存储和更新 QKD 网络拓扑和节点信息。③路由模块计算并选择节点对之间的 QKD 路径。④密钥生成速率模块在每个 QKD 链路上存储和更新其密钥生成速率信息。⑤QKD 模块为密钥分发服务执行按需分配密钥的功能。

应用层主要是发起 QKD 服务请求;控制层接收到这些请求后监测密钥分发层和物理层上的量子密钥资源和传统网络资源,对这些业务请求进行密钥路



❶	应用层中的用户向控制层发送业务请求;
❷	控制层分别计算在密钥分发层和物理层所需路径和资源;
❸	密钥分发层中选定路径的节点进行连通,反馈连接信息;
❹	密钥分发层中选定路径的节点分配得到资源,反馈分配结果;
❺	物理层中选定路径的节点分配得到资源,反馈分配结果;
❻	物理层中测量机与密钥分发层中量子密钥同步分配资源,反馈给控制层结果信息;
❼	物理层中选定路径的节点进行连通,反馈连通信息;
❽	物理层中选定路径的节点分配得到资源,反馈分配结果;
❾	控制层回复应用层发出的请求。

❶	应用层中的用户向控制层发送业务请求;
❷	控制层计算物理层所需路径和资源;
❸	物理层中选定路径的节点分配得到资源,反馈分配结果;
❹	物理层中选定路径的节点进行连通;反馈连接信息;
❺	控制层回复应用层发出的请求。

图 3 QKD 网络体系结构及工作流程

由计算、传输路由计算、密钥及波长资源分配、传送信令和 QKD 以及光网络设备的配置；物理层和密钥分发层共享光传送网资源，使用波分复用技术在同一光纤通道中分割构建量子密钥资源生成所需的数据通道、密钥通道和测量通道。密钥分发层可以通过密钥通道分发物理层和控制层通信所需的密钥，从而保证光网络的安全。

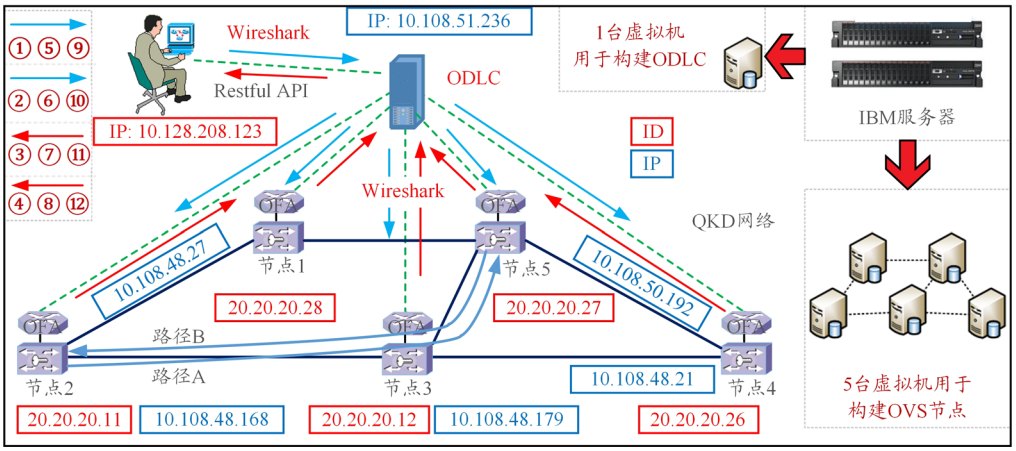


图 4 QKD 光网络实验平台

No.	Time	Source	Destination	Protocol	Length	Info	
节点2	2.810913	10.108.51.236	10.108.48.168	OpenFlow	80	Ty	初始化请求类型(30) 初始化响应类型(31)
	2.811700	10.108.48.168	10.108.51.236	OpenFlow	108	Ty	
节点4	2.877830	10.108.51.236	10.108.49.21	OpenFlow	80	Ty	初始化请求类型(30) 初始化响应类型(31)
	2.878598	10.108.49.21	10.108.51.236	OpenFlow	100	Ty	
节点3	2.910164	10.108.51.236	10.108.48.179	OpenFlow	80	Ty	初始化请求类型(30) 初始化响应类型(31)
	2.910955	10.108.48.179	10.108.51.236	OpenFlow	104	Ty	
节点1	2.966392	10.108.51.236	10.108.48.27	OpenFlow	80	Ty	初始化请求类型(30) 初始化响应类型(31)
	2.967041	10.108.48.27	10.108.51.236	OpenFlow	96	Ty	
节点5	2.967759	10.108.51.236	10.108.50.192	OpenFlow	80	Ty	初始化请求类型(30) 初始化响应类型(31)
	2.968540	10.108.50.192	10.108.51.236	OpenFlow	100	Ty	

图 5 网络初始化 OFP 消息捕获

No.	Time	Source	Destination	Protocol	Length	Info	
① ④	45.310370	10.128.208.123	10.108.51.236	HTTP	268	POST /contro	①创建请求消息
	45.923492	10.108.51.236	10.128.208.123	HTTP	61	HTTP/1.1 200	④创建响应消息
⑤ ⑧	55.686806	10.128.208.123	10.108.51.236	HTTP	83	PUT /control	⑤修改请求消息
	55.756292	10.108.51.236	10.128.208.123	HTTP	61	HTTP/1.1 200	⑧修改响应消息
⑨ ⑫	59.552999	10.128.208.123	10.108.51.236	HTTP	290	DELETE /cont	⑨删除请求消息
	59.621965	10.108.51.236	10.128.208.123	HTTP	61	HTTP/1.1 200	⑫ 删除响应消息

图 6 应用层与控制层间 HTTP 消息捕获

图 3 中，黑线表示经过密钥分发机制建立的安全传送过程，红线表示无量子密钥加密过程建立的不安全传送过程。密钥分发层可以为物理层和控制层分发量子密钥来建立安全的光网络物理层及控制通道，通过利用波分复用技术在物理层实现资源共享，提高资源利用率，减少量子密钥独立运行成本。数据通道用来支持物理层，单根光纤里面可以使用多个波长；同时测量通道也位于物理层，占据的是传统通道。密钥通信节点可以完成密钥的传输和交换，光交叉连接和密钥通信节点在物理上是部署在同一节点，分别对应物理层和密钥分发层。

2.2 实验测试平台和结果

本文开发的 QKD 光网络实验平台如图 4 所示。

控制层由基于 OpenDayLight 控制器(OpenDayLight Controller，ODLC)平台开发的 SDN 控制器组成。Restful API 使用 JavaScript Object Notation (JSON)实现，并且可以支持 HTTP。我们基于 OF1.3 扩展了 ODLC 并且在每个节点上开发和部署 OF 代理。鉴于所提出的架构和工作流程不受任何特定供应商的 QKD 设备的约束，我们开发 Open vSwitch(OVS)作为量子通信节点，并在其连接的 OVS 中预存每个节点的详细信息。QKD 网络配备了 5 个量子通信节点，其中 5 个虚拟机在 IBM 服务器上运行并配置为 OVS。此外，一个虚拟机与 ODLC 一起安装。节点的唯一 IP 和 ID 以及密钥保密应用和 ODLC 的唯一 IP 在图 4 中用不同的颜色标记。使用 Wireshark 网络协议分析器捕获 HTTP 和 OFP(OpenFlow 协议)消息。最初，ODLC 配置每个节点以完成 QKD 网络初始化，OFP 消息捕获如图 5 所示。

初始化请求(req)和响应(rsp)的消息类型分别定义为 30 和 31。在 QKD 网络初始化之后，可以执行 QKD 服务供应以满足用户的节点间数据安全性要求。QKD 服务提供的整个过程在图 4 中显示出并编号，其中每个步骤详细描述于图 6~图 8 中。

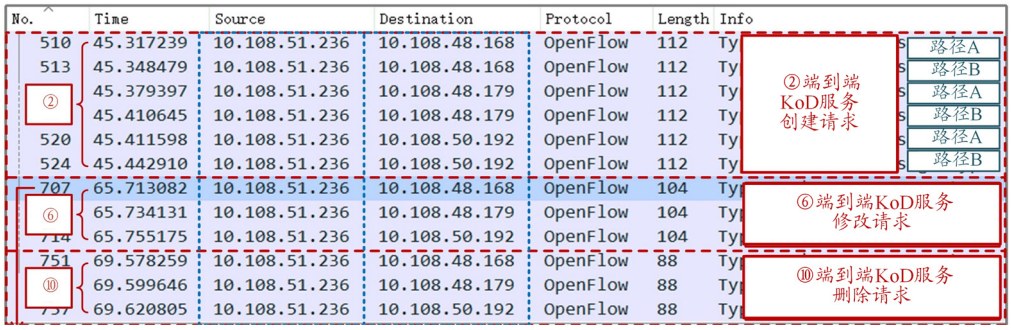


图 7 控制层和密钥分发层间的 req 消息捕获

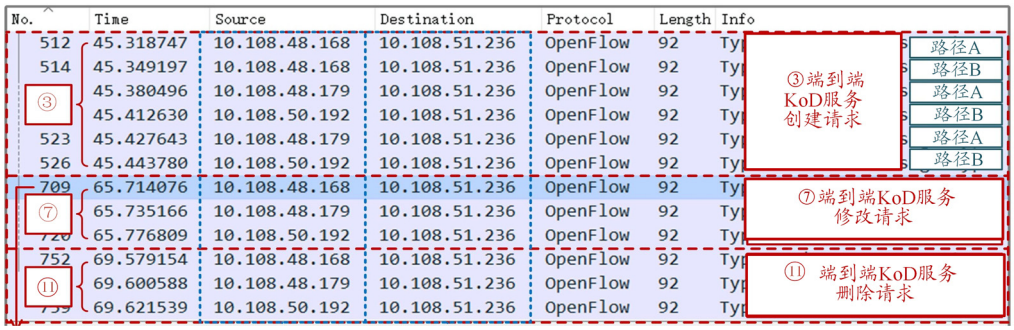


图 8 控制层和密钥分发层间的 rsp 消息捕获

对于节点 2 和节点 5 之间的 QKD 服务,图 6 中显示了量子保密应用和控制器 ODLC 之间的 QKD 服务 req 和 rsp 的 HTTP 消息捕获，而 QKD 服务的 OFP 消息捕获 ODLC 和节点之间的 req 和 rsp 在图 7 和图 8 中显示出。QKD 服务 req 和 rsp 的消息类型分别定义为 32 和 33。步骤①~④、⑤~⑧和⑨~⑫分别执行 QKD 服务创建、修改和删除。实际上,点到点 QKD 通常是单向的,用于产生密钥;而端到端 QKD 可以使用双向通信来中继密钥。因此,QKD 服务创建可以在节点 2 和节点 5 之间建立双向路径 A 和 B,其中节点 2 的输入端口(In-port)和节点 5 的输出端口(Out-port)以及路径 A 上节点 5 的输入端口以及路径 B 上的节点 2 的输出端口都是 NULL，同时使用 QKD 服务来修改 req 和 rsp 来说明扩展 OFP 的详细消息。

3 结束语

本研究基于点对点量子密钥生成、量子密钥池和网络集中管控等技术背景，分析了 QKD 网络体系功能模型,规范了 QKD 网络各层次间的接口机制,给出了一种集中管控的 QKD 网络体系结构及其工作流程，最后通过搭建量子密钥分发网络模型完成了 QKD 网络上节点间的 QKD 功能，验证了本文提出的 QKD 光网络体系结构与接口机制的可行性。与无安全保护的传统网络和其它形态的量子保密网络相比，本文所做的工作能够提供对密钥和加密业务服务质量变化需求的实时响应，提供具有保障的端到端 QKD 连接,为未来 QKD 网络的实际建设提供理论支持。

参考文献:

[1] 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.

[2] AGUADO A, VCTOR L, MARHUENDA J, et al. ABNO: a feasible SDN approach for multivendor IP and optical networks (Invited) [J]. IEEE/OSA Journal of Optical Communications & Networking, 2015, 7(2): A356–A362.

[3] AGUADO M, ALEJANDRO M A. Quantum-Aware Software Defined Networks [C]//6th International Conference on Quantum Cryptography, September 12–16, 2016, Washington, USA. Washington: Estados Unidos, 2016.

[4] YU W, ZHAO B, YAN Z. Software defined quantum key distribution network[C]//3rd IEEE International Conference on Computer and Communications (ICCC), December 13–16, 2017, Chengdu, China. Chengdu: IEEE, 2017.

[5] PEEV M. The Secoqc Quantum Key Distribution Network in Vienna[J]. New Journal of Physics, 2009, 11(7): 075001-1–075001-37.

[6] 曹原, 赵永利, 郁小松, 等. 基于量子密钥分发的可信光网络体系架构[J]. 信息通信技术,2016(6):48–54.

[7] IDQ. Quantum Key Distribution (QKD) achieved over record 421 km [EB/OL]. (2018–11–29) [2019–03–13]. https://www.idquantique.com/quantum-key-distribution-qkd-achieved-over-record-421-km/.