软件定义的量子密钥分发网络技术研究

Research on Software-defined Quantum Key Distribution Network Technology

马彰超[1]，曹　原[2]，董　凯[2]，赵永利[2]（1. 国科量子通信网络有限公司，北京 100193；2. 北京邮电大学，北京 100876）
Ma Zhangchao[1]，Cao Yuan[2]，Dong Kai[2]，Zhao Yongli[2]（1. CAS Quantum Network Co.，Ltd.，Beijing 100193，China；2. Beijing University of Posts and Telecommunications，Beijing 100876，China）

摘　要：
介绍国内外量子密钥分发网络的发展状况，提出了一种软件定义量子密钥分发网络体系架构，实现量子密钥分发网络的可编程性，有利于构建面向多种业务和复杂应用的开放、灵活、智能的量子密钥分发网络。从网络部署、管理及运营角度，概述了软件定义量子密钥分发网络在组网与应用中涉及的关键技术。

关键词：
量子通信；量子密钥分发；信息安全；网络架构
doi：10.12045/j.issn.1007-3043.2019.04.016
中图分类号：TN915.08
文献标识码：A
文章编号：1007-3043（2019）04-0071-05

Abstract：
It introduces the development of global quantum key distribution networks and proposes a software-defined quantum key distribution network architecture，which realizes the programmability of quantum key distribution network，and is helpful to the construction of an open flexible and intelligent quantum key distribution network for multiple services and complex applications. From the perspective of network deployment，management and operation，the key technologies of software-defined quantum key distribution network in networking and application are summarized.

Keywords：
Quantum communication；Quantum key distribution；Information security；Network architecture

引用格式：马彰超，曹原，董凯，等. 软件定义的量子密钥分发网络技术研究[J]. 邮电设计技术，2019(4)：71-75.

0 引言

随着信息技术的发展和互联网应用的普及，网络信息安全越来越受到人们的重视。特别是美国“棱镜门”事件被曝光后，各国在网络信息安全方面的投入开始加大，防止网络窃听、保障信息安全可靠传输再次受到各国的高度重视。基于量子通信的量子密钥分发（QKD——quantum key distribution）技术的出现及其实用化，为网络信息安全的发展开辟了一条新的道路。

量子通信作为量子信息科学的重要分支，是利用量子态作为信息载体的全新通信技术。量子通信不同于以电磁波为信息载体的经典通信，其具备由“测量塌缩理论”“海森堡测不准原理”和“量子不可克隆定律”等量子力学基本定律带来的全新特性，使得量子密钥分发具有理论上无条件安全的优势[1-2]。以量子密钥分发作为安全支撑手段可以保障网络信息传递的长期安全性。

欧盟发布的量子技术旗舰计划《量子宣言》，将以量子密钥分发为核心的量子保密通信网络作为网络信息安全领域未来发展的重要方向。

美国、英国、奥地利、瑞士、日本等国家和地区都积极研究基于量子密钥分发的量子保密通信网络，并进行相关实验和试点。同时，我国也先后开展了多项

收稿日期：2019-03-15

重大技术研究，针对量子保密通信局域网、城域网和广域网开展了相关实验和试点工作，包括用于连接城域网的量子保密通信网络京沪干线工程、星地一体化广域量子保密通信网络等。随着量子密钥分发技术的不断成熟和应用规模的不断扩大，研究构建高安全、高服务质量、低成本的量子保密通信网络具有重要的现实意义和长远的战略意义。

本文从量子密钥分发网络的研究进展出发，介绍了国际和国内量子密钥分发网络的发展状况，提出了一种软件定义量子密钥分发网络体系架构，并概述了软件定义量子密钥分发网络在组网与应用中涉及的关键技术。

1 量子密钥分发网络发展状况

网络化是QKD技术走向实用化的关键，一直以来受到各国研究机构和产业界的广泛关注。只有将点对点的QKD技术扩展为多用户的QKD网络，以实现多用户间的保密通信，例如多方的量子加密电话或视频会议，才能充分发挥QKD的应用潜力。全球典型QKD网络的发展如下：

2002—2007：美国建成包含10个节点、多种QKD协议、支持自由空间和光纤信道的DRAPA试验网。率先提出了QKD组网的基本思想[3]。

2004—2008：欧盟建设的SECOQC网络引入具备骨干传送和城域接入功能的可信中继节点，具备一定的广域部署能力，试图构建面向商业用户的量子保密通信网络[4]。

2013—：中国启动建设长达2 000多km的“北京—上海”量子保密通信骨干网络，连接多地QKD城域网，并于2016年与世界首颗量子信息科学试验卫星“墨子号”成功对接，建成“城域+骨干+卫星”的星地一体广域QKD网络[5]。

除此之外，日本、英国、韩国、俄罗斯等国家均在研发、计划部署或者已经部署了QKD网络。

同时，QKD组网理念和技术仍在不断演进。2018年6月，西班牙电信、华为和UPM大学在马德里进行了首次软件定义量子密钥分发网络（SD-QKDN）外场试验。

2 量子密钥分发网络体系架构

为了简化维护管理和提高网络运营效率，量子密钥分发网络应支持根据业务安全需求快速提供量子密钥服务，并实时满足密钥和加密业务QoS变化需求，提供保证成码率、时延、可用性、误码性能等的量子密钥分发连接。

将软件定义网络（SDN）的概念和技术应用于量子密钥分发网络构建SD-QKDN，可以对量子密钥分发网络的资源和状态进行逻辑集中控制，通过开放控制接口将抽象后的量子密钥分发网络资源提供给应用层，实现量子密钥分发网络的可编程性，有利于构建面向多种业务和复杂应用的开放、灵活、智能的量子密钥分发网络。

SD-QKDN体系架构基本功能包括：通过中继节点进行密钥中继传输，实现任意2节点间的高安全密钥分发；通过量子密钥分发光网络生成的共享密钥对为通信两端用户提供加密传输；当新增的量子密钥分发网络节点接入量子密钥分发网络时可进行身份认证；当节点的位置关系发生变化时，重新进行鉴权并更新路由关系及位置信息；网络可根据用户的业务请求、网络负载情况，提供最优的量子密钥传输路径；可根据用户的位置更新和节点/链路的故障信息进行密钥传输路径的重配置。

SD-QKDN具备三大基本特征：QKD网络控制面与数据面分离、逻辑集中式的控制平面、开放的控制接口。

a）控制与数据分离：通过将QKD网络控制与量子密钥分发设备分离，在控制层中屏蔽量子密钥分发网络量子层细节，简化现有量子密钥分发网络复杂和私有的控制管理协议。

b）逻辑集中式的控制平面：通过将量子密钥分发网络控制功能和策略集中化，可以实现全网资源的高效利用。这里的集中控制是逻辑集中，不限制控制器的物理位置和控制器软件的部署方式。

c）开放的控制接口：通过标准的网络控制接口，可以向量子密钥分发网络的外部业务和应用开放网络能力和状态信息，允许应用层业务获取量子密钥分发网络资源，并对量子密钥分发网络进行监控和调整。

根据SD-QKDN的基本特征和功能划分，本文提出了一种SD-QKDN体系架构，该架构包括4层：应用层、控制层、密钥管理层、量子层，如图1所示。其中密钥管理层功能可以作为控制层内部的独立功能，也可以由独立的密钥管理功能子系统实现。

SD-QKDN体系架构的主要接口包括：

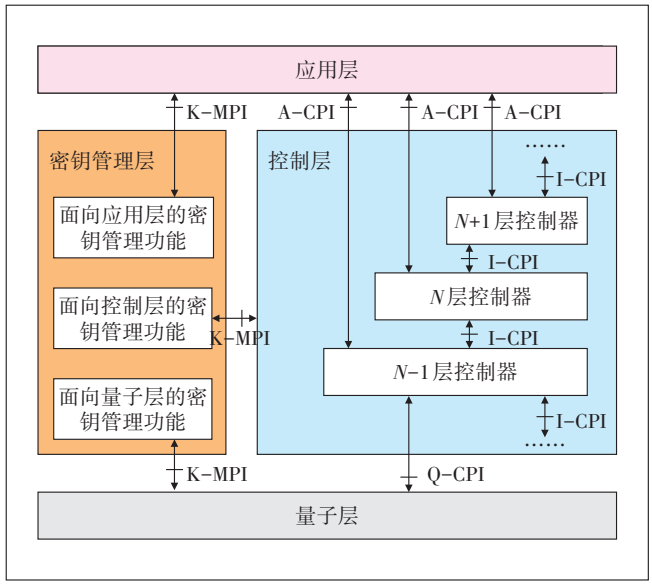

图1　SD-QKDN体系框架

a）量子控制接口（Q-CPI）：控制器与量子密钥分发设备之间的接口。控制器通过此接口控制量子层量子密钥分发资源。控制器与多个量子密钥分发设备相连，应支持多个量子控制接口。量子控制接口的代表性协议包括OpenFlow协议、OF-Config协议以及传统管理协议（如Qx、SNMP、TL1等协议）。

b）控制器层间接口（I-CPI）：高层控制器与低层控制器之间的接口。根据软件定义量子密钥分发网络的控制器分层部署情况，一个控制器可提供多个控制器层间接口，并允许同时接受多个高层控制器的控制。

c）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控制器接收服务。控制器应支持多个应用控制接口，为多个业务应用提供服务。应用控制接口的代表性协议包括RESTconf协议等。

d）密钥管理接口（K-MPI）：密钥管理层与量子层、控制层以及应用层之间的接口，密钥管理层通过该接口配置量子层的量子密钥资源，实现面向量子层、控制层和应用层的密钥管理功能。

2.1 量子层

量子层处于软件定义量子密钥分发网络架构的最底层，是软件定义量子密钥分发网络的技术基础。量子层要进行量子信息处理和经典信息处理。量子信息的处理包括：量子态制备、量子态探测、光量子交换等，其中量子态制备模块依据量子密钥分发协议完成量子态制备和发送，量子态探测模块接收量子态并依据量子密钥分发协议完成量子态解码和探测，光量子交换模块实现量子信道的切换。经典信息的处理主要完成量子密钥分发协议中需要的经典信息处理的功能。例如，BB84协议中经典信息处理需要完成的功能包括：基矢比对、信息纠错协商、安全密钥提取等。量子层的物理资源包括量子密钥分发物理节点和物理链路，具体可以用来完成点对点的量子密钥分发。

2.2 密钥管理层

密钥管理层的主要功能包括：设备管理、密钥存储、密钥中继、密钥输出等。设备管理功能是密钥管理层对量子层的设备进行状态管理。密钥存储功能是对接收到的量子层上传的量子密钥，进行双方的信息同步，并安全地存储到内部的存储模块。密钥中继功能是根据密钥中继路径的指引，将量子层上传的量子密钥中继到远端，从而形成端到端量子密钥。密钥输出功能主要是面向应用层和控制层输出安全一致的量子密钥，供业务应用加密和控制层安全加密使用。密钥管理层主要的设备有量子密钥管理服务系统、量子密钥管理机等。量子密钥是量子密钥分发网络最宝贵的网络资源，可以用来构建量子密钥池、量子密钥分发虚拟链路等。

2.3 控制层

控制层的主要功能是通过南向接口控制量子层的量子密钥分发行为，并通过北向接口向应用层开放量子密钥分发网络能力。控制层支持在多域、多技术、多层次和多厂商的量子密钥分发网络中实现连接控制、网络虚拟化、网络优化以及提供第三方应用的能力。控制层可以完成对多种量子密钥分发网络技术的控制，并支持跨多层网络的控制，实现多层的资源优化。控制层的控制器是对量子层资源实施控制，并通过标准接口开放量子密钥分发网络控制能力的软件实体，可以由分布在不同物理平台上的任意数量的软件模块实现。为实现控制层扩展性，根据地域、安全等策略划分控制边界，控制层应支持层次化结构、多个控制域划分和控制器分层嵌套，控制器之间通过分层迭代方式构成层次化控制架构。由下层控制器分别控制不同的量子密钥分发网络域，并通过更高层次的控制器负责域间协同，实现分层分域的逻辑集中控制架构。各层控制器是客户与服务层关系，各层控制器之间的接口通过控制器层间接口进行交互。

2.4 应用层

应用层处于软件定义量子密钥分发网络架构的最上层，是量子密钥最终应用的主要位置。应用层包含各种量子密钥应用设备以及相关的数据传输网络。应用层具有运营、服务等功能，包括密码服务和安全管理2个部分，密码服务能够为网络需要使用密码的功能如认证、加密、签名等提供密码服务，安全管理主要负责入侵检测、访问控制、病毒防护、安全态势等。

3 SD-QKDN关键技术

3.1 密钥池构建技术

为了实现业务的安全传输以及密钥资源的高效利用，SD-QKP构建技术被提出。它将密钥服务看成一种池化资源，使得密钥的生成以及密钥的使用解耦，具体如图2所示。图2中密钥池表示每对节点抽象成的一个设备，用于存储该对节点的KS中的密钥对，主要负责密钥资源的生成。VKP是指密钥池中抽象出来的一部分区域，用于存储密钥池中部分密钥。密钥即服务（KaaS——Key as a Service）式框架在原来的基础上增加了2个虚拟化步骤：KP构建和VKP构建，密钥池构建主要用于将QCN间KS存储的密钥虚拟化到KP中，便于密钥资源的管理。VKP构建主要用于将部分密钥池中的资源，虚拟化到VKP中，用来满足特定用户的需求，实现资源的高效利用。

为了更好地实现量子密钥池以及虚拟量子密钥池，引入SDN技术，实现对设备高效全局控制以及资源

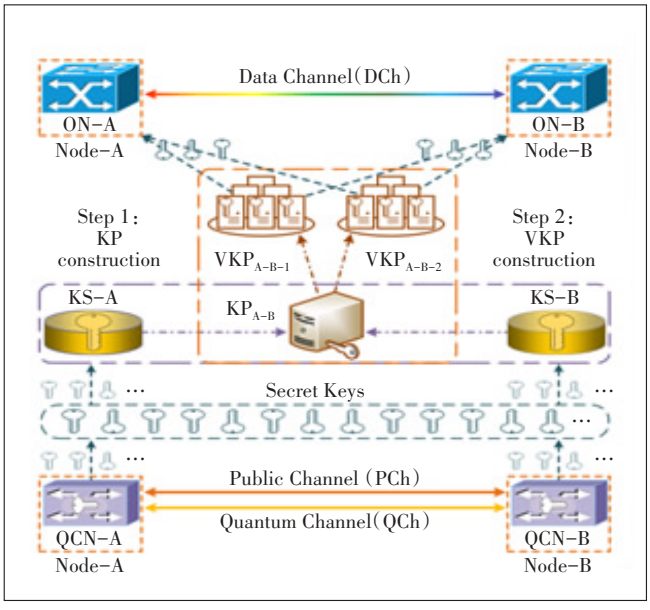

图2　KP构建示意图

的灵活调度。如图3所示，SD-QKDN架构从上到下分为4层，分别是应用层、控制层、密钥分发层以及数据层。数据层主要包括QCN和DCh，用于加密数据传输。密钥分发层主要包含QCN和QCh，QKD过程主要发生在这一层。在控制层，通过SDN，实现对密钥分发过程的调度。在应用层，用户提出一定的量子保密需求，同样通过控制器发出指令，实现对量子保密业务的承载，满足用户安全需求。

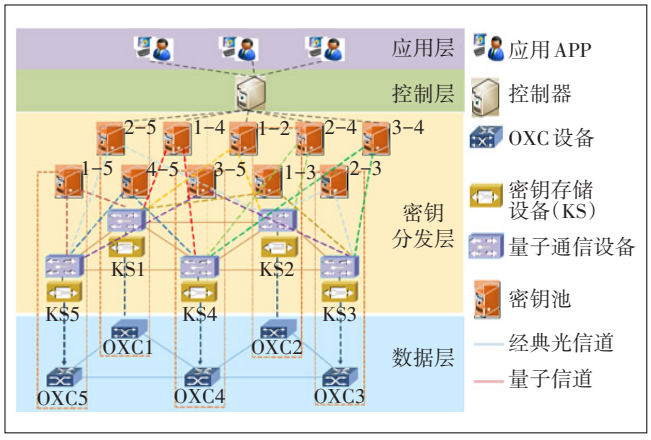

图3　SD-QKDN架构

3.2 路由与密钥资源分配技术

通过对KP以及VKP的构建可以实现在不同安全需求下，量子密钥资源的高效部署与使用。其中KP构建过程主要针对量子密钥的分发与存储，VKP构建过程主要针对密钥资源的消耗与使用。

如图4所示，本文提出了一种静态的KP构建方案以实现量子密钥资源的高效分发与部署。当加密业务需求到达的时候，使用Dijkstra算法找到一条最小跳数的路径，查询当前路径上是否有足够的时间片资源，如果没有足够时间片，该KP构建业务阻塞，如果有足够的时间片，采用首次命中算法（First Fit Algo-

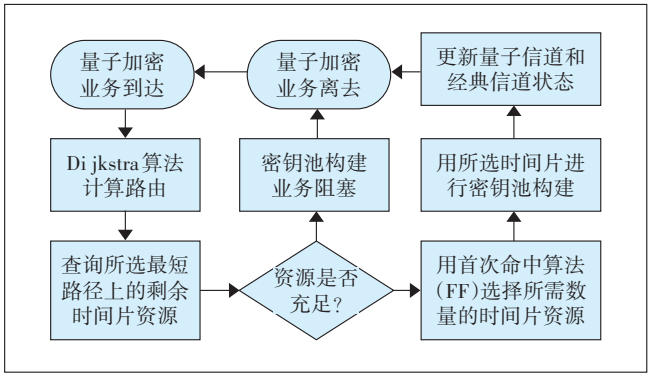

图4　路由与密钥资源分配流程图

rithm）分配时间片资源，最后更新QCh状态，等待下一个加密业务到达。

对于VKP构建来说，存储在KP中的密钥资源成了一个新的资源纬度，KP中的部分密钥可以用来虚拟化以构建VKP，用来满足特定用户的安全需求，可以使得密钥的需求与基础设施解耦。不同的VKP构建业务的密钥需求是不同的，这与其在光网络中需要加密传输的业务量有直接的关系。当VKP构建业务到达的时候，首先查询相关的KP，获取KP中的剩余密钥量，查询KP中是否有足够的密钥资源能够满足当前VKP构建业务密钥资源需求，如果不满足，那么该VKP构建业务阻塞，如果有足够的密钥资源，通过首次命中算法选择，选择对应数目的密钥资源进行VKP构建，最后更新密钥池资源并等待下一个VKP构建业务到达。

3.3 生存性技术

在SD-QKDN中，密钥服务可用性的增强技术可采用2种典型技术，即网络保护和恢复。网络保护是指采用一条预配置的备用路径来替代失效的工作路径，网络恢复是指利用空余资源进行重路由来替代失效的工作路径。基于SDN控制器的密钥服务保护和恢复机制可为量子密钥分发网络的运营和管理提供一种更灵活的、快速的网络生存性技术选择。特别是在跨多层、多域的SD-QKDN递归控制架构情况下，不同网络域采用不同的控制器控制，不同的QKD层面协议及其保护方案差异化的场景下，可采用基于控制器的多域分段保护与动态恢复相结合的网络生存性方案。SD-QKDN网络的保护恢复技术分为2类。

a）基于SDN控制器的加密服务保护：由控制器负责配置工作路径、保护路径和保护组属性参数等。在QKD平面检测到工作路径的故障或性能劣化后上报到控制器，由控制器负责在源、宿、中间节点之间的密钥服务保护倒换。

b）基于SDN控制器的加密服务恢复：控制器负责为工作路径配置预置恢复路径或动态恢复路径。在QKD平面检测到工作路径的故障或性能劣化后上报相关通知到控制器，由控制器负责从工作路径到恢复路径的倒换。

4 结束语

量子密钥分发技术可以保证密钥分发的信息理论安全性，利用经典光网络可以为量子密钥分发提供组网所需的通信管道资源，同时量子密钥分发的引入可以很大程度上提升现有网络的信息安全性。根据国家发改委发布的《组织实施2018年新一代信息基础设施建设工程的通知》，“国家广域量子保密通信骨干网络建设一期工程”明确提出构建量子保密通信网络运营服务体系，进一步推进其在信息通信领域及政务、金融、电力等行业的应用。随着相关技术的不断成熟、市场需求的持续扩大和应用场景的深入挖掘，一个大规模、多层级、跨行业的量子密钥分发网络将迅速成形。

本文从量子密钥分发网络研究进展出发，结合量子密钥分发技术发展趋势，介绍了国际和国内量子密钥分发网络发展状况。为了简化量子密钥分发网络的维护管理和提高量子密钥分发网络的运营效率，提出了一种软件定义量子密钥分发网络体系架构，实现了量子密钥分发网络的可编程性。通过研究量子密钥分发网络的高效组网与灵活应用关键技术，可以有效推动量子密钥分发网络建设与运营并提升网络信息安全性能，为实现安全可靠、开放互联、高服务质量的现代化量子密钥分发网络奠定基础。

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] SCARANI V, BECHMANN-PASQUINUCCI H, CERF N J, et al. The security of practical quantum key distribution [J]. Reviews of Modern Physics, 2009, 81(3): 1301-1350.

[3] ELLIOTT C, COLVIN A, PEARSON D, et al. Current status of the DARPA quantum network (Invited Paper) [J]. Proceedings of SPIE - The International Society for Optical Engineering, 2005, 5815(1): 138-149.

[4] PEEV M, PACHER C, ALLÉAUME R, et al. The SECOQC quantum key distribution network in Vienna [J]. New Journal of Physics, 2009, 11(7): 075001.

[5] LIAO S K, CAI W Q, HANDSTEINER J, et al. Satellite-relayed intercontinental quantum network [J]. Physical Review Letters, 2018, 120(3): 030501.

作者简介：
马彰超，国科量子通信网络有限公司标准总监，博士，主要研究方向为量子密钥分发网络技术与应用；曹原，博士研究生，主要研究方向为量子密钥分发组网；董凯，硕士研究生，主要研究方向为量子密钥分发组网；赵永利，教授，主要研究方向为量子密钥分发组网、人工智能与光联网。