量子保密通信技术发展及应用分析

Development and Application Analysis of Quantum Secure Communication Technology

申　虹（中国通信建设集团设计院有限公司，北京 100076）
Shen Hong（China Communication Construction Group Design Institute Co.，Ltd.，Beijing 100076，China）

摘　要：
量子保密通信是未来提升信息安全保障能力的重要技术手段之一。介绍了基于量子密钥分发（QKD）的量子保密通信关键技术，探讨了量子保密通信应用示范及标准化研究最新进展，提出了量子保密通信的系统架构和典型网络组织；同时为了更好地与现有通信系统融合，提出了一种QKD系统与大容量光通信系统共纤传输方案；最后对量子保密通信的发展前景进行了展望。

关键词：
量子密钥分发；量子保密通信；共纤传输；波分复用
doi：10.12045/j.issn.1007-3043.2019.05.015
中图分类号：TN914
文献标识码：A
文章编号：1007-3043（2019）05-0069-05

Abstract：
Quantum secure communication is the important technical method to enhance the capacity of information security. Based on the introduction of quantum key distribution (QKD) technology, the latest progress of application demonstration and standardization is reviewed, the system architecture and typical network organization is proposed. In order to better integrate with the existing communication system, a QKD system and a large capacity optical communication co-fiber transmission scheme is proposed. Finally, the prospect of quantum secure communication is prospected.

Keywords：
Quantum key distribution；Quantum secure communication；Co-fiber transmission；Wavelength division mutiplexing

引用格式：申虹．量子保密通信技术发展及应用分析[J]．邮电设计技术，2019(5)：69-73.

0　前言

上世纪中叶，人类以量子力学为基础开始认识和利用微观物理规律，推动产生了激光器、半导体和原子能等具有划时代意义的重大科技突破。进入21世纪，量子技术与信息技术深度融合，第2次“量子革命”正在到来。量子信息科学是量子力学与信息科学等学科相结合而产生的新兴交叉学科，目前其重点发展方向包括量子通信、量子测量和量子计算3个领域，分别以面向无条件安全的保密通信、超强的计算能力、精密探测突破了信息科学的经典极限。量子信息科学将为信息社会的演进提供强劲动力。

量子计算利用“量子比特”量子叠加态的特性，通过量子态的受控演化实现数据的存储计算。随着量子比特数量增加，量子计算算力可呈指数级规模拓展，理论上具有经典计算无法比拟的超强并行处理能力。以IBM的超级计算机Blue Gene为例，它需要花费上百万年才完成的数据处理，而量子计算机只需要几秒钟。如果将量子计算比喻成矛，将有望“吾矛之利，于物无不陷也”。量子计算在带来强大算力的同时，也将引发全新信息安全挑战。现有公钥体系的安全性是基于单向计算复杂度的数学难题，即便增加算法复杂度和密钥长度，也难于抵御量子计算攻击，经典加密通信面临严重威胁。当前信息社会和数字化经济时代，信息安

收稿日期：2019-02-28

全形势日益复杂，量子保密通信技术应运而生，将以“吾盾之坚，莫之能陷也”为目标构建信息安全关键屏障。

本文将介绍基于QKD的量子保密通信关键技术、量子保密通信技术应用示范及标准化情况、网络架构和典型网络组织，及其发展前景，并提出发展建议，为量子保密通信发展、应用、规模部署提供参考。

1 保密通信技术发展

G.Vernam在1917年提出一次一密（OTP）的思想，对于明文采用一串与其等长的随机数密钥进行加密，接收方使用相同的随机数密钥进行解密，随机数密钥真正随机且只使用一次，OTP加密技术已经被证明是安全的。但在经典通信领域，其所需的密钥很难在不安全的信道上实现无条件安全分发，采用不安全的密钥来实施“一次一密”加密仍然是不安全的。后来，出现了公钥密码体制，接收方有一个公钥和一个私钥，接收方将公钥公开出去，发送方用公钥加密信息后发给接收方，接收方用私钥解密信息。公钥密码体制的优点是不需要经过安全的信道对外传递密钥，但它的安全性是基于难于求解的数学难题，例如大数分解问题，业已证明，量子计算机的并行预算能力可以攻破RSA/DSA/ECDSA等密码，现有公钥体系将面临巨大挑战。

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，是基于量子密钥分发（QKD）技术，结合适当的密钥管理、安全的密码算法和协议而形成的加密通信安全解决方案。量子密钥分发可以在空间分离的用户之间以信息理论安全的方式共享密钥，这是经典密码学无法完成的任务。QKD结合OTP策略，实现“一次一密”的绝对安全通信。QKD技术的密钥分发与计算复杂度无关，即使拥有无限强的计算能力，也不能攻破。因此，量子保密通信被认为是未来提升信息安全保障能力的重要技术手段之一，受到广泛的关注。

2 量子密钥分发技术原理

QKD是一个通信双方协商产生共享密钥的过程，目前，实用化程度最高的QKD协议为BB84协议。BB84协议利用单光子的量子态作为信息载体进行编码、传递、检测等以实现量子密钥分发。按照BB84协议，每一个光子随机选择调制的基矢，接收端也采用随机的基矢进行监测。以偏振编码为例，采用了单光子的4个偏振态：水平偏振态（0°）、垂直偏振态（90°）、+45°偏振态和−45°偏振态，其中0°和90°构成水平垂直基（base0），±45°构成斜对角基（base1）。事先约订单光子的水平偏振态0°或−45°偏振态代表经典二进制码0，垂直偏振态90°或+45°偏振态代表经典二进制码1。发送方Alice随机使用2组基矢，将随机数0，1编码到单光子的相应偏振状态，通过量子信道发给合法用户Bob。Bob接收到光子后，随机地使用2组基矢的检偏器测量偏振态。若制备基矢和检测基矢兼容，则收发随机数完全一致，否则接收随机数与发送可能不同。为了提取一致信息，Alice和Bob在经典协商信道上进行制备基和测量基基矢比对，两端都保留基矢一致部分的信息，收发双方拥有完全一致的随机数序列密钥。如果存在窃听，根据量子不可克隆定理窃听者无法克隆出正确的量子比特序列，因此窃听者须采用截获光子测量后再重发的策略，按照量子力学的假定，测量会有25%的概率得到错误的测量结果并且会干扰到量子态，导致误码率增加，根据误码率评估决定密钥是否保留。保留的密钥通过纠错和保密增强最终获得安全密钥。图1示出的是QKD BB84协议原理示意图。

3 量子保密通信应用示范情况

近年来，国内外均在积极开展量子保密通信的研发和应用推广工作。量子保密通信的试点应用和产业推广呈现较快发展趋势。2003年，哈佛大学建立了世界首个量子保密通信实验网，随后日本、欧洲、韩国相继开展了实验网建设。2018年，美国公布了华盛顿-波士顿商用QKD系统建设计划。目前，我国是量子通信技术领域专利公开量最多的国家，已初步形成集技术研究、设备制造、建设运维、安全应用为一体的产业链，并已完成了一定规模的量子保密通信应用验证（见

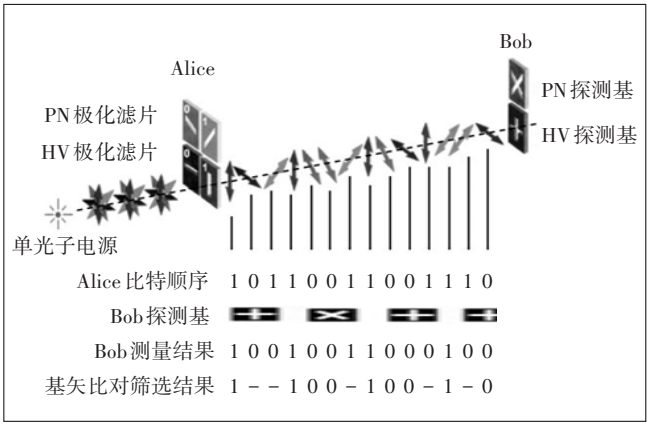

图1 QKD BB84协议原理示意图

图2）。

图2　量子保密通信应用验证情况

基于量子保密通信的信息安全应用呈现出需求牵引、政策驱动、快速发展的特点，目前已经在政务、金融、国防、数据中心等领域开展了示范应用。例如，在金融领域已形成6种应用示范，包括同城数据备份和加密传输、网上银行加密、异地灾备、视频会议、监管信息采集报送及大数据应用等；在云数据中心领域，在阿里云机房环境中搭建了测试平台，对量子设备与公共云平台的技术融合进行测试和验证，发布了云量子保密通信产品。

4　量子保密通信标准化进展

欧美在标准化方面起步较早，欧洲电信标准化协会（ETSI）、国际互联网工程任务组（IETF）、美国电气和电子工程师协会（IEEE）、ITU-T SG17工作组等都相继提出了相关量子保密通信的标准。我国在量子通信方向的标准化在2015年启动，其中CCSA于2017年成立了量子通信与信息技术特设任务组（ST7），推动量子保密通信标准体系建设。相关标准化工作进展如表1和表2所示。

5　量子保密通信网络组织

5.1　功能架构

表1　密码行业标准化技术委员会量子密码标准工作组标准化研究情况

项目名称	状态
诱骗态BB84量子密钥分配检测规范	在研标准
量子随机数研究	在研标准
量子保密通信中继安全性研究	在研标准
量子密钥接口应用规范	在研标准
相干态连续变量量子密钥分发技术规范	在研标准

表2　中国通信标准化协会量子通信与信息技术特设任务组（ST7）标准化研究情况

项目名称	计划完成时间
量子保密通信系统测试评估研究	研究课题已发布
量子通信术语和定义	2020-09-30
量子保密通信应用场景和需求	2020-09-30
量子密钥分发（QKD）系统技术要求 第1部分：基于BB48协议的QKD系统	2020-12-31
量子密钥分发（QKD）系统应用接口	2020-12-31
量子密钥分发（QKD）系统测试方法	2020-12-31

量子保密通信网络的部署需综合考虑保密通信服务和通信网络建维营等方面的要求，满足通信网络可用性、可靠性、灵活高效、可扩展的建设需求。QKD网络功能模型如图3所示，分为密钥生成层、密钥分发层、密钥应用层、网络管控、安全服务5部分。

在图3所示分层架构中，密钥生成层负责完成量子密钥的制备，为上层提供量子密钥。密钥分发层实现密钥中继、密钥转发、密钥存储及密钥输出等功能。密钥应用层提供使用量子密钥的保密通信服务。网络管控平台完成网络管理、运营管理、密钥路由、密钥生成控制等功能。安全服务平台包括密码服务和安全管理。

根据功能需求，量子保密通信系统站点间及站点内信息交互产生的通信需求如表3所示。站点间量子态承载的量子比特信号由量子信道传送；密钥协商和管理协商信息交互由协商信道传送；使用量子密钥服务的加密业务由经典数据信道传送。

5.2　典型网络组织

目前，国内典型QKD网络实现方案利用“量子密钥分发+可信中继+光传送”搭建。网络架构包括量子骨干网和量子城域网2部分，网络组织如图4所示。

表3　量子保密通信系统数据通信表

业务类型	业务描述
站点间通信	量子网关在量子密钥分发过程中进行的数据交互
	密钥管理机、密钥生成控制/中继路由服务器间的数据及指令交互
	密钥管理机间的中继密钥数据传输
	综合网络管理信息传输
	备份数据传输
站点内通信	量子网关和密钥管理机间的指令、密钥
	量子网关、密钥管理机、密钥生成控制/中继路由服务器上报给本地量子网络管理服务器（EMS）的网管信息
	本地量子网络管理服务器转发给量子网关、密钥管理机、密钥生成控制/中继路由服务器的下发配置消息、升级数据等

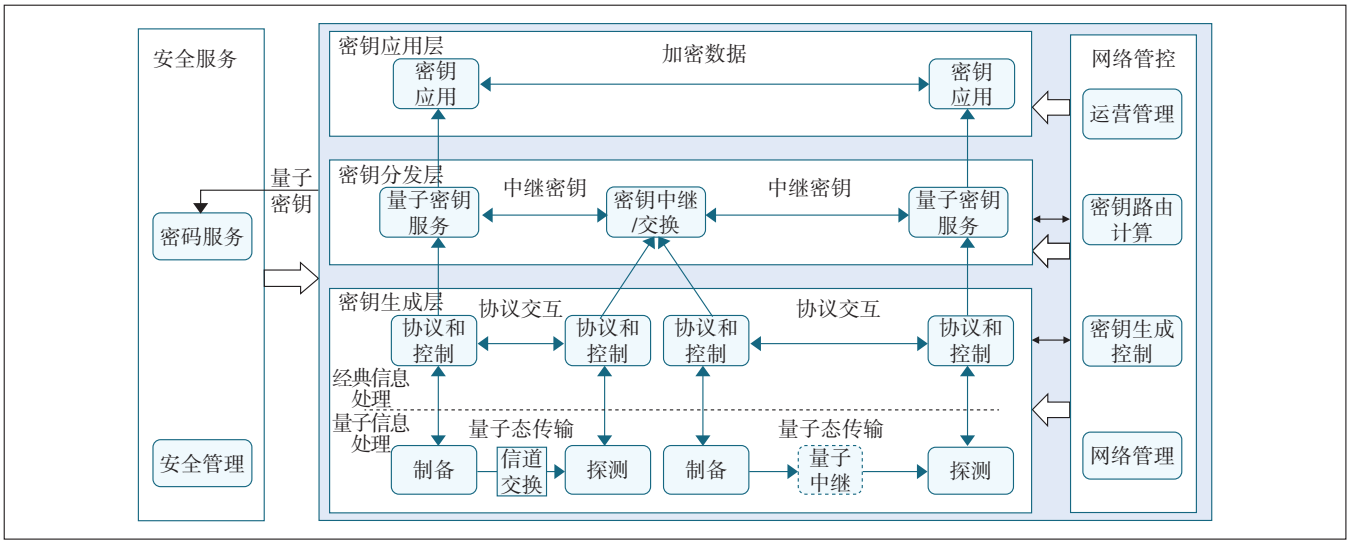

图3 QKD网络功能模型示意图

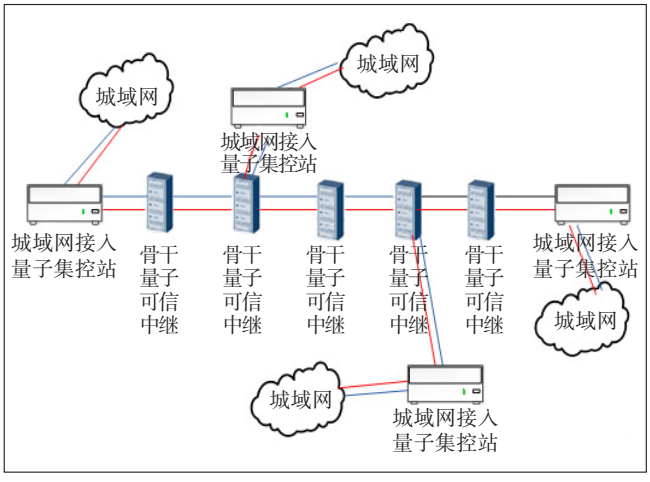

图4 典型QKD网络组网示意图

5.3 组网方式

量子骨干网是连接各个城域网的远距离、大容量主干量子保密通信网络。通常采用环形或Mesh组网。QKD受弱光源限制，要达到一定成码率，一般80~100 km需要可信中继。

量子城域网是一定区域范围内，以用户接入为主要功能的中小型量子保密通信网络。网络末梢通常采用星形组网。用户量级大时，可组织汇聚层网络，采用环形组网。

5.4 节点类型

QKD网络节点分为接入节点、中继节点、用户节点3类。

a）接入节点：负责其所辖区域内各用户节点或城域网接入，可实现量子密钥生成控制、密钥管理、中继路由等功能，设备类型包括量子设备、经典数通设备、传输设备、服务器集群等。

b）可信中继站：对量子密钥进行中继传输，通过多级密钥中继的方式实现各城域节点间的量子密钥的共享。可信中继站由量子密钥分发系统和数据传输系统组成。

c）用户节点：用户接入站点提供应用层服务。

5.5 建设内容

量子保密通信网络主要建设内容包括量子骨干网、IP承载网、光传送网、IT平台等子系统。

a）量子骨干网：传送量子信道。

b）IP承载网：承载协商信道。

c）光传送网：远距离广域通信基础网。

d）IT系统：目前主要包括网络管理、运营管理、安全管理。

5.6 可信中继

受限于量子信道的传输损耗，量子密钥分发距离被限制在百公里量级上，需设置中继节点完成长距离接力传送。现有较大规模的量子保密通信网络，都是基于可信中继技术实现的。原始的可信中继方案，需要在中继节点长时间保存量子密钥，因此安全防护困难比较大。目前，得到应用的可信中继技术是异或中继技术，在节点处只会暂存经过异或后的量子密钥，从而减轻了中继节点的安全防护难度。

5.7 共纤传输策略

经典光通信采用密集波分复用技术，传统80波波分复用（DWDM）系统入纤功率约20 dBm。QKD采用

近似单光子源，为弱光信号。经典强光产生的拉曼散射和四波混频效应会对量子信号产生干扰。在京沪干线中，量子信道和经典信道分别采用不同的纤芯传输，需要2对纤。量子信道和经典信道的共纤传输将在未来规模商用部署中有效节省纤芯资源，节约建设成本。为此，业界已开展广泛的共纤研究验证，通过提高波分设备器件性能、增大波长间隔、降低经典信号入纤功率、量子信道和经典信道同向共纤传输等策略可以实现大容量（80波）长距离（80~100 km）共纤传输。QKD系统与OTN的共纤传输如图5所示。

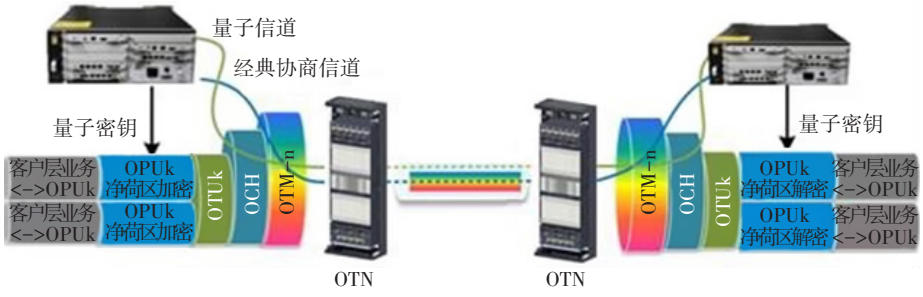

图5　QKD系统与OTN的共纤传输示意图

6 发展建议及未来展望

总体来说，量子保密通信技术应用处于业务试点期、市场培育期、商用推广初期，网络建设处于试点应用阶段，QKD组网理念和技术仍在不断演进中，还有诸多问题有待研究和探讨，商用推广还面临着诸多挑战。发展建议如下：

a）在国家政策支持的基础上，积极推进产业合作，引导和培育市场需求。

b）加快标准化研究工作，推动标准制定，为规模商用部署提供有效的标准引导。

c）加快测试评估体系建设，对网络建设和应用发展进行有效验证和引导。

d）积极探索多样化的商业模式。

e）统筹规划网络建设，充分利用现有网络资源，并兼顾未来网络按需供给、随需而变、灵活健壮的需求。

国家实施创新驱动发展战略，在“十三五”规划和国家大政方针中明确指出，量子信息技术是我国科技创新的重要领域和引领产业变革的颠覆性技术，量子信息产业是我国战略性新兴产业。新一代产业革命和技术革命正在孕育兴起，加快发展量子信息产业，推动量子技术和国民经济各领域深度融合，将对我国未来科技、国家安全、国防军事、产业经济等方面产生深远影响。

参考文献：

[1] 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.
[2] 王向斌. 量子通信的前沿、理论与实践[J]. 中国工程科学，2018(20)：87-92.
[3] 赖俊森，吴冰冰，李少辉，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)：39-45.
[4] 唐建军，李俊杰，张成良，等. 开放式量子保密通信系统架构及共纤传输技术研究与实验[J]. 电信科学，2018，34(9)：28-36.
[5] 吴华，王向斌，潘建伟. 量子通信现状与展望[J]. 中国科学：信息科学，2014，44(3)：296-311.
[6] 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.
[7] 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.
[8] BENNETT C H，BRASSARD G. WITHDRAWN：Quantum cryptography：Public key distribution and coin tossing[J]. Theoretical Computer Science，1984(560)：175-179.
[9] SHANNON C E. Communication theory of secrecy systems[J]. Bell System Technical Journal，1949，28(4)：656-715.
[10] WANG LIUJUN，ZOU KAIHENG，SUN W，et al. Long distance co-propagation of quantum key distribution and terabit classical optical data channels[J]. Physical Review A，2017，95(1)：012301.
[11] LIU Y，CHEN T Y，WANG J，et al. Decoy-state quantum key distribution with polarized photons over 200 km[J]. Optics Express，2010，18(8)：8587-8594.

作者简介：
申虹，毕业于南京邮电大学，高级工程师，主要从事光通信网络规划与设计工作。