

# Development Analysis on Global Quantum Secure Communication Network

Feifan Chen<sup>1</sup>, Xinyu Hu<sup>1</sup>, Yinghao Zhao<sup>1</sup>, Yongzhan Hu<sup>2</sup>, Zhengzheng Yan<sup>1</sup>, Hongxin Li<sup>1,3</sup>

<sup>1</sup>PLA Strategic Support Force Information Engineering University, Luoyang Henan

<sup>2</sup>Zhengzhou Audit Center, Zhengzhou Henan

<sup>3</sup>State Key Laboratory of Cryptology, Beijing

Email: lihongxin830@163.com

Received: Oct. 7<sup>th</sup>, 2018; accepted: Oct. 22<sup>nd</sup>, 2018; published: Oct. 30<sup>th</sup>, 2018

## Abstract

With the popularization of international Internet technology and the rapid development of quantum information technology, the construction of quantum secure communication networks (QSCN) has received extensive attention and the strategic significance of developing quantum secure communication technologies is becoming more and more important. This paper introduces and analyzes the construction of QSCN in major quantum R & D countries and regions such as the United States, the European Union, Japan and China around the world over the past decade in details. It researches and compares the pivotal technology used in the construction of typical QSCN. And the development trends and characteristics of future QSCN are summarized and forecasted.

## Keywords

Quantum Cryptography, Quantum Private Communication, Quantum Communication Network, Quantum Key Distribution

# 全球量子保密通信网络发展研究

陈非凡<sup>1</sup>, 胡鑫煜<sup>1</sup>, 赵英浩<sup>1</sup>, 胡勇战<sup>2</sup>, 闫争争<sup>1</sup>, 李宏欣<sup>1,3</sup>

<sup>1</sup>中国人民解放军战略支援部队信息工程大学, 河南 洛阳

<sup>2</sup>郑州审计中心, 河南 郑州

<sup>3</sup>密码科学技术国家重点实验室, 北京

Email: lihongxin830@163.com

收稿日期: 2018年10月7日; 录用日期: 2018年10月22日; 发布日期: 2018年10月30日

## 摘要

随着国际互联网技术的普及和量子信息技术的飞速发展, 量子保密通信网络建设受到了广泛关注, 发展

文章引用: 陈非凡, 胡鑫煜, 赵英浩, 胡勇战, 闫争争, 李宏欣. 全球量子保密通信网络发展研究[J]. 计算机科学与应用, 2018, 8(10): 1628-1641. DOI: 10.12677/csa.2018.810179

量子保密通信技术的战略意义越来越重要。本文对近十年来美国、欧盟、日本和中国等全球主要量子研发国家和地区的量子保密通信网络发展建设情况进行详细的介绍和分析, 研究对比了典型量子保密通信网络建设采用的关键技术, 总结和展望了未来量子保密通信网络的发展趋势和特点。

## 关键词

量子密码, 量子保密通信, 量子通信网络, 量子密钥分发

Copyright © 2018 by authors and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

## 1. 引言

随着经济全球化的发展和国际互联网的普及, 互联网信息安全受到世界的高度关注与重视。密码技术作为信息安全领域最重要的内容之一, 为确保一个国家的政治、经济、军事、社会等各方面的信息安全做出了突出的贡献。量子密码学作为密码技术领域的新星, 在近二十多年里发展迅速, 是公认的未来最可能成为主流密码技术的代表之一。量子保密通信技术则是基于量子力学原理, 利用量子纠缠效应进行通讯的新型安全通信技术, 其运用了大量的量子密码学相关知识原理。量子通信的最大优点是具有理论上的无条件安全性。因此, 量子通信技术以其无比的优越性, 在国家安全、金融经济等信息安全领域具有重大的应用价值与前景。

针对不断发展的量子保密通信技术, 上世纪 80 年代末开始, 美国、日本、欧盟等主要西方国家和组织的政府、军方及主要大型公司均制定了相应的量子保密通信发展计划、同时投入大量人力和资金进行研究, 在实现百公里级点对点量子密钥分发的基础上建立了各国的量子保密通信网络, 大量研究成果居于世界领先地位。

本世纪初, 量子保密通信技术的实地网络相继出现, 以美国研发的一系列量子通信网络最为突出, 首先是美国 DARPA 量子密钥分发网络, 随后, 美国国家标准技术局(NIST)量子网络、美国洛斯阿拉莫斯国家实验室量子网络和美国伯特利(Battelle)量子网络相继诞生, 其中伯特利量子网络作为商业公司研发的量子网络代表, 有着巨大的商业价值与应用前景。欧盟在量子通信网络方面的研究紧随其后, 从 2004 年开始, 欧盟组织及各成员国先后建立了欧洲 SECOQC 量子保密通信网络、瑞士日内瓦量子网络、西班牙马德里量子通信网络等。日本方面, 规划多年的东京量子通信网络(Tokyo Network)于 2010 年 10 月正式建成, 标志着日本也步入了量子通信领域发展的快车道。中国方面, 2016 年 8 月 16 日 1 时 40 分, 全球首颗量子通信卫星“墨子号”在酒泉成功发射升空, 这标志着量子密码的实用化进程迈出重要一步。

本文将从区域角度, 对全球主要国家和地区的量子保密通信网络建设发展现状进行总结性介绍, 对比典型量子保密通信网络特点, 有利于研究人员掌握关键技术、找到差距、提供建议, 加强人们对量子保密前沿技术的掌控的同时, 培育面对世界领先科技时的广阔视野和全球思维, 这对于量子保密通信发展建设的宏观研究具有重要的参考价值。

## 2. 美国量子保密通信网络发展

### 2.1. 美国 DARPA 量子通信网络

DARPA 即“Defense Advanced Research Projects Agency”(美国国防部高级研究计划局), 该局研发的 DARPA 量子密钥分发网络是世界上第一个实地建设的量子保密通信网络。

DARPA 量子密钥分发网络于 2002 年开始架构设计, 2003 年 10 月 23 日在 BBN 技术公司的实验室

正式开始全面运作。2004年6月,该网络在连接BBN、哈佛大学和波士顿大学的剑桥街地下光纤中进行了连续运行,此次连续运行的DARPA网络是一个六节点量子网络,如图1所示。2004年12月,该网络成为了国际上首个可应用于互联网的量子密码网络系统[1]。此次运行的网络同样包含了六个节点,其中四个节点在BBN公司内部,另外两个节点由美国国家标准技术局和QinetiQ公司提供。2006年,DARPA成功建设8节点的量子密钥分发网络。2007年,这个网络成功建设到10个节点。

DARPA量子密钥分发网络支持多种量子密钥分发技术,其中包括光纤信道的相位调制量子密钥分发、光纤信道的纠缠光源量子密钥分发和自由空间量子密钥分发技术。该网络包含的量子密钥分发系统有四种,其中两种是BBN技术公司团队研制的利用弱相干光源的量子密钥分发系统和基于纠缠光源的量子密钥分发系统,另外两种是由美国国家标准技术局(NIST)的利用了衰减激光脉冲原理的量子分配系统和QinetiQ公司的自由空间量子密钥分发系统。

### 2.2. 美国国家标准技术局(NIST)量子通信网络

2006年,美国国家标准技术局(NIST)演示了一个“三用户有源量子网络”,包括一个发射端(Alice)和两个接收端(Bob1, Bob2),发射端与接收端使用有源光开关相连接,每个接收端与发射端相距约1公里并通过光纤联通,其筛选之后的密钥速率超过1 Mb/s。

如图2所示,该通信网络在Alice发射端有两个用来改变通信波长的光开关。经典通信使用1550 nm波段,量子通信使用850 nm波段。在发射端(Alice)和一号接收端(Bob1)之间可以使用850 nm单模光纤的量子信道(HI780)或标准电信光纤的经典信道(SMF28),它们的长度均为1公里。在发射端(Alice)和二号接收端(Bob2)之间,经典信道和量子信道均为标准电信光纤(SMF28),长度也均为1公里。在量子信道末端,有一小段具有空间滤波器功能的HI780纤维,用来消除混杂在1550 nm纤维中的850 nm高模式成分。整个网络系统采用编程可控的偏振控制器补偿偏振在光纤中的传输变化,其中一号接收端(Bob1)采用液晶型偏振控制器,二号接收端(Bob2)采用压电型偏振控制器。

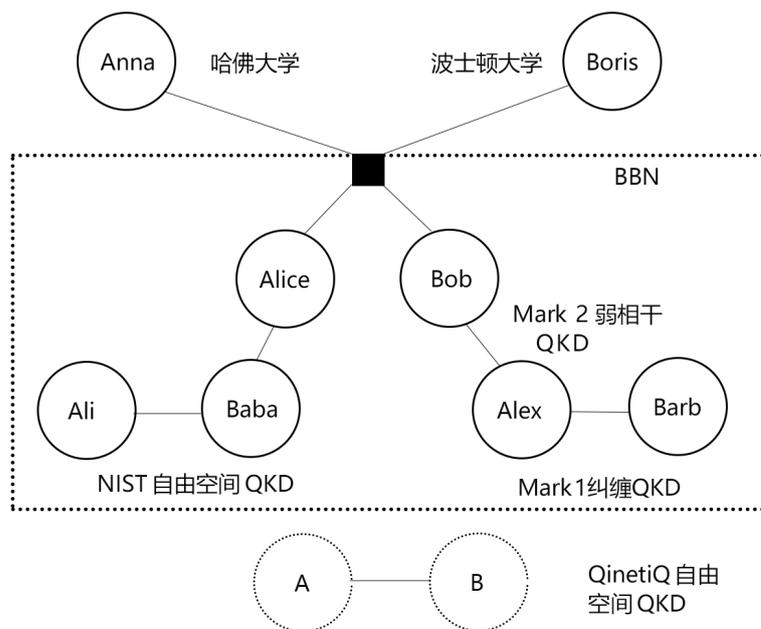


Figure 1. DARPA Quantum key distribution network structure  
图 1. DARPA 量子密钥分发网络结构

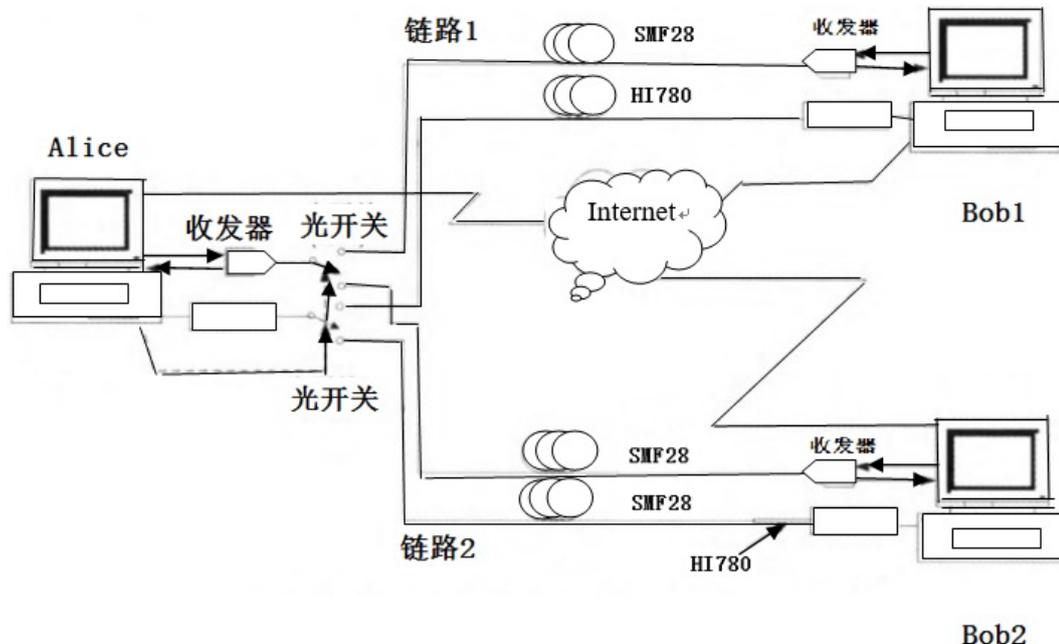


Figure 2. NIST Three-node quantum secure communication network structure  
图 2. NIST 三节点量子保密通信网络结构

### 2.3. 美国洛斯阿拉莫斯国家实验室量子通信网络

2000年,美国洛斯阿拉莫斯国家实验室(Los Alamos National Laboratory)的研究成果使量子通信在自由空间里进行的量子密钥分发的传输距离达到了1.6公里[2];2006年,该实验室进一步实现了其提出的诱骗态方案,完成了超过100公里的量子保密通信实验,基本达到城际量子保密通信在距离上的要求。

洛斯阿拉莫斯国家实验室的量子网络是一个以独立网络为核心的量子通信网。该实验室创建量子网络的方法是基于“轴-辐”式网络架构,所有传送的信息都经过“轴”,所有进入“轴”的信息都经过量子加密,当信息到达“轴”时,先转变成传统的信息形式,再转变成量子比特向外辐射状传送。所以,在该量子网络系统中只要“轴”安全,整个网络就安全。

2012年12月,洛斯阿拉莫斯国家实验室的研究小组在伊利诺伊大学香槟分校(University of Illinois Urbana-Champaign)演示了量子保密通信在政府能源电网可靠网络基础设施数据传输中的优势。在测试中,该小组使用了25公里的光纤链路,发现通信等待时间仅仅约为125微秒,与传统保密通信相比,有更高的安全性和更好的高效性。

### 2.4. 美国伯特利量子通信网络

2012年6月,美国伯特利公司和瑞士ID Quantique公司合作,开始着手建立美国首个商用量子加密通信网络——伯特利量子通信网络。

伯特利量子通信网络的具体建设主要分为以下四个步骤:

- 1) 在实验室内对30公里至100公里的盘卷光纤量子密钥分发系统进行测试;
- 2) 在俄亥俄州的哥伦布市,使用现有的商用通信设备及商用光纤,连接测试位于两个不同位置的量子密钥分发系统,测试距离为25公里至50公里;
- 3) 2015年中下旬,在哥伦布市内使用商用光纤以及可信的节点结构,建立一个城域环形拓扑结构量子密钥分发网络,并使其连接多个用户;

4) 2016 年, 使用可信的中继结构及商用光纤, 在哥伦布市与华盛顿特区之间建立一个长距离量子通信骨干网络连接两地, 位于首都华盛顿特区的伯特利办公室也将加入这个网络, 该骨干网络的拓扑网络如图 3 所示。

2013 年 10 月, 在 ID Quantique 公司的帮助下, 伯特利公司成功在公司总部所在地哥伦布市和位于俄亥俄州都柏林市的第二办公室之间建立起了量子保密通信网络, 全长约为 12 英里, 伯特利公司在这两个地方之间的金融、知识产权、图纸、设计以及其他机要通信数据都受到量子网络的保护。2014 年初, 伯特利量子网络的第一阶段已经完成, 其测试系统位于俄亥俄州哥伦布市的伯特利公司总部。

### 2.5. 美国 NASA 量子保密通信干线

2012 年, 美国国家航空航天局(NASA)联合澳大利亚 Quintessence Labs 公司提出建设量子保密通信干线, 其光纤线路由洛杉矶喷气推进实验室到 NASA 的 Amess 研究中心, 其规划包含星地量子通信、无人机及飞行器的量子通信链接。美国 NASA 建设的量子保密通信干线包括陆地 CV-QKD (Continuous Variable Quantum Key Distribution)网络和自由空间 CV-QKD 网络。其中, 陆地 QKD 网络部分在美国能源部能源科学网络(Energy Sciences Network)的暗光纤骨干网上运行。该陆地 QKD 网络由洛杉矶和加州湾区的杰尼维尔之间长达 550 公里的光纤进行连接, 量子密钥分发与经典通信共享光纤流量, 并且在量子通信中使用了密集波分复用技术。该保密干线主要使用短距离的量子中继器、长距离的量子转发器, 以及光路由器。

自由空间 CV-QKD 网络建立了城市间的量子通信链路, 包含与无人驾驶飞机和航天飞机之间的自由空间链路, 以及与卫星之间的自由空间链路, 同样也包括自由空间与光纤链路的光连接点。

## 3. 欧洲量子保密通信网络发展

### 3.1. 欧洲 SECOQC 量子通信网络

欧洲 SECOQC 量子通信网络(Secure Communication based on Quantum Cryptography)于 2003 年开始设

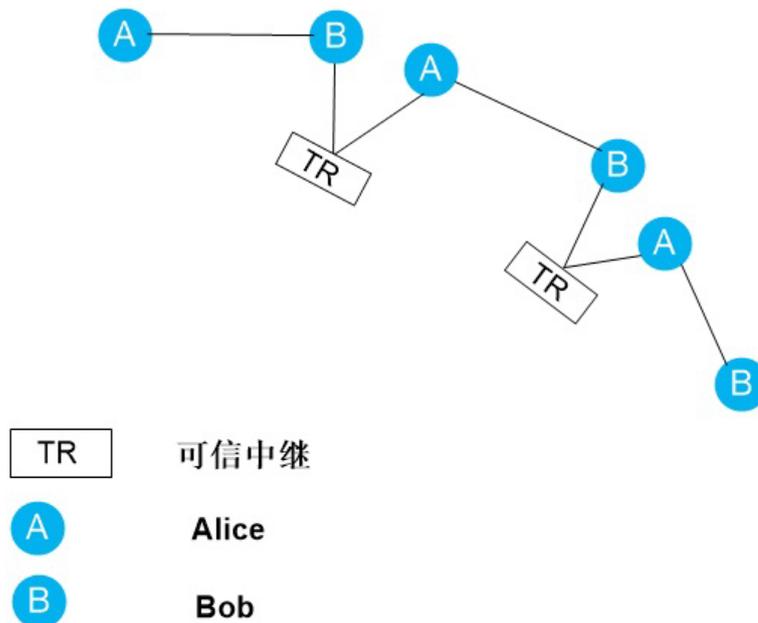


Figure 3. A long-distance metropolitan quantum communication network based on trusted relay nodes

图 3. 基于可信中继节点的长距离城域量子通信网络

计, 2004 年开始建设, 2008 年, 由英国、法国、德国、意大利等欧洲国家在奥地利首都维也纳成功建成。该量子通信实验网络集成了单光子、纠缠光子和连续变量光子等多种量子密钥收发系统, 使西门子公司总部和其子公司之间建立了量子通信连接。

图 4 为整个 SECOQC 量子通信实验网络的结构示意图。其中, 6 个网络节点之间通过 8 条点对点量子密钥分发系统相互连接[3]。SECOQC 量子通信实验网络的 8 条链路中, 有 7 条是光纤信道, 最长为 85 km, 平均链路长度为 20~30 km, 可确保在 25 km 光纤链路上安全密钥率每秒钟超过 1 Kb。

如图 5 所示, SECOQC 量子通信实验网络采用的是建立可信中继节点方式连接多个子网实现量子保密通信。基于可信中继网络及中间层的技术, SECOQC 量子保密通信网络可以做到应用层与底层密钥生成设备无关。只要密钥生成设备满足 SECOQC 量子网络的接口规范, 它可作为可信中继网络的节点进行接入。

SECOQC 量子通信实验网络建立之后经过了一个月的测试, 能够稳定运行。在运行过程中该量子通信实验网络也成功演示了定时更新密钥的 AES 加密算法(Advanced Encryption Standard)对 VPN

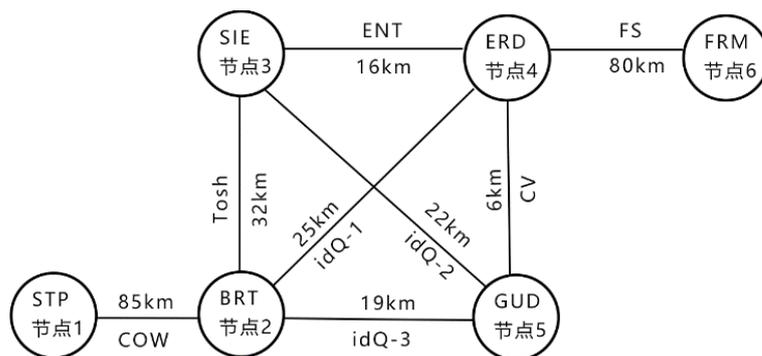


Figure 4. SECOQC Schematic diagram of experimental network connection  
图 4. SECOQC 实验网络连接示意图

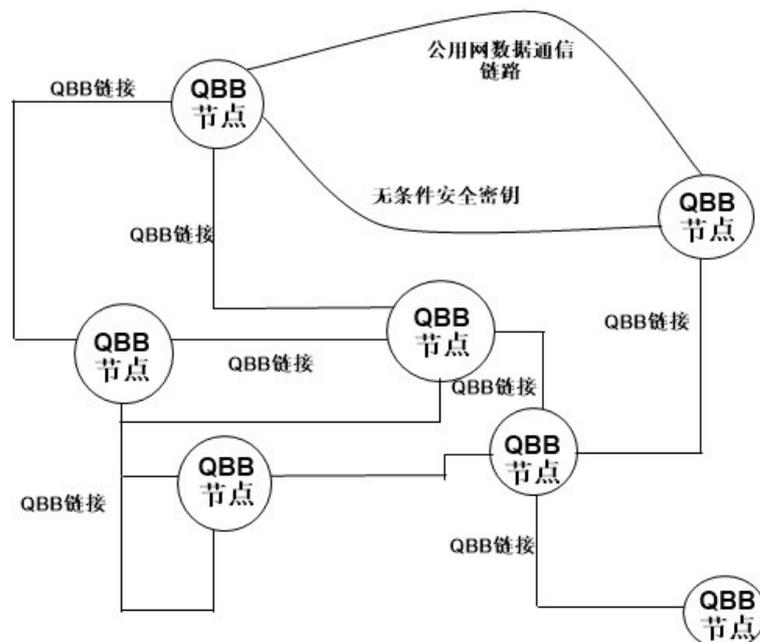


Figure 5. SECOQC Quantum secure communication network structure diagram  
图 5. SECOQC 量子保密通信网络结构图

(Virtual Private Network)进行加密的实验,检验了IP电话机和基于IP的视频会议系统的可靠性,实现了现有条件下的远距离、高安全通信。

SECOQC量子通信实验网络的缺点是,不能应用于目前广泛存在的通信网络,该网络只能在所有中继节点均完全可信的情况下才可运行。

如表1,欧洲SECOQC量子通信网络和美国DARPA量子密钥分发网络,在量子密钥的分配手段上有所不同。

### 3.2. 瑞士日内瓦量子通信网络

2009年,瑞士日内瓦量子城域网开始运行。该网络以三个节点为主体,每个主节点又分为两个子节点,构成了三条端到端的链路,最长的为17.1公里,最短的为3.7公里。该网络的节点分别位于瑞士和法国,是世界上第一个国际量子通信网络。

该网络由虚拟局域网监控,每条端到端的链路均有一个虚拟局域网。此外,还有两个防火墙,分别用来阻止非法用户通过网络连接服务器和限制访问管理网络。每个端到端链路均包括一对商用量子密钥分发设备id5100,该设备基于Plug & Play结构,网络运行标准为BB84协议或者SARG协议,用于密钥提纯,每次筛选的密钥约为125万~175万比特。

### 3.3. 西班牙马德里量子通信网络

2008年11月,Computing学院量子计算与信息研究所开发出了马德里量子保密通信网络。2010年,该网络被部署在西班牙各城市之间的通讯网络中。

该网络包括骨干网与接入网。与美国国家标准技术局(NIST)量子通信网络相比较该网络骨干网的量子信道使用1550纳米波长,经典信道使用1470纳米和1510纳米波长(如表2)。而其接入网使用GPON(Gigabit Passive Optical Network)标准,通信过程使用诱骗态BB84协议,信道容忍的损耗为15dB,每秒密钥生成率为几比特。在误码率为零的条件下,该网络传输速率最高为每秒100Kb。在骨干网端到端的测试中,当距离为6公里时,密钥生成率为每秒500b,距离为10公里时,密钥生成率为每秒100b。各个信道之间的串扰比较严重,距离增加到4.5公里时,系统已不能生成安全密钥[1]。

Table 1. Comparison diagram of quantum network distribution mode

表 1. 量子网络分配方式对比表

名称	采用量子密钥分发手段
美国 DARPA 量子密钥分发网络	光纤信道的相位调制量子密钥分发、光纤信道的纠缠光源量子密钥分发和自由空间量子密钥分发技术
欧洲 SECOQC 量子通信实验网络	“即插即用”量子密钥分发;单向相位编码诱骗态 BB84 协议系统;基于弱相干光的 COW 时间编码量子密钥分发;基于偏振纠缠光子对的系统(ENT);基于高斯调制的相干态,采用 RR 协议的连续变量量子密钥分发系统(CV);短距离自由空间诱骗态 BB84 系统。

Table 2. Quantum network distribution diagram

表 2. 量子网络对比表

名称	经典信道	量子信道	特点
西班牙马德里量子通信网络	1470 nm 和 1510 nm	1550 nm	1.各个信道之间的串扰比较严重 2.该网络能够满足 256 比特 AES 加密的密钥更新速率。
美国国家标准技术局(NIST)量子通信网络	1550 nm	850 nm	1.利用 HI780 纤维具有空间滤波器的功能,用来消除混杂在 1550 nm 纤维中的 850 nm 高模式成分 2.采用编程可控的偏振控制器补偿偏振在光纤中的传输变化

### 3.4. 法国巴黎量子通信网络

SECOQC 项目结束后,夏尔·法布里实验室把 CV QKD 研究成果转移到巴黎高等电信学院的量子信息小组,该组同时成立 SeQureNet 公司。与巴黎高等电信学院的量子信息小组共同推动 CV QKD 的发展。理论方面,该组近年来给出了一系列的 CV QKD 理论安全方面最前沿的证明。实用化领域,该小组提出的多维协商后处理方案以及使用在低信噪比的纠错码已经在 CV QKD 研究领域被广泛使用。

2011 年 SeQureNet 公司使用 CV QKD 设备配合传统 AES 加密设备在实际 20 km 光纤链路上稳定运行长达 6 个月。

2013 年 SeQureNet 公司实现了 80 公里范围内 CV QKD 传输距离的突破。期间,巴黎高等电信学院的量子信息小组还致力于 CV QKD 的研究,诸如 CV QKD 实际设备安全性和经典光网络融合。该小组将继续与巴黎高光所进行合作开展芯片集成和自由空间 CV QKD 的研究。

2014 年法国政府在巴黎创立了巴黎量子计算中心(Paris Center for Quantum Computing,简称 PCQC),将法国国家科研中心(CNRS),巴黎高等电信(Telecom ParisTech),INRIA 巴黎,巴黎六大,巴黎高光所(Institut d'Optique),法国原子能研究署(CEA)等法国顶尖研究机构联系起来,进行量子物理理论,量子通信,量子计算等方面的研究。

2016 年 5 月中旬,欧盟宣布投资 10 亿欧元启动 Quantum Flagship 计划,促进量子通信技术的研发。

### 3.5. 英国量子通信网络

2014 年,英国在 Birmingham, Glasgow, Oxford and York 四所大学设立量子中心用于量子保密通信的研究。同年,英国电信和东芝两家公司于东芝研究实验室,共同在常规光纤通信网络上整合量子保密技术,首次成功地将量子密码学搭载于 10 Gbps 数据传输信号的光纤上传输[4]。

2016 年底,东芝研究实验室发现量子密钥分发以及 100 Gbps 数据亦可融进该光纤。

英国电信与东芝欧洲研发中心亦在合作打造英国量子网络。连接 BT 阿达斯特拉尔科技园和剑桥科技园的线路已于 2017 年上半年完工。

## 4. 日本量子保密通信网络发展

日本政府从 2001 年开始,先后制定了以新一代量子信息通信技术为对象的长期研究战略和量子信息通信技术发展路线图,量子信息被确定为 21 世纪的国家战略项目,日本国家情报通信研究机构(National Institute of Information and Communications Technology, 简称为 NICT)为该项目的主要攻研机构。同年,该机构开始对量子信息通信项目中量子通信基础设施方面的研究。

而后,NICT 建成东京量子密钥分发系统。该系统最远通信距离为 90 公里,最快的节点间通信速率达到了每秒 304 kb,在全网络上可进行视频通话[5]。

2010 年 10 月,日本在 NICT 的 JGN2plus 宽带网络上,开发出了安全性强的以量子保密为原理的多点电视会议系统。该系统用于国家级的保密通信,和重要基础设施的监控和通信,也可实际应用于金融领域的保密通信。

2010 年,日本 NITC 与一些外国量子领域的研究机构合作,正式建成东京 4 节点城域量子通信网络并在该量子网络上开展了绝对安全的视频传输、窃听检测以及二次安全链路的重路由等关键技术的演示[6]。

2011 年 9 月,日本在东京量子密钥分发网络建立了新的试验床环境“JGN-X(JGN-extreme)”。自此日本 NITC 有关量子领域的研究实验进入第三阶段中期。如图 6 所示。

2016 年 3 月,NICT 项目第三阶段完成,开展量子密码网络的实用化应用。

东京量子实验网络由四个节点构成,如图 7 所示,节点之间由商用光纤线缆连接,包括许多接续点

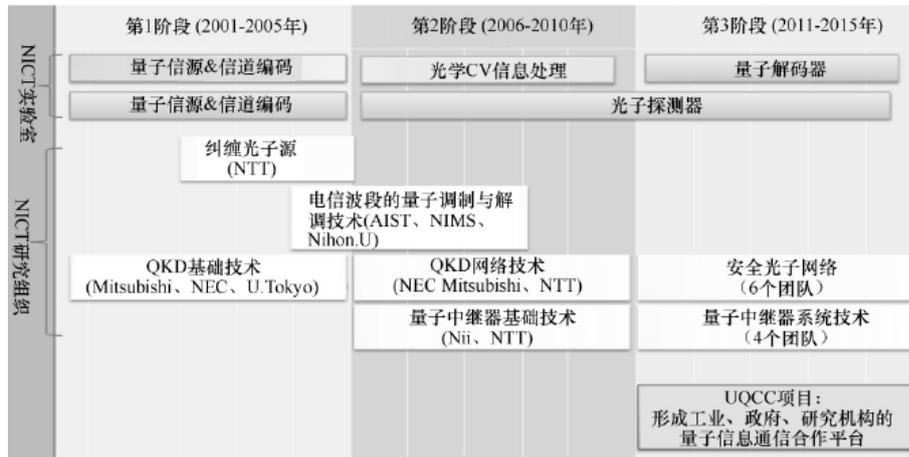


Figure 6. The research route of NICT  
图 6. NICT 研究路线

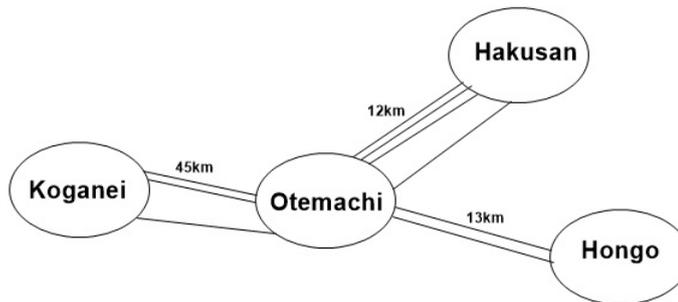


Figure 7. Tokyo quantum key distribution network node geographical distribution  
图 7. 东京量子密钥分发网络节点地理分布

和连接器，特点是网络损耗高且易受环境波动影响。该网络基于可信节点而建，并实验检测了电视会议和移动电话在该网络上的安全性。

东京量子实验网络融合了六套量子密钥分发系统，最远传输距离达到 90 公里，主要采用了包括诱骗态 BB84 协议、BBM92 协议、SARG 协议和差分相位协议在内的四种协议。图 8 为该通信网络的逻辑拓扑结构示意图。该网络采实现了在长达 45 公里的距离内进行安全有效的视频会议[1]。除此之外，该网络还开启了包括一个量子通信手机的应用接口作为创新。

东京量子网络主要在量子密钥分发系统的稳定性、应用平台、小型化装置和长期运行等方面进行了研究，其研究包括了在不同环境下的量子密钥分发系统稳定性技术、供电技术以及系统自动恢复技术等重要项目。该网络还建立了以量子密钥分发网络器件为基础的主动反馈机制，完成了应用平台的安全性保障、特定的身份认证以及长期运行性能的测试。

## 5. 中国量子保密通信网络发展

### 5.1. 北京四节点波长路由量子网络

2007 年，中国科学技术大学的郭光灿院士研究团队发明了基于波分复用器的多波长量子路由器，并基于此路由器建立了全时全通的量子密钥分发网络。随后，该小组又设计出了波长节约型量子路由器，与之前的全时全通型量子路由器相比，可节省一半的波长资源，有效地提高了波长资源的使用效率，降

低了量子密钥分发网络的建设成本。同年，郭光灿院士团队在北京市网通商业光纤上成功实现了 4 用户的城域量子光纤网络(如图 9)。用户之间的距离最短约为 32 公里，最长约 42.6 公里。并在该网络上完成了加密的多媒体通信实验[7]。

### 5.2. 芜湖量子政务网

2009 年，郭光灿院士团队在安徽省芜湖市建成了多层级的“量子政务网”，如图 10 所示，该网络采用了波长节约量子路由器。量子密钥分发网络骨干网四个节点分布在芜湖市科技局、市经委、总工会和电信机房，量子密钥分发子网的三个节点分布在质监局、招商局和电信机房，可信中继设置在电信机房，全时全通量子路由器和程控量子交换机均放在电信机房内该量子网络在同一系统中应用了 3 种组网技术[8]。

通过该网络可以完成任意两点之间的量子保密的通信过程，并可以满足视频保密会议和大量公文保密传输的需求，有很高的安全性。

### 5.3. 合肥三节点和五节点量子电话网络

2008 年，潘建伟院士团队基于诱骗态建立了一个“三节点量子安全通信网络系统”，该系统是以商业光纤网络为基础建成的。在系统的三个节点中，任意两个相邻的节点均由长约 20 公里的商用光纤相连，

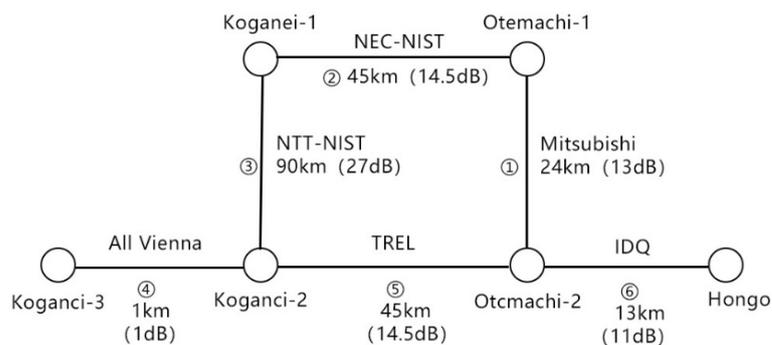


Figure 8. Tokyo quantum key distribution network logic topology  
图 8. 东京量子密钥分发网络逻辑拓扑结构

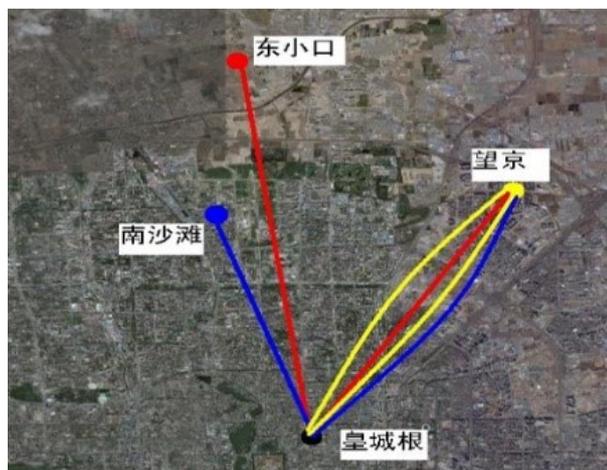


Figure 9. NIST Three-node quantum secure communication network structure  
图 9. NIST 三节点量子保密通信网络结构

实时进行全密钥交换与协议应用[9]。系统所生成的量子密钥在通信中可被立即使用，实现了三节点中任意两个通信节点之间的实时语音保密通信，以及从一个节点至另外两个节点的“一次一密”实时网络对讲。

图 11 为三节点量子电话网的体系结构，两套诱骗态量子密钥分发系统分别安置在滨湖 - 中科大线路与中科大 - 杏林线路上。其中滨湖 - 中科大线路上的最终成钥速率大于每秒 1.6 Kb，误码率约为 1.6%；中科大 - 杏林线路上的最终成钥速率大于每秒 1.5 Kb，误码率约为 1.4%。该系统为世界上首个三节点光量子电话网。

2009 年 9 月，潘建伟院士团队以三节点量子电话网为基础，利用自主研发的光量子程控开关，成功组建了“五节点全通型量子通信网络”。五节点全通型量子通信网络包括四个全通节点以及一个中继附

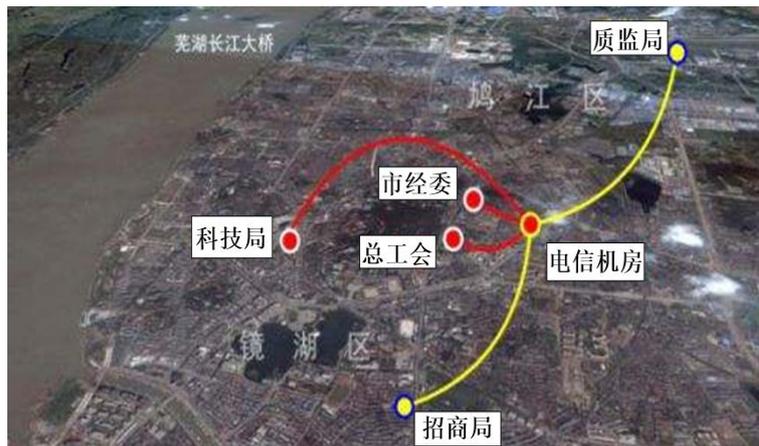


Figure 10. Qiang hu quantum government network  
图 10. 羌胡量子政务网

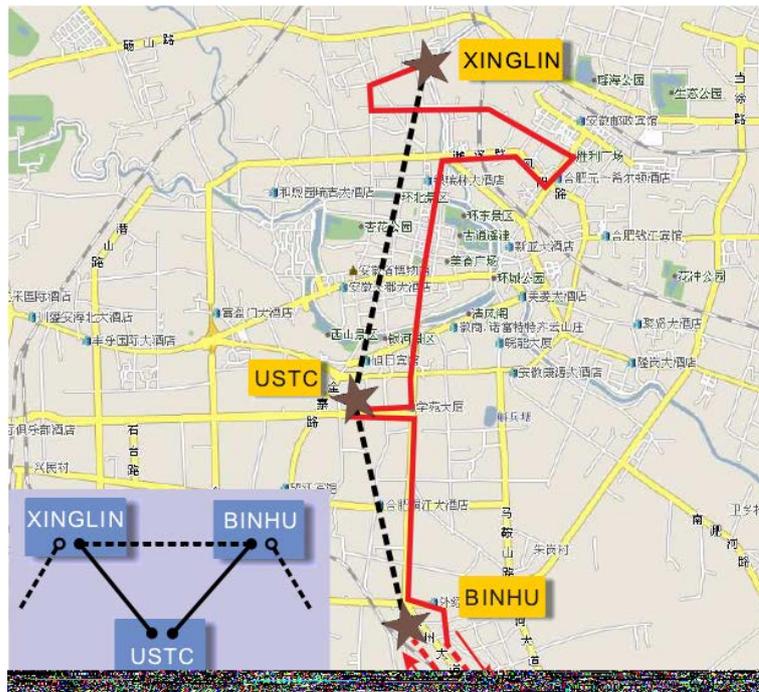


Figure 11. Architecture of three-node quantum telephone network  
图 11. 三节点量子电话网的体系结构

加节点。

中继附加节点位于中科大，四个全通节点分别位于中国科学技术大学、万安、美兰以及肥西。为了将位于中科大的节点模拟为远程独立节点，一条长为 10 公里的环形地下光缆从中科大发出，最终回到中科大。位于肥西县的节点与中科大节点大约相距 60 公里，在该节点移至桐城市后，其与中科大节点相距约 130 公里，最后经过进一步的连接实验，该系统的最终成码速率大于每秒 1.2 Kb，误码率低于 2%，基本上实现了城际量子通信保密。

与三节点量子电话网相比，五节点全通型量子通信网络(如图 12)的实用量子通信系统的有效通信距离与覆盖面积已达到城市范围。

#### 5.4. 合肥 46 节点量子城域网

2012 年 2 月，合肥市的城域量子通信实验示范网成功建成并投入试运行阶段，合肥市成为全国乃至全球首个拥有规模化量子通信网络的城市[10]。2012 年 3 月，46 个节点的城域量子通信网络搭建成功。该网络位于合肥市主城区，使用的光纤总长约 1700 公里，通过了 6 个接入交换和集控站，连接着 40 组“量子电话”用户和 16 组“量子视频”用户。该网络能够提供量子安全下的实时语音通信、实时文本通信以及实时文件传输等功能[11]。

截至 2015 年底，合肥量子城域通信网络通信正确率达到 99.6%，超过了当时的移动通信正确率水平。

#### 5.5. 合肥 - 六安 - 舒城城际量子通信网

2012 年 5 月，潘建伟院士团队实现了合肥 - 六安 - 舒城近 170 千米的城际量子通信。该量子通信网



Figure 12. Architecture of a five-node quantum telephone network

图 12. 五节点量子电话网的体系结构

络使用的是上海微系统所研制的 4 通道 SNSPD 系统,其在 1550 纳米光纤通信波长和 10 赫兹暗技术条件下,系统的量子效率达到 4% [12]。

### 5.6. 量子保密通信“京沪干线”

“京沪干线”项目于 2014 年 1 月被正式提上日程,项目计划连接山东“济南量子通信试验网”和安徽“合肥城域量子通信试验示范网络”,从而建成连接北京到上海总长 2000 余公里的国际首个广域光纤量子保密通信网络并进行安全性测评 2016 年底,“京沪干线”完成全线贯通和星地一体化对接。2017 年 8 月底,完成了全网技术验收。2017 年 9 月,“京沪干线”正式开通,如图 13 所示。

目前,“京沪干线”全线路密钥率大于 20 kbps。量子卫星兴隆地面站到北京接入站点全线密钥率大于 5 kbps,运行效果良好[13]。

中国京沪干线与美国的量子保密干线不相同,这尤其体现在中继器的选取上。如表 3。

### 5.7. 洲际量子保密通信

2017 年 9 月,中国“墨子号”量子卫星与奥地利地面站的卫星进行了量子通信。中国通过“京沪干线”北京中继接入点,实现了北京、上海、济南、合肥、乌鲁木齐南山地面站和奥地利科学院 6 点间的洲际量子通信视频会议与地理地面站的量子通信,这是世界上第一次洲际量子通信。

## 6. 总结与展望

目前,量子保密技术正在稳步发展,量子通信技术的实用化进程正在加快。2018 年,《物理学报》刊载介绍了基于光量子态避错及容错传输的量子通信,《电信科学》刊载提出了量子保密通信的国产密

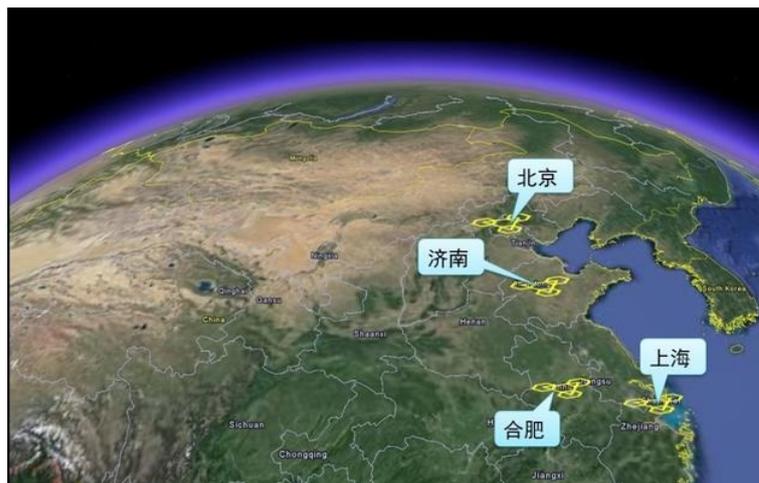


Figure 13. Schematic diagram of “Beijing-Shanghai line” quantum communication network

图 13. “京沪干线”量子通信网络示意图

Table 3. Comparison table of Beijing-Shanghai line and American quantum secret line

表 3. 京沪干线与美国量子保密干线对比表

	开通年份	总长度	中继器	全线密钥率	起止点
中国京沪干线	2017	大约 2000 km	可信中继	>20 kb/s	北京 - 上海
美国 NASA 量子保密干线	2012	550 km	量子中继	-	洛杉矶 - 杰尼维尔

码服务云平台建设思路；《海洋科学》刊载介绍了量子无线通信技术在海洋环境监测中的应用。可见，量子通信技术已经成为当今时代的重要攻研领域，不得不引起世界各国的重视。

通过对量子保密通信网络和各国量子信息技术发展计划分析总结，可以预见，未来量子通信网络的发展大致有如下特点：

- 1) 以目前普遍应用的光纤网络为基础，创建可拓展的量子通信通道；
- 2) 将支持多种通信协议兼容，多种量子网络形式共同发展；
- 3) 将更加注重于量子通信的实际层面的研究，例如量子通信在金融，政务领域的应用；
- 4) 向移动通信领域发展，比如量子保密通信手机；
- 5) 逐步建立起连接多个城域网的量子城际网络和基于卫星的全球量子通信网络，例如中国的“京沪干线”的创建模式。

量子保密通信技术作为保障未来信息社会通信安全的关键技术，在商业领域，国防建设，军事保障领域等方面都极具战略意义。量子保密通信技术多领域，多层次的发展特征越来越突出，未来，量子保密通信更将成为连接电子，通信技术，计算机科学，应用物理学等学科的关键中介点。不论是对于学科理论发展还是现实科技建设，都具有重要意义。

## 基金项目

国家自然科学基金项目(U1204602)，数学工程与先进计算国家重点实验室开放课题项目(2013A14)。

## 参考文献

- [1] 许华醒. 量子通信网络发展概述[N]. 中国电子科学研究院学报, 2014-6(3).
- [2] Butler, W.T., Hughes, R.J., Lamoreaux, S.K., *et al.* (2000) Daylight Quantum Key Distribution over 1.6 km. *Physical Review Letters*, **84**, 652-655. <https://doi.org/10.1103/PhysRevLett.84.5652>
- [3] The Home Page of the Integrated Project SECOQC, Sixth Framework Program of the European Union [EB/OL]. <http://www.secoqc.net/index.html>
- [4] 魏慧. 英国电信携手东芝揭幕全英首家量子保密展示厅[EB/OL]. 2016-10-17.
- [5] 周静, 张睿纳, 雷煜卿, 卢利峰, 卢锟. 日本量子信息通信技术研究现状及发展趋势[C]// 中国电力科学研究院. 2012年电力通信管理暨智能电网通信技术论坛论文集: 2012年卷. 北京: 人民邮电出版社, 2012.
- [6] 宋向东. 量子加密视频通信系统日本问世[EB/OL]. 2012-04-08.
- [7] 中国科学院量子信息重点实验室. 我国第一个量子密码网络系统在北京测试运行实现四端口量子密钥分发网络[EB/OL]. <http://lqcc.ustc.edu.cn/news/?article=43>, 2007-04-02.
- [8] 刘军. 世界首个绝对安全的政务网在安徽芜湖建成开通[EB/OL]. 2009-05-18.
- [9] Chen, T.-Y., Yang, L., Pan, J.-W., *et al.* (2009) Field Test of a Practical Secure Communication Network with Decoy-State Quantum Cryptography. <http://arxiv.org/abs/0810.1264>
- [10] 蒋瑜香. 合肥城域量子通信网络正式开通[EB/OL]. 2012-03-31.
- [11] 喻思奕. 潘建伟团队建世界首个城域量子通信网节点 46 个[EB/OL]. 2014-03-14.
- [12] 上海微系统与信息技术研究所. 上海微系统所超导单光子探测技术成功用于城际量子通信网[EB/OL]. 2012-06-14.
- [13] 董瑞丰, 徐海涛. 我国开通全球首条量子通信干线成功实现首次洲际量子通信[EB/OL]. 2017-09-29.

**知网检索的两种方式：**

1. 打开知网页面 <http://kns.cnki.net/kns/brief/result.aspx?dbPrefix=WWJD>  
下拉列表框选择：[ISSN]，输入期刊 ISSN：2161-8801，即可查询
2. 打开知网首页 <http://cnki.net/>  
左侧“国际文献总库”进入，输入文章标题，即可查询

投稿请点击：<http://www.hanspub.org/Submission.aspx>

期刊邮箱：[csa@hanspub.org](mailto:csa@hanspub.org)