世界各国竞相研发量子通信

古丽萍

（合肥市科技情报研究所，合肥 230061）

摘　要：随着电子信息技术的迅猛发展，安全高效的信息传输日益受到人们的关注。量子通信作为当今通信领域的新宠，以其绝对安全性、超大信通容量、超高通信速率、远距离传输和信息高效率等特点，引起了国际范围的广泛关注。本文概述了量子通信及其特点和应用，追溯了量子通信起源，介绍了美国、日本、欧洲等国的量子通信研究与发展状况，展望了量子通信发展前景。

关键词：量子通信；量子纠缠；安全通信；量子信息时代

中图分类号：TN929.1　**文献标识码**：A　**DOI**：10.3772/j.issn.1009-8623.2011.12.002

21世纪，随着电子信息技术的迅猛发展，高效安全的信息传输日益受到人们的关注，世界各国不惜耗巨资，全力进行通信安全方面的研发工作。以量子效应为基础的量子通信以其绝对安全性、超大信道容量、超高通信速率、远距离传输和信息高效率等特点，备受全球科学界关注，成为国际上量子物理和信息科学的研究热点，量子通信极可能引发军事领域继微电子技术之后的又一次重大革命。

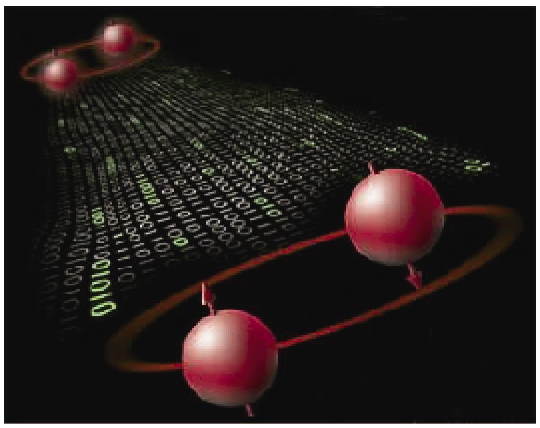

图1　量子通信模拟图

一、量子通信及其特点

量子通信（quantum communication）是利用量子纠缠（quantum entanglement）效应进行信息传递的一种新型的通信方式（图1）。从物理学的角度，量子是不可分的最小的能量单位。在量子力学中，这种微观粒子的运动状态，称为量子态。量子纠缠是指微观世界里，有共同来源的两个微观粒子之间存在着纠缠关系，两个处于纠缠状态的粒子无论相距多远，都能“感应”对方状态。

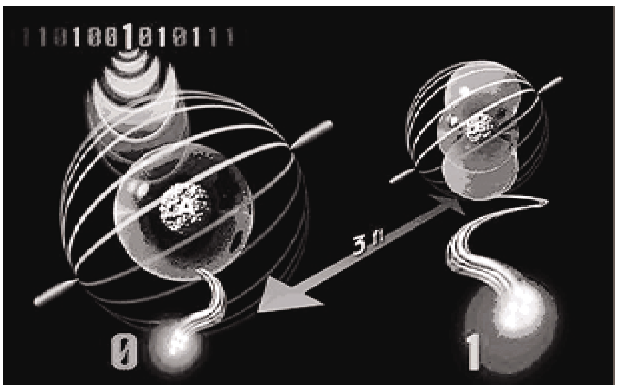

图2　量子通信示意图

量子通信是在物理极限下，利用量子效应实现的高性能通信方式，主要涉及量子密码通信、量子远程传态和量子密集编码等（图2）。量子通信系统的基本部件包括量子态发生器、量子通道和量子测

作者简介：古丽萍（1962-），女，合肥市科技情报研究所 研究员；研究方向：科技情报研究。

收稿日期：2011年9月15日

量装置。量子通信是经典信息论和量子力学相结合的一门新兴交叉学科，按其所传输的信息是经典还是量子而分为两类，前者主要用于量子密钥的传输，后者则可用于量子隐形传态和量子纠缠的分发。

量子通信在通信安全性、计算能力、信息传输通道容量、测量精度等方面突破经典技术极限，与目前成熟的传统通信技术相比，具有绝对安全性、超大信道容量、超高通信速率、远距离传输和信息高效率等特点。

量子通信网络包括传输平面(图3)、控制平面和管理平面。传输平面主要由光传输链路和量子交换模块组成，传输链路包括光纤、分束器、光复用器和解复用器等设备。控制平面是量子通信网络的核心部分，主要功能包括：信令传输、呼叫连接控制、链路资源管理、路由管理、用户接口等。管理平面由量子通信网络各个节点的管理层组成，实现管理功能分布化。当两个用户需要进行通信时，管理平面向控制平面发送通信请求消息，控制平面根据通信需求和传输平面的拓扑信息等寻找路由，并将控制消息传送给传输平面，在通信双方之间建立端到端的物理连接。在通信安全性方面，量子通信技术的信息安全基于量子密码学，以量子状态作为密钥突破了传统加密方法的束缚，具有不可窃听、不可复制性和理论上的“无条件安全性”。任何截获或测试量子密钥的操作，都会改变量子状态，量子通信确保两地之间密匙分配和通信的绝对安全性，是安全保密通信。量子通信所提供的密钥无法被破解，对于信息的加密不再是依靠传统加密技术所依赖的复杂算法，而是靠物理法则来保证，被认为是保障通信安全的终极技术手段。在信息传输通道方面，量子信息传递过程不为任何障碍所阻隔，线路时延可以为零，从而实现最快通信，且不存在任何电磁辐射污染，通信完全环保。在通信远距离方面，量子通信是远距离通信，量子隐形传态过程中穿越大气层的可能性，为未来基于卫星量子中继的全球化量子通信网奠定了可靠基础。

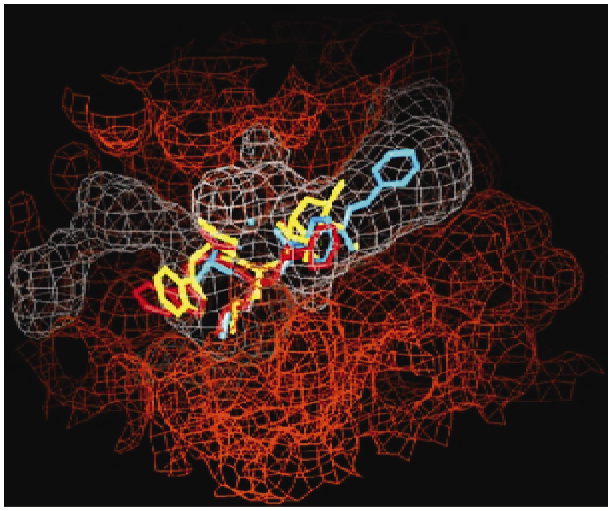

图3　量子通信网络模拟图

二、量子通信主要应用领域

量子通信在军事、国防、金融等信息安全领域有着重大的应用价值和前景，不仅可用于军事、国防等领域的国家级保密通信，还可用于涉及秘密数据、票据的政府、电信、证券、保险、银行、工商、地税、财政等领域和部门。在国防和军事领域，量子通信能够应用于通信密钥生成与分发系统，向未来战场覆盖区域内任意两个用户分发量子密钥，构成作战区域内机动的安全军事通信网络；能够应用于信息对抗，改进军用光网信息传输保密性，提高信息保护和信息对抗能力；能够应用于深海安全通信，为远洋深海安全通信开辟了崭新途径；利用量子隐形传态以及量子通信绝对安全性、超大信道容量、超高通信速率、远距离传输和信息高效率等特点，建立满足军事特殊需求的军事信息网络，为国防和军事赢得先机。在国民经济领域和部门，量子通信可用于金融机构的隐匿通信等工程以及对电网、煤气管网和自来水管网等重要基础设施的监视和通信保障，促进国民经济的发展。

三、量子通信起源

首先想到将量子物理用于密码术的是美国科学家威斯纳(S. Wiesner)。1970年，威斯纳提出可利用单量子态制造不可伪造的“电子钞票”。但这个设想的实现需要长时间保存单量子态，不太现实。在同他的讨论中，贝内特(C.C.Bennett)和布拉萨德(G. Brassard)受到启发，想到单量子态虽不好保存但可用于传输信息。1982年，法国物理学家艾伦·爱斯派克特(Alain Aspect)和他的小组成功地完成了一项实验，证实了微观粒子量子纠缠现象确实存在。1984年，贝内特和布拉萨德提出了第一个量子密码

术方案,称为 BB84 协议,由此迎来了量子密码术新时期。1989 年,量子密钥传输的演示实验首次获得成功。实验中,光子在自由空间传播 32 厘米,误码率为 4%,安全程度非常高,显示了量子密钥分发潜力。1991 年,埃克特(A.K.Ekert)提出用双量子纠缠态实现量子密码术,称为 EPR 协议。1992 年,贝内特提出一种更简单,但效率减半的方案,即 B92 协议。1993 年,贝内特提出量子通信的概念,6 位来自不同国家的科学家,提出利用经典与量子相结合方法实现量子隐形传态的方案。

四、世界各国竞相研发量子通信

量子通信近来已逐步从理论走向实验,并向实用化发展,世界各国政府、国防部门、科技界和信息产业界高度重视,量子通信技术已成为当今世界发达国家激烈竞争的焦点和热点。量子通信与国家安全紧密相连,美国、日本、欧洲等国均投入大量人力物力致力于量子通信的研究,积极推广应用量子通信技术。全球信息产业界国际巨头 IBM、Philips、AT&T、Bell 实验室、HP、西门子、NEC、日立、三菱、NTT 等对量子通信技术投入大量研发资本,开展量子通信技术的研发和产业化。

在美国,量子信息被列为“保持国家竞争力”计划的重点支持课题,美国国家标准和技术研究所(NIST)将量子信息作为三个重点研究方向之一。美国加州理工大学、麻省理工学院和南加州大学联合成立了量子信息和计算研究所,美国量子信息和计算研究所为美国军队研究部门所管理,隶属于美国国防部高级研究计划司超大规模计算工程。

1994 年,美国国防高级研究计划局致力于用 3~5 年的时间推进量子通信技术方面的研究,美军实施了“以不加外力传输的方式向战场和全球传输报文能力”的量子通信计划。1999 年,美国洛斯阿拉莫斯国家实验室量子信息小组实现 500 米的自由空间传输。2002 年,美国全国科学基金会投资 5000 万美元对量子通信进行研究。2003 年,美国国防部高级研究计划署领衔建设了 DARPA 量子通信技术试验网络。2004 年 6 月,美国马萨诸塞州剑桥城正式投入运行世界上第一个量子密码通信网络,主要通过普通光纤来传输采用量子密码术加密的数据,网络传输距离约为 10 千米。系统连接六个网络节点,涵盖剑桥城的哈佛大学、波士顿大学,以及 BBN 科技公司。2006 年,美国洛斯阿拉莫斯国家实验室实现了诱骗态方案,同时实现了超过 100 千米的量子保密通信实验。2007 年 9 月,美国科学家的一项研究,让相距一米的离子阱中的两个独立原子实现了量子纠缠和远距量子通信。2009 年,美国信息科学白皮书中要求各科研机构协调开展量子信息技术研究。2009 年,美国 DARPA 建成城域量子通信演示网。2009 年 8 月,美国麻省理工学院科学家在冷原子中量子存储和波动研究领域有了新突破,这方面的技术正是设计量子信息网络的关键,这使研究向未来广域量子通信网络的最终实现又迈出重要一步。

2010 年 10 月,美国国家标准和技术研究院(NIST)表示,科学家首次将量子源(半导体量子点)产出的波长为 1300 纳米的近红外单光子转换成波长为 710 纳米的近可见光光子。这种单光子波长(或颜色)转换的实现有望帮助开发出拥有量子通信、量子计算和量子计量的混合型量子系统。洛斯阿拉莫斯国家实验室正在研究量子局域网的密码体系和自由空间量子密码,美国白宫和五角大楼安装了量子通信系统,并已投入使用。2011 年 8 月,美国国家标准与技术研究院的物理学家使用单个铍离子量子位(qubit)进行简单的量子逻辑操作,通过改进试验方法,获得了单量子位处理量子信息的最低出错率,满足了科学家建立实用量子计算机的理论要求。

日本提出以新一代量子信息通信技术为对象的长期研究战略,计划在 2020-2030 年间,建成绝对安全保密的高速量子信息通信网,以实现通信技术质的飞跃,日本邮政省把量子通信作为 21 世纪的战略项目,制订了十年的中长期研究目标。

2000 年,日本邮政省将量子通信技术作为一项国家级高技术列入开发计划,10 年内投资 400 多亿日元,主要研究光量子密码及光量子信息传输技术。2002 年,日本 NTT 公司研发出差动移相量子密钥发送协议,并应用在试运行网络上。2004 年 6 月,日本研究人员用防盗量子密码技术传送信息获得成功,其传递距离长度可达 87 千米。2005 年 3 月,日本 NEC 开发出了一种即使气温与光纤长度等通信环境发生变化,其性能也不会下降的量子加密通

信系统。2005 年 4 月,日本松下电器产业和日本玉川大学利用光的量子扰动 (quantum fluctuation)现象,试制出防窃听性能更高的光通信系统。此次试制的系统属于量子加密通信的一种,传输速度高达 1 吉比特/秒,传输距离为 20 千米。2005 年 6 月,日本 NTT 公司成功完成单光子的量子保密通信试验,试验利用了 NTT 和斯坦佛大学合作开发的量子保密通信协议,通过 NTT 开发出的光交换机来控制光子流量,试验结果表明量子保密有望应用到光纤网络中。2007 年 1 月,日本一研究小组开发的量子密钥技术在现实条件下实现了信息经光纤的安全传输。2008 年 10 月,日本东芝公司研究人员在量子密码通信中,将密钥的传输速度成功提高,分别在 20 千米和 100 千米实验场合达到每秒 1.02 兆比特和每秒 10.1 千比特。2009 年 4 月,日本日立公司基础技术研究所和东京大学荒川泰彦教授领导的纳米量子信息电子技术研究所共同开发出利用下一代高速大容量光通信的"相位调制技术"。

2010 年 10 月, 日本独立行政法人信息通信研究机构(NICT)的量子 ICT 集团,受 NICT 的委托,与日本电气株式会社(NEC)、三菱电机株式会社(三菱电机)、日本电信电话株式会社(NTT),共同在 NICT 的 JGN2plus 超高速宽带网络上,采用量子密码技术开发出了不能窃密的多点电视会议系统,并开始试运行。2011 年 1 月,日本信息通信研究机构的 ICT 集团将量子密码技术应用于电视会议系统,实现了每秒 10 万比特的世界上最快的密钥生成速度。

欧盟在其"欧洲研究与发展框架规划"中提出用于发展量子信息技术的 "欧洲量子科学技术"计划以及《欧洲量子信息处理与通信》计划,欧洲成立了包括英国、法国、德国、意大利、奥地利和西班牙等国在内的量子信息物理学研究网,这是继欧洲核子中心和航天技术国际合作之后,又一针对科技重大问题的大规模国际合作, 主要研究量子通信、量子计算和量子信息科学。

1993 年,英国国防研究部在光纤中实现了基于 BB84 协议的相位编码量子密钥分发, 光纤传输长度为 10 千米。1993 年, 瑞士日内瓦大学用基于 BB84 协议的偏振编码方案,在 1.1 千米长的光纤中传输 1.3 微米波长的光子, 误码率为 0.54%。1995 年,一对三的网络量子密码通信演示实验,其发送、接收方距离为 5.4 千米, 传送比特率 1 千位/秒,误码率为 3%。1995 年,瑞士日内瓦大学在日内瓦湖底铺设的 23 千米长民用光通信光缆中进行了实地表演,误码率为 3.4%。1995 年,英国成功实现 30 千米长的光纤传输中量子密钥分发。1997 年,瑞士日内瓦大学利用法拉第镜消除了光纤中的双折射等影响因素,使得系统的稳定性和使用的方便性大大提高,被称为"即插即用"的量子密码方案。1997 年 12 月, 中国潘建伟与奥地利物理学家安东尼·赛林格等合作, 首次实现了 "量子态的隐形传输"。 1999 年, 欧盟集中国际力量致力于量子通信的研究,研究项目多达 12 个。1999 年,瑞典和日本合作,在光纤中也成功地进行了 40 千米的量子密码通信实验。2001 年,中国段路明及其奥地利、美国的合作者共同提出基于原子系综的另一类量子中继器方案。2002 年,德国慕尼黑大学和英国军方下属的研究机构合作,在德国和奥地利边境相距 23.4 千米的楚格峰和卡尔文德尔峰之间用激光成功传输了光子密钥。2003 年,瑞士日内瓦 idQuantique 公司和美国纽约神奇量子科技公司发布可以传送量子密钥的商品。2004 年秋,日内瓦因特网服务供给商 Deckpoint 与 idQuantique 共同展示的网络,可以将日内瓦内的好几个服务器数据备份到 10 千米外的站台, 并通过量子加密网络,频繁地发送新密钥。2004 年,奥地利蔡林格研究小组利用多瑙河底的光纤信道,将量子隐形传态距离提高到 600 米。2006 年,欧洲慕尼黑大学-维也纳大学联合研究小组实现了诱骗态方案, 同时实现了超过 100 千米的量子保密通信实验。2007 年 6 月,由奥地利、英国、德国研究人员组成的小组在量子通信研究中通过了通信距离达 144 千米的最远纪录。

2008 年 3 月,意大利和奥地利科学家小组首次识别出从地球上空 1500 千米处的人造卫星上反弹回地球的单批光子,实现了太空绝密传输量子信息的重大突破(图 4)。这一突破表明在太空和地球之间可以构建安全的量子通道来传输信息,用于全球通信。2008 年 9 月,欧盟发布了关于量子密码的商业白皮书,启动量子通信技术标准化研究,联合来自 12 个欧盟国家的 41 个最优秀的量子信息研究组成立了"基于密码的安全通信"工程。2011 年 5 月,德国马克斯普朗克量子光学研究所的科学家格

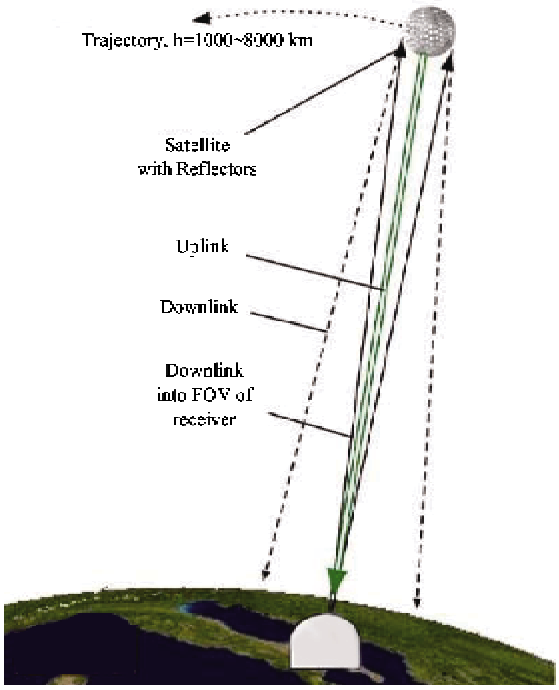

图 4　通过卫星实现量子通信示意图

哈德·瑞普领导的科研小组，成功地实现了用单原子存储量子信息，将单个光子的量子状态写入一个铷原子中，经过 180 微秒后将其读出，助力科学家设计出功能强大的量子计算机。2011 年 7 月，英国科学家研究证明，量子点和经典数据流能在传统的光纤网络内交织在一起，意味着量子密钥分配(QKD)能与传统的数据通道一起工作，为量子互联网建成铺平了道路。

五、量子通信前景展望

目前，量子通信的理论框架已经基本形成，理论体系日趋完善，量子通信技术已具备实用化和产业化的能力，成为世界主要发达国家优先发展的战略性科技。随着量子通信理论研究和量子通信实践应用的不断突破，量子通信产业化为期不远，市场前景不可估量。量子信息和量子通信研究具有广阔的应用前景，如今量子通信和量子计算潜在的重要科学价值和应用价值正在引领科学家研发未来的量子计算机，量子通信已成为 21 世纪通信与信息领域发展的方向和主流。科学家预计 10 年内有望实现全球化量子通信，量子通信技术在二三十年后将对人类社会发展产生难以估量的影响，量子通信将改变未来信息产业领域的发展格局，成为引领未来科技发展的重要领域，催生量子信息时代的来临。■

参考文献：

[1] 徐启建，金鑫，徐晓帆.量子通信技术发展现状及应用前景分析[J].中国电子科学研究院学报，2009，4(5)：491–497.

[2] 孙献平，罗军，詹明生. 自由空间量子通信实验研究与进展[J]. 自然科学进展，2006，16(2)：169–176.

[3] 陈彦，胡渝. 空间量子通信技术[J]. 光子技术，2006，2(1)：35–40.

[4] 刘晓慧，聂敏，裴昌幸. 基于 ASON 的量子通信网络构建和量子交换机设计[J]. 电信科学，2011，27(4)：49–53.

[5] Chen P X, Zhu S Y, Guo G C. General form of genuine multipartite entanglement quantum channels for teleportation. Phys Rev A, 2006, 74:032324.

[6] Cao Z L, Song W. Teleportation of a two-particle entangled state via W class states. Physica A, 2005, 347: 177–183.

[7] Cao H J, Song H S. Quantum secure communication scheme with W state. Chin Phys Lett, 2006, 23:290–292.

[8] Filips R, Fiurasek J, Marek P. Reversibility of Continuous-variable Quantum Cloning. Phys Rev Lett, 2004, 92:047901.

Many Countries Compete to Research and Develop Quantum Communication

GU Liping

(Institute of Scientific and Technical Information of Hefei, Hefei 230061)

Abstract: With the rocketing development of electronic information technology, secure and efficient communication has attracted increasing attention. As a new hotspot in present communication field, quantum communication has been causing extensive concern in the world by absolute security, large ICT capacity, ultra-high communication rate, long distance transmission and high information efficiency. The paper outlines the characteristics and applications of quantum communication, and traces its origin, introduces the situation of research and development of quantum communication in America, Japan and Europe, and makes prospects for the future of the quantum communication in the world.

Key words: quantum communication; quantum entanglement; secure communication; the quantum information age