“十二五”重点图书

研究生系列教材

量子通信

Quantum Communication

朱畅华 聂敏 阎毅 权东晓 编著

西安电子科技大学出版社
http://www.xduph.com

f 研究生系列教材

量子通信

裴昌幸　朱畅华
聂敏　阎毅　权东晓　编著

安徽大学图书馆
藏书
www.lib.ahu.edu.cn

西安电子科技大学出版社

内容简介

本书较为系统、全面地介绍了量子通信的概念、物理基础、具体形式、量子信道与编码及量子通信网等。全书共分8章，第1～3章重点讨论量子通信的基本概念、物理基础及量子隐形传态；第4～5章重点讨论量子密钥分发和量子安全直接通信；第6～8章重点讨论量子信道、量子编码和量子通信网络。本书具有文笔简练、内容深入浅出、说理透彻、结构合理、特色鲜明的优点。

本书可作为通信工程、电子与信息工程、信息工程、信息安全等专业高年级本科生或研究生教材，也可作为相关科技人员的学习参考书。

图书在版编目(CIP)数据

量子通信/裴昌幸等编著. —西安：西安电子科技大学出版社，2013.6
研究生系列教材
ISBN 978-7-5606-3048-9

Ⅰ. ① 量… Ⅱ. ① 裴… Ⅲ. ① 量子力学—光通信—研究生—教材 Ⅳ. ① TN929.1

中国版本图书馆 CIP 数据核字(2013)第 091701 号

策　　划　李惠萍
责任编辑　李惠萍
出版发行　西安电子科技大学出版社(西安市太白南路2号)
电　　话　(029)88242885　88201467　　邮　　编　710071
网　　址　www.xduph.com　　电子邮箱　xdupfxb001@163.com
经　　销　新华书店
印刷单位　陕西华沐印刷科技有限责任公司
版　　次　2013年6月第1版　2013年6月第1次印刷
开　　本　787毫米×960毫米　1/16　印　张　13
字　　数　227千字
印　　数　1～3000册
定　　价　23.00元
ISBN 978-7-5606-3048-9/TN

XDUP 3340001-1

＊＊＊**如有印装问题可调换**＊＊＊

“十二五”重点图书　　研究生系列教材

编审委员会名单

主　任　郝　跃

副主任　姬红兵

委　员　（按姓氏笔画排序）

马建峰　卢朝阳　刘三阳　刘宏伟

庄奕琪　李志武　张海林　武　波

郭宝龙　高新波　龚书喜　焦李成

曾晓东　廖桂生

前　言

量子通信是量子力学和通信理论相结合产生的交叉学科，诞生近30年来，已经从理论构想向实用化过渡。量子通信技术所具有的高速、超大容量和无条件安全使其具有无与伦比的发展潜力和应用前景，已引起学术界、企业界和国防部门的高度重视，成为当前研究和开发的热点。

量子通信的主要形式包括基于量子密钥分发(Quantum Key Distribution，QKD)的量子保密通信、量子密集编码(Quantum Dense Coding)和量子隐形传态(Quantum Teleportation)等。量子密钥分发建立在量子力学的基本原理之上，应用量子力学的海森堡不确定性原理和量子态不可克隆定理，在收发双方之间建立一串共享的密钥，通过一次一密(One-Time-Pad，OTP)的加密策略，实现了真正意义上的无条件安全通信；量子密集编码利用在收发双方之间事先共享的纠缠光子对，只需传输一个量子比特就等效于传输2比特的经典信息；量子隐形传态是间接的量子态传输方式，它基于非定域性(Non Local)，利用收发双方事先共享的EPR粒子对具有的量子关联特性建立量子信道，可以实现未知量子态的远程传输。

基于量子叠加态理论，可以用量子叠加的方式来处理信息，一个N量子比特的存储器，可存储的数字高达2^N个，实施一次量子运算就可同时对2^N个输入数进行数学运算。采用Shor算法可以在几分之一秒内实现1000位数的因式分解，这将使现有的公钥RSA体系无密可保！量子特性在提高运算速度和增大信息容量等方面可能突破现有经典信息系统的极限！

不少发达国家在银行、国防部门都已经建立了实用化的短距离光纤量子通信系统。美国国防部已建成了全球第一个量子通信网络

此为试读，需要完整PDF请访问：www.ertongbook.com

(the DARPA Quantum Network)，进一步的计划是通过卫星建立全球量子通信网络。日本把量子通信技术作为一项国家级高技术研究开发计划，在10年内将投资约400亿日元研究密码技术及量子通信所需要的超高速计算机。其目标是，在2020到2030年期间使量子通信网络技术达到实用化水平。

量子通信中所采用的源主要有单光子源和纠缠光子源；通信信道主要包括光纤信道和自由空间信道；信息编码方式有偏振编码和相位编码等多种方式。自从IBM实验室的Bennett等人在1989年完成量子通信的第一个演示性实验以后，国际上采用弱相干光源(准单光子源)方案建立的光纤量子信道传输距离已经达到了250 km，自由空间量子信道也达到了144 km。

量子通信的实现方案目前大多以光子作为载体，这是因为光子和环境相互作用所产生的退相干(decoherence)容易控制，而且还可以利用传统光通信的相关器件和技术。这也是量子通信最先使用光子的主要原因。基于光纤的量子密钥分发设备已经商用化，但由于单模光纤存在着双折射、损耗和背景噪声，加之探测器技术、单光子源或者纠缠光源不完美等原因限制了光纤信道的通信距离。为了解决长距离光纤量子通信中光子损耗以及双折射引起的退相干效应带来的最大距离限制，采用量子中继器(quantum repeater)和自由空间量子通信是两种比较可行的方案。量子中继器目前离实用还有一定距离，而基于人造卫星的自由空间量子通信却表现出极大的可行性。目前，自由空间量子隐形传态已达到143 km，为实现覆盖全球的量子通信奠定了基础。

量子通信，首要问题是如何把消息变换成量子信息比特，依靠量子态作为信息的载体传输量子信息。量子信息的有效表示方法则是量子信源编码研究的中心问题。此外，量子系统不可能是完全孤立的，它必然要与环境相互作用，这里的环境指与所关心系统有相互作用的其它自由度。量子系统与环境的相互作用，一方面会改变量子比特对应的叠加态中的相对相位，使相对相位趋于无规则化，出现相位

错误；另一方面会使信号能量降低，导致比特翻转错误，以及相位-比特联合错误。这两方面综合即可导致退相干过程，从而产生量子码误码。采用量子纠错编码(Quantum Error Correct Coding，QECC)技术能够克服退相干以纠正信道中的误码。

量子通信及相关的理论、技术和应用发展极快。及时反映量子通信的发展动态，将相关理论和技术进行归纳、整理和提升，不论对于教学、科研还是对于促进量子信息技术发展都是十分必要的。本书正是出于这一目的，并在充分考虑了实际需要的基础上编著的。本书的出版体现着我们多年的科研实践和理论研究成果，书中突出了量子密钥分发、量子信道、量子编码、量子直传及量子通信网络等内容，对其原理及相关技术进行了较为系统与完整的分析和论述。

本书共分8章。第1章为概述，主要讲述量子通信的基本概念、性能指标、发展现状及展望；第2章主要讲述量子通信的物理基础，包括量子力学的基本假设、量子密度算子、量子纠缠和量子比特的概念及特性；第3章主要讲述量子隐形传态，包括量子隐形传态原理和多量子比特的隐形传态；第4章主要讲述量子密钥分发，包括BB84协议、B92协议、E91协议，以及诱骗态量子密钥分发的原理与实现；第5章主要讲述量子安全直接通信的相关协议与实现；第6章主要讲述量子信道，包括量子信道的表示、特定量子信道模型、光纤量子信道和自由空间量子信道；第7章主要讲述量子编码，包括量子信源编码和量子信道编码；第8章主要讲述量子通信网络，包括量子通信网络的体系结构、拓扑、量子交换技术、量子中继器和实验网。

本书由裴昌幸统稿，朱畅华、聂敏、阎毅、权东晓参编。编写过程中得到了李建东教授等学者的关注和指导，他们为本书的出版提出了许多宝贵意见；西安电子科技大学量子通信研究中心白宝明、李晖、陈南、易运晖、何先灯、赵楠等老师都非常关心本书的编写，并给予帮助；研究中心的博士、硕士研究生们为本书的资料收集、实验、绘图、文字校对等做出了积极的贡献；书末给出的参考文献，凝聚着原作者的真知灼见，编著者从中汲取了不少营养。在此一并表示

诚挚的感谢！

由于量子通信是一个比较新的领域，很多问题还在不断地深入与探讨之中，加之编著者水平有限，书中难免会有疏漏和不妥之处，敬请广大读者批评指正。

编著者

2013 年 4 月于西安

目　录

此为试读,需要完整PDF请访问: www.ertongbook.com

第1章 概 述

通信的目的是将信息从一个地方(信源)传送到另外一个地方(信宿),信息可装在信封里由邮递员送达,也可通过电信系统实现。电信系统是指将信息承载到电磁波上进行传输,电磁波可以是波长从几千千米到几纳米的无线电波、微波、红外线、可见光、紫外线等。其传输路径可以是自由空间,也可以是电缆或光缆等有线载体。量子通信利用量子力学的基本原理或特性进行通信,其信息的载体是微观粒子,如单个光子、原子或自旋电子等。因此,它的工作原理、发送装置和接收设备必定与其它通信方式不同。本章主要讲述量子通信的基本概念、量子通信的类型,并简要介绍量子通信的发展现状。

1.1 量子通信的基本概念和类型

量子通信起源于对通信保密的要求。通信安全自古以来一直受到人们的重视,特别是在军事领域。当今社会,随着信息化程度的不断提高,如互联网、即时通信和电子商务等应用,都涉及到信息安全,信息安全又关系到每个人的切身利益。对信息进行加密是保证信息安全的重要方法之一。G. Vernam 在 1917 年提出一次一密(One Time Pad, OTP)的思想[1],对于明文采用一串与其等长的随机数进行加密(相异或),接收方用同样的随机数进行解密(再次异或)。这里的随机数称为密钥,其真正随机且只用一次。OTP 协议已经被证明是安全的[2],但关键是要有足够长的密钥,必须实现在不安全的信道(存在窃听)中无条件地安全地分发密钥,这在经典领域很难做到。后来,出现了公钥密码体制,如著名的 RSA 协议[3]。在这类协议中,接收方有一个公钥和一个私钥,接收方将公钥发给发送方,发送方用这个公钥对数据进行加密,然后发给接收方,只有用私钥才能解密数据。公钥密码被大量应用着,它的安全性由数学假设来保证,即一个大数的质因数分解是一个非常困难的问题。但是量子计算机的提出,改变了这个观点。已经证明:一旦量子计算机实现了,大数很容易被分解,从而现在广为应用的密码系统完全可以被破解[4]。

幸运的是，在人们认识到量子计算机的威力之前，基于量子力学原理的量子密钥分发(Quantum Key distribution，QKD)技术就被提出来了[5]。量子密钥分发应用了量子力学的原理，可以实现无条件安全的密钥分发，进而结合 OTP 策略，确保通信的绝对保密。这里先给出量子通信的定义，再看看它的具体形式。

1.1.1 量子通信的基本概念及特点

量子通信是指应用了量子力学的基本原理或量子特性进行信息传输的一种通信方式。它有以下特点：

(1) 量子通信具有无条件的安全性。量子通信起源于利用量子密钥分发获得的密钥加密信息，基于量子密钥分发的无条件安全性，从而可实现安全的保密通信。QKD 利用量子力学的海森堡不确定性原理和量子态不可克隆定理，前者保证了窃听者在不知道发送方编码基的情况下无法准确测量获得量子态的信息，后者使得窃听者无法复制一份量子态在得知编码基后进行测量，从而使得窃听必然导致明显的误码，于是通信双方能够察觉出被窃听。

(2) 量子通信具有传输的高效性。根据量子力学的叠加原理，一个 n 维量子态的本征展开式有 2^n 项，每项前面都有一个系数，传输一个量子态相当于同时传输这 2^n 个数据。可见，量子态携载的信息非常丰富，使其不但在传输方面，而且在存储、处理等方面相比于经典方法更为高效。

(3) 可以利用量子物理的纠缠资源。纠缠是量子力学中独有的资源，相互纠缠的粒子之间存在一种关联，无论它们的位置相距多远，若其中一个粒子改变，另一个必然改变，或者说一个经测量塌缩，另一个也必然塌缩到对应的量子态上。这种关联的保持可以用贝尔不等式来检验，因此用纠缠可以协商密钥，若存在窃听，即可被发现。利用纠缠的这种特性(量子力学上称为非局域性，参见第 2 章)，也可以实现量子态的远程传输(详见第 3 章)。基于纠缠的 QKD 将在第 4 章详细介绍。

1.1.2 量子通信的类型

目前，量子通信的主要形式包括基于 QKD 的量子保密通信、量子间接通信和量子安全直接通信。下面简要说明。

1. 基于 QKD 的量子保密通信

如前所述，基于 QKD 的量子保密通信是通过 QKD 使得通信双方获得密钥，进而利用经典通信系统进行保密通信的，如图 1.1 所示。

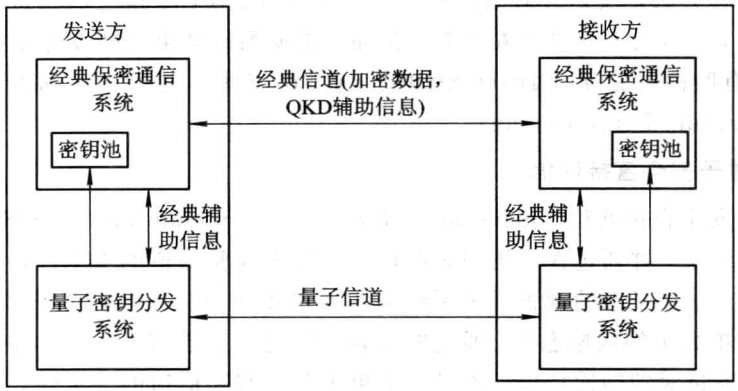

图 1.1　基于 QKD 的量子保密通信系统示意图

由图 1.1 可见，发送方和接收方都由经典保密通信系统和量子密钥分发(QKD)系统组成，QKD 系统产生密钥并存放在密钥池当中，作为经典保密通信系统的密钥。系统中有两个信道，量子信道传输用以进行 QKD 的光子(若采用光量子通信的话。本书中如不特别说明，都认为是采用光量子通信)，经典信道传输 QKD 过程中的辅助信息，如基矢对比、数据协调和密性放大(详见第 4 章)，也传输加密后的数据。基于 QKD 的量子保密通信是目前发展最快且已获得实际应用的量子信息技术。

2. 量子间接通信

量子间接通信可以传输量子信息，但不是直接传输，而是利用纠缠粒子对，将携带信息的光量子与纠缠光子对之一进行贝尔态测量，将测量结果发送给接收方，接收方根据测量结果进行相应的酉变换，从而可恢复发送方的信息，如图 1.2 所示。这种方法称为量子隐形传态(Quantum Teleportation)。应用量子力学的纠缠特性，基于两个粒子具有的量子关联特性建立量子信道，可以在相距较远的两地之间实现未知量子态的远程传输。

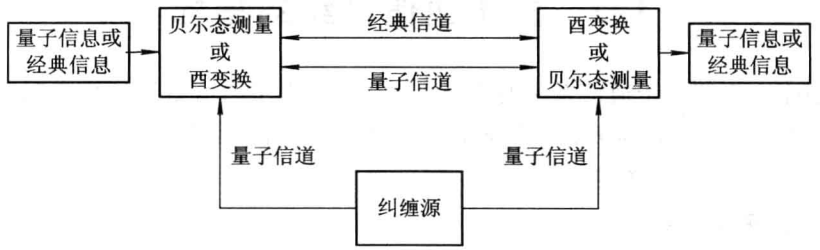

图 1.2　量子间接通信示意图

另一种方法是发送方对纠缠粒子之一进行酉变换，变换之后将这个粒子发到接收方，接收方对这两个粒子联合测量，根据测量结果判断发方所作的变换类型(共有四种酉变换，因而可携带两比特经典信息)，这种方法称为量子密集编码(Quantum Dense Coding)。

3. 量子安全直接通信

量子安全直接通信(Quantum Secure Direct Communications，QSDC)可以直接传输信息，并通过在系统中添加控制比特来检验信道的安全性，其原理如图 1.3 所示。量子态的制备可采用纠缠源或单光子源。若为单光子源，可将信息调制在单光子的偏振态上，通过发送装置发送到量子信道；接收端收到后进行测量，通过对控制比特进行测量的结果来分析判断信道的安全性，如果信道无窃听则进行通信。其中经典辅助信息辅助进行安全性分析。其原理详见第 5 章。

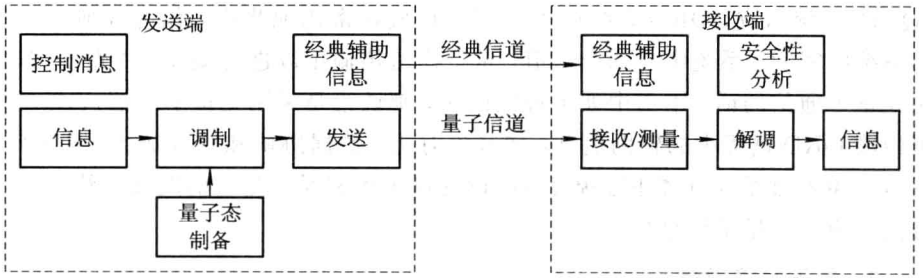

图 1.3 量子安全直接通信示意图

除了上述三种量子通信的形式外，还有量子秘密共享(Quantum Secret Sharing，QSS)、量子私钥加密、量子公钥加密、量子认证(Quantum Authentication)、量子签名(Quantum Signature)等，这里不再赘述，读者可参见相关文献。

1.2 量子通信系统的指标

根据 1.1 节量子通信系统的特点可见，衡量量子通信系统的指标和经典通信系统基本一样，但也有其特别强调的特点，如通信距离。本节介绍量子误码率、通信速率和通信距离三个指标。

1. 量子误码率

量子误码率(Quantum Bit Error Rate，QBER)是指承载信息的光量子波包

中，能用来使发送和接收双方进行有效通信的那部分信息的误码率。由于信道的损耗和接收机探测器的效率等原因，使得发送的大部分光子不能得到有效的计数，而实际通信系统中只保留双方认可的那部分比特值。在基于单光子的QKD系统中，只有发送方的编码基和接收方的测量基一致且被接收方测量计数的比特才被留下来进行进一步处理。QBER就是衡量这部分比特的误码性能的参数。

通信协议不同，系统保证安全的量子误码率限也不同。一般来说，量子保密通信系统中，QKD的量子误码率都必须小于11%。量子误码率和信道噪声、接收机噪声(包括探测器的暗计数)有关，必须通过信道补偿和压低暗计数来降低系统量子误码率。

2. 通信速率

量子通信系统的速率随通信的样式不同而不同。在量子保密通信系统中，除了加密数据传输的经典通信速率外，更重要的是密钥产生速率。衡量不同QKD系统性能时，往往用密钥产生率(key rate)，其含义是发送一个光脉冲，它能形成最后密钥的概率。若系统时钟为 f_s，密钥产生率为 r，密钥速率为 f_k，则有：$f_k = f_s \cdot r$。在间接量子通信系统和量子安全直接通信系统中，通信速率指传输经典信息(用经典比特表示的信息)或量子信息(用量子态表示的信息)的传输速率。

3. 通信距离

由于量子信号不能放大，而且量子中继器还处在实验室研究阶段，所以通信距离是一个重要指标。由于量子信道的损耗，随着通信距离的增加，量子通信的速率(不是加密后的经典数据的通信速率)迅速下降，所以实际应用时往往要在两者之间进行权衡。

1.3 量子通信的发展现状与展望

自从1989年美国IBM公司的C. H. Bennett领导的小组成功完成第一个QKD实验后，量子通信得到了迅速的发展。图1.4是第一个实验平台，采用32 cm长的自由空间量子信道[19]。

目前量子通信已经在某些领域得到了应用，出现了商业化的产品，如瑞士ID Quantique公司的Cerberis[6]，如图1.5所示。Cerberis采用QKD技术可以实现点到点的无条件的安全数据传输。图1.5中最下方是QKD终端，上方为高速加密数传系统。

此为试读，需要完整PDF请访问：www.ertongbook.com