# 量子通信*

薛 鹏† 郭光灿

(中国科学技术大学 中国科学院量子信息重点实验室 合肥 230026)

**摘 要** 量子通信是经典通信和量子力学相结合的一门新兴交叉学科.文章综述了量子通信领域的研究进展,既包括人们所熟知的量子隐形传态、密集编码和量子密码学,也包括刚刚兴起但却有巨大潜力的量子通信复杂度和远程量子通信等领域.文章介绍了量子通信的基本理论框架,同时也涉及了这个领域最新的实验研究的进展.

**关键词** 量子通信,量子隐形传态,量子密集编码,量子密码术,量子通信复杂度,远程量子通信

# QUANTUM COMMUNICATION

XUE Peng† GUO Guang-Can

(*Laboratory of Quantum Information and Department of Physics, University of Science and Technology of China, Hefei* 230026, *China*)

**Abstract** Quantum communication is a rising interdisciplinary field which combines classical communication and quantum mechanics. We summarize the new developments of quantum communication, which includes quantum teleportation, quantum superdense coding and quantum cryptography. Recently, there has been much interest in using quantum resources to reduce communication complexity and to prepare or control quantum states remotely. An introduction is given to the basic theoretic framework of quantum communication and the lastest development in experimental research.

**Key words** quantum communication, quantum teleportatiom, quantum superdense coding, quantum cryptography, quantum communication complexity, quantum remote state preparation

## 1 引言

我们生活在一个信息时代,信息科学在改善人类的生活品质以及推动社会的文明发展中发挥着令人惊叹的作用,这是其他学科所无法比拟的.随着人类社会对于信息的需求日益增加,人们不断地致力于信息技术的进一步发展,这必然导致现有的信息系统其功能被开发至极限.因此,信息科学的进一步发展势必要借助于新的原理和方法,于是一门将量子力学应用于信息科学的新兴学科——量子信息学便应运而生.这里我们着重介绍量子信息学的重要分支之一——量子通信.量子通信是量子信息学中研究较早的领域.广义上讲,它包括量子密码术、量子隐形传态、密集编码、远程量子通信,以及量子通信复杂性等.近年来在理论和实践上均已取得了重要的突破,引起各国政府、科技界和信息产业界的高度重视.量子通信理论是 1993 年由美国 IBM 的研究人员提出的,目前美国国家科学基金会、美国国防部等部门正在着手研究此项技术,欧盟从 1999 年开始研究,日本也从 2001 年将量子通信纳入十年计划.

## 2 量子信息基础理论

现有的经典信息以比特作为信息单元,从物理角度讲,比特是一个两态系统,它可以制备为两个可识别状态中的一个,如是或非,真或假,0 或 1.在数字计算机中,电容器平板之间的电压可表示信息比特,有电荷代表 1,无电荷代表 0.量子信息单元称为量子比特(qubit),它是两个逻辑态的叠加 $|\phi\rangle = c_0|0\rangle + c_1|1\rangle$,$|c_0|^2 + |c_1|^2 = 1$.经典比特可以看成量子比特的特例($c_0 = 0$ 或 $c_1 = 0$).用量子态来表示信息是量子信息的出发点,有关信息的所有问题都必须采用量子力学理论来处理,信息的演变遵从薛定谔方程,信息传输就是量子态在量子通道中的传

* 国家自然科学基金(批准号:69878025/F05,10004009/A040405),国家重点基础研究发展规划(973)(批准号:2001CB309300)资助项目
2002-01-29 收到

† 通讯联系人.E-mail:xuepeng@mail.ustc.edu.cn

送，信息处理（计算）是量子态的幺正变换，信息提取便是对量子系统实行量子测量.

在实验中，任何两态的量子系统都可以用来制备量子比特，常见的有：光子的正交偏振态、电子或原子核的自旋、原子或量子点的能级、任何量子系统的空间模式等.

信息一旦量子化，量子力学的特性便成为量子信息的物理基础，其主要的有：

（1）量子纠缠：$N$（大于 1）个量子比特可以处于量子纠缠态，子系统的局域状态不是相互独立的，对于一个子系统的测量会获取另外子系统的状态.

（2）量子不可克隆：量子力学的线性特性禁止对任意量子态实行精确的复制，量子不可克隆定理和不确定性原理构成量子密码术的物理基础.

（3）量子叠加性和相干性：量子比特可以处在两个本征态的叠加态上，在对量子比特的操作过程中，两态的叠加振幅可以互相干涉，这就是所谓的量子相干性.

## 3 量子隐形传态和密集编码

量子隐形传态和密集编码是量子通信中比较典型的两种方式，前者利用经典辅助的方法传送未知的量子态，而后者则是利用量子信道传送用经典比特表示的信息.

在科幻电影中，常常出现这样的场景：一个神秘的人物在某处突然消失，而后却在异地莫名其妙地显现出来. 隐形传送（teleportation）一词即来源于此. 遗憾的是，在经典通信中，这种实现隐形传送的方法违背了量子力学的基本原理之一——不确定关系. 因此长期以来，这只不过是一种科学幻想而已.

然而量子通信除了推广经典信息中的信源与信道等概念外，还引入了其特有的量子纠缠（quantum entanglement）[1]，创造了量子隐形传态这样一个经典通信中不可思议的奇迹. 1993 年，Bennett 等六位科学家在 Phys. Rev. Lett. 发表了一篇开创性文章[2]，提出将未知量子态的信息分为经典信息和量子信息两部分，分别由经典信道和量子信道传送给接受者. 经典信息是发送者对原物进行某种测量（通常是基于 Bell 基的联合测量）所获得，量子信息是发送者在测量中未提取的其余信息.

如图 1 所示，假设发送者 Alice 欲将粒子 1 所处的未知量子态传送给接收者 Bob，在此之前，两者之间共享 Einstein – Podolsky – Rosen（EPR）对（即由 Einstein，Podolsky，Rosen 提出的处于最大纠缠态的两个粒子组成的对）. Alice 对粒子 1 和她拥有的 EPR 粒子 2 实施 Bell 基联合测量（BS），测量的结果将出现在四种可能的量子态当中的任意一个，其几率为 1/4，对应于 Alice 不同的测量结果，Bob 的粒子 3 坍缩到相应的量子态上. 因此，当 Alice 经由经典通道将她的探测结果告诉 Bob 之后，他就可以选择适当的幺正变换 U（4 个泡利（Pauli）矩阵）将粒子 3 制备到精确复制态上（如图 1）.

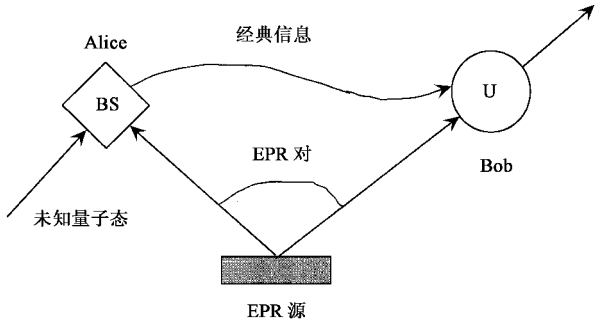


图 1 量子隐形传态原理图

量子隐形传态的特点是，仅仅是量子态被传送，但粒子 3 本身不被传送. 而在 Alice 测量之后，初态已被破坏，因此这个过程不是量子克隆.

目前，已有多个小组在实验上实现了量子隐形传态. Innsbruck 小组采用Ⅱ型参量下转换过程所产生的自发辐射孪生光子对作为 EPR 粒子，实现了将一个光子态传送到另一个光子上[3]. Rome 小组则采用了一个更为简单的办法[4]，把量子态从纠缠光子对中的一个传递到另一个光子上. 最近，CIT 小组根据 Vaidman 的方案[5] 完成了连续变量的隐形传态[6]. 另外一个实验[7] 是在 NMR（核磁共振）中实现的，把态从样品分子中的一个原子传递到另一个原子上.

近年来人们又将注意力转向传送一个未知的纠缠态，就此提出了一些理论方案[8–10].

最近，Bennett 等人提出了远程量子态制备（RSP）的理论方案[11]，与量子隐形传态不同的是，在 RSP 中发送者确定性地知道需要复制的态. 他们证明在 RSP 过程中，只需传送一个经典比特的信息，通信复杂度仅为隐形传态的一半.

在量子隐形传态中，实现了经典信息对量子信息的传输. 那么，我们是否可以利用量子信道来传送经典信息呢？

假设 Alice 和 Bob 共享处于纠缠态的一对粒子，

从而建立量子通道. Alice 在四种可能的幺正变换中任选一种对其纠缠粒子 A 进行操作,这种作用实际上是将两个比特的经典信息进行编码. 其后,Alice 将粒子 A 发送给 Bob,Bob 通过对两个粒子进行 Bell 基联合测量,即可确认 Alice 所做的变换,从而获得 2 个比特的信息,也就是说,仅仅通过传送一个粒子便能成功地传送 2 个比特的经典信息. 这就是所谓的‘密集编码’(dense coding)[12].

Innsbruck 小组利用与量子隐形传态相同的装置实现了四种操作的三种,即传送了 1.58bit[13]. 最近,山西大学的研究小组完成了连续变量的密集编码[14].

## 4 量子密码术

广泛用于网络金融行业的保密通信系统是一种所谓的 RSA 公钥体系,它的安全性基于大数因式分解这样一类不易计算的单向函数(one-way function),其原理如图 2 所示. 数学上虽然没有严格证明这种密钥不可破译,但现有的经典计算机几乎无法完成这种运算.

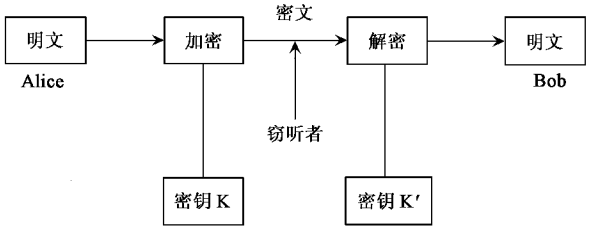


图 2 保密通信原理图

Shor 算法[15]证明,采用量子计算机可以轻而易举地破译这种公钥体系. 也就是说,一旦量子计算领域获得重大突破,它所具有的特殊性能,将使现在的公钥体系彻底地‘无密可保’.

另一方面,量子通信是目前科学界公认的惟一能实现绝对安全的通信方式,它利用量子力学的测不准原理和量子不可克隆定理,通过公开信道建立密钥,当事人之外的第三方根本不可能破解其密码. 其最终目标是解决通信的绝对安全等经典通信所存在的一系列根本性问题.

量子密码学是量子物理学与密码学相结合的一门新学科,它的理论首先是由美国哥伦比亚大学的 S. J. Wiesner 提出的,1970 年左右,他撰写了一篇题为‘共轭编码’的论文,文中提出了量子物理学至少在原则上可用于完成两项从经典物理学观点看来不可能进行的工作,其一是制造物理学上不可伪造的钞票,另一项就是利用量子来传送消息的方案. 遗憾的是,由于想法过于离奇,他的文章被拒绝刊登,直到 1983 年才得以在会议上发表[16]. 与此同时,1979 年 IBM 公司的 C. H. Bennett 和蒙特利尔大学的 G. Brassard 了解到 Wiesner 的观点,便开始考虑量子密码术具体的实施方法,提出了一些早期的方案(如 BB84 方案)[17],1989 年在 IBM 公司 Thomas J. Watson 研究中心建立起一个完全能工作的原型样机. 目前,量子密码术的研究引起了人们的广泛兴趣,在理论和实验方面均取得了重要进展. 采用光纤传输线已实现 48km 的密钥传送,自由空间的量子密码实验也取得了很大进展. 量子密码术的实用化已经指日可待.

目前,量子密码的方案主要有以下几种:

(1) 基于两种共轭基的四态方案,其代表为 BB84 协议[17].

(2) 基于两个非正交的两态方案,如 B92 协议[18].

(3) 基于量子纠缠的 EPR 粒子对方案,由 Ekert 于 1991 年提出,称为 E91 协议[19].

(4) 基于正交态的密钥分配方案,其基础为正交态的不可克隆定理[20—22].

最近,Lo 等人提出了一种改进的四态方案[23],不等几率地选择测量基使得密钥分配的效率接近 100%. 在此基础上,我们提出了一种高效率两态的 EPR 方案[24],以及基于三个非正交态的三态方案,利用一种‘空间光开关’(space optical switch)的装置有望实现密码网络[25],其结构如图 3 所示.

近年来,人们开始寻求一种严格证明量子密钥分配(QKD)的安全性的方法[26—28],起初的几种证明方法都不尽如人意,甚至需要用到量子计算机. 2000 年,Shor 和 Preskill 提出了一种简单的方案[29],巧妙地将纠缠纯化方案[30]和量子纠错码(CSS 码)[31]结合起来,严格地证明了 BB84 方案的安全性. 在此基础上,Lo 等人也采用类似的方案证明了一种六态协议的安全性[32].

量子密钥分配的第一个演示性实验由 Bennett 等人完成[33]. 随后,美国洛斯阿拉莫斯国家实验室,创造了目前光纤中量子密码通信距离的新纪录. 他们采用类似英国的实验装置,通过先进的电子手段,以 B92 方案成功地在长达 48km 的地下光缆中传送量子密钥[34]. 自由空间中的 QKD 也不断地取得突破,现在达到的传输距离为 1.5km[35]. 在中国,量子

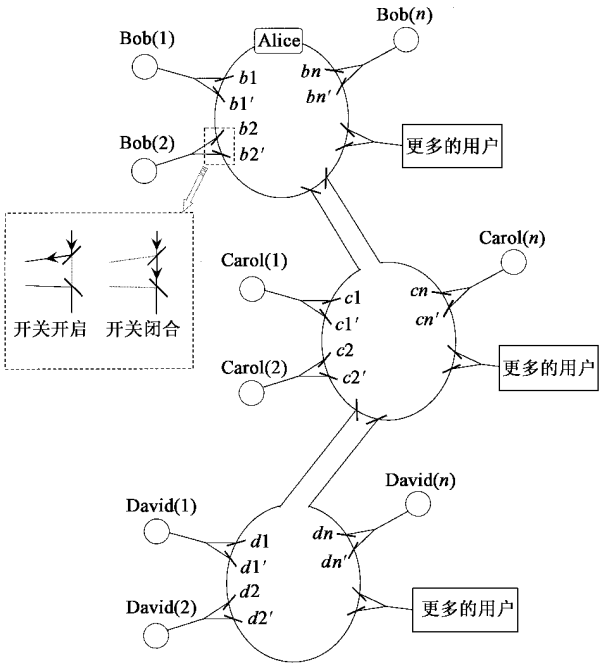


图 3　量子密码网络原理图

密码通信的研究刚刚起步，中国科学院物理研究所于 1995 年以 BB84 方案在国内首次做了演示性实验[36]，华东师范大学用 B92 方案做了实验，但也是在距离较短的自由空间里进行的[37]．2000 年，中国科学院物理研究所与中国科学院研究生院合作，在 850nm 的单模光纤中完成了 1.1km 的量子密码通信演示性实验．

在上述方案中，量子密钥是在两点之间传输、建立的，因而都是点对点的传输系统．密钥分配想要实用化，就必须在网络中得以实现，能够进行一点对多点或者任意两点之间的密钥传递．网络密钥传输有树状、环状、链式等多种结构，这里就其中树状结构网络做简要介绍．

树状结构网络可以用下面的示意图（图 4）简单表示，其中 S 是发送端，而 R1 是其中的一个接收端，O 代表光纤分束器．尽管树状网中有很多接收端，但是由于量子密钥中的载体一般情况下都是单粒子态，因而他们既不能被分流也不能被克隆．从发送端 S 发送的一个单粒子只能被其中的一个接收端接收，这相当于发送者 S 与这个接收端之间经历了一个点对点的密钥分配系统．因此，在一系列的数据传输完成之后，各个单粒子态分别随机地被某个接受端接收，最终的效果相当于发送者 S 与 $n$ 个接收者之间分别建立一套点对点的密钥传输系统，分别建立和分配了一组密钥序列．建立的方式可以是现存方法中的任何一种（相干态方案除外）．英国 BT 实验室的科学家 Townsend 采用上述模型，利用光子相位干涉的方法实现了一点对三点的密钥分配．发送者与每个接收者之间的距离为 4.4km，密钥分配的速率为 1kb/s，误码率 3%．该项成果证明了量子密钥在光纤网络中分配的可行性．尽管该实验仅实现了发送者与接收者之间的距离为 4.5m 的密钥分配，但原则上分配的距离不受限制，影响的因素是探测设备的性能．该项成果被作为量子密钥分配的重大突破发表在权威杂志 Nature 上[38]．

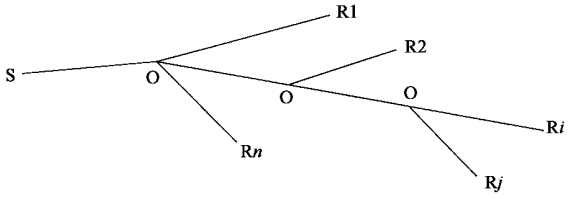


图 4　树状结构网络示意图

关于量子保密通信，依然存在很多问题需要解决，其中包括量子秘密共享、网络量子密码、身份认证、数字签名，以及最近提出的量子指纹[39]等．这些方案的优越性在理论上已经得到证实．

## 5　量子通信复杂度

在提高通信效率方面，量子通信同样具有经典世界中无可比拟的某种优越性．一般来说，通信各方分别拥有一部分输入，并希望共同完成某个布尔函数的计算，各方都能获知函数正确值的情况下，所需要的最小通信量被称为通信复杂度（communication complexity）．

假设通信双方 Alice 和 Bob 相距一段距离，需要合作解决一个由分布式输入决定的任务：$f(x,y)$：$x\times y\to z$　$(x,y\in\{0,1\}^n)$．Alice 和 Bob 分别拥有这个方程的输入的一部分，他们的目的在于计算出方程的值．通常，我们会对输入加一个条件，使之满足一个布尔方程．最普通的解法是 Alice 将她的输入值告诉 Bob，由 Bob 来计算方程 $f$ 的结果 $z$．如果要求双方都知道最终的结果，Bob 再将结果 $z$ 传送给 Alice．如果我们关心的是完成这个任务所需的通信量，对一些具有特殊形式的方程来说，如果允许小的出错概率 $\varepsilon$，则存在更为有效的解决方法．

在通信复杂性的经典模式中，通常允许 Alice 和 Bob 事先分享一组随机的变量，虽然从数学的角度来看，这样做并没有多大意义．在这种方案中，假设 Alice 根据某种特定的输入持有一随机比特串（或者

整数),或者有时甚至是一个随机的实数,她告诉 Bob 这串数据初始的相位.这一切发生在双方交换数据之前,因此不会计入通信量.

继 1979 年提出经典通信复杂性的概念[40]之后,Yao(姚以智)又首次将量子资源应用于解决分布式的布尔函数的计算[41].他设想了一种量子通信复杂度的模型,通信方除了各自拥有一组字符串作为函数的初始输入外,还分别有一组独立的量子比特置于初始态.在通信过程中,其中的一方根据计算函数的需要,对自己的量子比特做一个幺正变换,然后把其中一部分量子比特传送给另一方.最后,另一方测量他的量子比特,其结果即为函数的输出结果.这就是最早的量子通信复杂性的方案,然而,根据 Holevo 理论[42],这样做并不能降低通信复杂度.Holevo 定理指出:仅通过传送 $m$ 个量子比特不能够传送多于 $m$ 个经典比特的信息.

第一次成功地证明了利用量子信息可以减少通信复杂度的是 Cleve[43,44]等人.他们设计了与上述量子模型不同的一种模型——纠缠模型,即通信仍然限于使用经典比特,但是通信各方事先分享一组处于最大纠缠态的量子比特,也就是说利用 EPR 态作为量子信道,在传送经典信息的同时,传送量子信息,藉此来减少通信复杂度.在这个模型中,他们证明了在三方确定性方案中,事先共享的纠缠可以减少一个比特的通信量.

在这类纠缠模型研究上,我们小组也提出了一些方案,例如,利用两粒子非最大纠缠纯态[45]或 GHZ 态[46]作为量子信道来完成两方以及三方概率性通信方案,并在实验上进一步验证了上述结果.图 5为我们利用纠缠降低通信复杂度的实验装置图.图中,我们使用氩离子连续激光器作为光源,依次经过紫外偏振分束器(UV PBS)、紫外二分之一波片(UV HWP)和紫外四分之一波片(UV QWP),再经过两块晶轴相互垂直的 BBO 晶体,发生Ⅱ型参量下转换非线性光学过程,产生的自发辐射孪生光子对作为非最大纠缠态光子源,通过调节 QWP 可以产生不同纠缠度的光子对.局域的旋转操作算符 $R(\phi_1)$ 和 $R(\phi_2)$是由每条光路中的 HWP 实现的.对每个非最大纠缠态,均有四组经典字符串 00,01,10 和 11 作为输入,对应于每组输入,纠缠态被施以相应的旋转操作,之后经过一个偏振分束器,进入相应的单光子探测器 D.最后,我们可以通过每组输入及与之对应的单光子探测器的两两符合,来统计出成功降低通信复杂度的几率 $P$ 与纠缠度的函数关系.另外,图 5 中 IF 表示干涉滤波片.

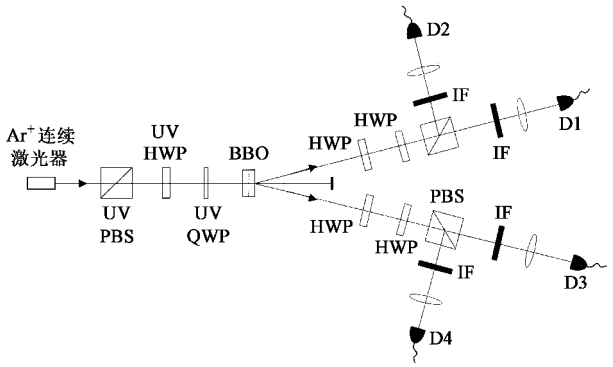


图 5 利用纠缠降低通信复杂度的实验装置图

下面将简要地介绍一下在参考文献[45]中我们如何利用纠缠概率性地降低通信复杂度.Alice 和 Bob 分别有一部分待计算函数的初始值 $x,y\in\{0,1\}^2$,可以用二进制数表示为 $x_1x_0,y_1y_0$.他们的目的在于计算函数 $f(x,y)=x_1\oplus y_1\oplus(x_0\wedge y_0)$的值.假设两者事先分享一个二粒子的非最大纠缠态,即 $|AB\rangle=\alpha|00\rangle+\beta|11\rangle$.两者分别作以下操作:若 $x_0(y_0)$为 0,Alice(Bob)将算符 $R(\phi_1)=\begin{pmatrix}\cos\phi_1 & -\sin\phi_1\\ \sin\phi_1 & \cos\phi_1\end{pmatrix}$作用在各自的量子比特 $A(B)$上;若 $x_0(y_0)$为 1,两人选择算符 $R(\phi_2)$作用在其粒子上,然后测量得到一个比特 $a(b)$,则等式 $a\oplus b=x_0\wedge y_0$ 以一定的几率成立.最后,Alice 将比特$(x_1\oplus a)$发送给 Bob,同样,Bob 也将$(y_1\oplus b)$传送给 Alice.于是两者能够以特定的几率 $P(\alpha,\beta)$完成上述布尔函数 $f(x,y)=(x_1\oplus a)\oplus(y_1\oplus b)=x_1\oplus y_1\oplus(x_0\wedge y_0)$.

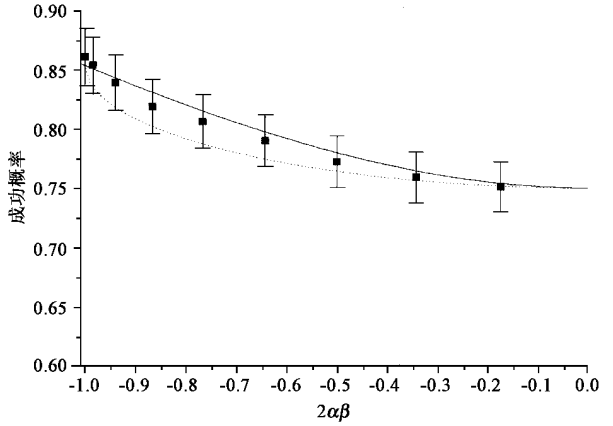


图 6 降低通信复杂度的实验曲线

利用纠缠概率性地降低通信复杂度的实验曲线如图 6 所示,$\alpha,\beta$ 是初始态的两个系数,由此表示的

横坐标 $2\alpha\beta$ 可以标志初态的纠缠程度，而降低通信复杂度的成功概率 $P$ 是 $2\alpha\beta$ 的函数.

因此利用非最大纠缠通道只需传送 2 个比特就可以完成通信任务，与经典模型相比，复杂度降低了一个比特.并且，我们利用一个简单的全光学系统验证了上述结论[45].

## 6 量子远程通信

远程量子通信(long distance quantum communication)开辟了新型的通信系统，可实现量子因特网、多方分布式计算等.而实现这种通信系统的基本部件包括量子纠缠态的发生器、量子通道及测量装置.众所周知，光在微观世界中有粒子特性以及具有最快的传播速度，这些特征使光子成为一种优于其他粒子的信息载体，广泛应用于量子信息中.但是由于存在严重的消相干及消纠缠，利用光子作为载体的量子通信受到时间和空间的限制，不适于长时间的保存.因此人们提出用量子存储器来解决上述问题.例如采用高 $Q$ 腔中的原子[47]作为存储器，利用光和原子的相互作用，将光子的信息存储在原子中.但是，为克服腔损耗的影响，该系统需要在极低的温度下运行，而且对腔的 $Q$ 值要求很高，这在技术上很难实现.我们小组提出了一种易于实现的量子信息处理器[48]，可以有效地克服光腔消相干的影响.有趣的是，在文章发表两个月之后，巴黎高等师范学校的著名学者在实验上初步验证了我们的理论模型.

量子通信的基础是，在两个相距一定距离的点之间产生量子纠缠态.但是由于光子的吸收和其他的通道噪声，纠缠度会随着通道的长度而降低.因此现有量子通信的诸多方案都只能局限于在几十公里的距离内操作.最近，段路明与其国际合作的同事提出一个涉及量子中继器的新设想，有可能克服这一局限性[49].其基本思想是：将信道分成长度一定的若干段，每段都包括量子纠缠的产生和纯化两个过程.通过纠缠交换将两个相邻信息段的纠缠态连接起来.交换后形成的新纠缠态的纠缠度会有所降低，这就需要再次纠缠纯化.在段路明等人提出的方案中，利用光子和原子的相互作用，在原子集团之间产生纠缠态，相对于单个原子的纠缠态来说，纠缠产生的效率大大提高了.而纠缠态的连接则是通过简单的线性光学操作即可完成，并且在每个步骤中都包含一个本征的纠缠纯化的过程.最后生成的远距离原子集团的纠缠态在量子通信中有着一系列广泛的应用.例如，量子隐形传态、基于 EPR 的量子密钥分配、Bell 不等式的验证等.这个方案只涉及到现有技术基础上对于原子集团、线性光学元件和单光子探测器进行操作，因此应当可能在实验上得以实现.

## 7 结束语

尽管有着广泛应用前景的量子通信的基本框架已经成型，但是我们也应当看到目前量子通信领域中还有许多问题亟待解决.例如在实验单元技术上，如何有效地产生多粒子纠缠态，哪一种物理体系更适合存储量子信息等问题.在理论上，在量子信息领域中占有特殊地位的纠缠，其特性尚未完全揭示清楚，甚至有关纠缠的度量问题也远未解决.然而这将无损于量子通信的发展势头，反而会吸引各方面的专家学者参与到量子通信的研究中来.我们有理由相信，量子通信科学的明天会更加辉煌，人类从经典通信时代进入量子通信时代不再只是一种梦想.

## 参 考 文 献


[1] Einstein A, Podolsky B, Rosen N. Phys. Rev., 1935,47:777
[2] Bennett C H *et al*. Phys. Rev. Lett., 1993,70:1895
[3] Bouwmeester D *et al*. Nature(London),1997,390:575
[4] Boschi D *et al*. Phys. Rev. lett., 1998,80:1121
[5] Vaidman L. Phys. Rev. A, 1994,49:1473
[6] Furusawa A *et al*. Science, 1998,282:706
[7] Nielsen M A, Kill E, Laflamme R. Nature(London),1998,396:52
[8] Lombardi E, Sciarrino F, Popescu S *et al*. e-print quant-ph/0109160
[9] Wang X G. Phys. Rev. A, 2001,64:022303
[10] Lee H W. e-print quant-ph/0104097
[11] Bennett C H *et al*. Phys. Rev. Lett., 2001,87:077902
[12] Bennett C H, Wiesner S J. Phys. Rev. Lett., 1992,69:2881
[13] Mattle K *et al*. Phys. Rev. Lett., 1996,76:4656
[14] Li X Y *et al*. e-print quant-ph/0107068
[15] Shor P W. Proc. of 35th Ann. Symp. on the Foundations of Computer Science. 1994. 124
[16] Wiesner S J. SIGACT News, 1983,5:78
[17] Bennett C H, Brassard G. Proc. IEEE Internet. Conf. On Computers, Systems and Signal Processing, Bangalore. New York: IEEE, 1984. 175
[18] Bennett C H. Phys. Rev. Lett., 1992,68:3121
[19] Ekert A K. Phys. Rev. Lett., 1991,67:661
[20] Mor T. Phys. Rev. Lett., 1998,80:3137
[21] Goldenberg L, Vaidman L. Phys. Rev. Lett., 1995,75:1239
[22] Masato, Imoto N. Phys. Rev. Lett., 1997,79:2383
[23] Lo H K, Chau H F. e-print quant-ph/0010056

[24] Xue P, Li C F, Guo G C. Phys. Rev. A, 2001,64 :032305 ;Xue P, Li C F, Guo G C. Phys. Rev. A, 2002,65 :034302
[25] Xue P, Li C F, Guo G C. Phys. Rev. A, 2002,65 :022317
[26] Lo H K, Chau H F. Science, 1999,283 :2050
[27] Mayers D J. Assoc. Comput. Mach. (to be published), quant-ph/9802025
[28] Biham E *et al*. Proc. of the 32th Ann. ACM Symp. on Theory of Computing. 2000. 715
[29] Shor P W, Preskill J. Phys. Rev. Lett., 2000,85 :441
[30] Bennett C H, Divincenzo D P, Smolin J A *et al*. Phys. Rev. A, 1996,54 :3824
[31] Calderbank A R, Shor P W. Phys. Rev. A, 1996,54 :1098 ;Steane A M. Proc. R. Soc. London A, 1996,452 :2551
[32] Lo H K. e-print quant-ph/0102138
[33] Bennett C H, Brassard G. SIGACT News,1989,20 :78
[34] Hughes R J *et al*. J. Mod. Opt., 2000,47 :533
[35] Butter W T *et al*. Phys. Rev. Lett., 2000,84 :5652
[36] 邵进,吴令安.量子光学,1995,1 :41[Shao J, Wu L A. Quantum Optics, 1995,1 :41(in Chinese)]
[37] 张涌.华东师大博士学位论文,1997[Zhang Y. A Dissertation Submitted to the Department of Physics and the Committee on Graduate Study of East China Normal University for the Degree of Doctor of Philosophy, 1997(in Chinese)]
[38] Townsend P D *et al*. Nature(London),1997,385 :47
[39] Buhrman H, Cleve R, Watrous J *et al*. Phys. Rev. Lett, 2001, 87 :167902
[40] Yao A C. Proc. of the 11th Ann. ACM Symp. on Theory of Computing. 1979.209
[41] Yao A C. Proc. of the 34th Ann. IEEE Symp. on Foundations of Computer Science. 1993.352
[42] Holevo A S. Problemy Peredachi Informatsii,1973,9 :3
[43] Cleve R, Buhrman H. Phys. Rev. A, 1997,56 :1201
[44] Buhrman H, Cleve R. e-print quant-ph/9705033
[45] Xue P *et al*. Phys. Rev. A 2001, 64 :032304
[46] Xue P, Li C F, Zhang Y S *et al*. J. Opt. B :Quantum Semiclass. Opt., 2001,3 :219
[47] Hood C J. *et al*. Science, 2000,287 :1447
[48] Zheng S B, Guo G C. Phys. Rev. Lett. 2000,85 :5392
[49] Duan L M. Lukin M, Cirac I *et al*. Nature (London),2001,414 : 413

## 封 面 说 明

用具有高空间分辨率(0.5 角秒)和高灵敏度的钱德拉 X 射线空间望远镜观测极亮红外星系 Mrk273 所得到的正在并合的星系的 X 射线像.图中所示的像是由红色(0.3—1keV),绿色(1—3keV)和蓝色(3—10keV)三个波段的像合成的.钱德拉 X 射线望远镜第一次接收到并合星系的非常扩展的热气体晕(尺度为 20—30 万光年).此项观测结果揭示了椭球星系的热气体晕起源于星系的并合过程.右方的插图显示了 Mrk273 星系核心的复杂结构,也表明硬 X 射线辐射主要来源于星系中心的活动星系核.

(夏晓阳,薛随健,邓祖淦,吴宏等提供,也见 Xia X Y *et al*. ApJ,2002,196 :564)

·读者和编者·

## 2002 年第 7 期《物理》内容预告

### 《物理》创刊 30 周年专辑(下)

(本专辑主要反映物理学对高新技术发展的推动作用)

物理学研究与高新技术产业的发展(宋菲君);
半导体物理效应与光电子高技术产业(王启明);
物理学研究与微电子科学技术的发展(王阳元等);
磁学研究与三环公司的发展(胡伯平等);
非晶态物理与软磁材料产业化(周少雄等);
自旋电子学和计算机硬件产业(赖武彦);
氮化镓发光二极管材料的物理问题(周均铭);
纳米储锂材料和锂离子电池(黄学杰等);
不透明玻璃显现出的曙光——块体金属玻璃的发现与材料领域的革命(潘明祥等).