中国科学: 信息科学 2014 年 第 44 卷 第 3 期: 296–311
www.scichina.com info.scichina.com
《中国科学》杂志社
SCIENCE CHINA PRESS
量子信息专刊 · 评述

量子通信现状与展望

吴华[①], 王向斌[②③④*], 潘建伟[①③]

① 中国科学技术大学公共事务学院, 合肥 230026
② 清华大学物理系低微量子物理国家重点实验室, 北京 100084
③ 量子信息与量子科学前沿协同创新中心, 合肥 230026
④ 济南量子技术研究院, 济南 250101
* 通信作者. E-mail: wang_xiangbin@hotmail.com

收稿日期: 2013–08–06; 接受日期: 2013–12–16
国家重点研究发展计划 (批准号: 2007CB907900, 2007CB807901)、国家自然科学基金 (批准号: 60725416, 11174177)、国家高技术研究发展计划 (批准号: 2006AA01Z420, 2011AA010800, 2011AA010803) 和山东万人计划项目资助

摘要 本文综述量子通信基本原理、方法、技术手段与应用. 介绍量子保密通信基本协议和诱骗态方法, 以及基于纠缠分发的量子通信, 含基于纠缠光子对的量子保密通信、量子态隐性传输、纠缠光子对操控等. 介绍量子通信的技术与应用现状并对未来发展方向做展望.

关键词 量子通信 量子密钥分发 BB84 协议 诱骗态方法 量子隐形传态 纠缠光子对操控 量子网络

1 引言

“最近的 16 公里量子态隐形传输的成功试验表明, 中国将有能力建立起卫星与地面的安全量子通信网络.”—— 美国《时代周刊》在 “爆炸性新闻” 栏目中以 “中国量子科学的飞跃” 为题, 对 2010 年中国科技大学与清华大学合作完成的 16 公里量子态隐形传输试验进行了评论. 相比于经典通信, 量子通信究竟有哪些优势, 有哪些应用, 源于何种原理以及方法和技术手段等, 无疑是大家所关心的. 我们将在此介绍量子通信的基本概念与方法、技术现状, 以及未来应用前景.

量子通信的基本思想主要由 Bennett 等于 20 世纪 80 年代和 90 年代起相继提出, 主要包括量子密钥分发 (quantum key distribution, QKD)[1] 和量子态隐形传输 (quantum teleportation)[2]. 量子密钥分发可以建立安全的通信密码, 通过一次一密的加密方式可以实现点对点方式的安全经典通信. 这里的安全性是在数学上已经获得严格证明的安全性, 这是经典通信迄今为止做不到的. 现有的量子密钥分发技术可以实现百公里量级的量子密钥分发 [3], 辅以光开关等技术, 还可以实现量子密钥分发网络 [4,5]. 量子态隐形传输是基于量子纠缠态的分发与量子联合测量, 实现量子态 (量子信息) 的空间转移而又不移动量子态的物理载体, 这如同将密封信件内容从一个信封内转移到另一个信封内而又不移动任何信息载体自身. 这在经典通信中是无法想象的事. 基于量子态隐形传输技术和量子存储技术的量子中继器可以实现任意远距离的量子密钥分发及网络.

引用格式: 吴华, 王向斌, 潘建伟. 量子通信现状与展望. 中国科学: 信息科学, 2014, 44: 296–311, doi: 10.1360/N112013-00120

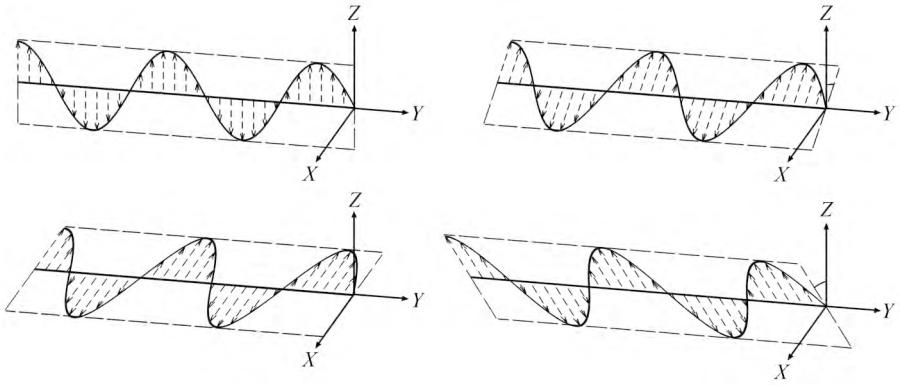

图 1 单光子偏振

Figure 1 Single photon polarization

量子通信的实现基于量子态传输. 为便于传输, 现有的量子通信实验一般以光子为量子态载体, 其表现形式即为光子态传输. 量子信息的编码空间以光偏振 (见图 1) 为主.

如前所述, 量子态隐形传输只是在空间转移量子信息 (量子态), 但并不转移量子信息的物理载体. 若以光子为量子信息载体, 量子态隐形传输就是把量子信息从一个光子上转移到远处另外一个光子上. 这样的量子态隐形传输有一个明显的应用: 在恶劣通道情况下, 若直接传输光子本身进行量子通信, 将会由于误码率过大而无从实现通信任务. 而基于量子态隐形传输的量子通信由于无需传输光子本身, 其通信质量不受物理通道影响. 量子态隐形传输需要通信双方预先共享一个量子纠缠态 (常用的两光子量子纠缠态又称纠缠光子对, 或纠缠对). 为了预先共享纠缠对, 需要预先进行纠缠对分发. 实际上, 纠缠分发本身也可以用来实现量子密钥分发. 通信双方预先共享的纠缠对的质量取决于纠缠分发时的通道状况. 用于各类噪声的存在, 共享纠缠对一般是不理想的. Bennett 等人 [1,2] 的理论表明, 通过对不理想纠缠对纯化可以获得高质量纠缠对. 基于此可以实现高品质的量子态隐形传输. 目前, 量子态隐形传输 [6]、纠缠光子对分发 [7,8], 以及纠缠纯化 [9,10] 都已经获得广泛实验研究.

基于 BB84 协议的量子密钥分发无需共享纠缠对资源, 只需要单光子态传输. 目前真实系统没有理想单光子源, 采用的是近似单光子源, 即强度为单光子量级的弱激光源, 后简称弱光. 由于传输损耗, 基于弱光传输的量子密钥分发安全距离受到严重限制. 另一方面, 窃听者可以冒充通道损耗进行光子分数攻击 (photon number splitting attack, PNS attack)[11,12]. 文献分析表明, 现有技术的安全距离实际上不到 20 公里. 一个行之有效的办法是采用近年发展起来的诱骗态方法 (decoy-state method)[13~16], 它虽然继续采用现有光源, 但安全性等价于理想单光子源, 距离与理想单光子源距离基本相同.

基于量子力学原理, 单量子态信号不能被完全克隆放大, 而通道损耗随距离呈指数增长. 因此, 不论光源与检测技术如何发展, 单量子态的直接传输距离不可能无限发展. 一般认为, 其极限距离大概在数百公里量级. 远程量子通信的最终实现将依赖于量子中继概念. 其基本思想是: 在空间建立许多站点. 各相邻站点间预先共享并存储量子纠缠对. 采用量子态隐形传输技术可以实现量子纠缠转换, 即增长量子纠缠对的空间分隔距离. 如果预先将纠缠对布置在各相邻站点, 纠缠转换操作后便可实现次近邻站点间的共享纠缠. 继续操作下去, 原则上可以实现在很远的两个站点间建立共享纠缠, 即实现远距离量子通信. 基于量子中继 [17,18] 的量子通信距离没有原理上的限制. 基于量子中继的远程量子保密通信, 即便所有中继站都为敌方控制, 终端间的通信依然是安全的. 这是量子中继相比于经典中继 (又称可信中继) 的最大优势.

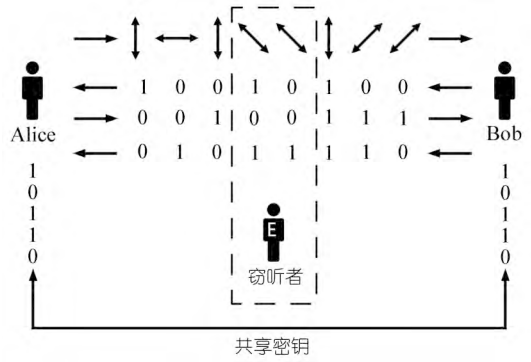

图 2　量子密钥分发

Figure 2　Quantum key distribution

近年来, 以 BB84 协议和量子态隐形传输为代表的量子通信理论与实验在以越来越快的速度朝实用化和商用化方向迅猛发展.

2　量子通信的基本原理

点对点保密通信最直接的办法是让通信双方先共享一串密码, 然后以此密码通过一次一密的加密方式对通信内容加密、解密. Shannon[19] 于 1948 年已经证明, 若密码是安全的, 则通信内容严格安全. 现有的经典协议不能确保通信双方的共享密码的安全性. 例如, 使用秘密信道建立共同密码的方法. 经典通信不存在可证实的绝对安全的秘密信道, 因为窃听者原则上总可以做到获取 “秘密通道” 的信息 (密码) 而又不留痕迹. 合法用户无从知晓通过 “秘密信道” 发送的密钥有没有被窃听. 建立密钥的另一种经典方法是基于对特定数学问题的复杂性假定. 然而, 现有的复杂性假定并未获得严格的数学证明, 基于量子逻辑的大数分解算法 [20] 却从理论上证明了经典 RSA 通信协议不安全. 下面我们重点介绍量子密钥分发理论协议的安全性问题.

2.1　BB84 协议及其安全性

相比于经典通信, 量子通信的一个重大优势是可以实现严格数学证明下的安全性 (绝对安全性). 为实现绝对安全的保密通信, Benett 与 Brassard 于 1984 年提出了首个量子密钥分发协议 [1](见图 2), 即著名的 BB84 协议. 这种方案的安全性基于量子力学的两个基本原理: 单光子的不可分割性和单光子量子态的测量塌缩性.

在 BB84 协议以及大多数量子信息处理中, 以单量子态对应于经典二进制码 (bit). 基本要求是所选择的量子系统有两个基本态. 在 BB84 协议中水平或 45° 偏振对应于经典比特 0; 竖直或 135° 偏振对应于经典比特 1. Alice 向 Bob 发射一系列单光子偏振态. 每个光子的偏振从水平、竖直、45° 或 135° 中随机选出. 或者说, Alice 随机使用了两组基, 我们称之为直角基 (水平, 竖直偏振) 及斜角基 (45° 偏振或 135° 偏振). 对每个飞入光子, Bob 随机选用直角或斜角基测量其偏振. Bob 丢弃那些使用了错误基得到的测量结果. 对于剩下的测量记录, 随机抽取一部分与 Alice 对照, 检验每组基下各态的误码率并丢弃这些公开宣布的用作检验的测量结果. 再对剩余数据 (我们称之为初始码) 通过纠错, 隐私放大而提炼出最终码.

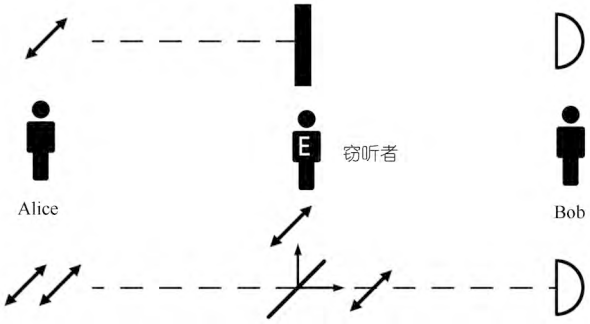

图 3 光子数分离估计

Figure 3 Photon number splitting attack

光子总是以一个整体出现. 半个光子的事件从来不会发生. BB84 协议要求传输的单光子脉冲, 原理上不允许窃听者通过分割光子并保留部分光子的办法进行窃听. 窃听者要么获得完整光子, 要么什么都没有获得. 量子物理学把测量视为物理学过程的一部分. 对一个量子体系观测, 原则上会带来扰动. 量子世界里不存在 "静悄悄地偷看", 即观测而又不对被观测系统产生扰动. 就是说, 观测就会留下痕迹, 这些构成量子密钥安全性的物理基础.

严格的安全性证明最早由 Mayers[21] 于 1996 年给出. Shor 与 Preskill[22] 于 1999 年给出了大为简化的证明, 其主要结论是: 任何窃听者对最终码的信息量大于 δ 的概率小于 ε, 其中 ε, δ 为指数接近于零点小量, 如 100 亿分之一. 最终码的产出率取决于通道误码率. 就 BB84 方案而言量子密钥分发误码率上限值为 11%.

虽然 BB84 方案已经被证明是绝对安全的, 这并不意味着任何以该方案为基础的实验都是安全的. 这是因为所进行的实验未必真正符合 BB84 安全性证明中所要求的前提条件. 证明中假设了单光子源, 由于技术难度极高, 现有的实验多采用单一强度弱激光, 即弱相干态光. 其安全性上存在一定问题, 下面我们做简要的介绍.

2.2 光子数分离攻击

如前所说, 单光子的不可分割性是量子密码安全性的重要物理基础. 然而, 多光子脉冲不再拥有不可分割性. 例如, 一个包含两个光子的脉冲, 原则上可以被分割为两个单光子脉冲, 所以其安全性基础就不复存在了, 就会遭受光子数分离攻击, 下面我们来具体介绍下光子数分离攻击 [11,12]. 由于量子通信通道损耗率极大, 对于 100 km 以上的距离, 加上探测效率, 整体效率将小于千分之一. 根据理论证明, 理想单光子源即便在高损耗通道下也是绝对安全的, 可是实际系统使用的弱光在高损耗通道下则结果完全不同: 窃听者可以冒充通道损耗通过光子数分离攻击而获得全部密码. 如图 3 所示, 为表述方便, 我们以偏振空间为例. 弱相干态脉冲实际上是单光子与多光子脉冲的概率混合. 即, 在所发出的非真空脉冲中, 有些是单光子的, 有些是多光子的 (2 光子, 3 光子, ...). 多光子脉冲即包含了多个全同偏振光子. 窃听者可将其分离, 自己留下一个, 将剩余光子送到远程合法用户. 对于这些多光子脉冲, 窃听者可以拥有与合法用户完全一样的偏振光子而不对远程合法用户的光子偏振态造成任何扰动. 即, 对于多光子脉冲, 窃听者可以拥有 100%的信息而不被察觉. 窃听者可以选择将所有单光子脉冲完全吸收而使得远程合法用户的所有比特皆由光源的多光子脉冲产生. 窃听者的行为不会被合法用户察觉, 因为窃听者可以对每个单独脉冲随时调整通道衰减系数, 从而使得远程合法用户的探测器计数率等同于高损耗自然通道.

对于 2005 年以前的弱相干态密钥分发实验 [20,23~27], 窃听者可获取全部信息而不留下任何痕迹. 事实上, 量子密码发明者之一, Brassard 等 [11,12] 早在 2000 年就对弱相干态量子密码实验做出批评, Brassard 等在其著名论文的摘要部分指出: "Existing experimental schemes (based on weak pulses) currently do not offer unconditional security for the reported distances and signal strength", 即: "现有基于 (相干态) 弱脉冲的做法, 据其所报告的距离及所采用的脉冲强度, 并不提供绝对安全性." Brassard 的这一评论适用于 2005 年以前所有基于弱相干光的量子密钥分发实验 [20,23~27]. 幸运的是, 于 2005 年起发展起来的诱骗态量子密码理论, 提供了一个基于弱相干光源的安全量子密钥分发方案.

2.3 侧信道攻击和木马攻击

尽管量子通信技术在理论上具有 "无条件安全性", 但理论方案安全性和实际系统安全性这两个层面之间仍存在一条狭窄但分明的缝隙. 利用量子保密通信系统器件的性能缺陷进行窃听, 或者针对器件的弱点进行主动攻击都可能削弱甚至破坏量子保密通信系统的安全性. 自 2000 年以来, 随着量子通信技术的逐步实用化, 实用系统中的安全攻防问题变得越来越重要, 并引起研究者的高度重视. 针对早期方案和实验技术中的安全性漏洞, 已提出了大量的攻击方案, 如伪装态攻击、相位重映射攻击、定时侧信道攻击、大脉冲攻击、光学部件高能破坏攻击等. 这些攻击方案, 统称为侧信道攻击和木马攻击.

"木马攻击" 中的木马是指实际的量子保密通信系统其信号源、接收器以及其他部件有可能存在的某种弱点, 针对这种弱点, 可以设计攻击方案, 主动诱使系统内部信息泄露. 如果不弥补器件的弱点, 这种攻击常常能有效地击破量子保密通信系统的安全性. 比如说 "大脉冲攻击" 法, 由于光学器件总会有一定反射能力. 窃听者因此向光路中发射高亮度激光. 对于某些量子保密通信系统的实现方案, 被反射回来的光会被系统中的极化或相位调制器调制, 这样, 攻击者就得到了发射方信号态的极化或相位信息, 而不会引入额外的干扰, 也就不会被发现. 再如 "高能破坏攻击" 使用高亮度激光击毁衰减器, 破坏了弱相干光源, 随后就可以使用 "分束器攻击" 或者 "分离光子数攻击" 窃取密钥. 主动攻击法还有 "伪装态攻击"、"相位再映射攻击" 等. 而侧信道攻击法是指量子通信系统可能存在泄漏密钥信息的侧信道. 侧信道攻击最出名的就是分离光子数攻击, 此外, 最近提出的针对有记忆的装置无关 QKD 系统的攻击就利用了经典协商信道的侧信道泄漏.

3 量子通信的基本方法

3.1 实用化点对点量子通信

该方法要求随机改变相干态脉冲强度而测出单光子计数率 [13~16]. 以此为输入参数提炼出最终码. 采用该法所得最终码, 其安全性与用理想单光子源所获最终码等价. 对于弱相干态光源所发射的脉冲, 有一部分是多光子脉冲, 一部分是单光子脉冲. 诱骗态方法的主要功能是测算在接受端 Bob 的探测结果 (初始码) 中, 有多少起源于发射端 (Alice 端) 光源的单光子脉冲, 多少起源于发射端的多光子脉冲. 基于这个至关重要的参数, 就可以提炼出安全的最终码, 其安全性等同于只采用了由发射端单光子脉冲产生的那部分初始码而抛弃了多光子脉冲产生的那部分初始码. 在安全性方面最后的效果就等同于使用了理想单光子源.

2003 年, 美国西北大学黄元瑛博士提出了在量子密码理论实用化上具有革命性的 Decoy-State 思想 [13] 用以解决光子数分离攻击. 可是黄的结果尚不能立即实用于现有真实系统, 清华大学王向斌教

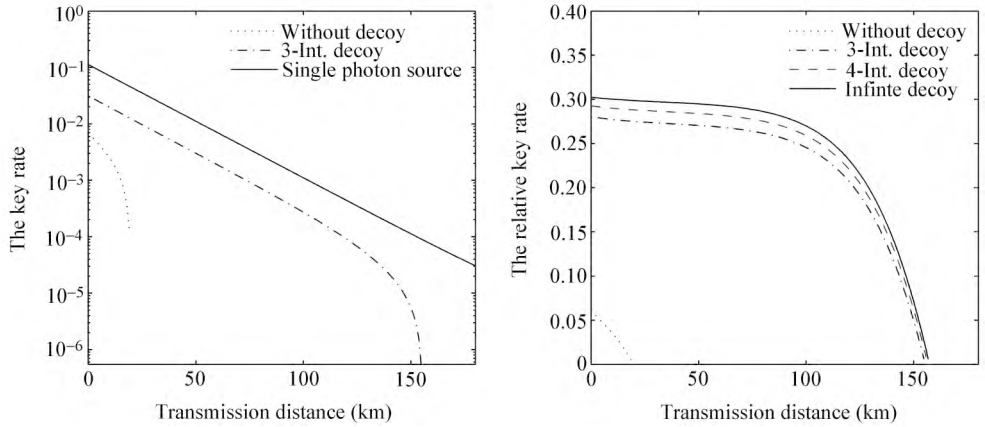

图 4 诱骗态方法的安全距离. (a) 非诱骗态方法, 三强度诱骗态方法和理想单光子源的成码率; (b) 各种方法对理想单光子源的相对成码率

Figure 4 Secure distance of the decoy-state method. (a) Key rates of simple protocol without using decoy state method, 3-intensity decoy state method, and key rate with perfect single-photon source; (b) relative key rates of different protocols to the key rate with perfect single photon source

授于 2005 年的理论研究 [14] 表明, 采用三强度随机切换的诱骗信号量子密码方案可以准确侦察出任何窃听行为, 包括所谓的光子数分离攻击, 并可立即实用于现有真实系统, 其中包含通道噪声, 大损耗等. 三强度诱骗信号方法可以让合法用户计算出至关重要的参量: 多光子脉冲份额的上限值. 有此上限值, 结合前人理论结果, 便可以获得绝对安全的最终码. 由该理论给出的关键计算公式, 诱骗态方法具有了立即的实用价值 (见图 4). 这也使得量子密钥分发有可能成为整个量子信息领域最先走入社会实用的分支.

诱骗态方法的首个实验由清华大学和中国科技大学等单位的联合团队完成 [28], 这也成为历史上首次超过 100 km 的安全量子密钥分发. 同一时期的实验还有美国橡树岭国家实验室与美国国家标准局团队的合作实验 [29]、维也纳大学等单位的实验 [30] 等. 此后, 中国科技大学结合光开关技术, 把诱骗态方法用于量子网络, 先后实现了 3 节点与 5 节点的量子网络安全通信 [4]. 迄今为止, 基于诱骗态方法的量子密钥分发已经至少获得世界主要研究机构近 20 个公开发表的在不同条件下的实验证实. 尽管诱骗态方法未必就是唯一方法 [31,32], 由于其安全性和实用性, 事实上, 诱骗态方法已经成为当前量子密码走向实际应用的最重要方法. 近年来, 中国科学家们致力于参与这一主战场的研究, 在实验与理论方面取得国际领先的广泛成果. 自清华 — 中科大联合团队 2007 年在国际上率先利用诱骗态手段实现了绝对安全距离超过一百公里的量子密钥分发 [28] 以来, 中国科技大学潘建伟小组又于 2010 年率先实现绝对安全距离达 200 km 的量子密钥分发 [3], 为目前国际上绝对安全量子密钥分发最远距离. 他们还采用光开关技术, 于 2008 年 10 月初完成了诱骗态量子密钥分发的 “光量子电话网”[4](此前国内外其他小组的量子密码网络的实验因为没有采用诱骗态方法而不安全). 清华大学王向斌小组则通过系统化的理论研究已经证明即便光源强度有较大涨落诱骗态方法依然有效, 给出了相关安全成码的计算公式 [7,33~38].

3.2 量子网络通信

辅以光开关技术后, 诱骗态方法还可用以实现量子通信网络. 由于没有量子存储器, 这种网络的量子密钥分发距离不能超越点对点的量子密钥分发距离. 然而, 网络上的任何两个用户可以通过光开

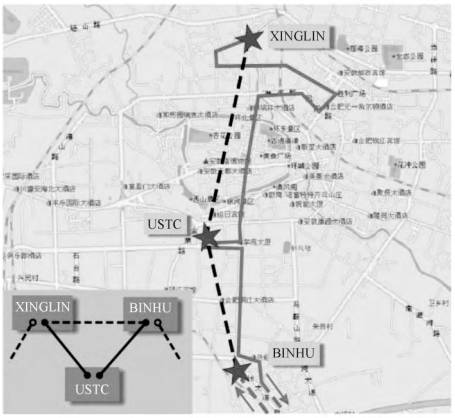

图 5　3 节点量子电话网

Figure 5　Three-node QKD network

表 1　链路主要参数

Table 1　Main parameters of the Link

Link	Communication wavelength	QBER	Sifted-key rate	Final key rate
Binhu-USTC	1550.12 nm	∼1.6%	>10.5 kbps	>1.6 kbps
USTC-Xinglin	1550.12 nm	∼1.4%	>9.0 kbps	>1.5 kbps

关切换实现量子密钥分发. 我国在 2009 年实现了 3 节点的链状量子通信网络 [4], 为世界上首个基于诱骗态方案的量子语音通信网络系统, 实现了实时网络通话和三方对讲功能, 演示了无条件安全的量子通信的可实用化. 此成果很快被美国《Science》杂志以 “量子电话” 为题进行了报道, 亦被欧洲物理学会《物理世界》以 “中国诞生量子网络” 为题做了专题报道. 随后, 又实现了 5 节点城域量子通信网络 [5], 是国际上首个全通型的量子通信网络, 各节点全部演示了安全的语音通信. 值得指出的是, 与欧洲 SECOQC 网络以及 Tokyo QKD network 不同, 这两个量子通信网络是基于诱骗态方案的成熟技术, 追求并逐步实现满足信息论定义下严格安全性要求的实用性, 而不是欧洲、美国和日本同行所做的多种技术的混合展示. 我国此类小规模的演示性网络还有多节点的城域量子政务网.

3.2.1　3 节点量子电话网

2008 年 10 月, 中国科学技术大学潘建伟组在合肥建成了一个基于可信中继方式的 3 节点量子电话网. 采用相位编码的诱骗态 BB84 方案. 网络结构如图 5 所示.

图 5 中实线为光纤量子信道, 虚线为经典信道. USTC 和 Binhu 以及 USTC 和 Xinglin 之间各建成了一套诱骗态 QKD. USTC 的节点同时充当了可信中继的角色. 原则上, 另两个节点也可以充当可信中继, 进一步扩展网络.

两条链路的量子信道光纤长度都在 20 km 左右, 最终成码率均大于 15 kbps, 如表 1 所示. 这个指标可以满足基于 “One Time Pad” 的保密电话需求.

该网络在国际上第一个实现了实时量子加密电话应用的网络, 时间上和 SECOQC 基本同步, 性能指标也基本上相同. 该网络的建成是量子通信一次最生动的应用展示, 使我国量子通信的应用水平一下子步入国际前列, 在世界上激起了很大的反响.

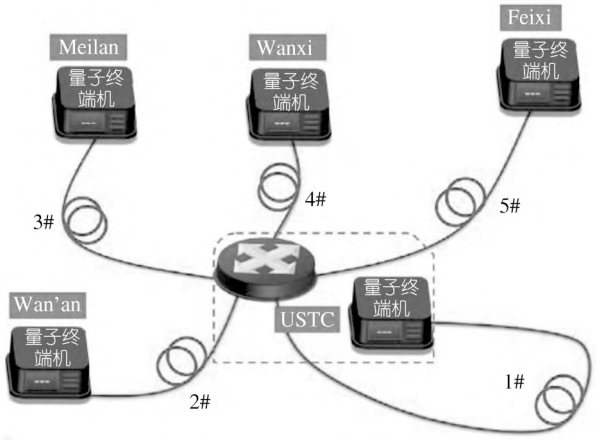

图 6 5 节点量子电话网

Figure 6 Five-node QKD network

表 2 链路主要参数

Table 2 Main parameters of the link

Link	Circle linke USTC	Wan'an	Meilan	Wanxi	Feixi
Distence(km)	10.047	8.447	9.904	8.417	60
Fiber loss(dB)	2.82	2.65	2.86	2.75	17

表 3 各节点安全成码率

Table 3 The safe final rate of various nodes

Para.	Meilan-USTC	USTC-Meilan	USTC-Wanxi	Wanxi-USTC	Wanxin-Wan'an
Sifted R	11.0k	9.74k	10.0k	8.02k	8.00k
Final R	1.45k	1.20k	1.95k	1.45k	1.30k
Para.	Wan'an-USTC	Meilan-Wanxi	Meilan-Wanxi	USTC-Wan'an	Wanxin-Meilan
Sifted R	8.33k	8.54k	9.39k	8.17k	7.97k
Final R	1.40k	1.43k	2.54k	1.82k	1.75k
Para.	Wan'an-Meilan	Wan'an-Wanxi	Fei-USTC		
Sifted R	7.33k	8.39k	18.0k		
Final R	1.40k	1.21k	4.50k		

3.2.2 5 节点量子电话网

2009 年 8 月, 中国科学技术大学潘建伟小组在合肥建成了一个星型 5 节点全通量子电话网络. 网络结构示意如图 6.

图 6 中所示 1#光纤长 10.047 km, 2#光纤长 8.447 km, 3#光纤长 9.904 km, 4#光纤长 8.417 km, 5#光纤长 60 km, 如表 2 所示.

该网络节点最短通信距离约为 17 km. 各节点安全成码率如表 3 所示.

从表 3 中可见, 该网络在通信距离为 20 km 时, 安全成码率最低, 仍可达 120 kbps. 因此该网络可实现基于 “One time pad” 的安全保密电话功能.

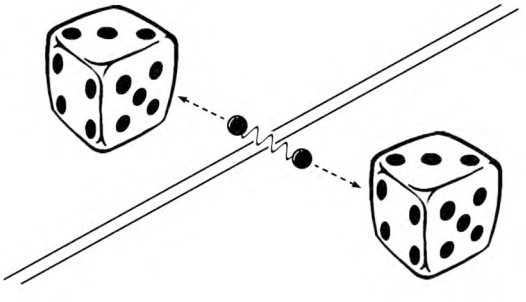

图 7　量子纠缠分发

Figure 7　Quantum entanglement distribution

该网络第一次实现了任意节点间实时互联互通的网络控制功能, 对于量子通信网络组网技术的成熟具有重要意义.

3.3　量子纠缠与量子通信

作为量子信息处理上最重要的资源之一, 量子纠缠在量子保密通信上的应用价值主要有两个方面: 一是直接基于纠缠分发可以实现共享量子密钥, 二是基于量子中继的远程量子通信的基础. 传统的量子纠缠态是指一种两光子态的线性叠加态.

$$|\Phi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle_1|\leftrightarrow\rangle_2 \pm |\updownarrow\rangle_1|\updownarrow\rangle_2),$$
$$|\Psi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle_1|\updownarrow\rangle_2 \pm |\updownarrow\rangle_1|\leftrightarrow\rangle_2).$$

由于两个光子可以位于空间不同地点, 纠缠光子对可以形成不同地域的非经典关联. 这种关联性可以直接用于共享密钥. 借助于不同地点预先共享纠缠光子对, 可以实现量子态隐形传输. 这也是基于量子中继的远程量子通信的基础技术. 量子纠缠对还可用于一类容错量子保密通信中 [38].

3.3.1　量子纠缠分发

所有基于纠缠的量子通信任务都需要通信双方预先共享量子纠缠态 (见图 7). 因此, 纠缠光子对分发技术是一切后续目标的基础. 光子对在偏振空间的纠缠态由于检测方式简单和各种其他的易操作性, 这种纠缠光子对具有特别重要的应用前景. 近年来, 这方面的实验研究十分活跃. 维也纳小组于 2003 年完成了 600 m 距离的自由空间偏振纠缠分发 [7]. 后来有其他欧美小组在光纤中实现了 1 km 的量子纠缠分发. 我国科学家于 2006 年完成了 13 km 距离的自由空间偏振纠缠分发 [8]. 其纠缠源来自基于 BBO 晶体的 II 型参量下转换. 在经过滤波片后每秒约产出 10000 个纠缠对, 波长为 702.2 nm, 后光路采用了大型望远镜系统进行接收探测. 此实验结果一个标志性的意义在于首次证实光子纠缠对分发距离可以超过与大气层等效衰减的距离. 这对尚在论证中的以卫星为中转站的洲际量子密钥分发的可行性无疑有着重要启示 [39]. 除了自由空间外, 纠缠光子对分发也在光纤中也成功实现了 [40~44]. 现今实用中的偏振纠缠对主要依靠下转换方法产生. 这是一种概率性纠缠源. 研究表明, 高品质确定性纠缠源是有可能的 [45].

3.3.2 量子态隐形传输

量子态隐形传输就是把量子信息从一个光子上转移到远处另外一个光子上而不必传输光子本身. 实现这一任务需要空间两处预先共享纠缠光子对, 在实施隐形态传输时还需在一个端点进行 Bell 测量, 之后依据此测量结果对另一个端点的偏振光子进行适当操作.

首个量子态隐形传输于 1997 年底在奥地利 Zeilinger 小组完成 [6]. 这项工作由 Bouwmeester 以及中国学者潘建伟等人基于下转换光子对以及分光镜的集体测量技术完成. 这项工作引起了全世界的广泛关注, 也使得全世界对量子信息的研究热潮空前高涨. 之后, 世界各国科学家对这一问题进行了更加广泛和深入的研究. 其中, 中国学者们在世界各地都取得了多项领先实验成果. 他们于 2003 年首次在室内实现了基本四光子的量子态隐形传输试验 [46], 使得量子态隐形传输能应用在更加广泛的量子通信和量子计算中. 2004 年, 在首次实现五光子纠缠的基础上, 又实现了一种更新颖的量子态隐形传输, 即终端开放的量子态隐形传输 [47], 为后继分布式量子信息处理做出了贡献. 2006 年, 首次实现了两光子复合系统的量子态隐形传输 [48]. 此前, 所有的量子态隐形传输实验都只能传输单个粒子的量子态, 而实现复合系统量子态隐形传输一直是个巨大的实验难题. 2010 年, 中国学者们在中国本土更实现了举世瞩目跨越长城的 16 km 距离的量子态隐形传输 [49]. 到 2012 年, 中国科学家们在青海湖地区已经实现了百公里量级的量子态隐形传输和量子密钥分发 [50], 这也是迄今为止真正量子纠缠分发的最远距离. 同 1997 年首个实验的厘米量级相比, 其进展在 10 多年前是根本不敢想象的. 这一成果将对远距离量子通信的实现产生深远影响.

量子态隐形传输技术可直接用于纠缠转换. 纠缠转换是量子中继的基本操作单元, 是可以用来克服远距离量子通信中的光子数损耗的最终手段 [51].

如图 8 所示, 通过对光束 4 和 2 的 Bell 测量, 在空间分离的光束 1 和 3, 形成纠缠光子对. 1998 年, 潘建伟等人首次实现了量子纠缠交换, 使得没有经过任何相互作用的两个光子产生了量子纠缠 [50,52]. 我们如果基于现有的远距离自由空间的量子传输技术, 实现同等距离量级的纠缠转换, 这将成为量子中继的重要基础.

3.3.3 量子纠缠纯化

纠缠是量子通信中的基本资源. 然而, 在纠缠分发过程中, 由于通道噪声, 远距离的共享纠缠光子对质量会有下降, 从而影响量子通信任务的实现. 纠缠对提纯理论结论是, 只要初始共享的纠缠对噪声低于一定水平, 就可以提炼出较少对的纯纠缠对, 对纯纠缠对在两端进行同一基矢测量即可获得绝对安全的密码. 最初的量子纠缠纯化方案需要用到受控非门, 但精确的受控非门无法用现有技术实现. 2001 年, 潘建伟等提出了无需受控非门的纠缠纯化理论方案 [9], 使得以现有技术实现纠缠纯化成为可能. 2003 年, 他们利用该方案成功实现了对任意纠缠态的纠缠纯化 [10] (图 9), 《Nature》杂志以封面论文的形式发表了该研究成果.

3.4 量子中继与远程量子通信及远程量子网络通信

目前采用诱骗态方法的最远实验距离是 200 km. 尽管随着检测技术的提高, 该距离还会进一步提高, 但是, 由于成码率随着距离呈指数衰减, 而单量子态信号又不能在中途放大, 因此, 基于经典相干态光源的诱骗态方法很难直接完成全球化量子通信任务.

远程量子通信的最终实现将依赖于量子中继 [17,18]. 其基本思想是: 在空间建立许多站点. 以量子纠缠分发技术先在各相邻站点间建立共享纠缠对, 以量子存储技术将纠缠对储存. 采用远距离自由空

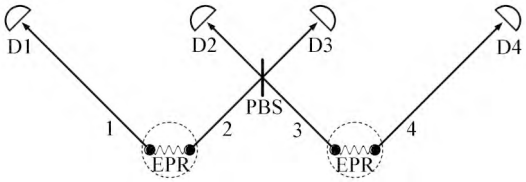

图 8　量子纠缠转换

Figure 8　Quantum entanglement swapping

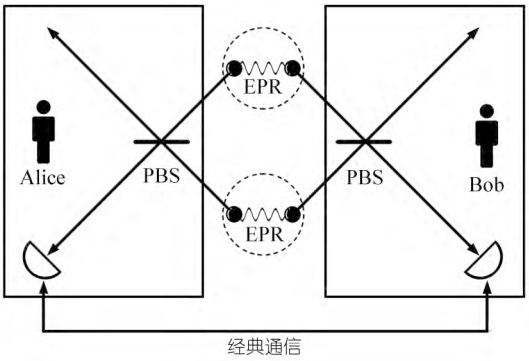

图 9　量子纠缠纯化

Figure 9　Entanglement purification

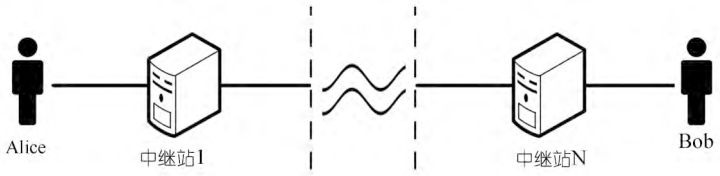

图 10　量子中继

Figure 10　Quantum repeaters

间传输技术实现量子纠缠转换, 即增长量子纠缠对的空间分隔距离. 如果预先将纠缠对布置在各相邻站点, 纠缠转换操作后便可实现次近邻站点间的共享纠缠. 继续操作下去, 原则上可以实现在很远的两个站点间建立共享纠缠. 即实现远距离量子通信.

量子中继与经典中继 (俗称 “可信中继”) 在安全性上是完全不一样的. 可信中继是通过中继把形成的密码 “接力” 下去. 它要求所有中继站都是安全的. 在通信双方跨越的中继站中只要有一个不安全, 则通信内容完全不安全. 而量子中继 (图 10) 的中继站只转换纠缠却看不到密码. 即便所有中继站都不安全, 两个通信终端间形成的密钥及以此为基础的通信仍然绝对安全.

如前文所述, 实现量子中继的几项基本技术组件, 量子纠缠分发, 量子纠缠转换已经获得 10 km 量级的实现, 这已经具备建立具有实际价值的量子中继站的要求. 要实现有意义的量子中继, 还需要能对量子纠缠态存储. 这项要求具有巨大挑战性, 实际上是量子中继的最关键技术. 2007 年, 潘建伟小组提出了具有存储功能并且对信道长度抖动不敏感、误码率低的高效率量子中继器的理论方案 [53]; 在此基础上, 2008 年, 该小组利用冷原子气体在国际上首次实现了具有存储和读出功能的量子中继器 [54], 建立了由 300 m 光纤连接的两个冷原子系综之间的量子纠缠. 这种冷原子系综之间的量子纠缠可以被读出并转化为光子纠缠, 以进行进一步的传输和量子操作.《Nature》杂志发布了题为 “量子推动” 的新闻稿, 称赞该工作 “扫除了量子通信中的一大绊脚石”, 并在网页上发布了题为 “量子密码可以走远了” 的报道. 同年底, 该成果入选欧洲物理学会评选的 “The best of 2008”. 2009 年, 清华大学小组提出了改进的方案 [55], 使得容错量子中继操作甚至无需校验光.

3.5　自由空间量子通信

自由空间量子通信是解决光子数信道损耗问题的另一有效途径. 研究表明, 利用低轨卫星和自由空间纠缠光子分发, 通过 “量子信号从地面上发射并穿透大气层 —— 卫星接收到量子信号并按需要

图 11 自由空间远程量子密钥分发

Figure 11 Long distance free-space quantum key distribution

将其转发到另一特定卫星 —— 量子信号从该特定卫星上再次穿透大气层到达地球某个角落的指定接收地点" 的方法 (图 11), 很有希望实现更远距离乃至全球化的量子通信. 由于量子信号的携带者光子在外层空间传播时几乎没有损耗, 如果能够在技术上实现纠缠光子在穿透整个大气层后仍然存活并保持其纠缠特性, 人们就可以在卫星的帮助下实现全球化的量子通信. 2005 年的 13 km 自由空间量子纠缠和量子密钥分发 [8], 和 2010 年的 16 km 远距离自由空间量子态隐形传输实验 [49], 2013 年实现的基于浮空平台, 利用了多项自动跟踪扫描对准技术的量子密钥分发实验 [50] 以及之前的量子纠缠实验 [56,57] 为星地量子通信打下了重要基础.

4 关键技术

现有的量子保密通信的物理实现方式大多基于单光子水平的弱相干光和纠缠光通信. 主要硬件技术包括弱相干光源和纠缠光源, 传输与检测. 在软体方面还包括最终码提炼 (编码) 技术. 衡量系统先进性的主要指标是产生安全最终码的成码能力. 系统每秒生成安全最终码正比于系统重复率与每脉冲成码率. 而每脉冲成码率除了受到误码率和损耗率的影响外, 还取决于提炼 (编码) 软体技术. 可以从提高光源编码质量, 通道传输, 以及同步检测, 探测器效率等方面来降低误码率. 此外, 对于无存储量子通信网络, 以光开关为代表的弱光传输路径的有效控制也是关键技术之一.

基于量子中继器的未来远程量子网络的技术基础包括光存储和两光子态的联合测量. 目前这两项技术都已经在实验室中获得实现 [6,10,46,54]. 然而, 量子关键器件的研发, 对量子通信网络实用化至关重要. 其中, 单光子探测系统是处于核心地位的量子关键器件, 其参数指标直接制约着量子通信系统的性能, 其性能提升对于量子通信系统起着基础性的作用, 目前较为前沿的有高速诱骗态光源技术、基于周期极化铌酸锂波导的上转换探测器技术、高速近红外单光子探测技术等.

5 总结与展望

经典保密通信的安全性未获数学证明. 借助量子特性可以实现严格数学证明的安全通信. 虽然以弱相干态为源的现有系统 [20,23~27] 对其所报告的密钥分发距离并不安全, 但我们仍然有其他办法用

现有技术实现绝对安全的量子密码系统, 例如诱骗态方法 [28~30]、纠缠对分发方法 [8] 等. 就未来而言, 理想单光子源或纠缠源技术的发展将会大大提高量子密码系统的效率与实用性能. 有了量子纠缠方法, 提炼、转换和存储为技术基础的量子中继技术将会最终实现任意远距离的安全量子通信及通信网络. 由于篇幅有限, 本文中有关量子通信的实现部分, 仅选择了部分基于线性光学的方法. 本文未涉及连续变量的量子通信 [58~60], 例如连续变量量子纠缠 [61~65]、连续变量量子隐型态传输 [66~70]、连续变量量子密钥分发等重要内容 [71~80]; 也未包含在量子通信上有重要潜在应用价的量子存储 [81~83]、指示单光子源诱骗态方法 [84,85] 等内容.

致谢 感谢中国科学技术大学彭承志研究员、印娟博士、济南量子技术研究院周飞博士、王晶晶以及清华大学周逸恒等对论文所提供的建议和帮助.

参考文献

1 Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems, and SignalProcessing, 1984
2 Bennett C H, Brassard G, Creacute C, et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys Rev Lett, 1993, 70: 1895–1899
3 Liu Y, Chen T Y, Wang J, et al. Decoy-state quantum key distribution with polarized photons over 200 km. Opt Express, 2010,18: 8587–8594
4 Chen T Y, Liang H, Liu Y, et al. Field test of a practical secure communication network with decoy-state quantum cryptography. Opt Express, 2009, 17: 6540–6549
5 Chen T Y, Wang J, Liang H, et al. Metropolitan all-pass and inter-city quantum communication network. Opt Express, 2010, 18: 27217–27225
6 Bouwmeester D, Pan J W, Mattle K, et al. Experimental quantum teleportation. Nature, 1997, 390: 575–579
7 Aspelmeyer M, Bohm H R, Gyatso T, et al. Long-distance free-space distribution of quantum entanglement. Science, 2003, 301: 621–623
8 Peng C Z, Yang T, Bao X H, et al. Experimental free-space distribution of entangled photon pairs over 13 km: towards satellite-based global quantum communication. Phys Rev Lett, 2005, 94: 150501–150504
9 PanJ W, Simon C, Brukner C, et al. Entanglement purification for quantum communication. Nature, 2001, 410: 1067–1070
10 Pan J W, Gasparoni S, Ursin R, et al. Experimental entanglement purification of arbitrary un-known states. Nature, 2003, 423: 417–422
11 Huttner B, Imoto N, Gisin N, et al. Quantum cryptography with coherent states. Phys Rev A, 1995, 51: 1863–1869
12 Brassard G, Lutkenhaus N, Mor T, et al. Limitations on practical quantum cryptography. Phys Rev Lett, 2000, 85: 1330–1333
13 Hwang W Y. Quantum key distribution with high loss: toward global secure communication. Phys Rev Lett, 2003, 91: 057901–057904
14 Wang X B. Beating the photon-number-splitting attack in practical quantum cryptography. Phys Rev Lett, 2005, 94: 230503–230508
15 Lo H K, Max F, Chen K. Decoy state quantum key distribution. Phys Rev Lett, 2005, 94: 230504–230509
16 Wang X B, Hiroshima T, Tomita A, et al. Quantum information with Gaussian states. Phys Rep, 2007, 448: 1–50
17 Duan L M, Lukin M D, Cirac J I, et al. Long-distance quantum communication with atomic ensembles and linear optics. Nature, 2001, 414: 413–418
18 Zhao B, Chen Z B, Chen Y A, et al. Robust creation of entanglement between remote memory qubits. Phys Rev Lett, 2007, 98: 240502–240506
19 Shannon C E. A mathematical theory of communication. Bell Syst Techn J, 1948, 27: 379–423, 623–656

20 Kimura T, Nambu Y, Hatanaka T, et al. Single-photon Interference over 150 km transmission using silica-based integrated-optic interferometers for quantum cryptography. Jpn J Appl Phys, 2004, 43: L1217–L1219

21 Mayers D. Unconditional security in quantum cryptography. JACM, 2001, 48: 351–406

22 Shor P W Preskill J Simple proof of security of the BB84 quantum key distribution protocol. Phys Rev Lett, 2000, 85: 441–444

23 Gobby C, Yuan Z L, Shields A J. Quantum key distribution over 122 km of standard telecom fiber. Appl Phys Lett, 2004, 84: 3762–3764

24 Yuan Z, Shields A. Continuous operation of a one-way quantum key distribution system over installed telecom fibre. Opt Express, 2005, 13: 660–664

25 Nambu Y, Hatanaka T, Nakamura K. BB84 quantum key distribution system based on silica-based planar lightwave circuits. Jpn J Appl Phys, 43: L1109–L1110

26 Hasegawa T. Experiments of quantum cryptosystem in 96 km installed fiber (in Japanese). In: Proceedings of the 2005 Symposium on Cryptography and Information Security 2F-3, 2005

27 Mo X F, Zhu B, Han Z F, et al. Faraday-Michelson system for quantum cryptography. Opt Lett, 2005, 30: 2632–2634

28 Peng C Z, Zhang J, Yang D, et al. Experimental long-distance decoy-state quantum key distribution based on polarization encoding. Phys Rev Lett, 2007, 98: 0105051–0105054

29 Rosenberg D, Harrington J W, Rice P R, et al. Long-distance decoy-state quantum key distribution in optical fiber. Phys Rev Lett, 2007, 98: 0105031–0105034

30 Manderbach T S, Weier H, Furst M, et al. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. Phys Rev Lett, 2007, 98: 0105041–0105044

31 Koashi M. Security of quantum key distribution with discrete rotational symmetry. arxiv: quant-ph/0507154

32 Scarani V, Acín A, Ribordy G, et al. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Phys Rev Lett, 2004, 92: 057901–057904

33 Wang X B, Peng C Z, Zhang J, et al. General theory of decoy-state quantum cryptography with source errors. Phys Rev A, 2008, 77: 042311–042415

34 Wang X B, Yang L, Peng C Z, et al. Decoy-state quantum key distribution with both source errors and statistical fluctuations. New J Phys, 2009, 11: 075006–075023

35 Wang X B, Peng C Z, Pan J W. Decoy-state quantum key distribution with both source errors and statistical fluctuations. Appl Phys Lett, 2007, 90: 075006–075023

36 Wang X B. Decoy-state quantum key distribution with large random errors of light intensity. Phys Rev A, 2007, 75: 052301–052305

37 Hu J Z, Wang X B. Reexamination of the decoy-state quantum key distribution with an unstable source. Phys Rev A, 2010, 82: 012331–012339

38 Wang X B. Quantum key distribution with two-qubit quantum codes. Phys Rev Lett, 2004, 92: 077902–077906

39 张军, 彭承志, 包小辉, 等. 量子密码实验新进展 ——13 km 自由空间纠缠光子分发: 朝向基于人造卫星的全球化量子通信物理 2005, 34: 701–707

40 Ribordy G, Brendel J, Gautier J D, et al. Long-distance entanglement-based quantum key distribution. Phys Rev A, 2000, 63: 012309–012321

41 Tittel W, Brendel J, Zbinden H, et al. Quantum cryptography using entangled photons in energy-time bell states. Phys Rev Lett, 2000, 84: 4737–4740

42 Dynes J F, Takesue H, Yuan Z L, et al. Efficient entanglement distribution over 200 kilometers. Opt Express, 2009, 14: 11440–11444

43 Jennewein T, Simon C, Weihs G, et al. Quantum cryptography with entangled photons. Phys Rev Lett, 2000, 84: 4729–4732

44 Naik D S, Peterson C G, White A G, et al. Entangled state quantum cryptography: eavesdropping on the ekert protocol. Phys Rev Lett, 2000, 84: 4733–4736

45 Wang X B, Yang C X, Liu Y B. On-demand entanglement source with polarization-dependent frequency shift. Appl Phys Lett, 2010, 96: 201103–201103

46 Pan J W, Gasparoni S, Aspelmeyer M, et al. Experimental realization of freely propagating teleported qubits. Nature, 2003, 421: 721–725

47 Zhao Z, Chen Y A, Zhang A N, et al. Experimental demonstration of five-photon entanglement and open-destination teleportation. Nature, 2004, 430: 54–58
48 Zhang Q, Goebel A, Wagenknecht C, et al. Experimental quantum teleportation of a two-qubit composite system. Nat Phys, 2006, 2: 678–682
49 Jin X M, Ren J G, Yang B, et al. Experimental free-space quantum teleportation. Nat Photon, 2010, 4: 376–381
50 Yin J, Ren J G, Lu H, et al. Quantum teleportation and entanglement distribution over 100-kilometre free-space channels. Nature, 2012, 488: 185–188
51 Zukowski M, Zeilinger A, Horne M A, et al. Event-ready-detectors Bell experiment via entanglement swapping. Phys Rev Lett, 1993, 71: 4287–4290
52 Pan J W, Bouwmeester D, Weinfurter H, et al. Experimental entanglement swapping: entangling photons that never interacte. Phys Rev Lett, 1998, 80: 3891–3896
53 Zhao B, Chen Z B, Chen Y A, et al. Robust creation of entanglement between remote memory qubits. Phys Rev Lett, 2007, 98: 240502–240506
54 Yuan Z S, Chen Y A, Zhao B, et al. Experimental demonstration of a BDCZ quantum repeater node. Nature, 2008, 454: 1098–1101
55 Gao M, Liang L M, Li C Z, et al. Robust quantum repeater with atomic ensembles against phase and polarization instability. Phys Rev A, 2009, 79: 042301–042305
56 Ursin R, Tiefenbacher R F, Schmitt-Manderbach T, et al. Entanglement-based quantum communication over 144 km. Nature Phys, 2007, 3: 481–486
57 Ursin R, Jennewein T, Kofler J, et al. Space-QUEST: Experiments with quantum entanglement in space. IAC Proceeding A2.1.3, 2008
58 Li X J, Pan Q, Jing J T, et al. Quantum dense coding exploiting a bright Einstein-Podolsky-Rosen beam. Phys Rev Lett, 2002 88: 047904–047907
59 Jing J T, Zhang J, Yan Y, et al. Experimental demonstration of tripartite entanglement and controlled dense coding for continuous variables. Phys Rev Lett, 2003, 90: 167903–167906
60 Jia X J, Su X L, Pan Q, et al. Experimental demonstration of unconditional entanglement swapping for continuous variables. Phys Rev Lett, 2004, 93: 250503–250506
61 Su X L, Tan A H, Jia X J, et al. Experimental preparation of quadripartite cluster and Greenberger-Horne-Zeilinger entangled states for continuous variables. Phys Rev Lett, 2007, 98: 070502–070506
62 Ou Z Y, Pereira S F, Kimbh H J, et al. Realization of the Einstein-Podolsky-Rosen paradox for continuous variables. Phys Rev Lett, 1992, 68: 3663–3693
63 Braunstein S L, van Loock P. Quantum information with continuous variables II. Rev Mod Phys, 2005, 77: 513–515
64 Wang X B, Hiroshima T, Tomita A, et al. Quantum information with Gaussian states. Phys Rep, 2007, 448: 1–111
65 彭堃墀, 苏晓龙, 贾晓军, 等. 连续波单共振光学参量振荡器的研究及进展. 山西大学学报, 2012, 35: 231–243
66 Furusaw A, Sorensen J L, Braustein S L, et al. Unconditional quantum teleportation. Science, 1998, 282: 706–709
67 Yonezawa H, Aoki T, Furusawa A, et al. Demonstration of a quantum teleportation network for continuous variables. Nature, 2004, 431: 430-433
68 Wang Y, Su X L, Shen H, et al. Toward demonstrating controlled-X operation based on continuous-variable four-partite cluster states and quantum teleporters. Phys Rev A, 2010, 81: 022311–022314
69 Zhang J, Peng K C. Quantum teleportation and dense coding by means of bright amplitude-squeezed light and direct measurement of a Bell state. Phys Rev A, 2000, 62: 064302–064306
70 Loock V P, Braunstein S L. Multipartite entanglement for continuous variables: a quantum teleportation network. Phys Rev Lett, 2000, 84: 3482–3485
71 Su X L,Wang W Z, Wang Y, et al. Continuous variable quantum key distribution based on optical entangled states without signal modulation. Europhys Lett, 2009, 87: 20005–20006
72 Silberhorn C, Ralph T C, Lutkenhaus N, et al. Continuous variable quantum cryptography: beating the 3 dB loss limit. Phys Rev Lett, 2002, 89: 167901–167903
73 Hillery M. Quantum cryptography with squeezed states. Phys Rev A, 2000, 61: 022309–022311
74 Reid M D. Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations. Phys Rev A, 2000, 62: 062308–062311

75 Silberhorn C, Korolkova N, Leuehs G. Quantum key distribution with bright entangled beams. Phys Rev Lett, 2002, 88: 1679021–1679024
76 Grosshans F, Assche G V, Wenger J, et al. Quantum key distribution using gaussian-modulated coherent states. Nature, 2003, 421: 238–241
77 Lorenz S, Korolkoca N, Leuehs G. Continuous-variable quantum key distribution using polarization encoding and post selection. Appl Phys B, 2004, 79: 273–278
78 Lance A M, Symul T, Sharma V, et al. No-switching quantum key distribution using broadband modulated coherent light. Phys Rev Lett, 2005, 95: 180503–180505
79 Su X L, Jing J T, Pan Q, et al. Dense-coding quantum key distribution based on continuous-variable entanglement. Phys Rev A, 2006, 74: 062305–062314
80 Leverrier A, Grangier P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. Phys Rev Lett, 2009, 102: 180504–180507
81 Clausen C, Félix B, Mikael A, et al. Quantum storage of heralded polarization qubits in birefringent and anisotropically absorbing materials. Phys Rev Lett, 2012, 108: 190503–190505
82 Mustafa G, Patrick M, Attaallah A, et al. Quantum storage of a photonic polarization qubit in a solid. Phys Rev Lett, 2012, 108: 1905041–1905045
83 Zhou Z Q, Ling W B, Yang M, et al. Realization of reliable solid-state quantum memory for photonic polarization qubit. Phys Rev Lett, 2012, 108: 190505–190507
84 Wang Q, Chen W, Guilherme X, et al. Experimental decoy-state quantum key distribution with a sub-poissionian heralded single-photon source. Phys Rev Lett, 2008, 100: 090501–090506
85 Krapick S, Stefszky M S, Jachura M, et al. Bright integrated photon-pair source for practical passive decoy-state quantum key distribution. Phys Rev A, 2014, 89: 012329–012331

Quantum communication: status and prospects

WU Hua[1], WANG XiangBin[2,3,4*] & PAN JianWei[1,3]

1 *School of Public Affairs, University of Science and Technology of China, Hefei* 230026*, China;*
2 *State Key Laboratory of Low-Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing* 100084*, China;*
3 *Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei* 230026*, China;*
4 *Jinan Institute of Quantum Technology, Jinan* 250101*, China*
*E-mail: wang_xiangbin@hotmail.com

Abstract The paper overviews the fundamental principles, methods, technologies and applications of quantum communication. It introduces the basic protocol of secure quantum private communication, including the decoy method, quantum communication based on the entanglement distribution, quantum teleportation, manipulation of entangled photonspairs in polarization space. This review introduces recent status in quantum technology and applications, and attempts to discuss future directions in which the field is likely to develop.

Keywords quantum communication, quantum key distribution, protocol BB84, decoy state method, quantum teleportation, the manipulation of entangled photons, quantum networks