特约专稿

量子密码实验新进展
——13km 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*

张 军　彭承志　包小辉　杨 涛　潘建伟†
（中国科学技术大学近代物理系　合肥微尺度物质科学国家实验室　合肥　230026）

摘　要　实验实现了纠缠光子对通过地面大气 13km 的自由空间分发. 实验表明,纠缠光子在通过超过大气层等效厚度的距离之后,纠缠特性依然能够很好保持. 文章作者观测了类空间隔 Bell – CHSH 不等式的破坏,其 S 值达到 2.45 ± 0.09. 在这个基础上,我们利用分发的纠缠光子对演示了 BB84 – Ekert91 量子密码协议. 这个实验第一次验证了用纠缠光子对进行地面和卫星量子通信的可行性,为未来的基于人造卫星全球化量子通信打下坚实的基础. 文章将首先回顾量子密码实验方面的最新进展,然后再详细介绍作者的实验.

关键词　纠缠,Bell 不等式,量子密码

New progress on experimental quantum cryptography
—— experimental free-space distribution of entangled photon pairs over 13km

ZHANG Jun　PENG Cheng-Zhi　BAO Xiao-Hui　YANG Tao　PAN Jian-Wei†
(*Department of Modern Physics and Hefei National Laboratory for Physical Sciences at Microscale, University of Science and Technology of China, Hefei* 230026, *China*)

Abstract　We have experimentally realised free-space distribution of entangled photon pairs through a noisy ground atmosphere of 13km. It is shown that the desired entanglement can still survive after both photons have traversed a distance beyond the effective thickness of the aerosphere. We observe a spacelike separated violation of the Bell-Clauser-Horne-Shimony inequality of 2.45 ± 0.09. With this source we have demonstrated the BB84-Ekert91 quantum cryptography protocol. Our experiment has shown for the first time the feasibility of using entangled photons for ground-to-satellite quantum communication, and presents a significant step towards satellite-based global quantum communication in the future. We first review the rapid progress in quantum cryptography over recent years and then describe our experiment in detail.

Keywords　entanglement, Bell inequality, quantum cryptography

1　量子密码简介

20 世纪最主要的革命性科学成果包括:相对论、量子力学、信息理论,相对论的成就已经得到公认,而最近几十年量子力学和信息科学相结合,诞生了一门崭新的学科——量子信息学[1,2],包括量子通信和量子计算两个部分. 量子信息学中发展速度最快的分支学科就是由量子力学基本原理保证安全性的密码通信即量子密码[更精确地,应该称之为量子密钥分发(quantum key distribution),不过使用

* 国家自然科学基金(批准号:10304016)、中国科学院知识创新工程和国家重点基础研究发展计划(批准号:2001CB309303)资助项目
2005 – 07 – 08 收到

† 通讯联系人. Email:pan@ustc.edu.cn

“量子密码”(quantum cryptography)这个众所周知的术语并不妨碍我们的描述,在下文中我们将始终使用这个名词][3],这个量子力学奇特的性质可以简单的表述为:不可能进行不扰动系统的测量.在经典密码系统中,非对称的公钥密码系统例如 RSA、RC5 等其安全性是基于大数因子分解,然而 Shor 算法[4]表明,量子计算机的诞生将彻底打破这些系统的安全性,相比较而言,对称性的私钥密码系统如 DES,AES,IDEA 等比公钥系统成本更低、速度更快,但是存在着分发密钥容易被窃听的问题.解决这些问题的方法就是采用量子密钥分发的手段以及利用 Vernam 密码[5]即一次性(one - time pad)密码进行加密和解密,也就是量子密码系统.近些年来,量子密码的理论、实验、实用化方面发展非常迅速,甚至已经有相关的量子密码产品问世,可以毫不夸张地说,量子密码是量子信息中第一个可以进行商业化应用并有可能改变未来安全通信方式的领域.

量子密码的第一个协议是在 1984 年的一次 IEEE 会议上由 Bennett 和 Brassard 提出,通常称之为 BB84 协议[6],我们简单介绍其原理过程:协议使用二能级系统的两套基矢四个量子态例如光子的极化态$|H\rangle$、$|V\rangle$以及$|+\rangle$、$|-\rangle$来实现,其中的两种量子态如$|H\rangle$、$|+\rangle$编码为“0”而另外两种为“1”;作为通信双方之一的 Alice 随机发送量子态给 Bob,而 Bob 也随机选择 HV 或 $+-$ 测量基矢;很明显,只有双方采用相同基矢他们才会获得相关的结果,通信完毕后,Bob 获得大量的原始密钥(raw key),然后 Bob 通过经典信道公开自己的测量基矢,而 Alice 获得 Bob 测量信息后也公开自己是否采用和 Bob 相同的基矢,双方仅仅保留基矢相同的密钥,通常称之为筛选密钥(sifted key);进一步地,双方可以通过经典密码系统的纠错(error correction)、隐私放大(privacy amplification)等技术降低密钥的错误率,提高密钥的安全性.BB84 协议刚提出时并没有得到重视,但是在最近十年却极大的促进了量子密码理论和实验方面的发展,成为整个量子密码领域的基石.另外,关于 BB84 协议的安全性,已经有人给出证明[7,8].除了 BB84 协议外,其他的量子密码协议有:两态协议(two - state protocol)[9]、六态协议(six - state protocol)[10,11]、基于纠缠光子的 Ekert91 协议[12]、多种 BB84 变种协议以及最近有人提出的差分相移协议(differential phase shift protocol)[13]等.从目前通过光学手段实现的一系列量子密码实验来看,实验中所采用的源主要有单光子源(或者称为弱激光脉冲源)和纠缠光子源两种,通信信道主要是光纤信道或者自由空间信道,编码方式有极化编码、相位编码、频率编码等多种方式.下面我们将介绍近些年来比较具有代表性和重要性的量子密码实验,并对不同实现方式的优点和缺点进行说明.

量子密码的第一个演示性实验是由 Bennett 等人在 1989 年完成的(文章是在 1992 年发表)[14],从那以后,国际上很多小组开始这方面的工作,主要实现的手段也是以光子作为载体,这是因为一方面光子和环境的相互作用——退相干(decoherence)比较容易控制,另一方面,可以利用传统光通信的相关器件、技术、工具等,这也是量子密码最先使用光纤信道的主要原因.第一个极化编码光纤量子密码实验是由日内瓦大学 Gisin 小组在 1993 年完成的[15],距离达到 1km,所采用的单模光纤截止波长为 800nm(这里需要说明一下,800nm 波长又被称作第一通信波长,因为这是光通信历史上最早采用的波长,这个波长最大的好处就是有成熟的光源和探测器技术,但是其致命的缺点就是光纤衰减大,所以现在的长程光通信波长一般选择衰减更小的 1300nm 或者 1550nm 波长,通常称之为第二、第三通信波长).实际上这个波长更适合于通过非线性晶体自发参量下转换技术(spontaneous parametric down conversion)[16]产生的极化纠缠光子对(polarization entanglement photon pairs)的光纤量子密码,实际上,这个实验直到 2000 年才由奥地利 Zeilinger 小组完成[17].相比于第一通信波长,更多的光纤量子密码实验是在 1300 或 1550nm 通信波长(习惯上,这两个波长简称为通信波长)完成的.而同样地,第一个基于极化编码的通信波长量子密码实验也是由 Gisin 小组在 1996 年通过日内瓦湖底的光纤完成的[18,19],距离为 23km.从此,大量利用不同手段和技术的通信波长量子密码实验相继开始展开,如爱尔兰 Townsend 小组利用被动光纤网络实现的多用户量子密码[20]、利用光纤多路复用技术实现的量子密钥和经典数据同步传输[21]等等.除了极化编码,在光纤中经常采用的是另外一种编码方式是相位编码.相位编码的概念最初是由 Bennett 在 1992 年两态协议的文章中提出的[9],其基本思想是态制备和态测量都是在干涉仪中完成,不同的相位对应不同的编码.此后,更多的相位编码方案相继提出如双 Mach - Zehnder 干涉仪(double Mach - Zehnder interferometer)[22]、即插即用系统(plug - and - play system)[23]、基于能量 - 时间纠缠(energy - time entan-

glement)[24]相位编码及相位 - 时间编码(phase - time coding)[25]等等,相位同步和系统稳定性是相位编码最大的障碍. 值得一提的是,最近 Gisin 小组的即插即用光纤量子密码系统已经把光纤长度提高到 67km[26],这也是目前量子密码领域里唯一产品化的方案.

但是光纤也存在很大的缺陷,最主要因素就是单模光纤中的双折射效应以及光纤损耗. 光纤中心附近存在的应力分布以及光纤几何的非对称将会使得光纤中传输的两个正交极化态的光子产生不同的相速度也就是双折射效应,这种效应在光纤工程中经常被有意制造成特殊功能的光纤如保偏光纤(polarization - maintaining fiber),但这种保偏光纤并不能解决光纤双折射引起的对光纤量子密码影响最大的极化模式色散(polarization mode dispersion)效应,因为保偏光纤只能保持某个特殊方向的极化而不是任意极化方向. 简单地说,就是光纤中不同极化模式具有不同的传输速度,从而通过光纤的传输时间不同,出射的极化态和入射的极化态也不完全相同. 这里需要特别提到一下的是,虽然由于单模光纤的种种原因使其不利于基于极化纠缠光子对的量子密码,但最近加拿大滑铁卢大学的 Laflamme 小组提出利用极化模式的时间延迟方法来克服单模光纤双折射效应引起的退相干[27],我们小组已经完成了这个方案的实验演示并获得重要的结果. 当然,除了极化模式色散效应,单模光纤中还存在着其他次要的非对称效应如几何相位(geometric phase)、极化相关损耗(polarization - dependent loss)等,这些效应对光纤量子密码影响不是很大. 在实验中光纤这些双折射效应是通过自补偿装置(self - compensating configurations)来消除的,如前面提到的 Gisin 小组的即插即用系统就是用法拉第镜(Faraday mirror)来被动补偿光纤极化波动从而提高系统稳定性. 另一方面,虽然通信波长的光纤比 800nm 波长的光纤衰减要小得多,但是光纤衰减对长距离光纤量子密码还是有着本质的影响,由于背景噪声、探测器技术、单光子源或者纠缠光子源的不完美性等原因限制了光纤信道的通信距离,最大距离大约在 100km 左右. 事实上,由于纠缠光子源的亮度限制使其很难用来作为长距离光纤通信,单光子源是比较现实的方案,但是为了防止如光子数攻击(photon number splitter attack)等窃听策略其每脉冲平均光子数(mean photon number)不能太高,同时目前探测器探测效率的不完美导致长距离光纤量子密码的密钥生成速度很难达到理想要求,目前光纤量子密码的光纤最远距离是 122km[28],是由 Toshiba 欧洲研究中心在 2004 年完成的.

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,量子中继器(quantum repeater)和自由空间量子密码(free space quantum cryptography)是两种比较可行的方案. 量子中继器方案[29]包括纠缠制备(entanglement preparation)、纠缠交换(entanglement swapping)[30]、纠缠纯化(entanglement purification)[31]、量子存储器(quantum memory)等部分,利用这个方案可以在遥远两地制备高品质的纠缠态,从而可以用于量子通信. 近些来年,这方面的实验进展非常迅速,特别是在 2003 年,我们小组完成了量子中继器的实验演示[32]. 另外一种解决长距离光纤通信问题的方法是基于人造卫星的自由空间量子密钥分发,其基本思想是,在地面上制备好单光子源或者纠缠光子源,通过望远镜装置发送到人造卫星上,然后反射到其他卫星或者地面的其他地点,从而完成自由空间信道的建立. 实际上,由于整个大气层厚度衰减等效于地面大气长度只有 5km 左右,而在外太空的衰减基本可以忽略不计,所以如果纠缠光子在地面大气分发距离能够超过 10km 的话(这里的意思是指通过 10km 距离以后依然能够在有限时间内获得令人满意的纠缠光子对数量),那么理论上地面和卫星之间的量子通信是完全可行的,从而未来的全球化量子通信的可行性得到验证. 自由空间信道的另外一个重要的优势是大气中本质上不存在双折射效应,同时大气传输损耗曲线表明在纠缠光子波长范围内(目前实验上纠缠光子的波长均在 700—800nm 内)信道的传输损耗是相当小的,另外这个波长范围内成熟的探测器技术、弱色散效应等都给自由空间量子密码实验带来便利的条件. 但是,背景光噪声(background lights noise)、大气扰动(atmospheric turbulence)带来的到达时间偏差(arrival - time jitter)和光斑晃动(beam wander)光斑发散(beam divergence)、天气能见度(weather visibility)、信号同步等等多种因素将会给自由空间信道量子密码带来一系列问题,后面我们还会详细的讨论.

在自由空间量子密码实验方面,目前国际上有多个小组开展这方面的工作,如美国 Los Alamos 国家实验室的 Hughes 小组、英国 Bristol 大学的 Rarity 小组、德国慕尼黑大学的 Weinfurter 小组、奥地利维也纳大学的 Zeilinger 小组、中国科学技术的潘建伟

小组等等. 自由空间量子密码实验最早是由 Hughes 小组在 2000 年完成[33]，距离为 1.6km，采用单光子源方案. 实际上在 2003 年 Zeilinger 小组完成 600m 自由空间纠缠光子分发[34] 之前的所有自由空间实验中包括 2001 年 Rarity 小组的 1.9km 自由空间密码[35]、2002 年 Hughes 小组 10km 白天自由空间量子密码[36]、2002 年 Weinfurther 小组的 23.4km 自由空间量子密码[37]（这也是目前自由空间量子密码最远距离）等等都是采用单光子源的方案. 而在我们的实验中[38]，利用信号同步技术、自行设计参数的望远镜系统、高亮度纠缠光子源等优势，完成了通过地面大气 13km 的自由空间纠缠光子分发，这也是目前自由空间纠缠光子分发的最远距离，实验表明，纠缠光子在通过超过大气层等效厚度的距离之后，纠缠特性依然能够很好保持. 另外，我们观测了类空间隔 Bell－CHSH 不等式的破坏，在这个基础上，我们利用分发的纠缠光子对演示了纠缠光子对 BB84 协议——Ekert91 量子密码协议. 这个实验第一次验证了地面和卫星进行量子通信的可行性，为未来的基于人造卫星全球化量子通信打下坚实的基础. 下面我们来详细说明这个实验.

2　13km 自由空间纠缠光子分发实验

如图 1 所示，实验中纠缠源地点选择在合肥市西郊海拔 281m 的大蜀山顶安徽电视台发射塔下，两个接收者 Alice 和 Bob 分别坐落在离纠缠源 7.7km，5.3km 的中国科学技术大学西校区和肥西县桃花镇，纠缠光子对中的一个光子通道通过了合肥市区上空，受到城市环境如空气污染、背景光等的严重影响，而另外一个通道由于在城市郊区，所以环境的影响相对来说要小一点. 两个接收者的直线距离是 10.5km，由于建筑物的阻挡，两个接收端无法相互目视可见.

在发送端，我们使用 351.1nm 波长的氩离子激光器产生的激光，通过非线性晶体——BBO（beta－barium－borate）晶体，利用 II 型参量下转换技术产生极化纠缠光子对. 当激光器功率为 300mW 时，在单光子探测器前面加 2.8nm 相干滤波片（interference filter）的情况下可以获得大约每秒 10,000 对 702.2nm 波长的纠缠光子.

为了获得更好的通信信道的传输效率以及信道系统稳定性，我们自行设计了两套传输系统，共包括 4 个相同的大型折射式望远镜. 每个望远镜的长度

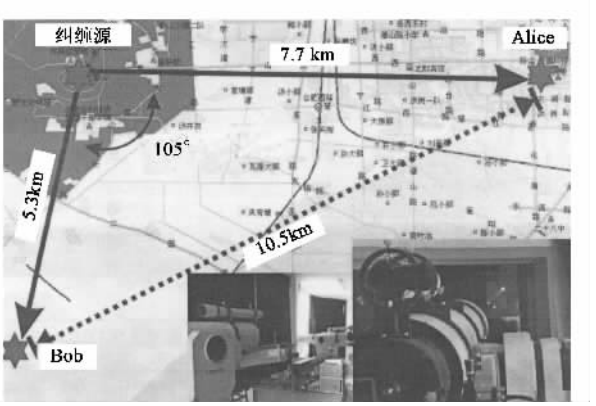

图 1　实验地点示意图（实验中纠缠源的地点我们选择在合肥市西郊大蜀山顶安徽电视台发射塔下面. 通信双方之一的 Alice 选择在中国科学技术大学西校区，而 Bob 选择在肥西县桃花镇. 纠缠光子通过了城市上空大气噪声环境，受到空气污染以及背景光的严重影响，在接收端没有加相干滤波片时夜晚的背景光计数依然能够达到大约每秒钟 30,000 个. 左边的插图为发送端照片，右边的插图为 Alice 端在夜间拍摄到的来自发送端的对准激光和同步激光的照片）

为 3.4m，高度为 1.7m，重量为 800kg，移动精确度为 0.1 角秒，焦距可达 2m，同时每台望远镜配备一个小型望远镜，以便定位以及多个目镜以获得不同的聚焦效果. 望远镜的主要重量集中在底座上，从而保证了地面上望远镜的稳定性，而如果望远镜安装在卫星上，这种底座是不需要的. 望远镜内部的每块镜片均镀了一层膜，使得在纠缠光子波长 702.2nm 的透过率最大，每两个望远镜之间也就是每套传输系统的整体光学传输效率可以达到 70%. 实验期间，大蜀山顶的恶劣环境尤其是长年累月的大风给实验带来巨大的困难，当然我们采取了许多相应的措施来克服这些困难，例如建造两个特别的窗户来降低大风对发射望远镜稳定性的影响等等.

发送端的纠缠光子收集到两根单模光纤（single－mode fiber）中并分别连接到两个发送望远镜，由于光纤中存在着前面我们提到的极化模式色散效应影响光子的极化方向，所以在纠缠光子扩束发射之前需要我们利用波片组成的极化控制器（polarization controller）进行极化补偿，并把单模光纤固定起来. 因为自由空间信道的距离较远，光斑的发散和晃动较大，接收端的光斑位置会随机地变化，从而降低收集效率，所以我们利用发送端的望远镜把发射光斑直径扩束到 12cm 以后再发送，同样地，在接收端利用一个完全一样的望远镜进行接收，经过聚焦以及光学测量系统以后纠缠光子耦合到 62.5μm 直径的多模光纤（multimode fiber）并进入单光子探测器

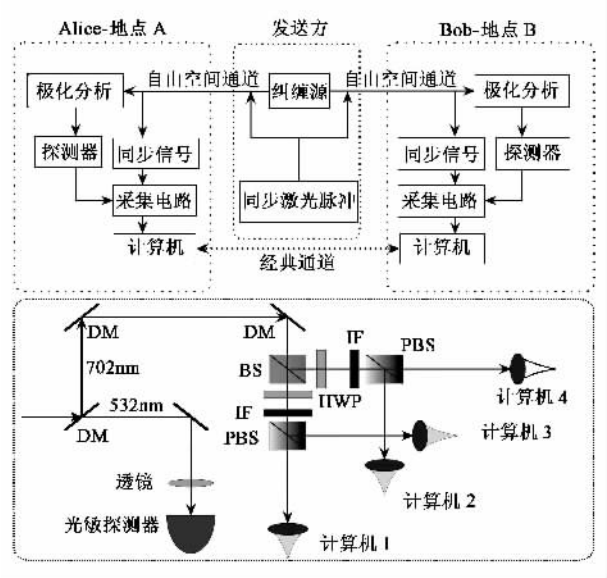

图 2　实验方框图以及接收端光学示意图(在纠缠源发送端,我们首先把纠缠光和同步脉冲激光光束通过双色镜片耦合到一起,并利用望远镜系统分别分发到两个接收端. 在接收端,类似地,用双色镜片把不同的波长的光束即纠缠光和同步脉冲激光分开. 其中 532nm 的同步脉冲激光通过反射镜和透镜耦合到光敏接收器上,把同步脉冲转化为幅度正比于能量的电信号,这个周期性的同步脉冲经过恒比定时器后的信号作为整个后端数据采集系统的触发信号. 另一方面,纠缠光进入单光子极化分析系统,分束器用作基矢的随机选择,半波片和极化分束器进行极化测量. 在极化分束器前面加入 2 个 2.8nm 相干滤波片是为了降低背景光的计数. 两个极化分束器分出的 4 个通道的光子通过耦合装置收集到多模光纤中并进入单光子探测器测量,探测器的输出信号进入数据采集系统. 数据采集系统通过 USB2.0 接口连接计算机,两个接收端的计算机通过经典通信方式进行数据的离线软件处理)

(single photon detector). 通过种种努力,我们可以使得整个系统稳定工作数个小时. 在图 1 的右边插图中,我们可以看到非常清晰明亮的来自发送端的对准激光光束和同步激光光束.

由于发送端到两个接收端的距离不等,所以纠缠光子到达接收端的飞行时间不同,同时由于空气扰动的原因导致光子到达时间存在晃动(时间晃动为 ΔT),为了更好地符合两个接收端的探测事件,必须要求符合时间窗口(coincident time window)大于时间晃动 ΔT. 但是如果为了获得足够的符合计数而增大符合时间的话,会导致偶然符合(accidental coincident)事例增多,从而影响了纠缠光子的对比度. 一般地,为了解决这种远程符合问题,通常有三种方法. 第一种是电缆延迟符合. 就是把 Alice(或者 Bob)的探测器信号通过电缆(或者中间可以利用放大器进行中继)拉到 Bob 处和 Bob 的探测器信号进行符合,当然,Bob 的信号也需要一定的延迟以便两个接收端信号对齐符合,Bob 的延迟可以通过光子飞行时间的差值以及 Alice 的电缆长度进行计算. 这种方法的优点就是简单、方便,适合于短距离的符合,但是缺点就是笨重,架设工程浩大,尤其在城市中操作起来更是相当麻烦. 实际上,Zeilinger 小组在 2003 年的 600m 纠缠光子分发的实验中[34],采用的就是这种远程符合方法. 第二种方法是采用原子钟同步,就是说 Alice 和 Bob 两端分别记录光子探测事件的精确时间,并进行软件比较,在合适符合窗口出现的两个事例就可以认为是纠缠光子的符合事例. 这种方法的最大优点就是精度非常高,但是这也导致了原子钟同步的高成本、需要初始化同步等问题. 第三种方法就是我们采用的这种激光脉冲同步的方法,如图 2 所示,我们利用一个 532nm 波长的调 Q 激光器(Q - switched laser)脉冲分成两份,并分别和纠缠光子耦合到一起,再通过望远镜发送给接收端. 这样同步激光脉冲和纠缠光子飞行相同的距离,在接收端,我们测量每个单光子探测事例和相应的同步脉冲信号的时间差,通过经典通信以及软件分析,如果 Alice 和 Bob 两端事例相对各自同步脉冲信号时间差的差值在符合时间窗口之内的话,我们可以认为这两个事例是好符合事例,也就是这两个光子是纠缠光子. 实验中,考虑到有多种因素会造成时间晃动,我们把符合时间窗口设定为 20ns 左右.

在接收端,如图 2 所示,首先用双色镜片(dichroic mirror)把在发送端同样用双色镜片耦合的不同波长的光束即纠缠光和同步脉冲激光分开. 其中 532nm 的同步激光脉冲通过反射镜和透镜耦合到光敏接收器(photon receiver)上,把同步脉冲转化为幅度正比于能量的电信号,这个周期性的同步脉冲经过恒比定时器(constant fraction discriminator)后的信号作为整个后端数据采集系统的触发(trigger)信号,这里需要说明的是,在 Alice 端,由于距离较远而且由于城市空气污染等原因,使得同步激光脉冲的衰减比 Bob 端大很多,所以 Alice 端的光敏接收器信号是经过一个放大器后才进入恒比定时器的,而 Bob 端则不需要放大器. 另一方面,双色镜片分开的另一路纠缠光进入单光子极化分析系统,分束器(beam splitter)用作基矢的随机选择,半波片(half wave plate)和极化分束器(polarization beam splitter)进行极化测量. 两个极化分束器分出的 4 个通道的光子分别通过相同的耦合装置(coupler)收集到多

模光纤(multi mode fiber)中并进入单光子探测器测量,探测器的输出信号进入数据采集系统. 数据采集系统通过 USB(universal serial bus)2.0 接口连接计算机,两个接收端的计算机通过经典通信方式进行数据的离线软件处理(offline software process).

为了降低背景光计数,实验时间一般都选择在晚上进行,同时每个接收端都加了两个 2.8nm 的相干滤波片,这样背景光计数一般可以降低到每秒钟 400 个左右. 在天气能见度很好的情况下(大于 15 km),在 Bob 端的单光子计数率大约为每秒 40,000 个而 Alice 端只有大约每秒 18,000 个,符合计数率大约为每秒 300 个. 而在正常的能见度条件下(10km 左右),符合计数率大约可以达到每秒 150 个左右.

在发送端的纠缠态可以写成如下形式:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B), \quad (1)$$

其中 A,B 分别代表发送到 Alice 端和 Bob 端的光子,H,V 代表光子的水平极化(horizontal polarization)和垂直极化(vertical polarization). 纠缠源的本身对比度(也就是发送前)在 HV 基矢下可以达到 98%,而在 +45°/ −45°基矢下可以达到 94%. 而在两个接收端获得的纠缠光子中,如图 3 所示,在 HV 基矢和 +45°/ −45°基矢下的对比度分别为 94% 和 89%,平均对比度为 91%,远远高于破坏 Bell 不等式[39]所要求的 71% 的对比度. 为了进一步验证我们获得的纠缠光子的品质,我们测量了 Bell 不等式的一种特殊形式——CHSH 不等式(clauser − horne − shimony − holt inequality)[40]. 其中极化相关系数定义如下:

$$E(\phi_A,\phi_B) = \frac{N_{++} + N_{--} - N_{+-} - N_{-+}}{N_{++} + N_{--} + N_{+-} + N_{-+}}, \quad (2)$$

其中 $N_{ij}(\phi_A,\phi_B)$ 代表了 Alice 的第 i 通道的极化角度为 ϕ_A 和 Bob 第 j 个通道极化角度为 ϕ_B 的符合计数. 在 CHSH 不等式中,其参量 S 值定义为

$$S = |E(\phi_A,\phi_B) - E(\phi_A,\phi_B') + E(\phi_A',\phi_B) + E(\phi_A',\phi_B')|. \quad (3)$$

从局域实在(local realistic)观点来看,不论 ϕ_A 和 ϕ_B 设成什么角度,值总是小于 2 的. 但是量子力学认为,S 值可以大于 2,尤其当 4 个角度 $(\phi_A,\phi_A',\phi_B',\phi_B') = (0°,45°,22.5°,67.5°)$ 时,S 可以达到最大值 $2\sqrt{2}$. 这里需要说明一下的是,在以前的用光学方法检测局域实在理论或者说检测 Bell 不等式破坏的实验中,主要存在两个漏洞,即探测效率漏洞和局域性漏洞,其中探测效率漏洞存在所有的光学实验中. 而在我们这个实验中,我们演示了一种类空间隔的 Bell 不等式的破坏,消除了局域性漏洞. 实验中,如图 2 所示,每端的观测者利用分束器作为真随机基矢选择,再使用 4 个单光子探测器进行(0°,45°,22.5°,67.5°)极化测量. 实验的整个测量时间为 20s,也就是两个类空间隔观测者的 16 个符合计数是同时测量的. 另外,由于实验中的每个探测器的探测效率并不一样,所以两重符合计数需要按照其单路计数进行归一化. 最后,我们获得 S 的实验值为 2.45 ±0.09,见表 1,违反了 CHSH 不等式 5 个标准方差. 这个结果也说明了两个相距 10 多千米的接收端之间建立了纠缠.

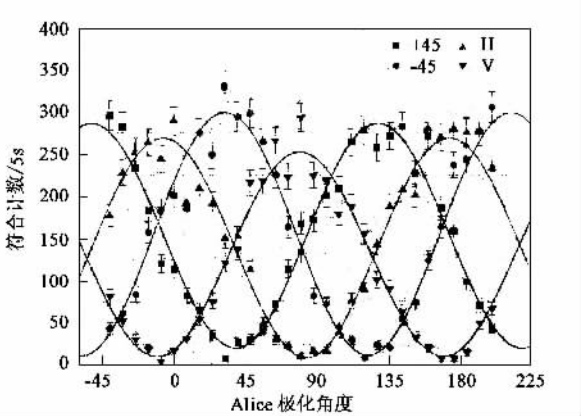

图 3 量子纠缠分发的验证曲线(为了验证两个接收端纠缠态的品质,我们测量了随 Alice 极化角度变化的符合计数曲线. 4 条曲线分别对应了 Bob 端 4 个不同的极化角度 H、V、+45、−45. 通过图中 4 条拟合的正弦曲线,我们可以看出在 HV 基矢下对比度可以达到 94% 而在 +45/ −45 基矢下可以达到 89%,平均对比度为 91%,远远高于破坏 Bell 不等式所需要的对比度)

表 1 CHSH 不等式相关系数测量值*

$E(\phi_A,\phi_B)$	(0,22.5°)	(0°,67.5°)	(45°,22.5°)	(45°,67.5°)
数值	−0.681	0.764	−0.421	−0.581
偏差	0.040	0.036	0.052	0.046

* CHSH 不等式 4 个相关系数值如上表所示,其参量 S 值为 2.45 ± 0.09,获得了 5 个标准方差的 CHSH 不等式的破坏

接下来,我们利用了已经建立的纠缠资源进行纠缠光子 BB84 量子密码协议[6](也就是 Ekert91 量子密码协议[12])的演示. Alice 和 Bob 利用分束器随机选择接收光子的测量基矢:HV 基矢或者 +45/ −45 基矢,当双方选择相同的基矢时,他们的测量结果始终是反关联的,从而可以很简单地产生密钥. 实验中在 4 分钟里总计产生了 29,433 个符合计数,由

于接收端的每个耦合装置的接收效率不一样，所以我们随机丢弃了一些高效率通道的探测计数，使得每个通道的接收效率基本相当. 通过这样的处理，我们仍然获得 15,308 个原始密钥. 进一步，我们首先丢弃 Alice 和 Bob 选用不同基矢的事例，剩下的筛选密钥总计为 7,956 个，其量子比特错误率(quantum bits error rate)为 5.83%. 然后我们再进行纠错处理，密钥数量降低为 4,869，而错误率也下降为 1.46%，接着我们进行隐私放大处理，最终获得的安全密钥数量为 2,435 bits，平均安全密钥产生速度为 10 bits/s. 当然，如果利用高亮度纠缠源的话[41]，密钥产生率可能会达到每秒钟几百个.

3 结论、意义和展望

虽然同以前类似的实验相比，我们这个实验似乎只是前进了一小步，但是，这一小步是意义深远的. 首先，我们这个实验第一次证明了经过大气层等效厚度的大气之后，纠缠光子依然可以存活，纠缠特性依然可以保持，并且演示基于类空间隔 Bell – CHSH 不等式的破坏，而这个破坏完全保证了量子密码协议的绝对安全性，也就是消除了通信过程的窃听漏洞. 其次，我们这个实验中的纠缠光子对的最终收集效率或者说衰减为百分之几，远远高于基于人造卫星的自由空间量子通信的信道衰减阈值[42]，这也充分说明了地面 – 卫星之间量子通信的可行性. 再次，在这个实验中开发出来或者利用的一些技术和手段(如建立高稳定性的传输信道、遥远两地接收者的同步等等)为未来的全球量子通信实验研究打下良好的技术基础. 最后，需要指出的是，利用脉冲调制以及可以门控的纠缠源，加上精密的空间滤波和精确的光谱滤波等技术，完全可以进行白天的自由空间量子通信[36].

参 考 文 献

[1] Nielson M A, Chuang I L. Quantum Computation and Quantum Information. Cambridge University Press, 2000

[2] Bouwmeester D, Ekert A, Zeilinger A. The Physics of Quantum Information. Springer – Verlag Berlin：Heidelberg, 2000

[3] Gisin N, Ribordy G, Tittel W *et al*. Rev. Mod. Phys., 2002, 74：145

[4] Shor P W. Proc. 35th Annu. Symp. on the Foundations of Computer Science. IEEE Computer Society Press, Los Alamitos, California, 1994. 124 – 134

[5] Vernam G. J. Am. Inst. Electr. Eng., 1926, 45：109

[6] Bennett C H, Brassard G. Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing. Bangalore, India(IEEE, New York, 1984). 175 – 179

[7] Lo H. – K, Chau H F. Science, 1999, 283：2050

[8] Shor P W, Preskill J. Phys. Rev. Lett., 2000, 85：441

[9] Bennett C H. Phys. Rev. Lett., 1992, 68：3121

[10] Bruß D. Phys. Rev. Lett. 1998, 81：3018

[11] Bechmann-Pasquinucci H, Gisin N. Phys. Rev. A, 1999, 59：4238

[12] Ekert A. Phys. Rev. Lett., 1991, 67：661

[13] Inoue K, Waks E, Yamamoto Y. Phys. Rev. Lett., 2002, 89：037902

[14] Bennett C H *et al*. J. Cryptology., 1992, 5：3

[15] Muller A, Breguet J, Gisin N. Europhys. Lett., 1993, 23：383

[16] Kwiat P G, Mattle K, Weinfurther H *et al*. Phys. Rev. Lett. 1995, 75：4337

[17] Jennewein T, Simon C, Weihs G *et al*. Phys. Rev. Lett., 2000, 84：4729

[18] Muller A, Zbinden H, Gisin N. Nature, 1995, 378：449

[19] Muller A, Zbinden H, Gisin N. Europhys. Lett., 1996, 33：335

[20] Townsend P. Nature, 1997, 385：47

[21] Townsend P. Electron. Lett., 1997, 33：188

[22] Hughes R, Morgan G, Peterson C. J. Mod. Opt., 2000, 47：533

[23] Ribordy G, Gautier J-D, Gisin N *et al*. J. Mod. Opt., 2000, 47：517

[24] Ribordy G, Brendel J, Gautier J – D *et al*. Phys. Rev. A, 2001, 63：012309

[25] Tittel W, Brendel J, Zbinden H *et al*. Phys. Rev. Lett., 2000, 84：4737

[26] Stucki D, Gisin N, Guinnard O *et al*. New. J. Phys., 2002, 4：41

[27] Boileau J – C, Laflamme R, Laforest M *et al*. Phys. Rev. Lett., 2004, 93：220501

[28] Gobby C, Yuan Z L, Shields A J. Appl. Phys. Lett., 1997, 70：793

[29] Briegel H – J, Dür W, Cirac J I *et al*. Phys. Rev. Lett., 1998, 81：5932

[30] Zukowski M, Zeilinger A, Horne M A *et al*. Phys. Rev. Lett., 1993, 71：4287

[31] Bennett C H *et al*. Phys. Rev. Lett., 1996, 76：722

[32] Zhao Z, Yang T, Chen Y-A *et al*. Phys. Rev. Lett., 2003, 90：207901

[33] Buttler W T *et al*. Phys. Rev. Lett., 2003, 84：5652

[34] Aspelmeyer M *et al*. Science, 2003, 301：621

[35] Rarity J G *et al*. J. Mod. Opt., 2001, 48：1887

[36] Hughes R J *et al*. New J. Phys., 2002, 4：43

[37] Kurtsiefer C *et al*. Nature, 2002, 419：450

[38] Peng C-Z *et al*. Phys. Rev. Lett,. 2005, 94：150501

[39] Bell J S. Physics(N. Y.), 1964, 1：195

[40] Clauser J, Horne M, Shimony S *et al*. Phys. Rev. Lett., 1969, 23：880

[41] Kurtsiefer C, Oberparleiter M, Weinfuter H. Phys. Rev. A, 2001, 64：023802

[42] Aspelmayer M *et al*. IEEE J. Sel. Top. Quantum Electron., 2003, 9：1541