自由空间量子通信实验研究与进展*

单 欣[1] 孙献平[1] 罗 军[1] 詹明生[2]

1. 中国科学院武汉物理与数学研究所，波谱与原子分子物理国家重点实验室，武汉 430071

2. 中国科学院研究生院，武汉 430071

摘要 量子通信的安全性是基于Heisenberg测不准原理、单光子不可分割性和量子不可克隆定理，它遵从物理规律，是绝对安全的. 近年来量子通信技术的迅速发展加快了量子通信的实用化进程. 文中综述自由空间量子通信实验研究进展，简要介绍几种量子编码协议、不同类型单光子源的量子通信实验，说明全球量子通信的实现可能存在的问题与技术挑战，展望了自由空间量子通信的未来.

关键词 量子通信 量子编码协议 自由空间量子通信 单光子源

20世纪以来，随着信息交流的密切，对信息安全的要求也愈加严格，因而出现了一门新兴的学科——密码学，它的研究目的是如何防止非法的第三方窃听通信双方之间的信息. 早在上世纪人们就提出了多种加密方式，其中最著名的是Vernam密码和公钥密码. 但随着科学技术的日新月异，这些加密方式渐渐不能满足人们对它们的基本要求——安全、有效. 因此，对更加安全有效加密方式的需求导致了量子通信的诞生. 1983年“量子钞票”[1]概念的首次提出，将量子力学和传统密码术相结合，开创了量子密码时代. 受这种思想的启发，现在已提出多种量子密码协议，从此量子通信实验研究逐渐兴起并在近20年里获得了迅速发展. 迄今为止正式报道的最远距离的量子通信是Gobby等[2]在2004年实现的122 km光纤中的量子通信实验演示. NEC公司已成功进行了150 km[3]光纤里单光子传送演示，Mo等[4]也完成了室内150 km和室外北京到天津125 km的光纤量子通信实验. 与此对应，自由空间的量子通信距离已达23.4 km[5]. 这些量子通信演示实验距离上的突破预示了量子通信实用化的可能性.

1 量子通信的基本原理

量子通信传送的是密钥而非密文本身，是一个量子密钥的分发过程，作为标准对称密码体系的补充. 由于量子通信的安全性依赖于量子力学中的Heisenberg测不准原理、单光子不可分割性和量子不可克隆定理，它们都客观存在于任何微观量子体系中. 根据这些原理，测量通常会对被测体系引入干扰，因此无法得到体系测量前状态的完整信息，所以说量子通信遵从物理规律，是无条件安全的.

在实验演示中，发送方(Alice)向接收方(Bob)发送一系列随机的量子态，Bob随机地对这些量子态进行测量，然后，Alice和Bob由经典通信得到最终密钥. 而窃听过程相当于一个测量过程，一旦窃听者(Eve)进行了窃听操作，必然会在量子通信过程中引入误码，增加误码率，Alice和Bob就一定能发现Eve的存在. 通过量子通信产生的密钥是绝对安全的，现行的应用演示中都是将得到的量子密钥通过一次一密的方式对文字文件或者图片等信息明文进行加密，密文通过经典方式在通信双方之间进行传输而不存在失密的危险.

2005-06-28收稿，2005-09-05收修改稿

* 国家重点基础研究发展规划(批准号：2001CB309300)及国家自然科学基金(批准号：60477043)资助项目

E-mail：shanxin@wipm.ac.cn

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

2 量子密码协议和编码方式

目前在量子通信中使用最普遍的密码协议为BB84协议[6]，B92协议[7]和EPR协议[8]. BB84协议是1984年由Bennett和Brassard首次提出的，该协议利用属于两组共轭基的4个不同光子偏振态对信息进行编码. 共轭是指一组基中的每个基矢在另一组基中的所有基矢上的投影都相等，即以一组基对与其共轭基中的基矢进行测量，得到完全随机的结果. 因此，可消除它测量前具有的全部信息. 光子的偏振态可以表示为($\cos\theta$, $\sin\theta$)，这里，θ表示光子偏振方向与水平方向的夹角. 以一对相互共轭基为例，光子的线偏振基和圆偏振基可分别表示为$\boldsymbol{R}$：(0, 1)，(1, 0)和$\boldsymbol{C}$：($1/\sqrt{2}$, $i/\sqrt{2}$)，($i/\sqrt{2}$, $1/\sqrt{2}$). BB84协议的量子密钥分发步骤见图1所示.

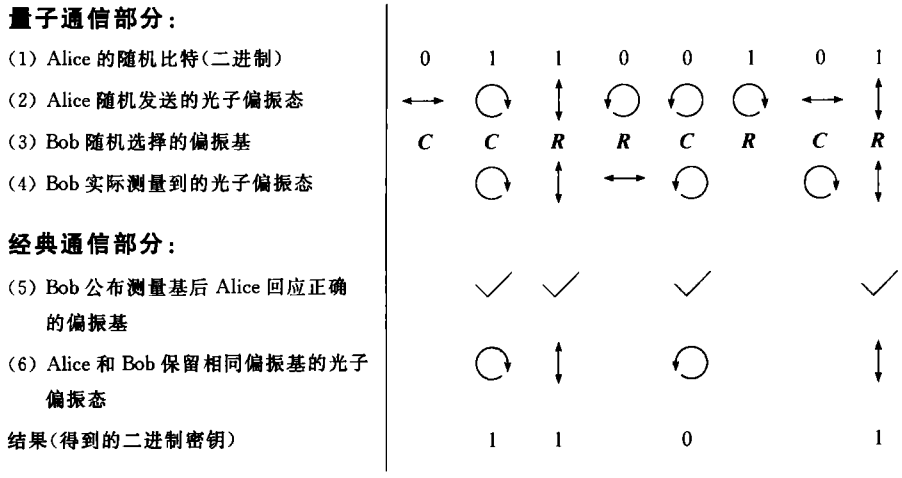

图1 BB84协议密钥分发步骤

以BB84协议为例，考虑一种简单的俘获后再重新发送(intercept-resend)的窃听方案. 由于窃听行为会在Bob的接收数据中引入25%的错误，密钥的误码率增大，Alice和Bob通过公共信道比对数据时，能够发现Eve的存在.

B92协议与BB84协议本质上相同，仅将使用的光子偏振态个数减少了一半，但是通信效率也减半，只有四分之一的光子最终被接收到. EPR协议则与上述两种协议不同，主要是通过纠缠光子对的纠缠性质来保证密钥的安全性. 纠缠光子对用于建立通信双方之间的量子信道，而Bell不等式则用于探测通信过程中是否存在窃听. 这3种协议利用的是单光子现象和离散变量编码.

随着量子通信的发展，近几年提出一些不同的编码方式，它们多是利用连续变量对信息进行编码，属于多光子协议类. 目前提出的连续变量量子通信可以分成以下几种：

(1) 压缩态方法. 由Ralph[9]最早提出利用压缩态进行编码的方案，使用两束压缩光均携带信息的方法. Bob在检测时只可能测到一束光束所携带的信息，然后通信双方比对测量结果，建立量子密钥. 之后，Hillery[10]提出信息由发送压缩真空态的两个场正交部分中被压缩的那一个携带的方案. 量子密钥的安全性由两个正交部分之间的测不准关系得以保证. 虽然，对于压缩态量子密码协议已可证明在某种情况下(当压缩参数超过某一个阈值时)是无条件安全的[11]，但是由于压缩态是一种非经典态，不易制备. 因此，目前仅有理论方案的提出，没有相关的实验实现.

(2) 相干态[12,13]方法. Gauss分布的信息被编码在两个相互正交的基上(如振幅和与其正交的相位)，通过随机编码基矢的测量，可得相干的密钥信息，然后由分割、反向调制等方法提取密钥. 虽然目前仍没有证明相干态编码是无条件安全的，但是利用反向调制的方法可使相干态在进行密钥分发时不受量子信道衰减的限制，而且，制备方便使这种编码方式在量子通信中具有好的发展前景.

(3) EPR相干光束，也称为多光子纠缠方法.

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

较特殊的是，这种编码方式是对不同的测量方式进行编码[14]. 例如，通信双方都对相位进行测量得到二进制比特“1”或都对振幅进行测量时得到“0”，这与单光子协议中的 EPR 协议类似. 不同之处是利用纠缠光束编码，其安全性不再依赖 Bell 不等式是否违背，而是通过验证两个光束间的纠缠关系是否被破坏而得到保证.

与基于单光子的协议相比较，使用连续变量协议的量子通信对随机序列中的每个脉冲不再要求只含有一个光子，其最大优势在于能显著提高密钥传输率. 而且，在这类协议的测量中普遍使用了零差探测技术，利用的是标准 PIN 光电二极管，进行光子计数时比雪崩二极管要快得多. 例如，在不计衰减时，利用 Gauss 相干光进行量子密钥分发[13]的传输率可达 1.7 Gb/s，在衰减为 3.1 dB 时也可达到 75 kb/s，这是目前基于单光子协议的量子通信不能达到的.

3 自由空间量子通信及其实验实现

在量子通信实验中，根据光子传输通道的不同特性使用相应的编码方式，自由空间量子通信通常采用偏振编码方式，而光纤量子通信通常使用相位编码. 因为，光子在光纤中传播时偏振态易发生改变，会导致通信过程中误码率增加.

自由空间量子通信研究的主要方向是连接地面与近地卫星、卫星与卫星，建立全球量子通信网络. 由于光子在大气中传播不存在双折射问题，而且随着海拔高度的增加光子在传播过程中的损耗极大地降低. 特别是，波长在近红外区(例如，～800 nm 附近)的光子在通过空气传输时，很少被吸收且受大气扰动的影响较少，形成一个大气传输窗口. 自由空间量子通信通常选用该波段的光子作为信息的载体，降低了通信过程中的损耗. 而且，在这个波段，具有商业上可获得的～70%量子效率的单光子探测模块等，这是实验研究和成功演示的基本保证. 一些技术问题，例如 Alice 和 Bob 之间的连接，完全可以借用于成熟的大气激光通信中 APT(acquisition, pointing and tracking)技术来解决. 使用原子频标和 GPS 技术是解决信号同步较好方法中的一种. 自由空间量子通信研究中存在的关键问题之一是：缺少成熟商业可获得的真正意义上的长距离可定向发送的单光子源，但是，在下面介绍中可以看到这个问题已经有了一些解决的建议和方案.

根据在自由空间量子通信实验中所使用单光子源的不同，可大致分成三类，简述如下：

3.1 以衰减激光作为单光子源的自由空间量子通信实验

由于激光光源的粒子数分布服从 Poisson 分布，那么在单个脉冲中含有 n 个光子的几率可以表示为[15]

$$P(n,\mu)=\frac{\mu^n}{n!}e^{-\mu}, \tag{1}$$

这里 μ 为平均光子数. 而在非空脉冲中每个脉冲含有多个光子的几率为[15]

$$\begin{aligned}P(n>1\mid n>0,\mu)&=\frac{1-P(0,\mu)-P(1,\mu)}{1-P(0,\mu)}\\&=\frac{1-e^{-\mu}(1+\mu)}{1-e^{-\mu}}=\frac{\mu}{2},\end{aligned} \tag{2}$$

虽然降低 μ 可减小每个脉冲中含有多个光子的几率，但是由于 μ 始终大于 0，不能完全避免多光子脉冲的存在. 相应的单光子源可以表示成

$$\begin{aligned}\text{source}=a_0|0\rangle+a_1|1\rangle+a_2|2\rangle+\cdots+a_i|i\rangle+\cdots\\ i=0,1,2,\cdots,\end{aligned} \tag{3}$$

这里 $|i\rangle$表示每个脉冲中含有 i 个光子；$a_i=P(i,\mu)$. 只有当 μ 处于一个较低的水平时，才可认为其等效于单光子源. 量子通信实验中，通常使用的平均光子数约为 0.1，由(2)式此时可知仍有 5%的非空脉冲是多光子脉冲. 所以，系统实际上是弱相干脉冲，而非真正意义上的单光子源. 这类实验均使用 BB84 或者 B92 协议.

1989 年 Bennett 等[16]实现的世界上第一个量子通信实验就是使用衰减激光作为单光子源，如图 2 所示，Alice 向 Bob 发送一个单光子序列来建立安全的量子信道. 虽然密钥传输效率低，传输距离仅为 32 cm，误码率为 4.375%，但是它成功演示了量子密钥分发过程，证明了量子通信的可行性.

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

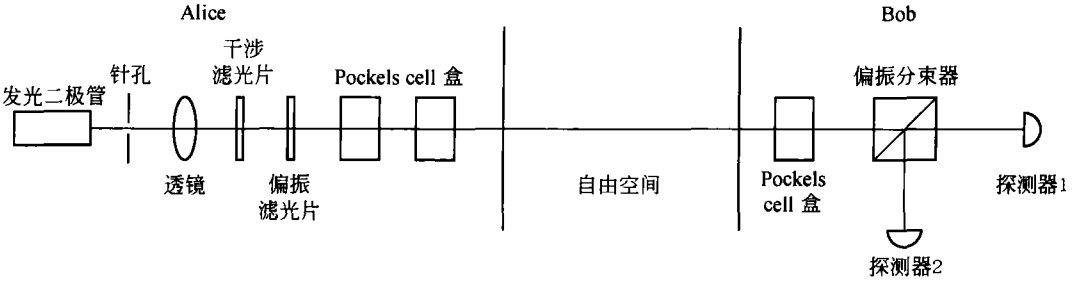

图2 Bennett等的量子通信实验示意图

Bennett等使用BB84协议，Alice通过干涉滤光片将发射光束的光强衰减到单光子水平，平均光子数仅为0.1—0.2，谱宽选择在光电倍增管较高量子效率频段. Alice的偏振滤光片和两个Pockels盒随机地改变光子的偏振态，实现Alice向Bob随机发送0°，45°，90°，135°四种不同偏振方向的光子. Bob的Pockels盒、偏振分束器(方解石Wollaston棱镜)和探测器实现对光子的随机测量.

表1 利用衰减激光作为单光子源的自由空间通信实验的进展

实验时间	密钥分发协议	密钥分发距离/m	原码误码率/%	原始密钥传输速率/Hz	参考文献
1996	BB84	75(强日光) 150(室内)	2	1000	[17]
1997	B92	205(室内)	6	50	[18]
1998	B92	1000(月光)	1.5	50	[19]
1998	B92	500(日光)	1.6	5000	[20]
1999	B92	1600(日光)	5.3	5400	[21]
2001	BB84	1900(月光)	6	500	[22]
2001	BB84	10 k	5(日光) 2(月光)		[23]
2002	BB84	23.4 k(月光)	5	1500—2000	[5]

随后几年的自由空间量子通信实验进展如表1所示. 自由空间量子通信实验的困难在于其要求单个光子能够在复杂的大气环境中进行传输，同时在强的背景光下仍然能够被探测. 使用非常窄的时间窗(亚纳秒)，较小接收角度的光学望远镜，滤光器件，准直器件等作为时间或者空间滤波，极大地降低了背景光噪声，使实验误码的大部分仅由探测器暗计数产生，因此，自由空间量子通信实验才能走出实验室[17]. Hughes等[20]的室外日光条件点对点量子通信实验，利用强光脉冲作为触发信号激活计数器，有效降低了暗计数引起的误码率. 实验的平均光子数典型地为0.3，背景光引起的误码率为0.4%，而暗计数引起的误码率仅为0.1%，使密钥传输率达到5 kHz. 这种方法被广泛应用到之后的一些实验中.

2001年Rarity等[22]的量子通信实验证明了量子密钥可在损耗高达20 dB的信道上传输，表明了在近地卫星间进行量子密钥传输的可能性. 在Hughes等[23]的10 km自由空间距离的量子通信实验中，Alice和Bob都处于高海拔区，减小了大气对单光子传输的干扰. 实验的平均光子数在白天为0.2—0.8和晚上为0.1—0.2，最终得到完全保密的密钥，在白天生成率为245 b/s和晚上为570 b/s. Rarity等分析了平均光子数、大气量子信道的质量指标和秘密密钥之间的关系. 当量子信道质量指标低于某一极限(在这次实验的条件下为0.0016)时无论平均光子数为多大都不可能得到最终的安全密钥. 同样，如果平均光子数太小，则由于筛选密钥的误码率太大，纠错过程中会泄漏过多信息而无法得到密钥；而当平均光子数过大时，Eve可以通过多光子脉冲方式得到足够的信息而使得整个量子通信过程不可靠.

目前，利用衰减激光作为单光子源的自由空间量子通信实验的最远纪录为由Kurtsiefer等[5]在位于德奥边境的Zugspitze(Alice，2950m)和Westliche Karwendspitze(Bob，2244m)两山间实现的23.4 km距离.

3.2 以纠缠光子对作为单光子源的自由空间量子通信实验

这类密钥分发实验为量子纠缠的分发. 单光子源为纠缠的光子对，也称为EPR对. 纠缠光子对

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

具有多种形式，其中一种可以表示为

$$源(\text{source}) = (|\boldsymbol{H}_1\boldsymbol{V}_2\rangle - |\boldsymbol{V}_1\boldsymbol{H}_2\rangle)/\sqrt{2}\,, \quad (4)$$

这里 $\boldsymbol{H}$ 和 $\boldsymbol{V}$ 分别表示光子的偏振方向：水平和垂直偏振；下标1和2区分纠缠光子对的两个不同光子. 由于纠缠光子对中的两个粒子具有关联特性，一旦知道其中一个粒子的偏振方向，则不需对另一个粒子进行测量就可以确定地知道其偏振方向. 尽管它与衰减激光系统的粒子束分布都符合 Poisson 分布，但由于只有通信双方都探测到粒子时才能将其作为密钥进行处理，因此，这种系统可以有效地消除空脉冲，具有较优的信道信噪比.

由不同原理生成的单光子源，所以量子纠缠分发实验通常使用 EPR 协议. 早期的这类实验大多数使用光纤通信，纠缠分发距离从几百米到 10 km[24—26]. 近几年已经实现了长距离自由空间量子纠缠分发实验演示. 表2中的例子都是利用偏振纠缠光子对的实验，将 EPR 协议与 BB84 协议结合起来实现量子纠缠的分发. 实验使用的单光子源是由激光入射到 BBO 晶体上通过参量下转换产生的，其形式如(4)式所示. 在 Alice 和 Bob 进行计数时，通信的一方先通过半波片将纠缠对中一个粒子的偏振方向改变 90°，以便能同时探测到粒子. 第一个自由空间量子纠缠分发实验是由 Aspelmeyer 等在多瑙河两岸完成的[27].

表2 利用纠缠光子对作单光子源的自由空间量子密钥实验进展

实验时间	密钥分发距离/km	误码率/%	原码传输率/(b·s^{-1})	参考文献
2003	0.6(月光)	8.4	10	[27]
2004	13(日光)	5.83	100	[28]
2004	7.8(月光)	9.9	25	[29]

Peng 等[28]报道了 13 km 的目前最远自由空间距离量子纠缠分发的实验，但是经过筛选、纠错和秘密放大步骤后得到的秘密密钥传输率仅为 10 b/s.

2004 年 Resch 等使用时间标签技术(time-stamping technique)代替了传统的脉冲同步方法[29]，实现了在维也纳市中心 7.8 km 的量子纠缠分发. 其实验的示意图如图3所示.

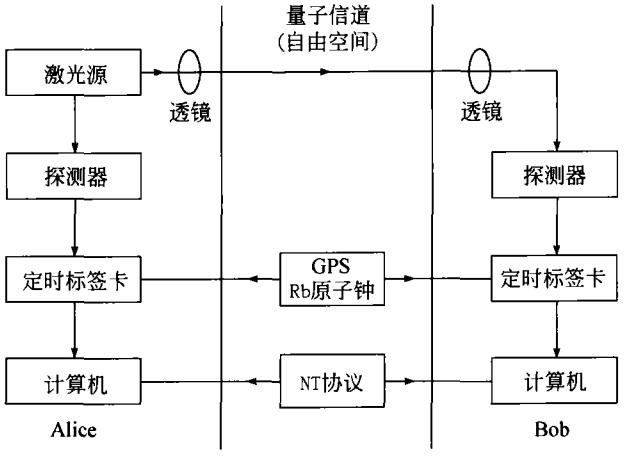

图3 Resch 等的自由空间纠缠分发实验示意图

时间标签记录了是否探测到光子及光子到达时间(精度 125 ps). 由于 Rb 原子频标的稳定性，实验用它对时间标签进行稳频，GPS 的 pps 信号提供频标的时基. 同时通过 NT 协议(network timing protocol)使通信双方的测量时间差保持在约 10^{-2} s 之内. 由参量下转换产生的光子本身也具有时间相关性. 这些技术的时间稳定特性，使得通信双方保持完全同步.

自由空间量子纠缠分发实验表明了纠缠光子在穿透等效于整个大气层厚度的地面大气后，仍然保持其纠缠特性，可用于安全的空间量子通信. 利用这一研究结果可以基本实现地对星的量子纠缠分发[28,29]，为全球化的量子通信奠定了实验基础. 但是，存在的问题是纠缠光子量子通信的原始数据传输速率相当低，如表2所示.

3.3 真正意义上的单光子自由空间量子通信实验

上述两类实验中的单光子源并不是真正意义上的单光子源，理想的单光子源是指每次只释放一个光子的装置，又可称之为“光子枪”. 迄今已提出了多种“光子枪”的实现方案[30—32]，其中一些方案成功用于自由空间量子通信实验演示，如表3所示. 利用物质中的分子、原子或者色心等两能级系统，当这些系统受到脉冲激发时能够每次只产生一个光子，所以它们可以等效于单光子源. 而另外一种产生单光子源的办法是利用半导体量子点，当脉冲激发量子点时会产生一些电子空穴对，而这些空穴对重新复合后就可以产生特定波长的光子.

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

表3 使用单光子源自由空间量子密钥实验

实验时间	密钥分发距离/m	误码率/%	原码传输率/(kb·s^{-1})	参考文献
2002	50	4.6	17.7	[33]
2002	1	2.5		[34]
2004	30	1.7	40	[35]

Beveratos等[33]完成了第一个真正意义上的单光子源自由空间量子通信. 实验使用传统的BB84协议，位于室内. 利用脉冲激发纳米钻石晶体中单个氮空穴色心(nitrogen-vacancy colour center)发出的荧光作为单光子源. 在室温下，该单光子源发出的荧光光谱范围为637—750 nm，一个高通滤波器滤去激光的杂散光. 对于Poisson分布的光子，自相关系数表明每个脉冲中光子对数目减少的程度，所以，单光子源的质量控制主要由检测光子的自相关系数来完成. 衰减激光脉冲系统的自相关系数为1[36]，而这种单光子脉冲系统的自相关系数小于1，含有两个光子的脉冲数目比衰减激光脉冲系统的低. 所以，单光子脉冲系统不需要降低平均光子数就可使发射多光子脉冲的几率保持在较低水平，显著提高了量子密钥的生成率. 从表3中可以看到实验原码的传输率可高达17.7 kb/s，而最终得到的秘密密钥的生成率仍可达7.7 kb/s.

Waks等[34]使用单个量子点方法的单光子源演示了量子通信. 虽然实验中密钥的传输距离很短，但误码率可保持在较低水平，同时秘密密钥的传输率可达到25 kb/s. 由于这种系统中量子点效率和接收装置损耗的限制，在信道损耗较小时，其传输效率低于衰减激光脉冲系统，只有在信道损耗较大时，单个量子点系统才能体现出它的优越性.

2004年，Alleaume等使用色心类型单光子源[35]在室外实现了30 m自由空间距离的量子密钥传输，秘密密钥的生成率高达16 kHz. 在同等条件下，单光子源系统比衰减激光脉冲系统可承受更大信道传输损耗. 真正意义上的单光子源有望在千米距离演示自由空间量子通信.

与纠缠光子系统的量子通信相比，单光子脉冲系统的密钥传输率更高；而与衰减激光脉冲系统的量子通信相比，该系统具有安全性好、通信效率高的优点. 尽管目前的单光子源量子通信实验的密钥分发距离仍然不理想，随着量子通信技术、单光子源的发展，相信单光子脉冲系统具有很好的发展潜力.

4 自由空间量子通信的技术挑战

自由空间量子通信实验发展十分迅速，但有一些关键技术问题尚待改进，主要是单光子源、大气量子信道、单光子探测3方面.

(1) 真正意义上的单光子源还不是商业可获得的. 目前使用的单光子源主要是利用衰减激光和参量下转换产生的纠缠光子来模拟单光子源，但它们仍无法消除多光子存在的可能性. 纠缠光子源产生多光子的几率远小于衰减激光，但它们都属于伪单光子源(pseudo-single-photon source). 因此无法完全避免受到多光子攻击的可能性. 目前建议或者实现的“光子枪”方案存在着各自的不足，有许多可改进的空间，没能真正投入商业使用. 例如，在约1550 nm通用光纤通信波长范围工作的色心或者量子点单光子源. 虽然色心的单光子源在室温下较稳定但是效率低. 量子点单光子脉冲源可以发射非常窄带宽、更短的脉冲，对有效的量子通信非常有利，然而，其要求液氦温度环境工作，不适合室外工作. 通过发展高温工作的半导体量子点(例如，II-VI半导体)或者使用另外改进性能的色心可能解决这些限制.

(2) 大气量子信道中的背景光和大气扰动会增大通信误码率. 从上述实验发展可见，尽管实验演示中采取各种技术手段来减小这种干扰，例如利用强光触发探测装置，通过时间窗控制探测装置的开启时间，使用干涉滤光片去除大气背景光，或者提高实验区的海拔高度来减小大气扰动等，但是，这些方法只能减小而不能完全消除大气信道中的干扰，在实验中仍不可避免地会引入误码. 原子蒸汽滤光是消除背景光噪声的方法之一，我们已经使用装备了原子蒸汽滤光器件的集成系统[37,38]在室外(星光，白天条件)几十米的距离里实验演示了空间量子通信.

(3) 由于现阶段还不可能广泛使用真正的单光子源，所以量子通信的成功与否很大程度上要依赖于单光子的探测能力. 一个理想的探测装置应该满足大范围，低暗计数，时间稳定和死时间短4个要

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

求. 目前在自由空间量子通信中普遍使用硅雪崩二极管(APD)替代光电倍增管作为单光子探测器，其量子效率最高可以达到76%[39]. APD在低光子水平下具有较大噪声，这一缺陷不但使探测器的误测漏测率较高，还限制了通信过程中密钥的生成速率，使得量子通信实用化始终存在着技术瓶颈. 目前实现的最高的密钥生成率为100 kb/s，由日本NEC公司和信息通信研究机构(NICT)合作在40 km的光纤中实现的，使用了他们自主开发的低噪音APD，其噪声降低到原来的十分之一，极大地提高了密钥生成率. 商用的单光子计数模块也显示出发展潜力，例如在我们的自由空间量子通信系统中使用的是SPCM-AQ-14Y (EG&G, OPTOELECTRONICS)，它在780 nm波长的量子效率为60%.

5 量子通信的应用和发展前景

自从第一个量子通信实验完成之后，量子通信的实验研究逐渐发展起来并日趋成熟，目前主要工作是寻求量子通信与实际应用的结合. 2004年4月21日Lorunser等利用量子纠缠分发第一次实现了1.45 km的银行间数据传输[40]，标志着量子通信从实验室走向应用.

目前的量子通信实验多是以单向点对点方式实现的，若希望量子通信能得到广泛应用，需要在网络中建立点对多点或者多点之间的通信. 2004年6月BBN公司、哈佛大学和波士顿大学合作实现了世界上第一个量子通信网络. 这套网络包括六个节点[41]，成功地实现了BBN公司与哈佛大学之间的连接，并试图延伸至波士顿大学. 它通过普通光纤传输量子密钥加密的数据，与现有因特网技术完全兼容，能实现普通网络的各种功能，同时保证了整个传输过程的数据绝对安全性.

随着量子通信技术的发展，相关的商用产品[42—44]已经推出市场. 例如，瑞士id Quantique公司的Clavis量子通信系统的密钥最远传输距离为100 km，在超过25 km时原码传输率仍可达1.5 kb/s以上，美国MagiQ公司的QPN产品的传输距离可达120 km，日本NEC公司也推出了相应的量子通信系统产品，它们都属于使用光纤的量子通信类型.

在卫星通信迅速发展和普及的今天，可以通过地对星、星对星的传送方式实现大范围、远距离的空间量子通信. 目前自由空间量子通信的密钥传输距离已达23.4 km，考虑到大气密度的变化，这一水平距离相当于在垂直方向上的整个大气层厚度，完全可能实现地对星的量子密钥传输. 但是，从上述实验可见，自由空间量子通信的密钥生成率比较低，要达到实际通信的要求还有一定距离. 尽管多个连续变量协议的提出可部分地解决数据传输率低这个关键问题，但是连续变量协议是否绝对安全仍然需要实验与理论的验证.

量子通信是基础研究和高新技术相结合的产物，它的发展离不开量子规律，但更依赖于高新科技的帮助，只有发展更高、更新的科学技术，才可能将科学设想变成现实. 量子通信的研究与进展表明量子通信的实用化进程正在加速，或许，距离量子通信全球化的最终目标将不再遥远.

参 考 文 献

1 Wiesner S. Conjugate coding. SIGACT News, 1983, 15: 78—88

2 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

3 Tadamasa K, Yoshihiro N, Takaaki H, et al. Single-photon interference over 150 km transmission using silica-based integrated-optic interferometers for quantum cryptography. Jpn J Appl Phys, 2004, 43(9): 1217—1219

4 Mo X F, Zhu B, Han Z F, et al. Intrinsic-stabilization uni-directional quantum key distribution between Beijing and Tianjin. http: //arxiv. org/abs/quant-ph/0412023

5 Kurtsiefer C, Zarda P, Halder M, et al. Quantum cryptography a step towards global key distribution. Nature, 2002, 419: 450

6 Bennett C H, Brassard G. Quantum cryprography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Processing, Bangalore, India, (New York: IEEE), 1984, 175—179

7 Bennett C H. Quantum cryptography using any two nonorthogonal states. Phys Rev Lett, 1992, 68(21): 3121—3124

8 Ekert A K. Quantum cryptography based on Bell' s theorem. Phys Rev Lett, 1991, 67(6): 661—663

9 Ralph T C. Continuous variable quantum cryptography. Phys Rev A, 2000, 61: 010303

10 Hillery M. Quantum cryptography with squeezed states. Phys Rev A, 2000, 61: 022309

11 Gottesman D, Preskill J. Secure quantum key distribution using squeezed states. Phys Rev A, 2001, 63: 022309

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

12 Grosshans F, Grangier P. Continuous variable quantum cryptography using coherent states. Phys Rev Lett, 2002, 88(5): 057902

13 Grosshans F, Assche G V, Wenger J, et al. Quantum key distribution using gaussian-modulated coherent states. Nature, 2003, 421: 238—241

14 Silberhorn C H, Korolkova N, Leuchs G. Quantum key distribution with bright entangled beams. Phys Rev Lett, 2002, 88(16): 167902

15 Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography. Rev Mod Phys, 2002, 74: 145—195

16 Bennett C H, Bessette F, Brassard G, et al. Experimental quantum cryptography. J Crypto, 1992, 5: 3—28

17 Jacobs B C, Franson J D. Quantum cryptography in free space. Opt Lett, 1996, 21(22): 1854—1846

18 Buttler W T, Hughes R J, Kwiat P G, et al. Free-space quantum-key distribution. Phys Rev A, 1998, 57(4): 2379— 2382

19 Buttler W T, Hughes R J, Kwiat P G, et al. Practical free-space quantum key distribution over 1 km. Phys Rev Lett, 1998, 81(15): 3283—3286

20 Hughes R J, Nordholt I E, Derkacs D, et al. Free-space quantum key distribution in daylight. J Mod Opt, 2000, 47(2/3): 549—562

21 Buttler W T, Hughes R J, Lamoreaux S K, et al. Daylight quantum key distribution over 1.6 km. Phys Rev Lett, 2000, 84(24): 5652—5655

22 Rarity J G, Tapster P R, Gorman P M. Secure free-space key exchange to 1.9 km and beyond. J Mod Opt, 2001, 48(13): 1887—1901

23 Hughes R J, Nordholt I E, Derkacs D, et al. Practical free-space quantum key distribution over 10 km in daylight and at night. New J Physics, 2002, 4: 43. 1—43. 14

24 Tapster P R, Rarity J G, Owens P C M, Violation of Bell's inequality over 4 km of optical fiber. Phys Rev Lett, 1994, 73(14): 1923—1926

25 Tittel W, Brendel J, Zbinden H, et al. Violation of Bell inequalities by photons more than 10 km apart. Phys Rev Lett, 1998, 81(17): 3563 —3566

26 Jennewein T, Simon C, Weihs G, et al. Quantum cryptography with entangled photons. Phys Rev Lett, 2000, 84(20): 4729—4732

27 Aspelmeyer M, Bohm H R, Gyatso T, et al. Long-distance free-space distribution of quantum entanglement. Nature, 2003, 301: 621—623

28 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

29 Resch K J, Lindenthal M, Blauensteiner B, et al. Distributing entanglement and single photons through an intra-city, free-space quantum channel. http: //arxiv. org/abs/quant-ph/0501008

30 Brunel C, Lounis B, Tamarat P, et al. Triggered source of single photons based on controlled single molecule fluorescence. Phys Rev Lett, 1999, 83(14): 2722—2725

31 Beveratos A, Kuhn S, Brouri R, et al. Room temperature stable single-photon source. Eur Phys J 2002, 18: 191—197

32 Santori C, Pelton M, Solomon G, et al. Triggered single photons from a quantum dot. Phys Rev Lett, 2001, 86(8): 1502—1505

33 Beveratos A, Brouri R, Gacoin T, et al. Single photon quantum cryprography. Phys Rev Lett, 2002, 89(18): 187901

34 Waks E, Inoue K, Santori C, et al. Quantum cryptography with a photon turnstile. Nature, 2002, 420: 762

35 Alleaume R, Treussart F, Messin G, et al. Experimental open-air quantum key distribution with a single-photon source. New J Physics, 2004, 6: 92. 1—92.14

36 Beveratos A, Brouri R, Gacoin T, et al. Nonclassical radiation from diamond nanocrystals. Phys Rev A, 2002, 64: 061802

37 Sun X P, Li R H, Luo J, et al. Free-space quantum communication device using atomic filter. Chinese Invent Patent Application Number: 200310111370.4

38 Sun X P, Luo J, Zhan M S., Free-space quantum communication device with atomic filters. United States Patent Application Number: 11/187, 488

39 Kwiat P G, Steinberg A M, Chiao R Y, et al. High-efficiency single-photon detectors. Phys Rev A, 1993, 48: 867—870

40 Poppe A, Fedrizzi A, Ursin R, et al. Practical quantum key distribution with polarization entangled photons. Optics Express, 2004, 12(16): 3865— 3871

41 Stix G. Best-kept secrects: Quantum cryptography has marched from theory to laboratory to real products. Sci Am, 2005, 292(1): 65—69

42 id Quantique SA (Geneve, Switzerland), http: //www. idquantique. com

43 MagQ technologies (Sommerville, USA), http: //www. magiqtech. com

44 NEC Ltd. (Tokyo, Japan), http: //www. nec. com

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net