自由空间量子密钥分发关键技术的研究进展

杨汝, 李云霞, 石磊, 蒙文, 罗均文

空军工程大学信息与导航学院, 陕西 西安 710077

摘要 自由空间的量子密钥分发(QKD)技术已成为量子通信领域的研究热点之一,连续变量 QKD 与离散变量 QKD 是其两大技术分支。介绍了近年来国内外自由空间 QKD 技术的研究进展,从实际应用角度出发,对比分析了两大分支主要的技术难点,重点分析了背景光干扰、大气信道中单光子的退偏振特性以及湍流引起的相位畸变等现象,并对自由空间 QKD 技术的发展前景进行了展望。

关键词 量子光学; 自由空间量子密钥分发; 连续变量; 离散变量; 背景光; 退偏振特性; 相位畸变

中图分类号 O431.2 **文献标识码** A **doi**: 10.3788/LOP55.020003

Research Progress on Key Technologies of Free-Space Quantum Key Distributions

Yang Ru, Li Yunxia, Shi Lei, Meng Wen, Luo Junwen

Institute of Information and Navigation, Air Force Engineering University, Xi'an, Shaanxi 710077, *China*

Abstract The free-space quantum key distribution (QKD) technology has become one of the research hotspots in the field of quantum communications, and the continuous variable QKD and the discrete variable QKD are two major technical branches of this technology. The recent research progresses of free space QKD technology at home and abroad are reviewed. From the viewpoint of practical applications, the technical difficulties of these two branches are compared and analyzed. The phenomena like the background light interference, the single photon depolarization characteristics in the atmospheric channel and the phase distortion caused by turbulence are analyzed emphatically, and the development foreground of free space QKD technology is prospected.

Key words quantum optics; free-space quantum key distribution; continuous variables; discrete variables; background light; depolarization characteristics; phase distortion

OCIS codes 270.5565; 270.1670; 270.5570; 010.1330

1 引 言

近年来,“棱镜门”、苹果“iCloud 泄露门”等信息安全事件层出不穷,人们对信息安全的需求越来越迫切。量子保密通信因其无条件的安全性而得到广泛关注和深入研究。传统保密通信系统的安全性来源于数学问题的求解复杂性,但穷尽密钥的搜索算法始终存在,密钥只在一定时间内具有安全性。针对这一情况,学者们提出了一种在理论上可以满足“一次一密”加密系统要求的密钥分发系统——量子密钥分发(QKD)协议。QKD 协议的安全性来源于量子物理的原理,而不依赖于数学问题求解的复杂性。因此,QKD 协议具有理论上的无条件安全性。经过 30 年的发展,QKD 技术已经形成了严格的安全证明体系,并开始进入实用化阶段。QKD 技术是量子信息技术中发展最快、最接近实用化的技术之一。

QKD 技术有两大技术分支:离散变量量子密钥分发(DV-QKD)技术和连续变量量子密钥分发(CV-QKD)技术,其典型协议如下。

DV-QKD 技术的协议主要分为单光子类协议和纠缠光子类协议两大类。

1) 单光子类协议

收稿日期: 2017-07-07; **收到修改稿日期**: 2017-08-14

作者简介: 杨汝(1995—),男,硕士研究生,主要从事空间量子密钥分发方面的研究。E-mail: 1443364980@qq.com

导师简介: 石磊(1980—),男,博士,副教授,博士生导师,主要从事激光信息与量子通信方面的研究。E-mail: slfly2012@163.com(通信联系人)

单光子类协议主要包括 BB84 协议、B92 协议、六态协议、SARG04 协议等。BB84 协议是第一个也是目前应用最广泛的 QKD 协议，该协议利用单光子的 4 种偏振态对随机密钥信息进行编码，并采用两组非正交基进行编解码以保证其安全性。B92 协议(二态协议)只需随机选择两种量子态进行编码，相比于 BB84 协议，降低了量子态制备的难度，其安全性同样由使用的两种非正交量子态保证。六态协议采用 6 个不同的量子态进行编码，可以作为 BB84 协议的一种扩展。六态协议的三组基之间都是非正交的，彼此之间是轮换对称的，因此其安全性同样可以得到保证。SARG04 协议的量子态制备和测量过程与 BB84 协议的完全相同，可以看作是 BB84 协议的一种改进，其可以更好地解决 BB84 协议在实际应用中遇到的“光字数分离攻击”问题。

2) 纠缠光子类协议

纠缠光子类协议主要包括 Ekert91 协议和 BBM92 协议。Ekert91 协议(E91 协议)利用纠缠态的分发与测量来实现 QKD，其安全性通过检验测量结果是否违背 Bell 不等式或 CHSH 不等式来判断。BBM92 协议选取的光源与 Ekert91 协议的相同，均利用 Bell 态的关联性来建立一致的密钥。其安全性分析与 BB84 协议的类似，通过对比数据误码率来判断窃听情况。

CV-QKD 技术的协议主要分为三大类：压缩态协议、相干态协议、纠缠态协议。

1) 高斯调制压缩态协议使用在相空间上沿 x 方向或者 p 方向压缩的相干态进行编码，使用零差探测器进行测量，x 基和 p 基是非正交的，其安全性分析与 BB84 协议的类似。

2) 相干态平衡零差探测协议(GG02 协议)使用相干态进行编码，现使用的纠错协议普遍为反响协调协议，测量方式同样是零差探测。相干态外差探测协议与 GG02 协议一样，以高斯相干态作为信源，但在接收端采用可同时测量相干态 x 分量和 p 分量的外差测量方法。

3) 上述三个协议都有与其等价的纠缠协议，Alice 和 Bob 的数据都是通过测量纠缠源的一个模式而得到的。

随着点对点量子保密通信的不断发展和完善，建立全球量子保密通信网络成为研究热点，而该网络的建立离不开自由空间 QKD 技术。自由空间 QKD 的可行性在实验室环境及外场实验中都得到了很好的证明，但仍未达到实用化条件。目前存在的主要技术难点在于自由空间通信的链路特性对 QKD 的影响以及光源、探测器等器件对 QKD 性能的限制。

本文总结了近年来国内外自由空间 QKD 技术的研究进展以及存在的问题，对 DV-QKD 技术和 CV-QKD 技术进行了比较，对自由空间 QKD 技术的前景进行了展望。

2 研究进展

DV-QKD 的研究起步较早，其技术发展较为成熟，但背景光的干扰导致其不能实现全天时通信。CV-QKD 虽然研究起步较晚，但其具有信号光制备简单、密钥分配速率高、测量方便、通信容量高等诸多优点，成为了自由空间量子保密通信领域新的研究热点之一。

2.1 DV-QKD

1987 年，Bennett 等[1]首次在桌面平台上完成了自由空间 QKD 的实验验证，通信距离为 32 cm。

2002 年，慕尼黑大学 Weinfurter 小组的 Kurtsiefer 等[2]将自由空间 QKD 的传输距离提高到了 23.4 km。该实验将相干光衰减成微弱脉冲(单个脉冲的平均光子数小于 0.1)以代替理想的单光子源。模拟单光子源中既有单光子又有多个光子，这样既会造成 QKD 的低效率，也会对整个系统的安全性造成隐患。2012 年，Moll 等[3]首次将 BB84 系统与机载平台集成在一起，实现了机载运动平台与地面站之间的 QKD，通信距离为 20 km。该实验为飞机、卫星等移动平台之间的 QKD 奠定了基础。机载平台 QKD 示意图如图 1 所示。为了避免衰减光源带来的不利影响，2014 年，Rau 等[4]在慕尼黑完成了基于单光子源的 500 m 自由空间 QKD 实验，该实验采用 BB84 协议，安全密钥率为 517 kHz，光源是电子驱动的量子点单光子源，不需要单独的激光设置光泵。

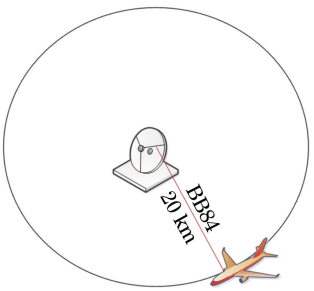

图 1 机载平台 QKD 示意图

Fig. 1 Schematic of airborne platform for QKD

2007 年,欧洲联合实验室的 Ursin 等[5]实现了 144 km 的自由空间纠缠光子单向传输实验。随后在 2009 年,Fedrizzi 等[6]验证了经历 144 km 大气高损耗自由空间信道的纠缠高保真传输。

2015 年,意大利的 Vallone 等[7]对建立地面和卫星之间的量子通信链路的可行性进行了验证实验。该实验使用激光测距卫星对地面发射的光进行反射,通信距离为 1336 km,采用双路偏振编码的 BB84 协议。

2012 年,Yin 等[8]在青海湖实现了 101 km 自由空间的量子纠缠分发实验。2013 年,Wang 等[9]在青海湖完成了关于星地 QKD 的全方位验证实验。2016 年,“墨子号”量子科学实验卫星(如图 2 所示)在酒泉卫星发射中心成功发射,轨道高度为 500 km,该卫星预计完成的科学实验包括星地高速 QKD 实验、广域量子通信网络实验、星地量子纠缠分发实验、地星量子隐形传态实验。“墨子号”卫星所进行的量子科学试验为未来的星地量子通信和全球化量子通信网络铺平了道路[10]。2017 年 7 月,Liao 等[11]在国际上首次成功实现了白天远距离的自由空间 QKD,通信距离为 53 km,通过地基实验在信道损耗和噪声水平方面有效验证了构建基于量子星座的星地、星间量子通信网络的可行性。为了抑制白天背景杂光的影响,该小组从三个方面发展关键技术。首先,他们采用 1550 nm 波段光源开展实验,优化光学系统,将噪声降低了超过一个数量级。其次,发展频率上转换单光子的探测技术及自由空间的单模光纤耦合技术,将噪声降低了约四个数量级。该小组在相距 53 km 的两点间完成了白天阳光背景下的 QKD 实验。

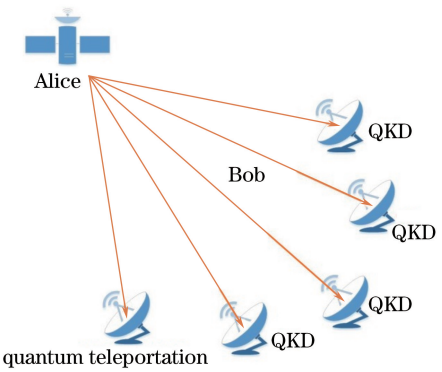

图 2 “墨子号”卫星 QKD 的示意图

Fig. 2 Schematic of QKD of satellite "Micius"

2.2 CV-QKD

2008 年,Heim 等[12-14]首次在实验上证明了自由空间 CV-QKD 技术的可行性,通信距离为 100 m。该实验在白天进行,以平衡零拍探测器作为空间滤波器和频率滤波器,滤除了背景光。其原理示意图如图 3 所示,其中 PBS 表示偏振分束器,HWP 表示半波片,S2 表示输出的电信号。

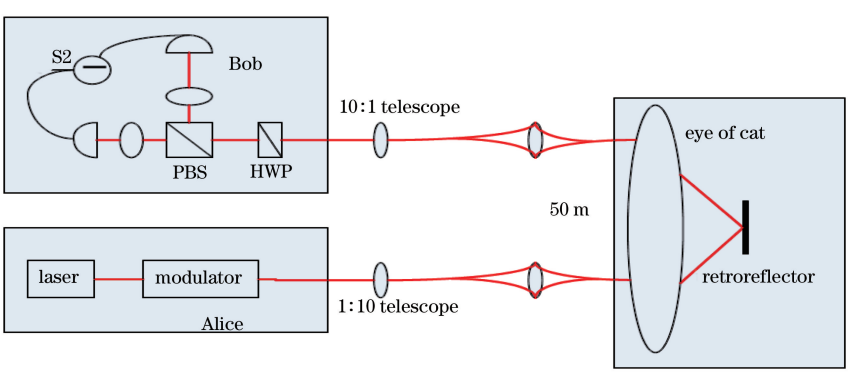

图 3 100 m 自由空间 CV-QKD 实验原理图

Fig. 3 Schematic of experimental principle of 100 m free space CV-QKD

2012 年,Usenko 等[15-17]验证了大气湍流环境下自由空间 CV-QKD 的可行性,实现了 1.6 km 的自由空间 CV-QKD。该实验在夜间进行,因为大气湍流强度在夜晚较小,且夜间实验可以提高传输效率。其原理示意图如图 4 所示,其中 EOM 表示电光调制器,QWP 表示四分之一波片,BS 表示分束器,S1 为输出的电信号。

2014 年,低轨卫星与地球静止轨道卫星之间的相干光通信的可行性已被证实[18]。2015 年,地面站到低地球轨道卫星之间通信的可行性已被证实[19]。2015 年,Elser 等[20]融合了 CV-QKD 技术与空间相干光通信技术,为空间 CV-QKD 技术创建了标准,从而使其更好地融入到已经商业化的激光通信体系中。

2016 年,Günthner 等[21]提出并探讨了测量地球静止轨道卫星发出的光信号的量子相干性的方

法。光信号从地球静止轨道卫星发送到光学地面站，通信距离为 38600 km，通过对通信链路噪声进行定量限定，分析了空间 CV-QKD 技术用于全球量子保密通信网络的可行性。

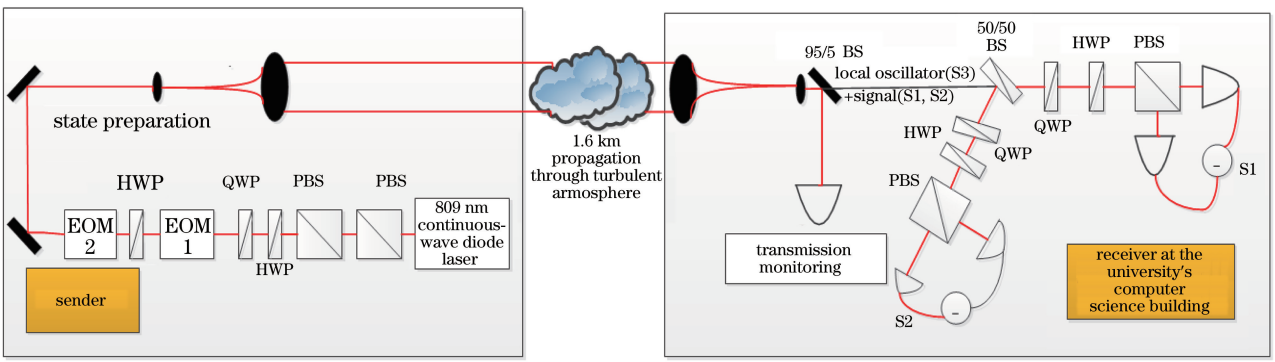

图 4 1.6 km 自由空间 CV-QKD 实验原理图

Fig. 4 Schematic of experimental principle of 1.6 km free space CV-QKD

3 技术难点

自由空间 QKD 技术存在的主要难点：1）自由空间量子信道的传输特性[22-23]对 QKD 存在影响，主要影响因素包括信道上存在的背景光、散射光以及大气衰减现象；2）实际应用中，通信器件性能的不完善所引入的额外噪声会降低通信效率，甚至严重影响通信的安全性，因此需要消除空间的量子通信噪声[24]。

3.1 DV-QKD 的技术难点

虽然 DV-QKD 技术在理论和实验上都发展得比较成熟，但在实用化过程中仍有一定的局限性，主要表现在以下几个方面。

1）背景光和散射光导致通信误码率的增大[25-27]。DV-QKD 受背景光影响的程度存在昼夜差别。白天产生漫反射的主要是大气粒子对太阳光的散射，夜晚大气中的光散射主要由月亮和银河系的辐射激发。白天太阳直射时，探测器接收到的背景光功率远大于经远距离传输后接收到的信号光功率，此时探测器要实现对远距离目标端的跟踪和通信都十分困难。而在夜晚，探测器接收到的背景光功率一般小于探测器本身的噪声功率，其对通信链路的影响较小。

探测器接收到的背景辐射光子在探测器上产生的光功率的计算公式为

$$P_r = W(\lambda)\,\Delta\lambda\Omega_r A_r, \tag{1}$$

式中 $W(\lambda)$ 为辐射谱函数，λ 为波长，$\Delta\lambda$ 为接收光谱带宽，Ω_r 为接收机视场，A_r 为接收机的光学孔径面积。

尽管背景光和散射光的干扰可以通过各种技术手段来减小，例如强光触发探测装置，通过时间窗控制探测装置的开启时间，使用干涉滤波片去除大气背景光以及通过三域（时域、空域、频域）滤波去除大气背景光等。但大气量子信道中背景光的干扰不能完全消除，在通信中仍然会不可避免地引入误码。因此，可以通过基于频率上转换单光子探测技术以及自由空间光束的单模光纤耦合技术，降低背景光和散射光对通信系统的干扰，潘建伟小组在 2017 年 7 月实现的白天远距离自由空间的 QKD 实验已经成功证明了这点。

2）单光子偏振态的随机旋转和退偏振[28-30]。自由空间的 DV-QKD 采用正交的光子偏振态实现编码，即偏振编码。这意味着单光子偏振态的随机旋转和退偏振都会导致不能传输正确的量子态，从而引入额外的误码率。

在自由空间中传播的单光子不可避免地与大气粒子发生相互作用，产生多次散射效应。单光子每被散射一次即会产生一次退偏振效应，其传输方向也被改变。因此，在经过与大气粒子的多次散射作用后，单光子的偏振态可能会发生改变，且单光子可能被散射出探测器的口径之外。

对于单次散射，单光子的偏振态可以通过 Stokes 矢量 $\boldsymbol{S}$ 来表征，即

$$\boldsymbol{S} = \begin{bmatrix} I \\ Q \\ U \\ V \end{bmatrix} = \begin{bmatrix} \langle |E_x|^2 \rangle + \langle |E_y|^2 \rangle \\ \langle |E_x|^2 \rangle - \langle |E_y|^2 \rangle \\ 2\mathrm{Re}\langle E_x E_y^* \rangle \\ 2\mathrm{Im}\langle E_x E_y^* \rangle \end{bmatrix}, \tag{2}$$

式中 I，Q，U，V 为矩阵分量，E_x 和 E_y 分别为垂直于光传播方向的两个正交的电场分量，Re 和 Im 分别代表取实部和虚部，符号 $\langle\rangle$ 和 $*$ 分别表示时间平均和复共轭。

角度 χ 表征了由大气散射引起的光子偏振态的旋转量，其表达形式为

$$\chi=\frac{1}{2}\arctan^{-1}\frac{U}{Q}。\tag{3}$$

因此，单光子的单次散射过程可由 Stokes-Mueller 公式描述，其形式为

$$\boldsymbol{S}=\begin{bmatrix}I\\Q\\U\\V\end{bmatrix}=\begin{bmatrix}m_{11}&m_{12}&m_{13}&m_{14}\\m_{21}&m_{22}&m_{23}&m_{24}\\m_{31}&m_{32}&m_{33}&m_{34}\\m_{41}&m_{42}&m_{43}&m_{44}\end{bmatrix}\cdot\begin{bmatrix}I_0\\Q_0\\U_0\\V_0\end{bmatrix}=\boldsymbol{M}\cdot\boldsymbol{S}_0,\tag{4}$$

式中 $\boldsymbol{M}$ 为 4×4 的矩阵，称为 Mueller 矩阵，m_{ij}(i，$j=1,2,3,4$)为其矩阵分量；$\boldsymbol{S}_0$ 和 $\boldsymbol{S}$ 分别表示散射前、后的光子 Stokes 矢量，I_0，Q_0，U_0，V_0 为 $\boldsymbol{S}_0$ 的矩阵分量。

散射问题的研究，一般选择一个由入射光和散射光束所构成的平面作为共同的参考平面。在 $\boldsymbol{S}_0$ 乘以散射矩阵 $\boldsymbol{M}$ 之前，应该先将 $\boldsymbol{S}_0$ 旋转一个角度 φ 至新的参考平面，φ 称为方位角。该旋转过程可通过一个旋转矩阵 $\boldsymbol{R}(\varphi)$来表示，其表达式为

$$\boldsymbol{R}(\varphi)=\frac{3}{4}\begin{bmatrix}1&0&0&0\\0&\cos(2\varphi)&\sin(2\varphi)&0\\0&-\sin(2\varphi)&\cos(2\varphi)&0\\0&0&0&1\end{bmatrix}。\tag{5}$$

这个旋转过程遵循沿着光传播方向的逆时针旋转规则。因此，散射后的光子偏振态为

$$\boldsymbol{S}=\boldsymbol{M}\cdot\boldsymbol{R}(\varphi)\cdot\boldsymbol{S}_0。\tag{6}$$

据此类推到 m 次散射的情况，有

$$\boldsymbol{S}=\boldsymbol{M}(\theta_m)\cdot\boldsymbol{R}(\varphi_m)\cdots\boldsymbol{M}(\theta_2)\cdot\boldsymbol{R}(\varphi_2)\cdot\boldsymbol{M}(\theta_1)\cdot\boldsymbol{R}(\varphi_1)\cdot\boldsymbol{S}_0。\tag{7}$$

从(6)、(7)式中可清楚发现，单光子经过与大气粒子的单次散射和多次散射后，偏振态发生改变，即产生了单光子偏振态的随机旋转和退偏振现象。

3) 器件的不完美带来的噪声和干扰。完美的单光子源制备起来比较困难，目前绝大多数 DV-QKD 系统是通过将相干光衰减成微弱脉冲(单个脉冲的平均光子数小于 0.1)以代替理想的单光子源。在模拟单光子源中，90%(光脉冲数百分数，全文同)的脉冲中是不含光子的，9.5%的脉冲含一个光子，0.5%的脉冲含多个光子，这造成了 QKD 的低效率，也会对整个系统的安全性造成隐患。虽然学者们提出了诱骗态方案来弥补这种缺陷，但会增加实际系统的复杂度。

4) 单光子的检测技术实现困难。现阶段普遍使用基于硅雪崩二极管的单光子探测器[31]，其量子效率最高可达 76%，但其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。用于超远距离(大于 200 km)密钥分发的低温超导单光子探测器[32]，体积较大且成本昂贵，目前仅用于科学研究，高效且实用的单光子检测技术还有待进一步的研究。

此外，DV-QKD 所携带的信息比特较少也是一个较大的局限。

3.2 CV-QKD 的技术难点

相比于 DV-QKD 的实现方案，CV-QKD 技术具有信号光制备简单、密钥分配速率高、测量方便、通信容量高等诸多优点[33]。

1) CV-QKD 可以全天时工作。其将信息加载到光场的正交振幅和正交相位上，通过平衡零差检测器对光场的两正交分量进行测量。不同于单光子探测器只进行单纯的强度测量，平衡零差检测器借助一束本地光进行干涉测量。因此，使用平衡零差检测的方法来检测信号光相当于加了一个天然的滤波器，可以有效滤除背景杂光，因此 CV-QKD 可以全天时工作。

2) CV-QKD 的光源可以是普通的相干激光源，无需制备复杂的单光子脉冲，所需的条件也没有单光子源的那么苛刻。CV-QKD 一般都采用 GG02 协议，普通的相干光源即可作为信源，不涉及光场的任何非经典性质，方案简单，容易实现。

3) 在检测方面，CV-QKD 采用平衡零差检测器[34]，与单光子探测器相比，具有成本低、易实现的优势。平衡零差检测器一般不需要进行制冷，在室温条件下即可工作，且制造成本相对较低。

此外，CV-QKD 技术分发的是符号而非比特，因此具有比 DV-QKD 更高的通信效率。因此，CV-QKD在量子通信实用化方面比 DV-QKD 更有优势。

CV-QKD 的理论安全性和实际可行性已被学者们证实。目前，CV-QKD 已逐步走向实用化，其系统的稳定性和兼容性成为下一步的研究重点。在实用化进程中，CV-QKD 技术应用中的发展方向主要有以下几个。

1) 更高的系统稳定性。CV-QKD 系统传输的是微弱的量子信号，因此容易受到大气环境的干扰。光源的不稳定性和相位抖动等因素都会对系统的工作状态产生很大的影响。在 CV-QKD 系统中，信号

光的强度在单光子级别上，非常容易受到环境因素和系统噪声的影响[35]，产生非常大的随机相位漂移[36]。相位抖动是 CV-QKD 系统的一大难题，环境因素造成的抖动往往通过影响平衡零差检测器而影响整个系统。最主要的环境因素是大气湍流，它会导致相位畸变[37-38]。当存在温度梯度时，大气湍流的运动引起了大气折射率的波动。大气湍流定义为由小的温度波动导致的大气折射率的波动，早期 Kolmogorov 的研究表明大气湍流具有一定的统计一致性。当光束通过大气湍流时，大气湍流效应将引起光波瞬时辐射强度的波动及相位波动。

对于一个具体的自由空间光通信系统，大气湍流引起的相位变化功率谱密度函数（以下简称相位功率谱密度函数）$\Phi_\phi(\kappa)$ 与折射率波动功率谱密度函数 $\Phi_n(\kappa)$ 的关系为

$$\Phi_\phi(\kappa)=2\pi^2\kappa^2L\Phi_n(\kappa), \tag{8}$$

式中 L 为光在大气中的传输距离，$\kappa=2\pi/\lambda$ 为波数。

Kolmogorov 谱的相位功率谱密度函数为

$$\Phi_\phi(\kappa)=0.49r_0^{-5/3}\kappa^{-11/3},\ 1/L_{\text{outer}}\ll\kappa\ll1/L_{\text{inner}}, \tag{9}$$

式中 L_{outer} 为湍流外尺寸，L_{inner} 为湍流内尺寸。

相位结构函数表示为

$$D_\phi(\kappa)=8\pi\int_0^\infty\kappa^2\Phi_\phi(\kappa)\left[1-\frac{\sin(\kappa R)}{\kappa R}\right]\mathrm{d}\kappa, \tag{10}$$

式中 R 为相位波前两个点的分隔距离。

Kolmogorov 大气湍流谱模型下的相位结构函数为

$$D_\phi(\kappa)=6.88\left(\frac{R}{r_0}\right)^{\frac{5}{3}}, \tag{11}$$

式中 $r_0=(0.432\kappa^2C_n^2L)^{-3/5}$ 为大气相干长度，也称作 Freid 参数，其中 C_n^2 为折射率结构常数。

CV-QKD 将信息加载到光场的正交振幅和正交相位上，大气湍流会导致信号光的相位畸变，从而使平衡零差探测器的误码率大大增加。军事或商业领域的实用化都对系统的稳定性有着很高的要求，因此使系统具备良好的抗干扰能力是 CV-QKD 系统研究的重要课题[39]。

2）更高效的后处理算法。后处理算法的好坏关系到最后能否生成用于实际加密的密钥。尤其是其中的密钥协商模块，它的效率对最终的安全密钥率和安全传输距离有着至关重要的影响。目前，CV-QKD 的后处理算法主要有两种：软件实现和硬件实现。软件实现后处理算法是一种常见的方法，但其速度受限于计算机性能，很难进一步提高，尤其是处理的数据规模较大时，计算机处理起来相当困难。近年来，硬件技术在通信领域发展很快，能显著提高处理性能，特别是低密度奇偶校验码（LDPC 码）可以使用并行译码来提高译码的速度。故利用硬件实现 CV-QKD 的后处理算法成为必然趋势，也是目前的研究热点之一。

3）更高的安全比特率。现有的 CV-QKD 系统，其传输的安全比特率普遍不高。受系统的工作频率和检测器的带宽所限，在超过 25 km 的距离下，其安全比特率通常从几百比特率到 100 kbit/s 不等。这样的安全比特率不足以应用到大数据流量的加密通信中，如视频通信或大文件传输等，因此，提高密钥的传输速率是实用化道路上十分关键的问题。

4）更集成化的系统结构。为了使 CV-QKD 系统逐步实现实用化，光路系统的小型化和电路系统的集成化是必然的发展趋势。现有的大多数 CV-QKD 系统，其体积较大、光路的空间利用率不高，控制电路系统也必须借助电脑，这些都为未来系统的实用化带来了不便。因此，优化光路、利用小体积的激光器来制备脉冲相干光源、脱离计算机使控制系统独立工作等都是亟待解决的问题。

4 结束语

介绍了量子通信的产生和发展历程、QKD 技术的概念及其在量子通信中的地位以及几种典型协议的发展近况与安全性。对基于连续变量与离散变量的自由空间 QKD 技术进行了对比。同时，探讨了自由空间通信的链路特性对 QKD 的影响以及光源、探测器等器件对 QKD 性能的限制，特别是信号光的退偏振特性以及相位畸变现象。在下一步的工作中，应找出合适的相位补偿算法，有效解决自由空间 CV-QKD 技术中的相位畸变问题，以降低误码率，提高安全密钥率。

参 考 文 献

[1] Bennett C H, Bessette F, Brassard G, *et al*. Experimental quantum cryptography[J]. Journal of Cryptology, 1992, 5(1): 3-28.

[2] Kurtsiefer C, Zarda P, Halder M, *et al*. A step towards global key distribution[J]. Nature, 2002, 419(6906): 450.

[3] Moll F, Horwath J, Fuchs C, *et al*. Air to ground quantum key distribution[C]. SPIE, 2013, 8518:

85180D.

[4] Rau M, Heindel T, Unsleber S, *et al*. Free space quantum key distribution over 500 meters using electrically driven quantum dot single-photon sources: a proof of principle experiment[J]. New Journal of Physics, 2014, 16(4): 413-418.

[5] Ursin R, Tiefenbacher F, Schmitt-Manderbach T, *et al*. Entanglement-based quantum communication over 144 km[J]. Nature Physics, 2007, 3(7): 481-486.

[6] Fedrizzi A, Ursin R, Herbst T, *et al*. High-fidelity transmission of entanglement over a high-loss free-space channel[J]. Nature Physics, 2009, 5(6): 389-392.

[7] Vallone G, Bacco D, Dequal D, *et al*. Experimental satellite quantum communications [J]. Physical Review Letters, 2015, 115(4): 040502.

[8] Yin J, Ren J, Lu H, *et al*. Quantum teleportation and entanglement distribution over 100-kilometre free-space channels[J]. Nature, 2012, 488(7410): 185-188.

[9] Wang J, Yang B, Liao S, *et al*. Direct and full-scale experimental verifications towards ground-satellite quantum key distribution [J]. Nature Photonics, 2013, 7(5): 387-393.

[10] Gibney E. Chinese satellite is one giant step for the quantum internet[J]. Nature, 2016, 535(7613): 478.

[11] Liao S K, Yong H L, Liu C, *et al*. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication [J]. Nature Photonics, 2017, 11(116): 509-513.

[12] Heim B, Elser D, Bartley T J, *et al*. Atmospheric channel characteristics for quantum communication with continuous polarization variables[J]. Applied Physics B, 2009, 98(4): 635-640.

[13] Elser D, Bartley T, Heim B, *et al*. Feasibility of free space quantum key distribution with coherent polarization states [J]. New Journal of Physics, 2009, 11(4): 045014.

[14] Heim B, Elser D, Bartley T, *et al*. Free space quantum key distribution with coherent polarization states [C]. European Conference on Lasers and Electro-Optics 2009 and the European Quantum Electronics Conference, 2009: ED5_4.

[15] Usenko V C, Heim B, Peuntinger C, *et al*. Entanglement of Gaussian states and the applicability to quantum key distribution over fading channels[J]. New Journal of Physics, 2012, 14(9): 093048.

[16] Heim B, Peuntinger C, Killoran N, *et al*. Atmospheric continuous-variable quantum communication[J]. 2014, 16(11): 113018.

[17] Peuntinger C, Heim B, Muller C R, *et al*. Distribution of squeezed states through an atmospheric channel[J]. Physical Review Letters, 2014, 113(6): 1210-1217.

[18] Heine F, Mühlnikel G, Zech H, *et al*. LCT for the European data relay system: in orbit commissioning of the Alphasat and Sentinel 1A LCTs[C]. SPIE, 2015, 9354: 93540G.

[19] Moll F, Weinfurter H, Rau M, *et al*. Aerospace laser communications technology as enabler for worldwide quantum key distribution [C]. SPIE, 2016, 9900: 99000K.

[20] Elser D, Gunthner K, Khan I, *et al*. Satellite quantum communication via the Alphasat laser communication terminal-quantum signal from 36 thousand kilometers above earth [C]. IEEE International Conference on Space Optical Systems and Applications, 2015: 1-4.

[21] Günthner K, Khan I, Elser D, *et al*. Quantum-limited measurements of optical signals from a geostationary satellite[J]. Optica, 2016, 4(6): 611-616.

[22] Tsiftsis T A, Sandalidis G K, *et al*. Optical wireless link with spatial diversity over strong atmospheric turbulence channels [J]. IEEE Transactions on Wireless Communications, 2009, 8(2): 951-957.

[23] Ricklin J C, Hammel S M, Eaton F D, *et al*. Atmospheric channel effects on free-space laser communication [J]. Journal of Optical & Fiber Communications Reports, 2006, 3(2): 111.

[24] Liu Y, Chen T Y, Wang L J, *et al*. Experimental measurement-device-independent quantum key distribution [J]. Physical Review Letters, 2013, 111(13): 130502.

[25] Peterson C G. Free-space quantum key distribution in daylight [J]. Journal of Modern Optics, 2002, 47(2/3): 549-562.

[26] Garcíamartínez M J, Denisenko N, Soto D, *et al*. High-speed free-space quantum key distribution system for urban daylight applications[J]. Applied Optics, 2013, 52(14): 3311-3317.

[27] Lu Q, Zeng F, Zhang Y L, *et al*. Influence of sky background radiation on bit error rate of atmospheric laser communication system [J]. Laser & Optoelectronics Progress, 2016, 53(7): 070103.
鲁强, 曾飞, 张玉良, 等. 天空背景辐射对大气激光

通信系统误码率的影响[J]. 激光与光电子学进展, 2016, 53(7): 070103.

[28] Yu Z Y, Li M, Lu P F. Photon polarizations in free-space quantum communication[J]. Journal of Beijing University of Posts & Telecommunications, 2013, 36(2): 1-9.

[29] Toyoshima M, Takenaka H, Shoji Y, *et al*. Polarization measurements through space-to-ground atmospheric propagation paths by using a highly polarized laser source in space[J]. Optics Express, 2009, 17(25): 22333-22340.

[30] Chen S Y, Ding P F, Pu J X. Research on beam and degree of polarization of partially coherent radially polarized beam in turbulent atmosphere[J]. Laser & Optoelectronics Progress, 2015, 52(9): 090101.
陈顺意, 丁攀峰, 蒲继雄. 大气湍流中部分相干径向偏振光束的光斑及偏振度研究[J]. 激光与光电子学进展, 2015, 52(9): 090101.

[31] Zhang X, Wan J, Yan C, *et al*. The development and application of single-photon detectors[C]. SPIE, 2008, 7055: 70550V.

[32] Dong W Q, Li A, Xu Z Z, *et al*. Development of cryogenic system used in quantum communication with superconducting single photon detector [J]. Cryogenics, 2016(4): 45-49.
董文庆, 李奥, 许哲真, 等. 量子通信用超导单光子探测低温系统的研制[J]. 低温工程, 2016(4): 45-49.

[33] Zhang Z, Zhu C, He G. Improving the performance of continuous variable quantum key distribution using fading effects of free-space channel[C]. SPIE, 2015, 9619: 96190B.

[34] Chen J J, Han Z F, Zhao Y B, *et al*. The effect of balanced homodyne detection on continuous variable quantum key distribution[J]. Acta Physica Sinica, 2007, 56(1): 5-9.
陈进建, 韩正甫, 赵义博, 等. 平衡零拍测量对连续变量量子密钥分配的影响[J]. 物理学报, 2007, 56(1): 5-9.

[35] Gui M, Huang M Q, Liang L M. Continuous-variable quantum key distribution with random intensity fluctuation of the local oscillator[C]. SPIE, 2016, 10158: 1015805.

[36] Jiao H S, Wang Y B, He M, *et al*. Research about effect of phase drift on phase-coding QKD system and intercept-resend attack[J]. Laser & Optoelectronics Progress, 2015, 52(4): 042703.
焦海松, 王衍波, 何敏, 等. 相位漂移对相位编码QKD系统及截获-重发攻击的影响研究[J]. 激光与光电子学进展, 2015, 52(4): 042703.

[37] Han B B, Pei C X. Analysis on free space quantum communication system [J]. Journal of PLA University of Science & Technology, 2011, 12(6): 574-576.
韩宝彬, 裴昌幸. 自由空间量子通信系统分析[J]. 解放军理工大学学报, 2011, 12(6): 574-576.

[38] Li J, Zhang Z, Gao J, *et al*. Bandwidth of adaptive optics system in atmospheric coherent laser communication[J]. Optics Communications, 2016, 359: 254-260.

[39] Ma X C, Sun S H, Jiang M S, *et al*. Local oscillator fluctuation opens a loophole for Eve in pratical continuous-variable quantum-key-distribution systems[J]. Physical Review A, 2014, 88(2): 290-296.