连续变量量子密码术*

陈进建　韩正甫†　赵义博　桂有珍　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　文章综述了连续变量量子密码术的基本原理，突出了其在光源制备、光子探测以及量子密钥生成的码率等方面相对于单光子量子密码术的优越性，给出了连续变量量子密码术的安全性以及对线路噪声的具体要求，提出了连续变量量子密码术目前所面临的主要困难和今后的发展前景.

关键词　密码学，量子密钥分配，综述，连续变量，相干态

Continuous variable quantum key distribution

CHEN Jin-Jian　HAN Zheng-Fu†　ZHAO Yi-Bo　GUI You-Zhen　GUO Guang-Can
(*Laboratory of Quantum Information*, *University of Science & Technology of China*, *Hefei*, 230026, *China*)

Abstract　This paper describes the primary principle of the continuous – variable quantum key distribution, comparing to single photon quantum key distribution, it is advantageous in preparing light sources, detecting photons and enabling higher key distribution rates. The security of this protocol and the limit of the excess noise have been shown in order to guarantee the key securely. Finally, we pick up the obstacle which will face and point its direction.

Keyword　cryptography, quantum key distribution, summary, continuous variable, coherent state

1　引言

在信息化时代，及时、准确、安全的信息传递尤为重要. 密码学正是研究如何有效安全地传递信息的一门学科，其基本思想是将传递的信息采用某种方式进行干扰，以至只有合法用户才能从中恢复出原来的信息，而非法用户无法理解被干扰了的信息. 实现这一目标需要通信双方共同掌握一组比特序列，这组比特序列像钥匙一样，本身并不包含任何信息，但是有使用价值，密码学中称为密钥，使得通信双方拥有密钥的过程称为密钥分配.

经典密码学可分为公钥密码和私钥密码，公钥密码的安全性多数建立在算法的复杂度之上. 例如 1977 年美国出了一道将一个 129 位数分解成一个 64 位和一个 65 位素数的乘积解密题，估计用当时的计算机需要用 4×10^{16} 年，然而到了 1994 年，只用了 8 个月就能解出[1]. 事实上，公钥密码面临着计算机速度、新计算方法和量子计算机的三重威胁，只能做到现时技术条件下的安全. 私钥密码采用一次一密的 Vernam 码，原则上可以做到绝对安全，但是密钥分配问题无法解决，一次一密的密钥分配更是不可企及的难题. 量子密码学巧妙地解决了密钥分配这一关键问题，其安全性基于量子力学的基本原理，只要量子力学的基本原理正确，就能保证密钥的安全性，从而克服了经典密码学的弊端.

最早的也是目前研究最多的量子密码协议是 Bennet 和 Brassard 于 1984 年提出的所谓 BB84 协议[2]，该协议以单光子作为信息载体，用光子的自旋、偏振或路径量子态编码信息，即以光子自旋的上与下、偏振的水平与垂直或光子通过的路径代表信

* 国家重点基础研究发展规划（批准号：2001CB309301）、国家自然科学基金（批准号：60537020）、中国科学院知识创新工程重要方向资助项目
2006 – 03 – 02 收到初稿，2006 – 04 – 13 修回

† 通讯联系人. Email：zfhan@ustc.edu.cn

息的 0 或 1,成为一个比特的信息. 这种信息传输以单光子方式进行,编码的变量也是分立的. 然而,以单光子为信息载体面临着很大的技术挑战. 首先,目前还没有理想的单光子源,多数是以强衰减弱相干激光脉冲模拟单光子源,使每个脉冲含有两个以上光子的几率很小,在实际的密码系统存在传输损耗的情况下,即使含有两个以上光子的脉冲很少也可能带来安全隐患[3];其次,不论是光纤还是自由空间传输,损耗都无法避免,再加上在通信波段,单光子探测器量子效率只有 10% 左右,传输距离有限,实际有效传输码率非常低. 目前在光纤中实验上的最远传输距离只做到 150 公里左右[4],实际传输码率更低达每秒零点几到几比特. 这种指标给量子密码技术的实际应用带来了严重的限制.

在保证量子密钥分配的安全性基础上,是否可以采用‘强光’而不是单个光子实现量子密钥分配?如果可能,或许可以改进密钥的分配距离,提高密钥分配速率?答案是并非完全不可能. 事实上,人们早在 1999 年就提出基于‘强光’的所谓连续变量量子密钥分配协议[5]. 目前已有基于压缩态、纠缠态和相干态为基础的多种量子密钥分配协议[6—12],安全性也得到了很好的证明[13—20],这种协议编码所用的变量是可连续取值的坐标、动量、振幅以及相位等. 正因为这些编码变量是连续变化的,通常称为连续变量量子密钥分配协议. 连续变量量子密钥分配所需光源发射频率高,使用多光子光源,信号较强,适合远距离的密钥传输,不需要复杂的单光子探测器,而是采用零拍探测测量光强,通常在室温条件下进行,而且几乎不受普通背景光噪声的影响,测量频率可达数 GHz,量子效率高达 99%,克服了单光子探测器探测效率低的弊端,可大幅度提升了码率,因此连续变量量子密钥分配正越来越多的受到人们的关注. 为介绍和比较连续变量量子密钥分配协议,我们先对涉及到的各种非经典光源和探测方式做简单的介绍.

2 光源

2.1 相干态

相干态[21]是量子理论所能容许的最逼近经典极限的量子态,它是消灭算符 a 的本征态 $a\mid\alpha\rangle=\alpha\mid\alpha\rangle$,由于 a 为非厄米算符,因此本征值 α 为复数,本征值 α 的模平方为相干态的平均光子数,光子数呈泊松分布. 相干态是非正交态,任何两个不同本征值的相干态互相不正交. 定义两个厄米算符 $x=\frac{1}{2}(a+a^{+})$,$p=\frac{1}{2i}(a-a^{+})$,其中 a^{+}、a 分别为产生、消灭算符. 经计算易知,两个算符的平均值分别为消灭算符本征值 α 的实部和虚部($\langle x\rangle=\mathrm{Re}\alpha$,$\langle p\rangle=\mathrm{Im}\alpha$),在 α - 复平面内(即相空间中),可理解为 α 的两个正交分量($x=\alpha\sin\theta$,$p=\alpha\cos\theta$),也可将这两个厄米算符 x 和 p 定义为广义的坐标和动量算符. 厄米算符 x 和 p 在相干态中的起伏$\langle(\Delta x)^2\rangle=\langle(\Delta p)^2\rangle=\frac{1}{4}$,因此相干态是厄米算符 x 和 p 的最小测不准态,两者的起伏相同,而且与相干态本征值 α 无关. 换句话说,任何相干态的量子起伏都相同,真空态($\alpha=0$)是相干态的特例,因此相干态的量子起伏实质上就是真空的起伏,相干态可以通过平移算符 $D(\alpha)$ 平移真空态得到. 相干态在相空间的起伏呈现如图 1 所示.

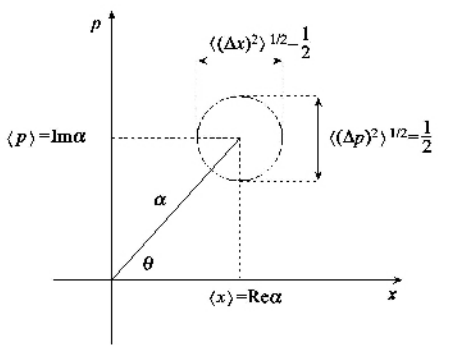

图 1 相干态在相空间中的表示

2.2 压缩态

压缩态[21]光场是非经典光场,泛指一个正交算符的起伏比相干态相应分量的起伏小的量子态,它也是一种非正交态. 压缩态可以由压缩算符 $S(r)$ 作用在真空态上,使其中一个正交分量上的真空起伏减少,而另一分量上的起伏变大,即圆状的零点起伏被压扁而变成椭圆,然后通过平移算符 $D(\alpha)$ 使压缩真空态产生平移而得到,r 为压缩参数. 压缩态的平均光子数$\langle n\rangle=\mid\alpha\mid^2+\mathrm{sh}^2 r$,第一项代表相干成分的平均光子数,第二项代表压缩效应的贡献. 经计算同样可得到厄米算符x和p在压缩态中的起伏$\langle(\Delta x)^2\rangle=\frac{1}{4}e^{-r}$,$\langle(\Delta p)^2\rangle=\frac{1}{4}e^{r}$,当 $r=0$ 时,压缩态便退化成相干态;而当 r 很大时,测不准椭圆被压扁呈垂直于 x 轴的直线,对应于 $r\to\infty$ 的压缩态,便是算符 x 的本征态,x 分量的起伏趋于零,而 p 分量的起伏按指数形式发散. 压缩态在相空间的起伏

呈现如图 2 所示的椭圆状.

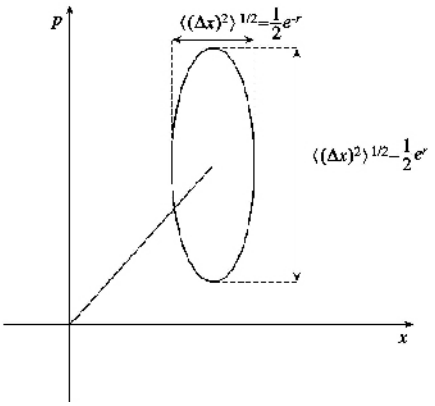

图 2　压缩态在相空间中的表示

2.3　纠缠态

纠缠态也是非经典光场,体现非局域的纠缠特性,最早对非局域关联的讨论仅局限于两个经典运动的粒子[22]. 1988 年,Reid 将坐标与动量的关联从理论上上升到对连续变量的量子非局域关联[23],从而确立了连续变量 EPR 纠缠对的数学模型. 连续变量 EPR 纠缠对可以由相干态经过 nondegenerate optical parametric amplifier(非简并光学参量放大器,简称 NOPA)过程来产生. 两束纠缠的 EPR 光束对应的分量存在一定的 EPR 关联,我们可以通过对其中一束光的某一分量进行测量来估算另一束光相应分量的值,从而体现 EPR 纠缠对的非局域特性.

3　平衡零拍探测

平衡零拍探测是连续变量量子密钥分配的基本测量方法,其原理见图 3. 这里以相干态为例对平衡零拍探测做简单描述,而压缩态和纠缠态的测量与此类似. 平衡零拍探测包括两路光:信号光 a 和参考光 b,根据经验,两者的比值在 40dB 以上为佳. 两路光经 50∶50 的分束器进行干涉,用两个探测器分别测量干涉后两路光的光强,最后经减法器相减后输出. 理论计算可得最终输出结果为 $|\alpha|\sin(\theta-\phi)$(已经归一化),其中 α 为信号光振幅,θ,ϕ 分别为信号光和参考光的相位. 当调制参考光的相位 $\phi=0$ 时,输出结果为 $|\alpha|\sin\theta$,对照相干态在相空间中的表示可知,得到的结果为相干态的 p 分量;当调制参考光的相位 $\phi=-\pi/2$ 时,输出结果为 $|\alpha|\cos\theta$,为相干态的 x 分量. 连续变量量子密钥分配正是通过调制参考光的相位来实现密钥分配.

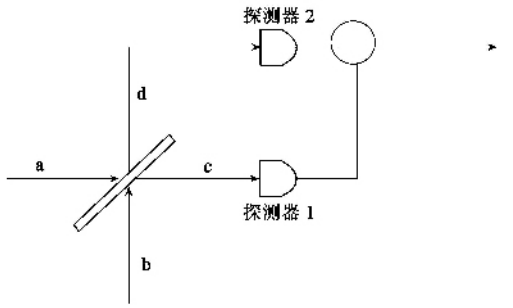

图 3　平衡零拍探测原理 其中 a,b 表示信号光和参考光的消灭算符,c,d 表示输出光的消灭算符,探测器 1,2 分别 测量 d,c 两路光的光子数相减后输出结果

4　连续变量量子密钥分配的基本原理

4.1　连续变量量子密码术的发展历程

早期的连续变量量子密钥分配方案是从单光子的量子密钥分配方案中发展而来的,由于使用了多光子光源和零拍探测,在一定程度上提升了密钥生成的码率[6,7,11],通常将这时期的方案称为 hybrid 型量子密码术. 虽然使用了多光子作为光源,但是由于方案本身的限制,平均光子数只有 1 光子/脉冲,对密钥的生成码率提高很有限. 另外,同单光子量子密钥分配类似,共享密钥的双方 Alice 和 Bob 直接共享的是二进制的密钥,这样一束脉冲光最多只能得到 1 比特的密钥,而根据信息论的 Shannon 原理,只要信噪比足够高,一束脉冲光能够获得多比特的密钥量. 为了充分利用信道的信噪比,Grosshans 等人最早提出了全连续变量量子密钥分配方案[9],这种方案共享的是十进制的密钥元素,再通过 reconciliation 和保密放大后转化为二进制密钥. 由于全连续变量量子密码术在码率和密钥量上有很大的优势,因此 hybrid 型量子密码术已经基本被摒弃,此后提到的连续变量量子密码术一般就指全连续变量量子密码术.

4.2　连续变量量子密钥的分配过程

连续变量量子密码术使用的多光子光源主要有相干态、压缩态和纠缠态,它们实现密钥分配的基本原理大致相同,都是由 Alice 制备光源,然后发送给 Bob,Bob 通过零拍探测随机选择测量信号光的 x 分量或者 p 分量来共享十进制的密钥元素. 压缩态和纠缠态在目前的实验条件下制备比较困难,更重要的是这两种非经典光场很不稳定,对损耗特别敏感,在光纤中传输

时,容易失去其非局域的纠缠性质而退化为相干态,无法实现远距离的密钥分配. 因此,压缩态和纠缠态的固有性质决定了其不能成为连续变量量子密钥分配的理想光源. Grosshans 等人在文献[9]中证明了实现密钥分配并不需要非经典光场,需要的只是非正交态,证明了使用相干态同样能实现相等安全水平的量子密钥分配,而且相干态在远距离光纤传输中非常稳定,与传输距离几乎没有关系,是实现远距离连续变量量子密钥分配理想的光源.

相干态的密钥分配过程如下:(1) Alice 从一个中心位置为 0、方差为 $V_A N_0$ 的高斯函数中,随机选取 x_A 和 p_A 两个数,其中 V_A 为信号的调制幅度,N_0 为真空起伏;(2) 接着,Alice 对从激光器中发射的信号光同时进行相位和振幅的调制,使调制后的信号光为相干态 $|x_A + \mathrm{i}p_A\rangle$,然后发送给 Bob;(3) Bob 随机选择测量 x_A 或者 p_A,并通过公开信道,告诉 Alice 每次所采用的测量基;(4) 经过多次的公开对基后,Alice 和 Bob 之间就建立了一组相关的十进制密钥元素,然后 Alice 和 Bob 通过公开信道公开一部分密钥元素进行比较,来估算误码率、信道传输率等参数,从而得到他们之间的互信息量 I_{AB} 以及可能泄漏给 Eve 的信息量 I_{AE}(或 I_{BE}). 理论上,Alice 和 Bob 能够从密钥元素中提取 $S = I_{AB} - I_{AE}$ 或($I_{AB} - I_{BE}$)的安全密钥,这主要是由 reconciliation[24—27] 和 privacy amplification(保密放大)两个步骤来完成;(5) Reconciliation 的作用是将 Alice 和 Bob 共享的十进制密钥元素编码为二进制的密钥,并进行纠错,使 Alice 和 Bob 共享相同的二进制密钥;(7) 通过 reconciliation 后,Alice 和 Bob 共享的相同的二进制密钥并非绝对安全,其中有部分信息可能被 Eve 窃听,需要通过保密放大过程来去掉被 Eve 窃听的信息,最终得到一组可以用来加密信息的安全的二进制密钥.

4.3 连续变量量子密钥分配的安全性分析

连续变量量子密码术的安全性和 reconciliation 有很大的关系,不同的 reconciliation 方案,连续变量量子密码术的安全性和安全距离是不一样的. 根据 reconciliation 的纠错方向,可以分为 direct reconciliation(简称 DR)和 reverse reconciliation(简称 RR). DR 是指 Alice 通过公开信道发送纠错信息给 Bob,Bob 猜测 Alice 的值,并通过纠错信息进行纠错,这时信号光的传输方向和纠错方向相同;RR 是指 Bob 通过公开信道发送纠错信息给 Alice,Alice 猜测 Bob 的测量值,并通过纠错信息进行纠错,这时信道光的传输方向和纠错信息的传输方向相反. 理论上证明,对于 DR 方案,在信道传输率大于 50%(信道衰减小于 3dB)时,密钥是安全的;对于 RR 方案,在任意的信道传输率下(突破了 3dB 极限),密钥均是安全的.

在 DR 方案中,当信道衰减小于 50%(小于 3dB)时,连续变量的量子克隆极限[28—31] 保证了非相干攻击[32,33] 方案下,密钥是安全的. 当信道衰减大于 3dB 时,通过分束攻击 Eve 能获得比 Bob 更多的信息量,这时的密钥不再安全,因此 DR 方案存在 3dB 的损失极限. 在 RR 方案中,Eve 需要通过测量 Alice 的值来间接猜测 Bob 的测量值,因此不管信道衰减有多大,Alice 和 Bob 之间的互信息量总是比 Eve 和 Bob 之间的互信息量要大,密钥总是安全的. 从信息论的角度来说,Alice 和 Bob 之间的互信息量 $I_{AB} = \frac{1}{2}\log_2 \frac{V+\chi}{1+\chi}$,而 Eve 和 Bob 之间的互信息量 $I_{BE} = \frac{1}{2}\log_2 G^2 (V+\chi)\left(\frac{1}{V}+\chi\right)$ [12],其中 G 为信道传输率,χ 为线路的额外噪声,包括由于信道衰减引起的真空噪声 $\chi_0 = \frac{1-G}{G}$,以及线路增加的额外噪声 ε. 如果不考虑线路增加的额外噪声 $\varepsilon = 0$,那么在任意的信道传输率下,均满足 $I_{AB} > I_{BE}$. 当 $\varepsilon \neq 0$ 时,要使密钥安全,ε 需满足 $\varepsilon < 1 - \frac{1}{V} - \frac{1}{G} - \frac{1}{2}\left(1 - \frac{1}{V}\right) + \sqrt{\frac{1}{G^2} + \frac{1}{4}\left(1 - \frac{1}{V}\right)^2}$,在信道传输率 $G \to 0$ 时,$\varepsilon < \frac{1}{2}\left(1 - \frac{1}{V}\right)$,由此可见,线路引入的额外噪声对相干态的密钥分配的安全性影响很大,在高损耗的信道中,只有满足 $\varepsilon < \frac{1}{2}\left(1 - \frac{1}{V}\right)$,密钥才是安全的. 图 4 是相干态、压缩态以及纠缠态所能允许的最大线路额外噪声的比较. 由图 4 我们可以看出,在高损耗信道中,EPR 纠缠态和压缩态所能允许的最大线路额外噪声要优于相干态,这是由它们的非局域纠缠性质决定的. 另外,在信道衰减不是很大的情况下,DR 方案所允许的线路最大噪声要优于 RR 方案,因此在低损耗高噪声的信道中使用 DR 方案代替 RR 方案来实现密钥分配更为合适.

5 连续变量量子密钥分配的实现

2003 年,Grosshans 等人在实验室里实现了连续

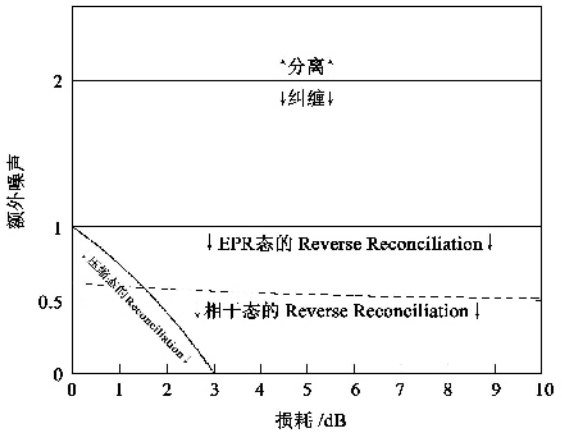

图4　各种连续光源下所能允许最大线路额外噪声的比较

变量的密钥分配. 实验主要由激光器、M－Z 干涉仪、零拍探测以及读出系统等几部分组成. Alice 通过 PM1 和 AM 来调制信号光的相位和振幅，将信息加载在信号光的相位和振幅上. Bob 通过 PM2 调制参考光的相位来随机选择测量信号光的 2 个分量，最后通过零拍探测实现密钥共享. 实验中采用 780nm 波长的激光作为光源，发射频率为 800MHz，信号光强度约 250 光子/脉冲，参考光为 1.3×10^{8} 光子/脉冲，整个实验的零拍探测效率为 0.81，其中包括光纤传输率 0.92，模式匹配效率 0.96 以及光电二极管的量子效率 0.92. 在这个桌面实现中，当模拟光纤无损耗时，可以得到 1.7Mbit/s 的安全密钥量，当模拟光纤损耗为 3.1dB 时，可以得到码率可达 75kbit/s 的安全密钥量.

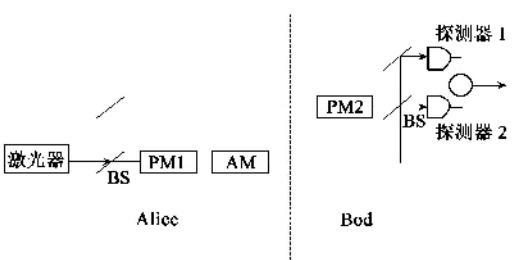

图5　连续变量量子密钥分配的实现

6　连续变量量子密码学当前所存在的困难

6.1　编码方案

连续变量量子密钥分配过程中，Alice 和 Bob 首先共享的是一组十进制的密钥元素，需要通过编码方案将其转化为二进制密钥. 理论上，编码前后 Alice 和 Bob 之间的互信息量应该是不变的，接近 Shannon 极限. 然而目前已知的编码方案还达不到这个要求，而且编码后损失的信息量会随着传输距离的增加而增加，这也是目前在信道损耗大于 6dB 时得不到安全密钥的根本原因. 按照目前的编码方案，要想提高效率，使编码后的互信息量达到 Shannon 极限，就必须加大计算量，而且随着效率的提高，计算量呈指数增长，目前计算能力还不足以应付如此庞大的计算量. 因此，能否找到一个合理有效的编码方案，使计算量随编码方案呈多项式增长，以求达到编码后的互信息量能任意接近 Shannon 极限，这是目前连续变量量子密码术所急待解决的问题.

6.2　噪声

连续变量量子密钥分配实验中存在各种各样的噪声，这些噪声影响着密钥生成的码率及密钥的安全性. 理论上分析，要使密钥安全，线路增加的额外噪声需要小于$\frac{1}{2}GN_0$[26]，当传输 50 公里时，这个噪声就需要小于$\frac{1}{20}N_0$，距离越远，对这个噪声的要求越高. 因此要想实现远距离的密钥传输，提高信号传输过程中的稳定性，减少线路增加的额外噪声是必须解决的问题.

7　连续变量量子密码术的发展前景

连续变量量子密码术作为量子密码术的一个新兴分支，从 1999 年的提出到如今各种各样分配方案的出现，只有短短的几年时间. 在这几年中，连续变量量子密码术得到了长足的发展，不仅理论上基本成熟，而且通过实验得到了验证. 连续变量量子密码术相对于单光子量子密码术在码率和密钥量上的巨大优势，必将越来越受到人们的关注. 但是，除线路噪声、Reconciliation 计算量等限制因素外，连续变量量子密码术是否还存在其他限制？如何去改进或提出更有效的协议、实验上如何实现真正意义上安全的连续变量量子密码术等，还有待我们去研究探索.

参　考　文　献

[1] 桂有珍，韩正甫，郭光灿. 物理学进展，2002，22：371 [Gui Y Zh，Han Zh P，Guo G C. Progress in Physics，2002，22 371(in Chinese)]

[2] Bennett C H，Brassard G. Proceedings of IEEE International Conference on Computers，Systems and Processing. Bangalore，1984(New York：IEEE)

[3] Felix S *et al*. J. Mod. Opt., 2001, 48:2009
[4] Mo X F, Zhu B. Optics Letter, 2005, 30:2632
[5] Ralph T C. Phys. Rev. A, 1999, 61:010303
[6] Hillery M. Phys. Rev. A, 2000, 61:022309
[7] Reid M D. Phys Rev A, 2000, 62:062308
[8] Cerf N J *et al*. Phys. Rev. A, 2001, 63:052311
[9] Grosshans F. Grangier P. Phys. Rev. Lett., 2002, 88:057902
[10] Silberhorn Ch, Ralph T C. *et al*. Phys. Rev. Lett., 2002, 89:167901
[11] Hirano T, Yamanaka H *et al*. Phys. Rev. A, 2003, 68:042331
[12] Grosshans F *et al*. Nature, 2003:238
[13] Ralph T C. Phys. Rev. A, 2000, 62:062306
[14] Namiki R, Hirano T. *et al*. Phys. Rev. A, 2003, 67:022308
[15] Grosshans F, Cerf N. J. Phys. Rev. Lett., 2004, 92:047905
[16] Namiki R, Hirano T. Phys. Rev. Lett., 2004, 92:117901
[17] Iblisdir S, Van Assche G, Cerf N J. Phys. Rev. Lett., 2004, 93:170502
[18] Grosshans F. Phys. Rev. Lett., 2005, 94:020504
[19] Navascues M, Acin A. Phys. Rev. Lett., 2005, 94:020505
[20] Lodewyck J. Phys. Rev. A, 2005, 72:050303
[21] 郭光灿. 量子光学. 合肥:中国科学技术大学出版社, 1998. 118-184, 517-605[Guo GC. Quantum Optics. Hefei: University of Science & Technology of China press, 1998, 118-184, 517-605(in Chinese)]
[22] Bell J. S. Speakable and UnSpeakable in Quantum Mechanics. Cambridge: Cambridge University Press, 1988
[23] Reid M D, Drummond P. D. Phys. Rev. Lett., 1988, 60, 2731
[24] Van Assche G, Cardinal J, Cert N J. IEEE Trans. Inf. Theory, 2004, 50 394
[25] Grosshans F, Grangier P. http://www.arxiv.org/pdf/quant-ph/0204127
[26] Grosshans F, Cerf N J *et al*. Quantum Inf. Comput., 2003, 3 535-552
[27] Van Assche G, Iblisdir S, Cerf N J. Phys. Rev. A, 2005, 71:052304
[28] Ribordy G N, Tittel G *et al*. Rev. Mod. Phys., 2002, 74:145
[29] Cerf N J *et al*. Phys. Rev. Lett., 2000, 85:1754
[30] Cerf N J *et al*. Phys. Rev. A, 2000, 62:040301(R)
[31] Grosshans F, Grangier P. Phys. Rev. A, 2001, 64:010301(R)
[32] Cirac J I, Gisin N. Phys. Lett. A, 1997, 229:1
[33] Slutsky B A, Rao R, Sun P C *et al*. Phys. Rev. A, 1998, 57:2383

封面说明

国家天文台兴隆基地李金增博士与英国阿尔玛天文台的 Michael D. Smith 教授合作,成功地解析了整个巨分子云范围内($2° \times 2°$, 1.5 kpc)恒星及星团的大尺度结构和形成模式. 该中英合作小组开创性地在 OB 星团的序列形成模式中全面引入了中、低质量原星团,使之更全面、更符合巨分子云中星团形成的实际图景,进而成功描绘出玫瑰巨分子云复合体中原星团形成的全景图(左上图). 下面两张图分别是玫瑰巨分子云区的光深分布图和玫瑰巨分子云区的尘埃色温分布图.

该系列研究的主要创新成果包括:(1) 提出了原星团形成所遵循的多种模式即孤立形成、协同形成及结构式形成模式;(2) 揭示了原星团在整个巨分子云约 100 pc 范围内的爆发式形成和大尺度结构,并提出了"玫瑰巨分子云中原星团形成的树形结构模型";(3) 发现了玫瑰星云与相接巨分子云之间环形交互作用界面内原星团的链式结构形成. 研究小组认为,该弧状作用界面以及其中原星团的形成,实际上减缓或阻挠了电离氢区对于相临分子云及其中原星团形成的直接影响;(4) 进一步证实了银河系内的巨分子云事实上是孕育恒星及星团的短暂存在的物质形态. 剧烈的大质量星团序列形成过程将不断瓦解并最终驱散其母分子云,使绝大部分参与了恒星及星团形成活动却未转化成恒星的气体以分子云碎片的形式存在,甚至由反馈过程重归星际介质的行列. 这些星团形成的残余物质在银河系漫长的演化过程中将开始新一轮的聚集并沉积在银盘上,变成其旋臂结构的组成部分. 新的分子云复合体最终形成并开始新的恒星形成过程,如此往复,周而复始;(5) 在巨分子云致密核区发现了特性及规模可与 NGC 2244 相媲美的新生 OB 星团,并揭示出该大质量原星团具有显著的次结构,而且各子星团及 NGC 2244 近乎完美地排列于所在旋臂的方向上;(6) 在 0.2 pc 投影尺度范围内,发现了一个由三个 O 型原恒星组成的多体系统,其中质量最大的一个拥有约 130 个太阳质量,并可能是银河系内已知质量最大的原恒星之一. 然而,令人不解的是,只有位于一个相接"扇"形区域中的一小群暗红外源与该多体系统成协,而且该子星团投影在远离原星团致密区的位置上,而不是位于其中心. 预示了这些大质量 O 型星的形成可能蕴含了异乎寻常的形成机制和局域初始质量函数.

(中国科学院国家天文台　李金增)