量子光学学报 8(2)：71～75,2002
Acta Sinica Quantum Optica

文章编号：1007－6654(2002)02－0071－05

利用正交压缩态光场实现连续变量的量子密码术

李永民， 张宽收， 谢常德

（量子光学与光量子器件国家重点实验室，山西大学光电研究所，山西 太原 030006）

摘要：文中提出一种利用单模正交压缩态光场作为密码载体的连续变量量子密钥传输方案。在该方案中，经典信号以二进制编码形式调制在单模正交压缩态光场的正交振幅分量或正交位相分量上。基于海森堡测不准关系，任何窃听都会导致合法通讯者之间的误码率升高，从而暴露了窃听者的存在，以保护密钥信息的安全，与采用同样方案的相干光相比，保密程度有较大的提高。

关键词：正交压缩态光； 连续变量； 量子密码术

中图分类号：O431 **文献标识码**：A

0 引言

量子密码术自从诞生以来[1]，便飞速发展：首先，基于分离变量的各种方案不断被提出[2~4]，并迅速在实验上得以实现[5~9]，目前最远的传输距离可达几十公里。由于分离变量方案中信息的载体是单量子态(如单光子)，可以采用符合记数法，因此它对损耗不敏感。但是单光子探测效率非常低，导致密码传送的速率大为下降。近期，T. C. Ralphy[10]和M. Hillery[11]等提出了连续变量的量子密码术，连续变量的量子密码术以光束作为信息载体，虽然压缩度受传输介质损耗的影响比较大，但其高的传输与探测效率增加了人们对它的研究兴趣。本文提出利用单模正交压缩态光场作为密钥载体的连续变量量子密码传输方案，通过调制单模正交压缩态光场的振幅和位相完成信息编码。与 M. Hillery 的编码方式相比，我们所提出的方法对压缩度的要求较低，易于实验实现[11]。

1 基于正交压缩态光场的量子密码方案

正交压缩态光场自从被实验产生以来[12~13]，便得到了广泛应用：填补分束器的真空通道，实现相移，偏振面的亚散粒噪声极限测量[14]；用于原子的光谱测量[15]和量子非破坏测量等[16]。近期又在量子信息科学中获得广泛应用。在此我们设计了一个应用正交压缩相干态光场完成量子保密通讯的新方案。

Alice 用来发送经典信息的载体为正交振幅压缩态 $|\Psi_1>$ 和正交位相压缩态 $|\Psi_2>$ (图 1)。对于 $|\Psi_1>$ 来说：

$$X_1(t) = a_1(t) + a_1^{\dagger}(t),$$
$$Y_1(t) = i(a^{+}(t) - a(t))$$
$$<(\Delta X_1(t))^2><1,$$
$$<(\Delta X_1(t))^2><(\Delta Y_1(t))^2>\geq 1 \quad (1)$$

收稿日期：2002－03－29
基金项目：国家自然科学基金(69938010)；山西省留学回国人员基金；山西省自然科学基金
作者简介：李永民(1977－)，男，山西运城人，山西大学博士研究生，研究方向：量子光学与量子通讯.

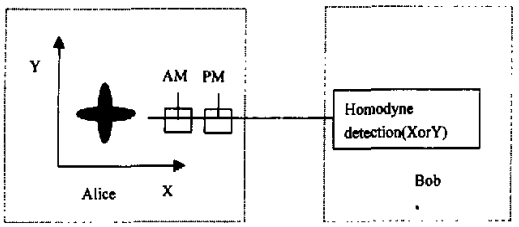

图 1 利用正交压缩光实现量子密码术的实验方案
AM 和 PM 分别为振幅调制器和相位调制器

对于 $|\Psi_2>$ 来说:

$$X_2(t)=a_2(t)+a_2^+(t),$$
$$Y_2(t)=i(a_2^+(t)-a_2(t))$$
$$<(\Delta Y_2(t))^2><1,$$
$$<(\Delta X_2(t))^2><(\Delta Y_2(t))^2>\geq 1 \quad (2)$$

Alice 随机选择 $|\Psi_1>$ 和 $|\Psi_2>$ 作为经典信息的载体:当 $|\Psi_1>$ 被选择时,Alice 把待传送的信息以振幅调制的方式调制到 $|\Psi_1>$ 上;当 $|\Psi_2>$ 被选择时,待传送的信息以位相调制的方式调制到 $|\Psi_2>$ 上(调制信号的功率与光场的散粒噪声功率可比拟)。然后,Alice 再把调制后的量子态($|\Psi_1>$ 或 $|\Psi_2>$)发送给 Bob,Bob 接收以后,再随机地选择测量其正交振幅分量或正交位相分量。只有当 Bob 选择测量了载有信号的分量,才能得到信息,即:当 Alice 发送态 $|\Psi_1>$,Bob 正好选择测量正交振幅分量;当 Alice 发送态 $|\Psi_2>$,Bob 正好选择测量正交位相分量。否则,Bob 将得不到任何信息。当信息发送完毕以后,Bob 在公开信道上告诉 Alice 她每次选择测量是正交振幅分量还是正交位相分量(但不公布测量结果),双方把 Bob 测量到信号的情况作为密钥,为了检测窃听者的存在,双方可公开一部分比特进行比较。如果误码率在容忍的范围内,则剩余的比特可作为安全的密钥使用。否则,可判定有窃听者存在。值得指出的是,在密钥发送的过程中,由于 Bob 只有一半的几率测量到信号,因此像通常的 BB84 模式一样整个通讯系统的效率只有 50%[1~5]。

在我们的方案中,信息以二进制码的形式调制到光场上,以态 $|\Psi_1>$ 为例,设 $X_1(t)$ 为正交振幅分量的大小,$<X_1(t)>$ 为正交振幅分量的平均值,$(\delta X_1(t))^2=<(\Delta X_1(t))^2>$ 为态 $|\Psi_1>$ 的正交振幅分量的起伏功率;调制信号的振幅为 V_S,功率为 V_S^2。我们采用振幅负调制的办法,这样被调制后的光场的正交振幅分量 $X'_1(t)$ 只有两个可能取值:$X_1(t)$ 和 $X_1(t)-V_S$。我们规定当 $X'_1(t)\geq<X_1(t)>-V_S/2$ 时,代表比特"1";当 $X'_1(t)<<X_1(t)>-V_S/2$ 时,代表比特"0"(对于 $|\Psi_2>$,我们规定 $Y'_2(t)\geq<Y_2(t)>-V_S/2$ 代表"1",$Y'_2(t)<<Y_2(t)>-V_S/2$ 代表"0")。在理想压缩的情况下,$<(\Delta X_1(t))^2>=0$,$X_1(t)=<X_1(t)>$,故 $X_1(t)\geq<X_1(t)>-V_S/2$ 代表比特"1",$X_1(t)-V_S<<X_1(t)>-V_S/2$ 代表比特"0"。然而,在实际情况中,不存在理想的压缩。即 $<(\Delta X_1(t))^2>\neq 0$,正交振幅分量不再是恒定值,而是以 $<X_1(t)>$ 为平均值随机起伏:$X_1(t)=<X_1(t)>+\delta X_1(t)$。当 $X_1(t)<<X_1(t)>-V_S/2$ 时,信号由"1"变为"0",出现误码;同理,当 $X_1(t)-V_S\geq<X_1(t)>-V_S/2$,也就是:$X_1(t)\geq<X_1(t)>+V_S/2$ 时,信号由"0"变为"1",也出现误码,如图 2 示。

由上面的论述我们可以计算误码率,当发送的

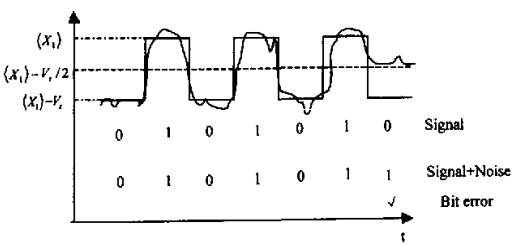

图 2 密钥串的产生

比特为"1"时，误码率

$$P_{1err} = P[X_1(t) < \langle X_1(t)\rangle - V_S/2] \quad (3)$$

当发送的比特为"0"时，误码率

$$P_{0err} = P[X_1(t) \geq \langle X_1(t)\rangle + V_S/2] \quad (4)$$

为了求解(3)式与(4)式我们需要知道 $X_1(t)$ 的分布函数。文献[11]给出了压缩真空态 $X_1(t)$ 的概率分布函数为：

$$P(X_1(t)) = \frac{1}{\sqrt{\pi\nu}} e^{-X_1(t)^2/\nu}, \quad \nu = 2e^{-2r} \quad (5)$$

由于 $< (\Delta X_1(t))^2 >= e^{-2r} = \frac{1}{2}\nu$，所以：

$$P(X_1) = \frac{1}{\sqrt{2\pi < (\Delta x_1(t))^2 >}} e^{-X_1(t)^2/2<(\Delta X_1(t))^2>} \quad (6)$$

我们可以清楚的看出，对于压缩真空态，$X_1(t)$ 的概率分布函数为均值为零的高斯分布，对于压缩相干态，我们知道，它相当于压缩真空态的平移变换，所以压缩相干态的概率分布函数仍为高斯分布，只是均值不为零[17]：

$$P(X_1) = \frac{1}{\sqrt{2\pi < (\Delta x_1(t))^2 >}} \cdot e^{-(X_1 - <X_1(t)>)^2/2<(\Delta X_1(t))^2>} \quad (7)$$

(7)式反映了压缩相干态的正交振幅分量 $X_1(t)$ 的概率分布。由(3)和(4)可知误码率：

$$P_{0err} = \int_{<X_1(t)>+V_S/2}^{+\infty} \frac{1}{\sqrt{2\pi < (\Delta x_1(t))^2 >}} \cdot e^{-(X_1(t) - <X_1(t)>)^2/2<\Delta X_1(t)^2>} dX_1(t)$$

$$P_{1err} = \int_{-\infty}^{<X_1(t)>-V_S/2} \frac{1}{\sqrt{2\pi < (\Delta x_1(t))^2 >}} \cdot e^{-(X_1(t) - <X_1(t)>)^2/2<(\Delta X_1(t))^2>} dX_1(t) \quad (8)$$

经过简单的计算可得，

$$P_{1err} = P_{0err} = \frac{1}{2} Erfc\left[\frac{1}{2}\sqrt{\frac{1}{2}\frac{V_S^2}{< (\Delta X_1(t))^2 >}}\right] \quad (9)$$

由(9)式我们可以看到，误码率只与信噪比 $\frac{S}{N} = V_S^2/< (\Delta X_1(t))^2 >$ 有关。

2　密钥安全性分析

假定作为信息载体的正交压缩态光场的压缩度为 6dB：$< (\Delta X_1(t))^2 >= 0.25$. 信号的幅度为 2，$V_S^2 = 4$；由上述可得信噪比：$\frac{S}{N} = V_S^2/< (\Delta X_1(t))^2 > = 16$。当不存在窃听者时，信号的误码率由(9)式可得为 2.3%。当窃听者存在时，他的任何窃听活动都会导致误码率的提高，从而暴露他的行为。值得指出的是，相干光场可看作是压缩度为零的正交压缩态光场：$< (\Delta X_1(t))^2 >= 1$，上述的密码方案同样可以适用，作为比较，我们假定，利用相干光作为密钥载体的信号功率为：$V_S^2 = 16$ 这样载有信号的压缩光和相干光的初始信噪比均为：$\frac{S}{N} = 16$。下面考虑窃听者可采用的三种方案[10]，并对应用压缩光的安全性和相干光的安全性作一比较。第一种方案，Eve 截获全部光束进行测量，然后再把测量的结果，调制到另一束具有同等压缩度的光束上，然后再发送给 Bob。由于 Eve 事先并不知道 Alice 要发送的信号是调制在正交振幅分量上还是调制在正交位相分量上，他只能采用猜测的办法，这时他有 50% 的几率测量到信号，50% 的几率测不到信号(猜错的情况下)，在测不到信号的情况下，他立刻能判断出，信号是调制在另一分量上，但却无法知道另一分量上的信号是"0"还是"1"，只能随机的猜测。总的来说，Eve 有 25% 的出错几率，当 Alice 和 Bob 在公开信道上公开比较一部分密钥时，将会发现有 25% 的误码率，远高于 2.3%，从而暴露出 Eve 的窃听行为。对于这一方案，压缩光和相干光的保密程度没有差别。

第二种方案，Eve 把全部光束截获，并用 50/50 的分束器等分为两部分，利用平衡零拍来同时测量光束的正交振幅分量与正交位相分量，并把测量到的结果发送给 Bob。对于正交压缩光，由于真空起伏的引入，信噪比由原来的 16 变为 3.2。由(9)式 Eve 和 Bob 的误码率为：18.5%。同第一种方案，通讯双方经过比较一部分比特数后，估计出误码率，从而暴露出 Eve 的窃听行为。对于相干光我们同理可

以得到 Eve 和 Bob 的误码率为:7.8%,同压缩光比较,Eve 获得的信息增加,同时不易被发现。

第三种方案,考虑一般情况,Eve 可以用反射镜分出一部分光进行探测以获取信号,其余的光仍沿原光路传输。Eve 企图获取足够多信号的同时不对 Bob 接收到的信号产生大的影响。图(3)是 Eve 处得到的误码率和 Bob 处测量到的误码率随着反射镜反射率的变化关系(实线为压缩光,虚线为相干光)。从图中我们可以看出,对于压缩光而言,当反射率比较小时,对 Bob 处的误码率影响较大,同时 Eve 得到很少的信息。例如,我们假设分出的一小部分光占总光束能量的 10%,这样 Bob 处误码率为 4.8%(同 2.3%相比较上升了一倍)。而 Eve 获得的信号的误码率为 37%。同样情况对于相干光,Bob 处误码率为 2.9%,而 Eve 获得的信号的误码率为 26%。同压缩光相比,Eve 在几乎不被发现的情况下,可以获得较多的信息。

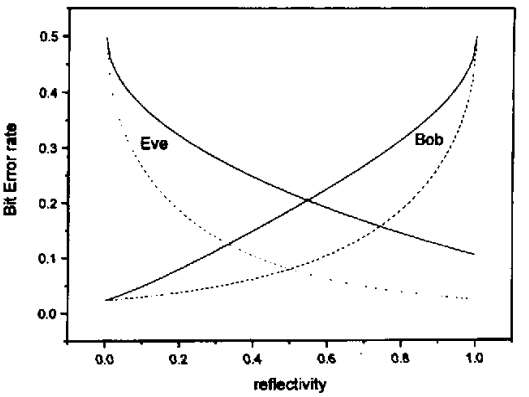

图 3 比特误码率随着反射率的变化关系
实线为正交压缩态,虚线为相干态

3 结论

本文基于应用正交压缩态光场提出一种连续变量的量子密码方案,外界任何窃听行为的存在都将导致通讯双方的误码率增加,从而暴露出窃听行为,保护了密码的安全。和利用同一方案的相干光相比,在较大程度上提高了保密度。在具体的实验中可以通过简并光学参量放大和缩小来实现正交位相压缩态和正交振幅压缩态[13,16,18,19]。同时,该方案对光场的压缩度要求不是很高,目前实验上已获得的压缩度即能满足要求。

参考文献:

[1] BENNETT C, BRASSARD G. in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing [M]. Bangalore, India(IEEE, New York,) 1984. 175.

[2] BENNETT C H. Quantum cryptography without Bell's theorem [J]. *Phys Rev Lett*, 1992, **68**:557.

[3] GOLDENBERY L, VAIDMAN L. Quantum Cryptography Based on Orthogonal States [J]. *Phys Rev Lett*, 1995, **75**:1239.

[4] EKERT A K. Quantum Cryptography Based on Bell's Theorem [J]. *Phys Rev Lett*, 1991, **67**:661.

[5] BENNETT C, BESSETTTE F, BRASSARD G, *et al*. Experimental Quantum Cryptography [J]. 1992, **5**:3.

[6] MULLER A, BREGUET J, GISIN N. Experimntal Demonstration of Quantum Cryptography Using Polarized Photons in Optical Fibre Over More Than 1km [J]. *Europhys Lett*, 1993, **23**: 383.

[7] FRANSON J, ILVES H. Quantum Cryptography Using Optical Fibers [J]. *Appl Opt*, 1994, **33**: 2949.

[8] TOWNSEND P D. Seaure Key Distribution System Based on Quantum Cryptograpny [J]. *Electron Lett*, 1994, 809.

[9] HUGHES R J, MORGAN G L, GLEN C G. Practical Quantum Key Distribution Over a 48 - km Optical Fiber Network [M]. e - print quant - phy 9904038.

[10] RALPH T C. Continuous Variable Quantum Cryptography [J]. *Phys Rev A*, 2000, **61**: 010303.

[11] HILLERY M. Quantum Cryptograpy With Squeezed States [J]. *Phys Rev A*, 2000, **61**: 022309.

[12] SLUSTER R E, *et al*. Observation of Squeezed States Generated by Four - Wave Mixing in an Optical Cavity [J]. *Phys Rev*

Lett, 1985, **55**: 2409.

[13] WU L A, KIMBLE H J, *et al*. Generation of Squeezed States by Parametric Down Conversion [J]. *Phys Rev Lett*, 1986, **57**: 2520.

[14] XIAO M, WU L A, KIMBLE H J. Precision Measurement Beyond the Shot - Noise Limit [J]. *Phys Rev Lett*, 1987, **59**: 278.

[15] POLZIK E S, KIMBLE H J. Spectroscopy with Squeezed light [J]. *Phys Ruev Lett*, 1992, **68**: 3020.

[16] BRUCKMEIER R, HANSEN H, SCHILLER S, MLYNEK J. Repeated Continuous Quantum Nondemolition Measurements [J]. *Phys Rev Lett*, 1997, **79**: 1463.

[17] BENCHEIKH K, SYMUL T H, JANKOVIC A, *et al*. Quantum key Distribution with Continuous Variables [J]. *Journal of Modern Optics*, 2001, **48**: 1903.

[18] ZHNAG Y, WANG H, LI X Y, *et al*. Experimental Generation of Bright Two - mode Quadrature Squeezed Light from a Narrow - band Nondegenerate Optical Parametric Amplifier [J]. *Phys Rev A*, 2000, **62**: 023813.

[19] LI X Y, PAN Q, JING J T, *et al*. Quantum Dense Coding Exploring a Bright Einstein - Podolsky - Rosen Beam [J]. *Phy Rev Lett*, 2002, **88**: 011204.

Quantum Cryptography of Continuous Variable with Quadrature Squeezed State Light

LI Yong - Min,　ZHANG Kuan - Shou,　XIE Chang - de

(*State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto - Electronics, Shanxi University, Taiyuan*, 030006, *China*)

Abstract: Scheme of quantum cryptography based on single mode quadrature phase and amplitude squeezed state lights is presented. The binary key is obtained by modulating the phase quadrature or amplitude quadrature of the quadrature squeezed coherent state. The uncertainty relation of quantum mechanics provides the quantum protection. Eavesdropping from optical tapping will degrade the signal to noise ratio of the results measured by the authorized receiver and hence be revealed. Comparing with that using a coherent state light, the application of the squeezed state light enhances the security significantly.

Key words: quadrature squeezed state light;　continuous variable;　quantum cryptography