第 56 卷 第 1 期 2007 年 1 月
1000-3290/2007/56(01)/0005-05

物 理 学 报
ACTA PHYSICA SINICA

Vol.56,No.1,January,2007
©2007 Chin. Phys. Soc.

平衡零拍测量对连续变量量子密钥分配的影响*

陈进建 韩正甫† 赵义博 桂有珍 郭光灿

(中国科学技术大学,中科院量子信息重点实验室,合肥 230026)

(2006 年 4 月 15 日收到;2006 年 5 月 16 日收到修改稿)

与单光子量子密钥分配采用单光子探测器不同,连续变量量子密钥分配采用平衡零拍测量技术.分析了由于参考光的真空噪声、分束器的透射率和反射率不相等引入的平衡零拍测量误差,以及平衡零拍测量探测器的电子噪声对连续变量量子密钥传输的最大安全距离的限制,给出了平衡零拍测量的探测噪声、电子噪声和密钥量之间的定量表达式.

关键词:密码学,连续变量,量子密钥分配,平衡零拍测量

PACC:0367,4250,0300,4630R

1. 引 言

量子密钥分配[1—3]是指彼此相隔一定距离的通信双方 Alice 和 Bob 通过量子信道和公开信道共享一组安全量子密钥的过程.任何企图窃听这组共享密钥的行为,最终都将在 Alice 和 Bob 进行数据校验后被发现,这是由量子力学的不确定性原理所保证的.单光子的量子密钥分配将信息加载在单光子偏振、相位或者路径的选择上,需要单光子源和单光子探测器,而在目前的实验条件下还没有理想的单光子源和高效的单光子探测器,使得生成的码率很低.连续变量量子密钥分配方案将信息加载在光源的相位、振幅等连续变量上,只需要普通光源和平衡零拍测量,不仅设备简单,而且可大大地提升密钥量.

自从 1999 年 Ralph 提出连续变量量子密钥概念后[4],连续变量量子密钥分配迅速得到发展,各种方案相继被提出[5—8].2003 年,Grosshans 等人提出了相干态的量子密钥分配方案,并且通过实验给予了很好的验证[9].在这个方案中,利用一种称为“reverse reconciliation,RR”[10]的技术从共享的十进制密钥元素中提取二进制密钥.理论上已经证明,使用 RR 技术提取的密钥在任意的信道传输率下均是安全的[11],这种方案又被称为 reverse reconciliation coherent state(RRCS)方案[12].

RRCS 方案的绝对安全是在忽略了各种噪声的情况下得到的,在实验上实现 RRCS 方案,这些噪声是不得不考虑的因素,它们不仅影响生成的密钥量,更影响生成密钥的安全性.RRCS 方案中的噪声主要有四种:真空噪声、线路噪声、Bob 的零拍测量噪声和电子噪声[9].真空噪声是相干态的固有噪声,表示真空态的量子起伏,不会随外界因素的变化而变化;线路噪声包括由于信道衰减引入的额外真空噪声以及线路引入的其他额外噪声(excess noise);而零拍测量噪声和电子噪声是由平衡零拍测量及其后续电路引入的.真空噪声和线路噪声已经得到了较好的研究[12],本文主要分析平衡零拍测量引入噪声的原因及其大小,给出其对生成密钥量的影响.

2. 平衡零拍测量对连续变量量子密钥分配的影响

平衡零拍测量的原理[13]如图 1 所示,a,b 分别表示信号光和参考光的湮没算符,c,d 分别表示两路输出光的湮没算符,则

$$\begin{aligned} c &= \sqrt{T}a + \mathrm{i}\sqrt{1-T}b, \\ d &= \mathrm{i}\sqrt{1-T}a + \sqrt{T}b, \end{aligned} \tag{1}$$

其中 i 表示透射光和反射光之间有 $\frac{\pi}{2}$ 的相位差,T

* 中国科学院知识创新工程重要方向项目,国家自然科学基金重点项目(批准号:60537020)和国家创新研究群体科学基金(批准号:60121503)资助的课题.

† 通讯作者:zfhan@ustc.edu.cn

为透射率,两路光经过分束器干涉后得到 c,d 两束光的光子数为

$$\langle c^+ c\rangle = T\langle a^+ a\rangle + (1-T)\langle b^+ b\rangle + \mathrm{i}\sqrt{T(1-T)}\langle a^+ b - b^+ a\rangle,$$
$$\langle d^+ d\rangle = (1-T)\langle a^+ a\rangle + T\langle b^+ b\rangle - \mathrm{i}\sqrt{T(1-T)}\langle a^+ b - b^+ a\rangle. \quad (2)$$

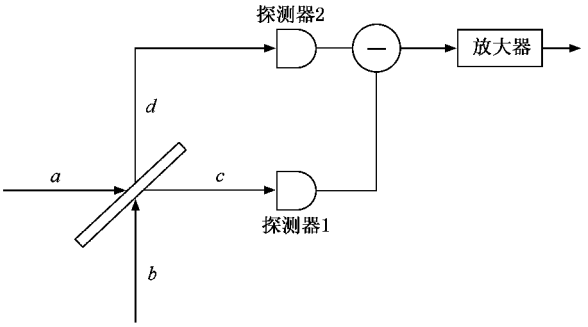

图 1 平衡零拍测量原理 其中 a,b 表示信号光和参考光的湮没算符,c,d 表示输出光的湮没算符

这样通过减法器相减后最后的输出结果为

$$\langle n_{\mathrm{cd}}\rangle = \langle c^+ c - d^+ d\rangle = (2T-1)\langle a^+ a\rangle + (1-2T)\langle b^+ b\rangle + 2\mathrm{i}\sqrt{T(1-T)}\langle a^+ b - b^+ a\rangle. \quad (3)$$

记信号光为 $\alpha \mathrm{e}^{\mathrm{i}\phi_\alpha}$,参考光为 $\beta \mathrm{e}^{\mathrm{i}\phi_\beta}$,则(3)式变为

$$\langle n_{\mathrm{cd}}\rangle = (2T-1)|\alpha|^2 + (1-2T)|\beta^2| + 4\sqrt{T(1-T)}|\alpha||\beta|\sin(\phi_\alpha - \phi_\beta). \quad (4)$$

对于平衡零拍测量,要求透射率等于反射率,即 $T=\frac{1}{2}$,则

$$\langle n_{\mathrm{cd}}\rangle = 2|\beta||\alpha|\sin(\phi_\alpha - \phi_\beta). \quad (5)$$

连续变量量子密钥分配首先要求发送方 Alice 将信息加载到相干态在相空间的两个分量 x_1 和 x_2 上,相干态在相空间的表示如图 2 所示.接收方 Bob 通过零拍测量,归一化后得到测量结果 $|\alpha|\sin(\phi_\alpha - \phi_\beta)$.如果 Bob 调制参考光相位为 0,则测量结果为 $|\alpha|\sin\phi_\alpha$,为信号光在相空间的 x_1 分量,如果 Bob 调制参考光相位为 $\frac{\pi}{2}$,得到信号光在相空间的 x_2 分量,这样 Alice 和 Bob 就共享了一组十进制密钥 x_1 或者 x_2,最后通过 Reverse reconciliation 和保密放大转化为二进制密钥.

相干态的信号光和参考光本身存在固有的真空噪声 N,这个噪声满足高斯分布,其方差为 N_0,参考光的真空噪声会给测量结果引入误差,引入真空噪

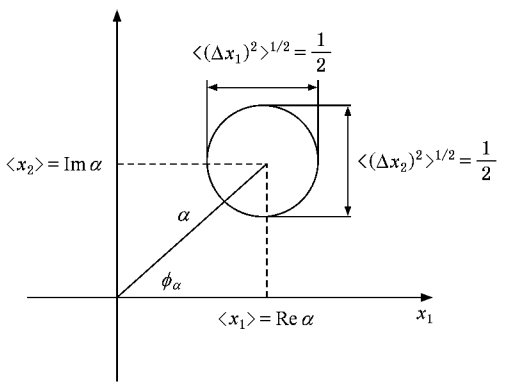

图 2 信号光在相空间的表示

声以后,(5)式变为

$$n'_{\mathrm{cd}} = 2|\beta|(|\alpha| + \sqrt{N})\sin(\phi_\alpha - \phi_\beta) + 2(|\alpha|\sqrt{N} + N)\sin(\phi_\alpha - \phi_\beta). \quad (6)$$

在实验中,第二项是由参考光的真空起伏引入的误差,将在测量结果中出现,其相对信号的误差大小为

$$e = \frac{|\alpha|\sqrt{N} + N}{|\alpha||\beta|}. \quad (7)$$

以 Grosshans 等人的实验参数[9]为例,参考光 n_β 为 10^8 光子/脉冲,信号光 n_α 为 10^2 光子/脉冲,$|\beta| = \sqrt{I_\beta} = \sqrt{n_\beta \cdot 2N_0}$,$|\alpha| = \sqrt{I_\alpha} = \sqrt{n_\alpha \cdot 2N_0}$. I_β,I_α 为参考光和信号光的光强,真空噪声能量的大小为 $\frac{1}{2}$ 个光子的能量,计算可得误差 e 的方差为 7.57×10^{-5}.表 1 给出了各种不同强度的信号光和参考光下的误差值的方差,从中可以看出,误差的方差随着信号光和参考光光强的增大而减小,当参考光趋于无穷大时,这个误差趋于 0,因此为了尽可能的减少这部分误差,参考光需要足够强,在参考光为 10^8 光子/脉冲的强度下,一般认为上述误差可以忽略不计.

在连续变量量子密钥分配实验中,一般情况下分束器很难精确达到 50∶50,总会有一点偏差,而这个偏差会使干涉后两路光除干涉项外另外两项不能完全抵消而引入噪声,为严格分析分束器分束不均对零拍测量的影响,记分束器的透射率 $T=\frac{1}{2}\pm\varepsilon$,则(4)式变为

$$\langle n''_{\mathrm{cd}}\rangle = \pm 2\varepsilon|\alpha|^2 \mp 2\varepsilon|\beta|^2 + 4\sqrt{0.25-\varepsilon^2}|a||\beta|\sin(\phi_\alpha - \phi_\beta). \quad (8)$$

由于在零拍测量中,参考光的光强比信号光强

很多，通常至少在 40dB 以上，因此(8)式的第一项可以忽略不计，而 ε 一般情况下也很小，$\varepsilon^2 \ll 0.25$，因此(8)式可以简化为

$$n''_{cd} = 2|\beta|[\mp\varepsilon|\beta| + |\alpha|\sin(\phi_\alpha - \phi_\beta)]. \tag{9}$$

要想获得较好的测量结果，噪声项 $\varepsilon|\beta|$ 需要小于 $|\alpha|\sin(\phi_\alpha - \phi_\beta)$，而 $|\alpha|\sin(\phi_\alpha - \phi_\beta)$ 表示信号光在相空间的一个分量，其测量值起伏的最小标准差为真空起伏的标准差 $\sqrt{N_0}$，得 $|\varepsilon| < \frac{1}{\sqrt{2n_\beta}}$. 取参考光为 10^8 光子/脉冲，ε 需要满足 $|\varepsilon| < 7.07\times10^{-5}$，即分束器的精确度要在 7.07×10^{-5} 范围内. 表 2 给出了在各种不同的参考光下，对分束器精度的要求，从表 2 中可以看出，参考光越强，对分束器的要求就越高.

表 1　不同的信号光和参考光光强下参考光真空噪声引入误差值的方差大小

n_α \ n_β	10^3	10^4	10^5	10^6	10^7	10^8
10^0	3.82×10^{-2}	1.21×10^{-2}	3.82×10^{-3}	1.21×10^{-3}	3.82×10^{-4}	1.21×10^{-4}
10^1	2.74×10^{-2}	8.65×10^{-3}	2.74×10^{-3}	8.65×10^{-4}	2.74×10^{-4}	8.65×10^{-5}
10^2	2.40×10^{-2}	7.57×10^{-3}	2.40×10^{-3}	7.57×10^{-4}	2.40×10^{-4}	7.57×10^{-5}

表 2　参考光光强和分束器精度的关系

n_β	10^4	10^5	10^6	10^7	10^8
ε	$\lvert\varepsilon\rvert < 7.07\times10^{-3}$	$\lvert\varepsilon\rvert < 2.24\times10^{-3}$	$\lvert\varepsilon\rvert < 7.07\times10^{-4}$	$\lvert\varepsilon\rvert < 2.24\times10^{-4}$	$\lvert\varepsilon\rvert < 7.07\times10^{-5}$

在 $n_\beta = 10^8$ 时，分束器精度的要求在目前实验条件很难达到，一种可行的方法是分束器后的光路较强的一路中加入可调衰减器，以降低或抵消因为分束器分束不均引入的噪声. 我们假定在 d 路光加一个衰减系数为 γ 的衰减器，为方便起见，记 $T = \frac{1}{2} + \varepsilon$，经衰减后(4)式变为

$$\begin{aligned} n'''_{cd} &= (2\varepsilon + 0.5\gamma - \varepsilon\gamma)|\alpha|^2 \\ &\quad + (-2\varepsilon + 0.5\gamma + \varepsilon\gamma)|\beta|^2 \\ &\quad + (2-\gamma)|\alpha||\beta|\sin(\phi_\alpha - \phi_\beta). \end{aligned} \tag{10}$$

考虑到参考光要远强于信号光，即 $|\beta|^2 \gg |\alpha|^2$：

$$\Delta n_{cd} = n_{cd} - n'''_{cd} = (-2\varepsilon + 0.5\gamma + \varepsilon\gamma)|\beta|^2. \tag{11}$$

因此为了抵消分束器不均引入的噪声，最终可得到 ε 和 γ 的关系为

$$\gamma = \frac{4\varepsilon}{2\varepsilon + 1}. \tag{12}$$

(12)式给出了衰减系数和分束器精度之间的定量关系，在分束器为理想的 50∶50 时，测量结果只存在干涉项，分束器的精度 ε 越差，就会导致测量结果的误差项 $-2\varepsilon|\beta|^2$ 越大，这时就需要在较强的一路光中调整更大的衰减系数 γ.

在连续变量量子密钥分配过程中，探测器的电子噪声同样会对密钥传输产生重大影响. 由(5)式可知，信号光存在真空噪声，这个噪声经过平衡零拍测量之后被放大了 $2|\beta|$ 倍，放大后真空噪声的标准差为 $2|\beta|\sqrt{N_0}$. 一般情况下，给定的探测器输出电子噪声引起的电压起伏 V_e 由探测器的性能决定. 假定探测器的后续电路放大倍数为 n，则电路放大之前探测器等效电子噪声的标准差为 $\frac{V_e}{n}$，为了和真空噪声比较，将这个电子噪声等效成零拍测量放大 $2|\beta|$ 前的外部线路引起的噪声 N_e，则

$$N_e = \left(\frac{V_e}{2n|\beta|}\right)^2.$$

连续变量量子密钥分配要求外部线路引起的噪声和真空噪声之比小于 $\frac{1}{2}G$[9]，G 为信道传输率，因此有

$$\left(\frac{V_e}{2n|\beta|\sqrt{N_0}}\right)^2 < \frac{1}{2}G. \tag{13}$$

因此，在给定探测器后，根据信道损耗大小，可给出密钥传输的最大安全距离 s，即

$$s < -\frac{10}{\xi}\lg\frac{V_e^2}{2n^2|\beta|^2 N_0}, \tag{14}$$

ξ 表示光纤损耗率率，从(14)式可以看出安全距离和探测器后续放大电路的放大倍数、参考光的光强成正比，与探测器的电子噪声成反比. 在 Gisin 等人的实验中[14]，平衡零拍测量的电子噪声为真空噪声的 10%，则最大安全距离可达 35km.

在文献[9]中给出了连续变量量子密钥分配的密钥量和噪声之间的关系，

$$\Delta I = -\frac{1}{2}\log_2[G^2(1+\chi)(V^{-1}+\chi)], \quad (15)$$

其中 G 表示信道传输率，V 是信号的调制幅度，χ 可以理解为总的等效输入噪声，在这个公式的基础上，我们给出密钥量和平衡零拍测量噪声 N_{hom} 之间的关系，令 $N_{\mathrm{hom}} = aN_0$. 第一种情况下我们假设 Eve 不知道 Bob 的测量噪声，这种假设称为“realistic assumption”[9]，这时密钥量和平衡零拍测量噪声之间的关系为

$$\Delta I_{\mathrm{r}} = \frac{1}{2}\log_2\left[\frac{1+aG\left(\chi+\frac{1}{V}\right)}{G^2\left(1+\chi+\frac{a}{G}\right)\left(\chi+\frac{1}{V}\right)}\right]. \quad (16)$$

第二种情况假设 Eve 的窃听能力无穷大，能控制并知道 Bob 的测量噪声，这种假设称为“paranoid assumption”[9]，这时候密钥量和平衡零拍测量噪声的关系为

$$\Delta I_{\mathrm{p}} = -\frac{1}{2}\log_2\left[G^2\left(1+\chi+\frac{a}{G}\right)\left(V^{-1}+\chi+\frac{a}{G}\right)\right]. \quad (17)$$

3. 结 论

本文分析了由于平衡零拍测量引入的各种噪声，以及这些噪声对密钥量的影响和对最大安全距离的限制，最后给出了平衡零拍测量噪声和密钥量之间的具体关系式，要想在实验中得到更大的密钥量，降低平衡零拍测量噪声是最关键的因素之一.

[1] Miao E L, Mo X F, Gui Y Z, Han Z F, Guo G C 2004 *Acta Phys. Sin.* **53** 2126 (in Chinese) [苗二龙、莫小范、桂有珍、韩正甫、郭光灿 2004 物理学报 **53** 2126]

[2] Liang C, Fu D H, Liang B, Liao J, Wu L A, Yao D C, Lü S W 2001 *Acta Phys. Sin.* **50** 1429 (in Chinese) [梁 创、符东浩、梁 冰、廖 静、吴令安、姚德成、吕述望 2001 物理学报 **50** 1429]

[3] He G Q, Zeng G H 2006 *Chin. Phys.* **15** 1284

[4] Ralph T C 1999 *Phys. Rev.* A **61** 010303

[5] Hillery M 2000 *Phys. Rev.* A **61** 022309

[6] Reid M D 2000 *Phys. Rev.* A **62** 062308

[7] Hirano T, Yamanaka H, Ashikaga M, Konishi T, Namiki R 2003 *Phys. Rev.* A **68** 042331

[8] Grosshans F, Grangier P 2002 *Phys. Rev. Lett.* **88** 057902

[9] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf N J, Grangier P 2003 *Nature* **238** 241

[10] Grosshans F, Grangier P 2002 http://www.arxiv.org/pdf/quant-ph/0204127

[11] Grosshans F, Cerf N J 2003 *Quantum Inf. Comput.* **3** 535

[12] Lodewyck J, Debuisschert T, Tualle-Brouri R, Grangier P 2005 *Phys. Rev.* A **72** 050303(R)

[13] Scully M O, Zubairy M S 1995 *Quantum Optics* (Cambridge University Press)

[14] Legre M, Zbinden H, Gisin N http://www.arxiv.org/pdf/quant-ph/0511113

The effect of balanced homodyne detection on 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*)
(Received 15 April 2006; revised manuscript received 16 May 2006)

Abstract

Different from single photon quantum key distribution, continuous variable quantum key distribution uses the balanced homodyne detection. In this paper, the detection error of balanced homodyne caused by vacuum noise of the local light and unbalance of beam splitter is analyzed, the maximal safe distance limited by the electronic noise of balance homodyne detector is given, finally, the relationship between the noise of balanced homodyne detection and key rate are shown.

Keywords: cryptography, continuous variable, quantum key distribution, balance homodyne detection
PACC: 0367, 4250, 0300, 4630R

* Project supported by the Funds of the Chinese Academy of Sciences for Key Topics in Innovation Engineering, the Funds for Creative Research Groups of China (Grant No. 60121503), and the State Key Program of National Natural Science of China (Grant No. 60537020).

† Corresponding Author. E-mail: zfhan@ustc.edu.cn