第 57 卷 第 2 期 2008 年 2 月
1000-3290/2008/57(02)/0678-07

物 理 学 报
ACTA PHYSICA SINICA

Vol.57,No.2,February,2008

诱惑态在“双探测器”准单光子光源量子密钥分发系统中的应用*

米景隆 王发强† 林青群 梁瑞生 刘颂豪

(华南师范大学信息光电子科技学院,光子信息技术广东省高校重点实验室,广州 510631)

(2007 年 1 月 31 日收到;2007 年 5 月 22 日收到修改稿)

现在诱惑态已被证明是一种可以大大提高量子密钥分发安全性能的现实可行的方法.由于考虑到现实应用中激光器在调制过程中的消光比不能做到 100%,以及激光器固有的自发辐射因而使得制备真空态并不是一件容易的事情. 因此本文将对理想情况下准单光子光源量子密钥分发系统应用中的诱惑态结论作了补充和扩展,提出了两个弱光强态的诱惑态方案和一个弱光强诱惑态方案.最后,将“双探测器”的理论应用在准单光子源(HSPS)光源系统中,使系统的安全传输距离可达到 221.5 km,比使用普通探测器的系统增加了约 50 km.

关键词:量子密钥分发,诱惑态,HSPS 光源,双探测器

PACC:0365,4250,4230

1. 引 言

在经典保密通信中,密钥分发的安全性是基于数学加密方法的复杂度,而且这种数学上的安全性并不是绝对安全的. 但在量子保密通信中,量子密钥分发(简写 QKD)利用量子力学中的测不准原理和不可克隆原理可以证明是安全的,也就是说 QKD 的安全性是物理意义上的绝对安全. 因此,QKD 作为一种可以绝对安全的使发送方(Alice)和接收方(Bob)共享密钥的方法协议,越来越受到人们的认可和重视. 虽然很多标准的 QKD 协议如 BB84 协议[1],已经被证明是无条件安全的[2—4]. 但是这些安全性的分析并不适用于现实情况. 由于在实际系统中,光源不是单光子光源,信道是有损耗的,探测器的效率也是有限等各种各样的因素使得实际情况下的安全性成为一个备受关注的问题.尽管如此,实际情况下的 QKD 也是无条件安全的,但是该安全性以牺牲传输距离为代价[5,6].

在各种现实设备的缺陷中,对安全性影响最大而对窃听者(Eve)最有利的缺陷就是,实际系统中的光源并不是理想的单光子光源. 因此光源输出的脉冲就会有一部分是含有多个光子的,这样 Eve 就可以对输出的脉冲实行光子数分裂(PNS)[7,8]攻击,这种攻击使 Eve 可以得到 Alice 和 Bob 所共享的信息而不被发现. 幸运的是现在已有对付这种攻击的方法,如 SARG 协议[9],强参考光方案[10]和诱惑态方案[11—16]. 其中最有效也是最现实可行的解决办法就是诱惑态方案.

诱惑态方案是由 Hwang[11]首先提出,后来由几个研究小组对这个方法进行完善和发展[12—16]. 其基本原理为:Alice 在发送光脉冲给 Bob 之前就随机的选择脉冲的强度,当 Alice 和 Bob 在量子通信阶段结束后,Alice 和 Bob 就利用检测到的诱惑态脉冲结果来估算信号光中单光子脉冲计数率的上限和单光子所引起的误码率的下限. 如果得到的结果与理论安全值相差太大,那就可以认为在量子通信过程中有窃听者的存在,在这种情况下,该次通信的结果将会被舍弃,重新开始下一次通信. 如果结果证明通信是安全的,接着就可利用 ILM-GLLP[5,6]的结果来提取密钥.

在之前的很多文献中,都是利用普通的激光光源,普通激光器输出的是相干态. 但在相干态光源的系统中,当系统的传输距离超过 100 km 后,系统

* 国家自然科学基金(批准号:60578055)与国家重点基础研究发展计划 973 项目(批准号:2007CB307001)资助的课题.

† 通信联系人. E-mail:fqwang98@sina.com

的暗计数就成为影响密钥生成率的主要因素. 因此,要提高系统的传输距离,就得想办法来减少系统的暗计数率. 由于现在用参量下转换来得到准单光子源(HSPS)的技术已经得到长足的进步[17—19],使得 HSPS 作为 QKD 系统的光源成为可能.

在文献[20,21]中,已经提出了如何在 HSPS 光源的系统中应用诱惑态. 通过改变抽运光的强度便可以在系统中引入诱惑态以提高系统的安全性. 但是,由于考虑到在实际应用中,由于激光器的消光比并不是 100%,因而要想随意制备真空态并不如想象中容易. 在这种情况下,文献[20,21]中所讨论的以真空态和弱光强态作为诱惑态的结果就不再适用,因而本文就提出了两个诱惑态都是弱光强态的方案,以适用于该情况. 另一方面,在现实应用中使用真空态和弱光强态作为诱惑态时,在激光器的调制电压为零时,激光器由于自身存在自发辐射,因此即使在调制电压为零的情况下所产生的态也不完全是真空态,这就使得不能用真空态来准确估算系统的暗计数. 在这种情况下,以真空态和弱光强态作为诱惑态,就会退化为只有一个弱光强态作为诱惑态,因此提出了一个弱光强态的诱惑态方案,以解决这一问题. 另外,最后本文将‘双探测器’的方法[22]和 HSPS 的 QKD 系统相结合,减少了秘密放大的无谓损耗,使系统的安全传输距离增加到 221.5 km,比没有使用‘双探测器’情况增加了约 50 km.

2. QKD 系统模型

由于要讨论实际 QKD 系统的情况,所以先要建立一个 QKD 系统模型,对系统的光源,计数率和量子误码率(QBER)进行说明.

2.1. 光源(HSPS)

HSPS 光源是由参量下转换触发机制所产生的,在此只讨论非简并参量放大过程,所产生的双模态为

$$|\varphi\rangle = (\cosh\chi)^{-1}\sum_{n=0}^{\infty}(\tanh\chi)^n|n,n\rangle, \quad (1)$$

其中 χ 为偶合常数和相互作用时间的乘积.

本文讨论的探测器都是最基本的门限探测器,就是说该探测器只能分辨真空态和非真空态,而不能分辨脉冲中光子数的数目. 另外,可以认为一个包含有 n 个光子的态中,这 n 个光子是相互独立的. 因此,对于门限探测器,包含有 n 个光子的光子态的传输效率为

$$\eta_n = 1-(1-\eta_A)^n, n = 0,1,2,\cdots, \quad (2)$$

其中 η_A 为 Alice 探测器的探测效率.

设 Alice 的探测算子为

$$M = d_A|0\rangle\langle 0| + \sum_{n=1}^{\infty}[1-(1-\eta_A)^n]|n\rangle\langle n|, \quad (3)$$

其中 d_A 为 Alice 端探测器的暗计数率.

因此,Alice 对光源的探测可以表述为

$$\begin{aligned}\rho &= \frac{1}{P_{post}}Tr_A(M|\varphi\rangle\langle\varphi|)\\ &= \frac{1}{P_{post}}\left\{\frac{d_A}{\cosh 2\chi}|0\rangle\langle 0| + \sum_{n=1}^{\infty}[1-(1-\eta_A)^n]|n\rangle\langle n|\right\}, \quad (4)\end{aligned}$$

其中 M 为测量算符,P_{post} 是归一化常数. 由于光源的平均光子数可表示为 $\mu = \sinh^2\chi$. 则上式可改写为

$$\begin{aligned}\rho &= \frac{1}{P_{post}}\left\{\frac{d_A}{\mu}|0\rangle\langle 0| + \sum_{n=1}^{\infty}[1-(1-\eta_A)^n]\right.\\ &\quad\left.\times\frac{\mu^n}{(1+\mu)^{n+1}}|n\rangle\langle n|\right\},\\ P_{post} &= \frac{d_A}{1+\mu}+\frac{\mu\eta_A}{1+\mu}.\end{aligned} \quad (5)$$

2.2. 计数率

根据文献[20]中对 HSPS 光源系统计数率的定义可得,一个含有 n 个光子的脉冲所引起的计数率 Y_n 可表示为

$$Y_n = Y_0 + \eta_n, \eta_n = 1-(1-\eta_B)^n, \quad (6)$$

其中 $Y_0 = d_B$ 为 Bob 端探测器的暗计数率,η_B 为系统总的传输效率,是信道的传输效率和 Bob 端探测器的探测效率的乘积.

因此,可以得到系统总的计数率为

$$\begin{aligned}Q_\mu &= \frac{1}{P_{post}}\left\{\sum_{n=0}^{\infty}Y_n[1-(1-\eta_A)^n]\frac{\mu^n}{(1+\mu)^{n+1}}\right\}\\ &= \frac{1}{P_{post}}\left\{\frac{d_A d_B}{1+\mu}+\sum_{n=1}^{\infty}Y_n[1-(1-\eta_A)^n]\frac{\mu^n}{(1+\mu)^{n+1}}\right\}.\end{aligned} \quad (7)$$

2.3. 量子误码率(QBER)

系统的误码率主要由两方面组成,一是探测器的暗计数率,另一方面,为由于环境等因素所引起的探测器的误探测,因此 n 光子态的误码率为

$$e_n = \frac{e_0 Y_0 + e_{\text{base}} \eta_n}{Y_n}, \tag{8}$$

其中 e_0 为暗计数所引起的误码率，假设系统采用两个探测器做探测，因此 $e_0 = 1/2$. e_{base} 表示探测器的误探测概率，探测器的误探测是由信道中的噪声、脉冲的后向反射和探测器的缺陷等因素所引起的.

系统总的量子误码率为

$$E_\mu = \left\{ \frac{e_0 d_{\text{B}}}{1+\mu} + \sum_{n=1}^{\infty} e_{\text{base}} Y_n \times [1-(1-\eta_{\text{A}})^n] \frac{\mu^n}{(1+\mu)^{n+1}} \right\} / Q_\mu . \tag{9}$$

3. HSPS 诱惑态

3.1. 两个弱光强态的诱惑态方案

当 Alice 随机改变抽运光的强度，就可以改变双模态中的平均光子数，从而可以在 HSPS 光源系统中应用诱惑态协议进行量子密钥分发. 根据文献[15]的理论证明和数值模拟可知，诱惑态的数量只要两个就已经足够. 由于随着光子数的增大，该光子数态对成码率的影响相对于光子数小的光子数态对成码率来说已经可以忽略不计，这一观点在文章中的数值模拟结果中可以直观的说明，采用两个诱惑态协议的理论曲线与采用无限多个诱惑态[23]协议的曲线非常接近，传输距离只差 2 km. 因此，在这里只讨论 Alice 和 Bob 采用两个弱光强光作为诱惑态，另外一个比较强的光作为信号脉冲的方案. 设 Alice 和 Bob 所采用的两个诱惑态脉冲的平均光子数分别为 x_1 和 x_2，信号光的平均光子数为 μ. 并且满足以下关系：

$$0 \leqslant x_1 \leqslant x_2, \frac{x_1}{1+x_1} + \frac{x_2}{1+x_2} < \frac{\mu}{1+\mu}. \tag{10}$$

3.2. Y_1 的下限

为简化计算设 $Q'_x = P_{\text{post}} Q_x$，因此根据方程(7)可以得到诱惑态脉冲和信号脉冲的计数率分别为

$$Q'_{x_1} = P_{\text{post}} Q_{x_1} = \frac{d_{\text{A}} d_{\text{B}}}{1+x_1} + \sum_{n=1}^{\infty} Y_n [1-(1-\eta_{\text{A}})^n] \frac{x_1^n}{(1+x_1)^{n+1}}, \tag{11}$$

$$Q'_{x_2} = P_{\text{post}} Q_{x_2} = \frac{d_{\text{A}} d_{\text{B}}}{1+x_2} + \sum_{n=1}^{\infty} Y_n [1-(1-\eta_{\text{A}})^n] \frac{x_2^n}{(1+x_2)^{n+1}}. \tag{12}$$

结合方程(11)，(12)和条件(10)，可得

$$\begin{aligned}&(1+x_1) Q_{x_1} - (1+x_2) Q_{x_2} \\ &\leqslant Y_1 \eta_{\text{A}} \left[\frac{x_2 - x_1}{(1+x_1)(1+x_2)} \right] \\ &\quad - \frac{(x_2 + x_1 + 2x_1 x_2)(x_2 - x_1)(1+\mu)^2}{(1+x_1)^2 (1+x_2)^2 \mu^2} \\ &\quad \times \left[Q'_\mu (1+\mu) - d_{\text{B}} d_{\text{A}} - Y_1 \eta_{\text{A}} \frac{\mu}{1+\mu} \right]. \end{aligned} \tag{13}$$

根据上述方程，可以得到 Y_1 的下限为

$$\begin{aligned} Y_1^{x_1, x_2} \geqslant & \frac{(1+x_1)^2 (1+x_2)^2 \mu}{(x_2 - x_1)[(1-x_1 x_2)\mu - (x_1 + x_2 + 2x_1 x_2)] \eta_{\text{A}}} \\ & \times \{ (1+x_2) Q'_{x_2} - (1+x_1) Q'_{x_1} \\ & - \frac{(x_1 + x_2 + 2x_1 x_2)(x_2 - x_1)(1+\mu)^2}{(1+x_1)^2 (1+x_2)^2 \mu^2} \\ & \times [Q'_\mu (1+\mu) - d_{\text{B}} d_{\text{A}}] \}. \end{aligned} \tag{14}$$

把 $Y_1^{x_1, x_2}$ 代入以下方程就可得到信号脉冲的单光子计数率为

$$Q_1^{x_1, x_2'} = Y_1^{x_1, x_2} P(n=1) = Y_1^{x_1, x_2} \eta_{\text{A}} \frac{\mu}{(1+\mu)^2}, \tag{15}$$

其中 $P(n=1)$ 是光源发射出单光子的概率.

3.3. e_1 的上限

根据方程(10)中误码率的表示式，可以得到诱惑态脉冲的 QBER 为

$$E_{x_1} Q_{x_1} = \frac{e_0 d_{\text{B}}}{1+x_1} + \sum_{n=1}^{\infty} e_{\text{base}} [1-(1-\eta_{\text{A}})^n] \times [1-(1-\eta_{\text{B}})^n] \frac{x_1^n}{(1+x_1)^{n+1}}, \tag{16}$$

$$E_{x_2} Q_{x_2} = \frac{e_0 d_{\text{B}}}{1+x_2} + \sum_{n=1}^{\infty} e_{\text{base}} [1-(1-\eta_{\text{A}})^n] \times [1-(1-\eta_{\text{B}})^n] \frac{x_2^n}{(1+x_2)^{n+1}}. \tag{17}$$

根据上述方程，可以得到

$$(1+x_2) E_{x_2} Q_{x_2} - (1+x_1) E_{x_1} Q_{x_1} \geqslant e_1 Y_1 \eta_{\text{A}} \left(\frac{x_2}{1+x_2} - \frac{x_1}{1+x_1} \right). \tag{18}$$

于是根据上式可直接得到单光子所引起的误码率 e_1 的上限为

$$e_1^{x_1,x_2} \leqslant \frac{(1+x_2)(1+x_1)[(1+x_2)E_{x_2}Q_{x_2} - (1+x_1)E_{x_1}Q_{x_1}]}{Y_1^{x_1,x_2}\eta_A(x_2-x_1)}. \tag{19}$$

3.4. 真空态 + 弱光强态的诱惑态方案

根据上述结果，可以将上述条件进行相应的简化，便可推导出文献[20,21]中以真空态和弱光强态作为诱惑态的方案. 这个方案有两方面的优点：其一，可以利用真空态来精确估算系统的暗计数率，其二，可以利用弱光强态做信号脉冲单光子计算率下限 Q_1 和单光子误码率 e_1 的估算. 而且从模拟结果可以看出以真空态和弱光强态作为诱惑态的方案要比一般的两个弱光强态的诱惑态方案更优.

根据上述理论，Alice 和 Bob 可估算系统的暗计数率及其引起误码的概率为

$$Q_{\text{vacuum}} = Y_0, \quad E_{\text{vacuum}} = e_0. \tag{20}$$

把上述方程代入方程(14)可得，在真空态和弱光强态做为诱惑态的情况下 Y_1 的下限为

$$Y_1^{0,x_2} \geqslant \left\{\frac{(1+x_2)^3\mu}{x_2}Q'_{x_2} - \frac{(1+\mu)^3x_2}{\mu}Q'_{\mu} + d_B d_A\left[\frac{(1+\mu)^2x_2}{\mu} - \frac{(1+x_2)^2\mu}{x_2}\right]\right\} \times \frac{1}{\eta_A(\mu-x_2)}. \tag{21}$$

同理，根据方程(19)可以得到信号脉冲中单光子所引起的误码率 e_1 的上限为

$$e_1^{0,x_2} \leqslant \frac{(1+x_2)^2E_{x_2}Q_{x_2} - e_0 d_A d_B(1+x_2)}{Y_1^{0,x_2}\eta_A x_2}. \tag{22}$$

把方程(21)和方程(22)中的 x_2 换成 μ，把 μ 换成 μ'，可以得到与文献[20]中，方程(6)和(8)完全一样的结果.

3.5. 一个弱光强态的诱惑态方案

现在讨论一个弱光强态的诱惑态方案，这个方案由于减少了一个诱惑态，也就降低了实际系统操作上的难度. 因此，这种方案比两个弱光强态的诱惑态方案更容易实现. 一个弱光强态的诱惑态方案是以真空态和弱光强态作为诱惑态方案的一种特殊情况. 如果采用以真空态和弱光强态作为诱惑态方案，当把激光器的调制电压设为零时，由于激光器固有的自发辐射，因此所制备的态并不全是真空态，在这种情况下，再也不能利用真空态来精确估算系统的暗计数率，于是以真空态和弱光强态作为诱惑态就相当于只使用了一个弱光强态作为诱惑态. 下面将讨论在这种情况下的诱惑态方案.

在一个弱光强态的诱惑态方案中，根据方程(17)可以得到系统暗计数的上限为

$$d_B = Y_0^{x_2} \leqslant \frac{(1+x_2)E_{x_2}Q_{x_2}}{e_0}, \tag{23}$$

把上述方程代进方程(21)，可以得到 Y_1 的下限为

$$Y_1^{x_2} = \left\{\frac{(1+x_2)^3\mu}{x_2}Q'_{x_2} - \frac{(1+\mu)^3x_2}{\mu}Q'_{\mu} + Y_0^{x_2}d_A\left[\frac{(1+\mu)^2x_2}{\mu} - \frac{(1+x_2)^2\mu}{x_2}\right]\right\} \times \frac{1}{\eta_A(\mu-x_2)}. \tag{24}$$

根据方程(17)可以得到单光子误码率 e_1 下限为

$$e_1^{x_2} = \frac{E_{x_2}Q_{x_2}(1+x_2)^2}{Y_1^{x_2}\eta_A x_2}. \tag{25}$$

3.6. 数值模拟

根据 ILM—GLLP[5,6] 理论，即使在现实非理想系统中，只要知道单光子脉冲计数率的下限和单光子误码率的上限，估算 Eve 所获得的信息量，从而可以进行秘密放大把最终生成密钥中 Eve 的信息量减少为零，以得到绝对安全的密钥. 因此，把 ILM—GLLP 理论[5,6] 和使用诱惑态方案结合后，就可得到系统的密钥生成率为

$$R \geqslant \frac{P_{\text{post}}}{2}\left\{-Q_\mu f(E_\mu)H_2(E_\mu) + Y_1\eta_A\frac{\mu}{(1+\mu)^2}[1-H_2(e_1)]\right\}, \tag{26}$$

其中，$\frac{1}{2}$ 为 BB84 协议的成码率[24]，$f(E_\mu)$ 为纠错效率，取 $f(E_\mu)=1.16$. $H_2(x)$ 为香农二元熵，具体形式为 $H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$. 利用以上的分析和推导，可以得到不同诱惑态方案中 Y_1 的下限和 e_1 的上限，代进方程(26)中可以计算出不同诱惑态方案它们各自的密钥生成率.

为了方便与弱相干脉冲(WCP)以真空态和弱光强态的诱惑态方案作比较，我们取 GYS 实验[25] 的参数，如表 1 所示. 而且 HSPS 光源与 WCP 光源信号脉冲平均光子数都分别取最优值.

数值模拟结果示于图 1，HSPS 光源的诱惑态方案的安全传输距离总体上比以 WCP 光源的诱惑态

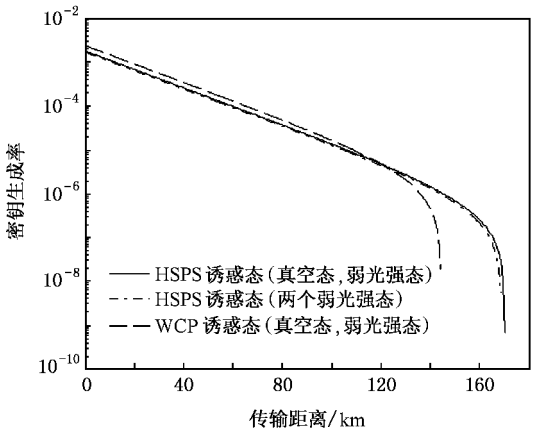

图 1 HSPS 光源诱惑态与 WCP 光源诱惑态的比较 其中 $\eta_A = 0.6, d_A = 5 \times 10^{-8}$

方案要远.而从两个 HSPS 诱惑态方案的模拟结果可以直观的看出,以真空态和弱光强态作为诱惑态方案比一般的两个弱光强态的诱惑态方案由更高的密钥生成率和更高的传输距离.这是由于,当 $x_1 + x_2$ 的值越小,则对 Y_1 和 e_1 的估算就越精确,从而将会提高成码率和传输距离.而且以真空态和弱光强态作为诱惑态方案的结果与文献[21]中的模拟结果相符.

表 1 GYS 实验参数[26]

λ/nm	α/(dB·km^{-1})	e_{base}/(%)	$d_B/10^{-6}$	η_B/(%)
1550	0.21	3.3	1.7	4.5

另一方面,从图 1 中可以看到,HSPS 光源的成码率要比 WCP 光源的成码率低,这是因为在非真空态中多光子的概率与成码率是成反比的. 由于 HSPS 光源的光子数分布服从热态分布,而 WCP 光源的光子数分布服从泊松分布,所以可得以下结论:

$$P^{th}(n \geqslant 2 \mid n \geqslant 1) = \frac{\mu}{1+\mu} < P^{Po}(n \geqslant 2 \mid n \geqslant 1) = \frac{1 - e^{-\mu(1-\mu)}}{1 - e^{-\mu}}, \quad (27)$$

其中,P^{th}和 P^{Po}分别为 HSPS 光源和 WCP 光源非真空态中的多光子概率. 因此,HSPS 光源的成码率要比 WCP 光源的成码率低.

4. 双探测器 HSPS

根据‘双探测器’理论[22],并且把它与 HSPS 光源诱惑态方案相结合. 从数值模拟结果可以看到系统在保证安全性的情况下,传输距离有明显的提高.

4.1. 双探测器理论

根据 ILM—GLLP 理论证明可知,当系统总的 QBER 超过阈值时,系统的安全性就再也得不到保证. 也就说 Alice 和 Bob 通过检测系统 QBER 是否超过阈值来确定通信过程是否有窃听者的存在. 当 QBER 没超过阈值时,Alice 和 Bob 可以通过秘密放大来把窃听者所获取的信息量减少为零,当 QBER 超过阈值,Alice 和 Bob 就终止该次通信,并舍弃该次通信的结果.

在 QKD 的实际应用中,由于各种各样的器件缺陷和受环境因素的影响,使得系统即使在没有 Eve 存在的情况下也会产生 QBER,这样的误码率称为系统的固有 QBER. 在各种系统缺陷中,探测器噪音所引起的暗计数是系统固有 QBER 的主要来源. 如果 Alice 和 Bob 不能区分系统的固有 QBER 和由于 Eve 的窃听所引起的 QBER,那么他们就把系统所有的固有 QBER 都归因于 Eve 的窃听所引起的. 这样 Alice 和 Bob 就要牺牲更多的密钥来进行秘密放大,以确保最终生成的密钥的安全性.

但事实上,即使 Eve 很有能力,也没有办法改变 Bob 端探测器的暗计数率. 由于 Eve 不能改变探测器的暗计数,所以可以认为 QBER 中暗计数部分不是由 Eve 所造成的,比暗计数高的部分才是由于 Eve 的窃听所引起的. 这样就可以对 Eve 在密钥分发过程中所得到的信息量给出一个更合理的评估,因而就可以减少在秘密放大中无谓的损耗.

另外,如果能够找到一种既重复频率高,噪声小的探测器,这样不但可以提高光源的重复频率,而且还可以进一步降低系统的固有 QBER,使得秘密放大的损耗进一步减少.因此,就可以进一步提高成码率和传输距离. 但是现实中重复频率高的探测器所引起的噪声也越大,而低噪声的探测器它的重复频率却又很低. 不过幸运的是,根据文献[22]中把重复频率高的探测器和低噪声探测器混合使用的‘双探测器’理论,这一问题得到很好的解决.

“双探测器’理论主要思想是,Bob 端使用两个不同的探测器进行探测,一个是重复频率高但噪声大,另外一个是噪声小但重复频率低. Bob 随机的选择其中一个来进行探测,在这种情况下 Eve 无法预测 Bob 是使用哪一个探测器进行探测. 根据 ILM-GLLP[5,6] 的理论,窃听所引起的 QBER 不能超过某一阈值,也就是说 Eve 的窃听受制于探测器的 QBER.

于是 Eve 为了使窃听不被发现，他只能同等对待这两种情况，认为 Bob 始终采用低噪声探测器进行探测. 因此，Alice 和 Bob 就可认为低噪声探测器的 QBER 就是系统的 QBER，并用这个 QBER 来评估 Eve 所获得的信息量.

4.2. 双探测的 HSPS

由于受 HSPS 光源特点的限制，假设一个普通的门限探测器和一个低噪声超导探测器在系统中混合使用. 根据上述理论，在双探测器系统中，可以利用超导探测器所引起的 QBER 来评估 Eve 所获得的信息量，从而减少秘密放大过程中的损耗，增加传输距离.

在数值模拟过程中，我们选用普通门限探测器的重复频率为 100 MHz 其余参数与 3.4 节所取的相同，超导探测器的参数为 $f = 2.5$ MHz，$\eta_D = 0.5$，$d_B = 3 \times 10^{-7}$ [27]. 数值模拟结果如图 2 所示，HSPS 光源系统的安全传输距离达到 221.5 km，比没有使用“双探测器”情况高出约 50 km，比“双探测器”WCP 光源的诱惑态增加了约 25 km. 根据“双探测器”理论，系统应用“双探测器”目的是在保证系统安全性的前提下，对 Eve 所获得的信息量给出一个更合理的评估，以减少在秘密放大中无谓的损耗. 从图2中可以看出，应用了“双探测器”的 HSPS 光源系统的曲线比没有使用“双探测器”的曲线所增长的部分，就是由于减少了秘密放大过程的损耗所得到的. 另一方面，从图 2 还发现了，不论是在 HSPS 光源系统还是在 WCP 光源系统中，应用了“双探测器”后系统的安全传输距离都比没有使用“双探测器”系统高出约 50 km. 也就是说，“双探测器”对于不同光子数分布的光源所产生的作用是近乎相同的.

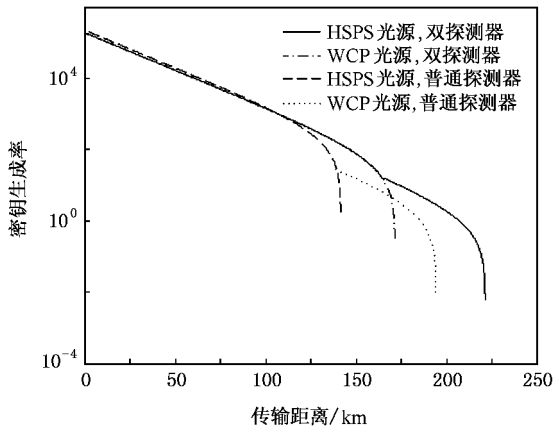

图 2 “双探测器”HSPS 诱惑态数值模拟

5. 结　论

由于考虑到实际应用中，激光器并不能做到完全消光，因而使得制备真空态并不容易. 在这种情况下，文献[20,21]中所讨论的以真空态和弱光强态作为诱惑态的情况就不再适用，因而针对这一实际情况本文提出了两个诱惑态都是弱光强态的方案. 另一方面，当把激光器的调制电压设置为零以使用真空态和弱光强态作为诱惑态时，激光器由于自身固有的自发辐射会随机的产生光脉冲，也就是说激光器所产生的并不全是真空态，因此再也不能用真空态来估算系统的暗计数. 在这种情况下，以真空态和弱光强态作为诱惑态的方案，就会退化为一个弱光强态作为诱惑态，因此本文提出了一个弱光强态的诱惑态方案，以解决这一问题.

由于本文引入“双探测器”理论，并进行了数值模拟. 由于“双探测器”能够进一步限制 Eve 的窃听和对 Eve 所获得的信息量进行更合理的评估，从而可以减少秘密放大中的损耗，以增加传输距离. 从模拟结果可以直观的看出，在同为 HSPS 光源的情况下，通过应用“双探测器”减少秘密放大过程的损耗，系统总的传输距离要比普通探测器的传输距离增加了约 50 km. 而在同为“双探测器”情况下，HSPS 光源诱惑态比 WCP 光源诱惑态情况要高出约 25 km. 而且通过不同光源的模拟比较，我们发现，“双探测器”在不同光子数分布的光源系统中，所增加的安全传输距离是近乎相同的.

[1] Bennett C H, Brassard G 1984 *Proceeding of IEEE International Conference on Computers, Systems, and Signal Processing* (New York: IEEE) p175

[2] Mayer D, Assoc J 2001 *Comput. Mach.* **48** 351

[3] Shor P W, Preshill J 2000 *Phys. Rev. Lett.* **85** 441

[4] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S, Sanpera A 1996 *Phys. Rev. Lett.* **77** 2818; 1998 *Phys. Rev. Lett.* E **80** 2022

[5] Inamori H, Lutkenhause N, Mayers D 2001 *http://arxiv.org/abs/quant-ph/0107017*

[6] Gottesman D, Lo H K, Lutkenhaus N, Preskill J 2004 *Quantum Inf. Comput.* **4** 325
[7] Huttner B, Imoto N, Gisin N, Mor T 1995 *Phys. Rev.* A **51** 1863
[8] Lutkenhaus N, Jahma M 2002 *New. J. Phys.* **4** 44
[9] Scarani V, Acin A, Robordy G, Ginsin N 2004 *Phys. Rev. Lett.* **92** 57901
[10] Koashi M 2004 *Phys. Rev. Lett.* **93** 120501
[11] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 57901
[12] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[13] Wang X B 2005 *Phys. Rev.* A **72** 12322
[14] Lo H K, Ma X, Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[15] Ma X, Qi B, zhao Yi, Lo H K 2005 *Phys. Rev.* A **72** 12326
[16] Harrington J W, Ettinger J M, Hughes, R J, Nordholt J E 2005 *http://arxiv.org/abs/quant-ph*/0503002
[17] Ji L L, Wu L A 2005 *Acta Phys. Sin.* **54** 736 (in Chiness) [季玲玲、吴令安 2005 物理学报 **54** 736]
[18] Ljunggren D, engner M 2005 *http://arxiv.org/abs/quant-ph*/0507046
[19] Pittmann T B, Jacobs B C, Franson J D 2005 *Opt. Commun.* **246** 545
[20] Wang Q, Wang X B, Guo G C 2006 *http://arxiv.org/abs/quant-ph*/06010134
[21] Horikiri T, Kobayashi T 2006 *Phys. Rev.* A **73** 32331
[22] Qi B, Zhao Y, Ma X F, Lo H K, Qian Li 2006 *http://arxiv.org/abs/quant-ph*/0611044
[23] Lo H K 2004 *Proceedings of the IEEE International Symposium on Information Theory* (New Jersey: IEEE) p137
[24] Yang L, Wu L A, Liu S H 2002 *Acta Phys. Sin.* **51** 2446 (in Chinese) [杨 理、吴令安、刘颂豪 2002 物理学报 **51** 2446]
[25] Gobby C, Yuan Z L, Shields A J 2004 *Appl. Phys. Lett.* **84** 3762
[26] Rosenberg D, Harrington J W, Rice P R, Hiskett P A, Petersoin C G, Hughes R J, Nordhotlt J E, Lita A E, Nam S W 2006 *http://arxiv.org/abs/quant-ph*/0607186

Decoy state quantum key distribution with dual detectors heralded single photon source*

Mi Jing-Long Wang Fa-Qiang† Lin Qing-Qun Liang Rui-Sheng Liu Song-Hao
(*Laboratory of Photonic Information Technology, School for Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou* 510631, *China*)
(Received 31 January 2007; revised manuscript received 22 May 2007)

Abstract

Decoy state has recently been proved as a useful method for substantially improving the performance of quantum key distribution (QKD). Considering the imperfect extinction ratio and the spontaneous emission of the practical Laser, vacuum states are not prepared easily. So in this paper, the optimal situation of the decoy state protocol applied to the QKD system with heralded single photon source (HSPS) is complemented and extended. The two weak decoy state protocol and the one decoy state protocol are proposed. At last, the theory of "dual detectors" is combined with the QKD system with HSPS. In the simulation, the secure distance is up to 221.5 km, which is approximately 50 km more than that of the on-off detectors.

Keywords: quantum key distribution, decoy state, heralded single photon source, dual detectors
PACC: 0365, 4250, 4230

* Project supported by the National Natural Science Foundation of China (Grant No. 60578055) and State Key Development Program for Basic Research of China (Grant No. 2007CB307001).

† Corresponding author. E-mail: fqwang98@sina.com