第 59 卷 第 1 期 2010 年 1 月
1000-3290/2010/59(01)/0287-06

物 理 学 报
ACTA PHYSICA SINICA

Vol.59,No.1,January,2010

基于条件参量下转换光子对的非正交编码诱惑态量子密钥分发*

胡华鹏[1)] 王金东[1)†] 黄宇娴[1)] 刘颂豪[1)] 路 巍[2)]

1)(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 510006)

2)(中国科学院合肥智能研究所,合肥 230031)

(2009 年 3 月 11 日收到;2009 年 4 月 30 日收到修改稿)

诱惑态方法和非正交编码协议可以有效的抵制光子数分束攻击,所以近来得到了广泛的关注.这里结合了这两种方法提出了一种新方案,光源采用呈泊松分布的参量下转换光子对,发送方随机的改变抽运光的强度获得不同强度的信号光,信号态用来产生密钥,诱惑态用来监测窃听,并估算单光子和两光子的计数率和量子误码率,模拟了密钥产生率与传输距离的关系曲线,分析了该方案可以进一步提高安全量子密钥分发的性能.

关键词:量子密钥分发,诱惑态,参量下转换

PACC:4250,4230Q,0365

1. 引 言

量子密钥分发(QKD)[1—3]作为量子力学和密码学结合的产物,允许通信双方在即使存在窃听者的情况下还能进行安全信.与传统的编码的不同,QKD 的绝对安全性是建立在物理基本规律的基础上.目前大量的实际的量子密钥分配系统采用的光源并不是理想的单光子源,通常采用的都是衰减的激光脉冲光源(弱相干态),这将不可避免的会产生多光子脉冲,所以在原则上会受到光子数分束(PNS)攻击[4,5]:首先,窃听者用非破坏测量技术测量出从 Alice 发出的脉冲的光子数,当是单光子脉冲时阻止它继续传送,当是多光子脉冲时截获其中一部分光子余下经无损耗信道传送给接收方 Bob,由于这两部分光子来自同一个多光子脉冲,所以窃听者将会获得与接收者完全相同的,QKD 的无条件安全性就会被完全破坏.

针对 PNS 攻击,2004 年 Scarani, Acin, Ribordy 和 Gisin 提出了 SARG04 协议[6],该协议采用与 BB84 协议[3]相同的两组共轭基中的四个基矢进行量子密钥分发,他们的区别仅在于经典的编码方式上,SARG04 协议采用四态非正交的编码方式,在该情况下窃听者无法确定的区分两光子态而不对系统产生扰动,所以 SARG04 协议中两光子脉冲也能产生密钥,文献[6]中已经充分证明了对于 PNS 攻击该协议要比 BB84 协议更安全.此外,另一种限制 PNS 攻击的方法就是采用诱惑态方案,国际上几个研究小组相继提出了几种弱相干态光源的诱惑态 QKD 的理论方案[7—11],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,实现信号态中随机的加入了诱惑态,信号态和诱惑态的物理本质上没有区别,只是强度不同,因此窃听者 Eve 是无法区分开它们的,故 Eve 进行光子数分束攻击时对诱惑态和信号态一视同仁,当 Alice 和 Bob 在量子通信阶段结束后,他们就利用检测到的诱惑态传输结果来估算信号光中单光子脉冲计数率的下限和单光子所引起误码率的上限,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,在这种情况下他们就舍弃该次通信的结果,重新开始下一次通信.随后相关的诱惑态 QKD 实际实验[12—14]也有了很大的进展,大大提高了密钥传输的距离.

近来随着参量下转化获得纠缠光子对技术[15,16]的发展,人们开始从理论上利用纠缠光子对来进行 QKD,由于这对光子几乎是同时产生的具有

* 广州市科技支撑计划(批准号:2008Z1-D501)和广东省工业攻关项目(批准号:2007B010400009)资助的课题.

† 通信联系人. E-mail:jindongw@126.com

相同的性质,所以可以让其中的一束作为信号光来实现 QKD,而另一束闲置光则被用来预报信号光中的光子数目,只有当信号光为非空脉冲时才开启接收方的探测器,这样就会大大减小长距离量子密钥分发过程中的暗计数,从而进一步提高系统的安全传输距离.SARG04 协议与诱惑态协议相结合的理论即 SARG04 协议诱惑态 QKD 方案[17—19]、基于参量下转换光子对的一些诱惑态 QKD 方案[20—24]相继被提出,本文在这些理论的基础上提出一种新的 SARG04 协议诱惑态 QKD 方案,值得一提的是这里的光子对是在特殊条件下参量下转化获得的,光子数服从泊松分布.

2. 基于条件下转化光子对的诱惑态 QKD 新方案

单色抽运光子流和量子真空噪声对非中心对称非线性晶体的综合作用,导致了在光的自发参量下转换过程中,一个高频光子在非线性晶体内会以某一概率自发地分裂为两个低频光子,分别称为信号光子和闲置光子,合称自发参量下转化(SPDC)光子对,文献[25,26]中已阐明了在特定的条件下的自发参量下转化可以获得双模态

$$|\psi\rangle = \sum_{n=0}^{\infty} \sqrt{p_n}\,|n\rangle_s\,|n\rangle_i, \tag{1}$$

光子数呈泊松分布,即

$$p_n(\mu) = e^{-\mu}\mu^n/n!, \tag{2}$$

式中 n 表示光子数,μ 表示平均强度.

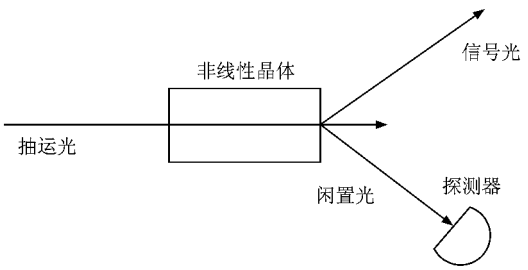

图 1 Alice 端 SPDC 产生光子对示意图

本文提出的新方案是基于该光源为前提的,如图 1 所示信号光和闲置光几乎是同时产生的具有相同的性质.假设 Alice 端的门限探测器的效率为 η_A,暗计数为 d_A,设 QKD 量子信道的衰减率为 α 则通信双方 Alice 和 Bob 间的传输率为 $\eta_{AB} = 10^{-\alpha L/10}$,Bob 端的探测器探测率为 η_{Bob},则信道总的传输率为 $\eta = 10^{-\alpha L/10}\cdot\eta_{Bob}$.用 Y_n 表示 Alice 发送 n 光子脉冲时引起 Bob 端探测器计数率,Y_n 主要包括背景噪声引起的暗计数 Y_0 和 n 光子脉冲引起的计数 $\eta_n = 1-(1-\eta)^n$ 两个方面,因为这两方面同时发生的概率非常小,所以 Y_n 可以表示为

$$\begin{aligned} Y_n &= Y_0 + \eta_n - Y_0\eta_n \\ &\approx Y_0 + 1 - (1-\eta)^n. \end{aligned} \tag{3}$$

用 e_n 表示 Alice 发送 n 光子脉冲引起 Bob 端错误探测的概率即错误率(或者误码率),设暗计数中误探测概率为 e_0,信道中的噪声,脉冲的后向反射和探测器本身的缺陷等因素所引起的 Bob 端探测器的错误响应概率为 e_d,那么 e_n 可表示为

$$\begin{aligned} e_n &= \frac{e_0 Y_0 + e_d\eta_n}{Y_n} \\ &= \frac{e_0 Y_0 + e_d[1-(1-\eta)^n]}{Y_0 + 1 - (1-\eta)^n}. \end{aligned} \tag{4}$$

以下将具体介绍基于条件参量下转化光子对再结合 SAG04 协议的诱惑态 QKD 方案.

2.1. 理想化的无限多诱惑态 QKD 方案

发送方 Alice 随机的调节抽运光的强度实现随机的发出各种强度的信号光(强度为 μ 的信号态和各种强度($\nu_1,\nu_2,\nu_3,\cdots,\nu_m$)的诱惑态),同时 Alice 用门限探测器探测与信号光成对的闲置光中的光子数来预报信号光的光子数,当探测到光子时开启接收端即 Bob 端的探测器,Alice 和 Bob 对信号态和各种诱惑态编码和解码实现 QKD,这里采用了非正交编码 SAG04 协议,双光子也能产生密钥进一步提高系统的安全性.当 QKD 完毕后,Alice 告诉 Bob 信号态和诱惑态的分布情况,由探测结果计算出信号态和各种诱惑态的计数率 $Q_\mu, Q_{\nu_1}, Q_{\nu_2}, Q_{\nu_3},\cdots, Q_{\nu_m}$ 及量子误码率 E_μ, $E_{\nu_1}, E_{\nu_2}, E_{\nu_3},\cdots, E_{\nu_m}$.然后 Alice 和 Bob 根据信号态和诱惑态的计数率及量子误码率计算出单光子和双光子的计数率 Y_1, Y_2 和量子误码率 e_1, e_2,下面来具体阐述诱惑态方法是怎样得出这些值的,信号态的计数率和量子误码率可以表示为

$$\begin{aligned} Q_\mu &= Y_0 d_A p_0(\mu) + \sum_{n=1}^{\infty} Y_n[1-(1-\eta_A)^n]p_n(\mu) \\ &= Y_0 d_A e^{-\mu} + \sum_{n=1}^{\infty} Y_n[1-(1-\eta_A)^n]e^{-\mu}\frac{\mu^n}{n!} \\ &= (Y_0 d_A e^{-\mu} + Y_0 - Y_0 e^{-\mu\eta_A}) \\ &\quad + (1 - e^{-\mu\eta} - e^{-\mu\eta_A} + e^{-\mu\eta-\mu\eta_A+\mu\eta\eta_A}), \end{aligned} \tag{5}$$

$$Q_{\mu}E_{\mu} = Y_0 e_0 d_A e^{-\mu} + \sum_{n=1}^{\infty} Y_n e_n [1-(1-\eta_A)^n] e^{-\mu} \frac{\mu^n}{n!}$$
$$= e_0 (Y_0 d_A e^{-\mu} + Y_0 - Y_0 e^{-\mu\eta_A})$$
$$+ e_d (1 - e^{-\mu\eta} - e^{-\mu\eta_A} + e^{-\mu\eta-\mu\eta_A+\mu\eta\eta_A}). \quad (6)$$

因为采用的诱惑态和信号态具有相同的特征(同波长,同时钟,等等),所以窃听者 Eve 从脉冲中的光子数中获得的信息无法区分出信号态和诱惑态,故

$$Y_n(\text{decoy}) = Y_n(\text{signal}) = Y_n,$$
$$e_n(\text{decoy}) = e_n(\text{signal}) = e_n,$$

那么对于强度为 $\nu_1, \nu_2, \nu_3, \cdots, \nu_m$ 的诱惑态的计数率也可表示为

$$Q_{\nu_1} = Y_0 d_A e^{-\nu_1} + \sum_{n=1}^{\infty} Y_n [1-(1-\eta_A)^n] \times e^{-\nu_1} \frac{\nu_1^n}{n!}, \quad (7)$$

$$Q_{\nu_2} = Y_0 d_A e^{-\nu_2} + \sum_{n=1}^{\infty} Y_n [1-(1-\eta_A)^n] \times e^{-\nu_2} \frac{\nu_2^n}{n!}, \quad (8)$$

$$Q_{\nu_3} = Y_0 d_A e^{-\nu_3} + \sum_{n=1}^{\infty} Y_n [1-(1-\eta_A)^n] \times e^{-\nu_3} \frac{\nu_3^n}{n!}, \quad (9)$$

$$\cdots$$

$$Q_{\nu_m} = Y_0 d_A e^{-\nu_m} + \sum_{n=1}^{\infty} Y_n [1-(1-\eta_A)^n] \times e^{-\nu_m} \frac{\nu_m^n}{n!}. \quad (10)$$

量子误码率可以表示为

$$Q_{\nu_1} E_{\nu_1} = Y_0 e_0 d_A e^{-\nu_1} + \sum_{n=1}^{\infty} Y_n e_n [1-(1-\eta_A)^n] \times e^{-\nu_1} \frac{\nu_1^n}{n!}, \quad (11)$$

$$Q_{\nu_2} E_{\nu_2} = Y_0 e_0 d_A e^{-\nu_2} + \sum_{n=1}^{\infty} Y_n e_n [1-(1-\eta_A)^n] \times e^{-\nu_2} \frac{\nu_2^n}{n!}, \quad (12)$$

$$Q_{\nu_3} E_{\nu_3} = Y_0 e_0 d_A e^{-\nu_3} + \sum_{n=1}^{\infty} Y_n e_n [1-(1-\eta_A)^n] \times e^{-\nu_3} \frac{\nu_3^n}{n!}, \quad (13)$$

$$\cdots$$

$$Q_{\nu_m} E_{\nu_m} = Y_0 e_0 d_A e^{-\nu_m} + \sum_{n=1}^{\infty} Y_n e_n [1-(1-\eta_A)^n] \times e^{-\nu_m} \frac{\nu_m^n}{n!}. \quad (14)$$

当 $m \to \infty$ 即理想化的采用无限多诱惑态时,通信双方根据以上的表达式组成的方程组理论上能够解得 $\{Y_n\}$ 和 $\{e_n\}$ 的准确值.最后通信双方 Alice 和 Bob 可以拿解的结果与系统理论安全值(可以用(3),(4)式来估算)比较,如果相差太大或者更准确的说是实际 QKD 过程单光子和双光子的计数率太低而量子误码率太高,就肯定存在窃听者 Eve,譬如 Eve 采用 PNS 攻击为了窃取更多的信息必然是尽可能的截掉单光子和双光子则单光子和双光子计数就仅剩背景噪声引起的暗计数,这肯定是不安全的了,那么就放弃本次通信,如果结果正常则经纠错和密性放大提取密钥.

2.2. 四诱惑态 QKD 方案

以上介绍了理想化的诱惑态 QKD 方案,这种方案要求使用无限多个诱惑态来准确计算出单光子和双光子的计数率 Y_1, Y_2 及量子误码率 e_1, e_2,显然这是不现实的.由于 QKD 采用的信号态的强度 μ 一般很小,脉冲中光子数 $n > 5$ 的概率的数量级为 10^{-9} 远小于暗计数 Y_0(数量级为 10^{-6})故可以忽略,所以只需少量的诱惑态就足够了.现在假设 Alice 随机的改变抽运光的强度进而随机的获得四种不同强度的信号光(信号态 μ,三种诱惑态 ν_1, ν_2, ν_3),强度满足以下关系:

$$0 < \nu_3 < \nu_2 < \nu_1 < \mu,$$
$$\nu_1 - \nu_2 - \frac{\nu_1^3 - \nu_2^3}{\mu^2} = 0,$$
$$\nu_1 + \nu_2 > \mu, \nu_2 + \nu_3 < \mu,$$

同时 Alice 用门限探测器探测与信号光成对的闲置光中的光子数来预报信号光的光子数,当探测到光子时开启接收端即 Bob 端的探测器,Alice 和 Bob 进行非正交编码和解码实现 QKD.完成 QKD 后 Alice 告诉 Bob 信号态和三种诱惑态的分布情况由 Bob 端的探测结果计算出 $Q_{\mu}, Q_{\nu_1}, Q_{\nu_2}, Q_{\nu_3}$ 及量子误码率 $E_{\mu}, E_{\nu_1}, E_{\nu_2}, E_{\nu_3}$,(5)—(9),(11)—(13)式为它们的表达式.接下来就是计算单光子和双光子的计数率 Y_1, Y_2 和量子误码率 e_1, e_2,这里只采用了少量的诱惑态来估算它们,具体推导过程如下.

由 $e^{\nu_2} \times$ [Eq.(8)] $- e^{\nu_3}$ [Eq.(9)] 得

$$Q_{\nu_2} e^{\nu_2} - Q_{\nu_3} e^{\nu_3} = Y_1 \eta_A (\nu_2 - \nu_3) + \sum_{n=2}^{\infty} Y_n [1-(1-\eta_A)^n] \frac{\nu_2^n - \nu_3^n}{n!}$$

$$\leqslant Y_1\eta_A(\nu_2-\nu_3)+\frac{\nu_2^2-\nu_3^2}{\mu^2}\sum_{n=2}^{\infty}Y_n[1-(1-\eta_A)^n]\frac{\mu^n}{n!}$$

$$=Y_1\eta_A(\nu_2-\nu_3)+\frac{\nu_2^2-\nu_3^2}{\mu^2}(Q_\mu e^\mu-Y_0 d_A-Y_1\eta_A\mu).$$

移项后可以得出单光子计数率 Y_1 的下限 Y_1^L，

$$Y_1\geqslant Y_1^L=\frac{\mu^2(Q_{\nu_2}e^{\nu_2}-Q_{\nu_3}e^{\nu_3})-(\nu_2^2-\nu_3^2)(Q_\mu e^\mu-Y_0 d_A)}{\mu\eta_A(\nu_2-\nu_3)(\mu-\nu_2-\nu_3)}. \tag{15}$$

类似地由

$$\begin{aligned}Q_{\nu_1}e^{\nu_1}-Q_{\nu_2}e^{\nu_2}&=Y_1\eta_A(\nu_1-\nu_2)+Y_2[1-(1-\eta_A)^n]\frac{\nu_1^2-\nu_2^2}{2}\\&\quad+\sum_{n=3}^{\infty}Y_n[1-(1-\eta_A)^n]\frac{\nu_1^n-\nu_2^n}{n!}\\&\leqslant Y_1\eta_A(\nu_1-\nu_2)+Y_2[1-(1-\eta_A)^n]\times\frac{\nu_1^2-\nu_2^2}{2}+\frac{\nu_1^3-\nu_2^3}{\mu^3}\\&\quad\times\sum_{n=3}^{\infty}Y_n[1-(1-\eta_A)^n]\frac{\mu^n}{n!}\\&=Y_1\eta_A(\nu_1-\nu_2)+Y_2[1-(1-\eta_A)^n]\frac{\nu_1^2-\nu_2^2}{2}\\&\quad+\frac{\nu_1^3-\nu_2^3}{\mu^3}\Big\{Q_\mu e^\mu-Y_0 d_A-Y_1\eta_A\mu-Y_2[1-(1-\eta_A)^2]\frac{\mu^2}{2}\Big\},\end{aligned}$$

得出双光子的计数率 Y_2 的下限 Y_2^L，

$$Y_2\geqslant Y_2^L=\frac{2\mu(Q_{\nu_1}e^{\nu_1}-Q_{\nu_2}e^{\nu_2})-2(\nu_1-\nu_2)(Q_\mu e^\mu-Y_0 d_A)}{\mu(\nu_1-\nu_2)(\nu_1+\nu_2-\mu)[1-(1-\eta_A)^2]}. \tag{16}$$

再由 $e^{\nu_2}\times$[Eq.(12)]$-e^{\nu_3}$[Eq.(13)]得

$$\begin{aligned}&Q_{\nu_2}E_{\nu_2}e^{\nu_2}-Q_{\nu_3}E_{\nu_3}e^{\nu_3}\\&=Y_1e_1\eta_A(\nu_2-\nu_3)+\sum_{n=2}^{\infty}Y_ne_n[1-(1-\eta_A)^n]\frac{v_2^n-\nu_3^n}{n!}\\&\geqslant Y_1e_1\eta_A(\nu_2-\nu_3).\end{aligned}$$

可以得出单光子的量子误码率 e_1 的上限 e_1^U，

$$e_1\leqslant e_1^U=\frac{Q_{\nu_2}E_{\nu_2}e^{\nu_2}-Q_{\nu_3}E_{\nu_3}e^{\nu_3}}{Y_1^L\eta_A(v_2-\nu_3)}. \tag{17}$$

类似地由 $\nu_2 e^{\nu_1}\times$[Eq.(11)]$-\nu_1 e^{\nu_2}$[Eq.(12)]可以得到

$$\begin{aligned}&\nu_2Q_{\nu_1}E_{\nu_1}e^{\nu_1}-v_1Q_{\nu_2}E_{\nu_2}e^{\nu_2}\\&=Y_0e_0d_A(\nu_2-\nu_1)+Y_2e_2[1-(1-\eta_A)^2]\frac{\nu_2\nu_1^2-\nu_1\nu_2^2}{2}\\&\quad+\sum_{n=3}^{\infty}Y_ne_n[1-(1-\eta_A)^n]\frac{\nu_2\nu_1^n-\nu_1\nu_2^n}{n!}\\&\geqslant Y_0e_0d_A(\nu_2-\nu_1)+Y_2e_2[1-(1-\eta_A)^2]\times\frac{\nu_2\nu_1^n-\nu_1\nu_2^n}{2}.\end{aligned}$$

可以得出双光子的量子误码率 e_2 的上限 e_2^U，

$$e_2\leqslant e_2^U=\frac{2\nu_2E_{\nu_1}Q_{\nu_1}e^{\nu_1}-2\nu_1Q_{\nu_2}E_{\nu_2}e^{\nu_2}-2Y_0e_0d_A(\nu_2-\nu_1)}{Y_2^L[1-(1-\eta_A)^2]\nu_1\nu_2(\nu_1-\nu_2)}. \tag{18}$$

将测算的 Q_μ，Q_{ν_1}，Q_{ν_2}，Q_{ν_3} 及 E_μ，E_{ν_1}，E_{ν_2}，E_{ν_3} 的值代入(15)—(18)式就可以估算出单光子和双光子计数率及量子误码率的限值.最后与理论值比较判断是否正常，不正常则放弃本次通信，正常则进一步纠错及保密放大提取密钥.

2.3. 安全性分析

QKD 系统的安全性可以从互信息的角度去评估，当 Alice 和 Bob 间的互信息 I(A,B)大于 Alice 和 Bob 间的互信息 I(A,E)时，通信双方可以采用单向

密性放大将 Eve 窃取的信息变为无效，这样就可以提取安全的密钥，文献[17,19]中从这一角度推导出了 SARG04 协议的安全密钥产生率为

$$R \geqslant q\{-Q_\mu f(E_\mu)H_2(E_\mu) + Q_1[1-H_2(e_1)] + Q_2[1-H_2(e_2)]\}, \quad (19)$$

式中 $q=\frac{1}{4}$ 为 SARG04 协议的效率，$f(E_\mu)$ 为纠错效率，取 $f(E_\mu)=1.16$，

$$H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$$

是二元熵.

对于采用上文中的四诱惑态 QKD 方案的实际系统来说，信号态的计数率 Q_μ 和量子误码率 E_μ 可以通过测量结果计算出来，各诱惑态的计数率 Q_{ν_1}，Q_{ν_2}，Q_{ν_3} 及量子误码率 E_{ν_1}，E_{ν_2}，E_{ν_3} 也可以测算出，再由(15)—(18)式可以估算出 Q_1，Q_2，e_1，e_2 的限值，将这些结果代入(19)式就可以估算实际 QKD 的安全密钥产生率，进而就可以评估系统的安全性能.

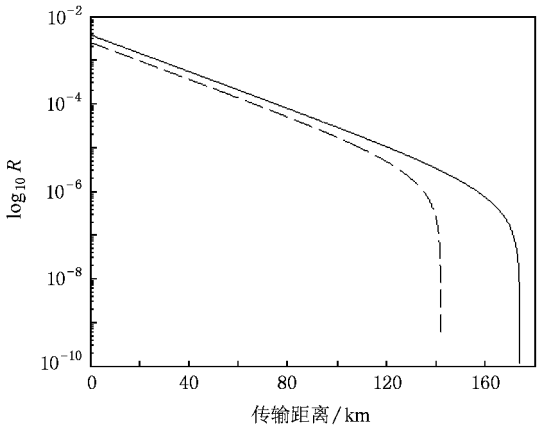

图 2　密钥产生率随传输距离变化曲线

理论上可以利用 GYS[27] 实验参数(波长 1550 nm，衰减率 $\alpha=0.2$ dB/km，$e_d=3.3\%$，$\eta_{Bob}=0.045$，$Y_0=1.7\times10^{-6}$) 对基于呈泊松分布参量下转换光子对的非正交编码 QKD 方案进行性能仿真. 根据(19)式可知安全密钥产生率 R 是关于信号强度 μ 和传输距离 L 的函数，可以用二元函数简单表示为 $R(\mu,L)$，利用 Matlab 进行优化处理后可以模拟出 R 随传输距离 L 的变化曲线，如图 2 中的实线所示，其中 Alice 端的探测器的暗计数率 $d_A=5\times10^{-8}$，探测效率 $\eta_A=0.99$. 图 2 中的虚线表示的是弱相干脉冲 BB84 协议诱惑态 QKD 方案[11] 的密钥产生率随传输距离变化的曲线，其中信号强度取 $\mu=0.48$，安全传输距离达到了 142.05 km. 从图 2 中的数据模拟结果可以直观的看出，基于泊松分布的参量下转化光子对的 SARG04 协议诱惑态方案比传统的弱相干脉冲 BB84 协议诱惑态方案有更高的安全密钥产生率和更远的安全传输距离，这与理论是相符的.

3. 结　论

本文提出了利用特定条件下参量下转化产生光子数为泊松分布的光子对，再结合 SARG04 协议进行诱惑态 QKD 的方案，推导了安全密钥产生率的计算公式，该方案有以下特点：1) 诱惑态量子密钥分发较非诱惑态量子密钥分发能够更好的估算出单光子的计数率和量子误码率，提高了安全密钥产生率和安全通信距离；2) 非正交编码协议即 SARG04 协议较 BB84 协议两光子脉冲也能产生密钥，因此在相同的安全条件下采用 SARG04 协议的信号态脉冲的强度可以比 BB84 协议强，从而提高安全密钥产生率；3) 与普通衰减光源相比较，利用参量下转换光子对中的闲置光去预报信号光的光子数情况可以大大减小长距离传输过程暗计数的影响，进而增大安全密钥传输距离；4) 与之前利用参量下转化光子对(光子数服从热态分布) 诱惑态 QKD 相比较，现在是在特定条件下自发参量下转化产生光子对，光子数为泊松分布，在强度相同的情况下 $P_{泊松}(n\geqslant2\mid n\geqslant1) < P_{热态}(n\geqslant2\mid n\geqslant1)$，而密钥产生率是同 $P(n\geqslant2\mid n\geqslant1)$ 成反比的，所以用泊松分布的参量下转化光子对作为信号光可以提高密钥产生率. 可见本文的诱惑态 QKD 方案是一种比较好的量子密钥分发方案，随着参量下转化获的光子对技术和光子数探测技术的进一步发展，应该会有很好的实际应用.

[1] Gisin N, Ribordy G, Tittel W, Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[2] Ekert A K, Huttner B 1996 *J. Mod. Opt.* **41** 2455
[3] Bennett C H, Brassard G 1984 *Proceeding of IEEE International Conference on Computers, Systems, and Signal Processing* (New York: IEEE) p175
[4] Huttner B, Imoto N, Gisin N, Mor T 1995 *Phys. Rev.* A **51** 1863
[5] Lutkenhaus N, Jahma M 2002 *New. J. Phys.* **4** 44
[6] Scarani V, Acin A, Ribordy G, Gisin N 2004 *Phys. Rev. Lett.* **92** 057901
[7] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[8] Wang X B 2005 *Phys. Rev.* A **72** 012322
[9] Wang X B 2005 *Phys. Rev. Lett.* **74** 230503
[10] Lo H K, Ma X F, Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[11] Ma X F, Qi B, Zhao Y, Lo H K 2005 *Phys. Rev.* A **72** 012326
[12] Zhao Y, Qi B, Ma X F, Lo H K 2006 *Phys. Rev. Lett.* **96** 070502
[13] Peng C Z, Zhang J, Yang D, Gao W B, Ma H X, Yin H, Zeng H P, Yang T, Wang X B, Pan J W 2007 *Phy. Re. Lett.* **98** 010505
[14] Yuan Z L, Sharpe A W, Shields A J 2007 *Appl. Phys. Lett.* **90** 011118
[15] Ji L L, Wu L A 2005 *Acta Phys. Sin.* **54** 736 (in Chinese) [季玲玲、吴令安 2005 物理学 **54** 736]
[16] Pittmann T B, Jacobs B C, Franson J D 2005 *Opt. Commun.* **246** 545
[17] Hang C, Fung F, Tamaki K, Lo H K 2006 *Phys. Rev.* A **73** 012337
[18] Li J B, Fang X M 2006 *Chin. Phys. Lett.* **23** 1375
[19] Li J B, Fang X M 2006 *Chin. Phys. Lett.* **23** 775
[20] Adachi Y, Yamamoto T, Koashi M, Imoto N 2007 *Phy. Re. Lett.* **99** 180503
[21] Wang Q, Wang X B, Guo G C 2007 *Phys. Rev.* A **75** 012312
[22] Wang Q, Karlsson A 2007 *Phys. Rev.* A **76** 014309
[23] Zhang S L, Zou X B, Li K, Jin C H, Guo G C 2007 *Phys. Rev.* A **76** 044304
[24] Mi J L, Wang F Q, Lin Q Q, Liang R S, Liu S H 2008 *Acta Phys. Sin.* **57** 0678 (in Chinese) [米景隆、王发强、林青群、梁瑞生、刘颂豪 2008 物理学报 **57** 0678]
[25] Riedmatten H D, Scarani V, Marcivic I, Acin A, Tittel W, Zbinden H, Gisin H 2004 *J. Mod. Opt.* **51** 1637
[26] Mori S, Söderholm J, Namekata N, Inoue S 2006 *Opt. Commun.* **264** 156
[27] Gobby C, Yuan Z L, Shields A J 2004 *Appl. Phys. Lett.* **84** 3762

Nonorthogonal decoy-state quantum key distribution based on conditionally prepared down-conversion source*

Hu Hua-Peng[1)] Wang Jin-Dong[1)†] Huang Yu-Xian[1)] Liu Song-Hao[1)] Lu Wei[2)]

1) (*Lab of Photonic Information Technology, School for Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou* 510006, *China*)

2) (*Heifei Institute of Intelligent Machines, Chinese Academy of Sciences, Heifei* 230031, *China*)

(Received 11 March 2009; revised manuscript received 30 April 2009)

Abstract

The decoy-state method and the non-orthogonal encoding protocol, being capable of resisting the photon-number splitting attack, have become attractive recently. Here, we combine both the methods and propose a new protocol using a conditionally prepared down-conversion source, following Poisson photon number distribution. In the protocol, Alice randomly changes the intensities of the pump light so that the intensity of signal photon of photon pair is randomly changed. The signal state is used for generating keys, the decoy states for detecting the eavesdropping and estimating the fraction of single-photon and two-photon pulses. We have simulated the final key rate over transmission distance, showing our scheme can enhance the performance of quantum key distribution.

Keywords: quantum key distribution, decoy state, parametric down-conversion

PACC: 4250, 4230Q, 0365

* Project supported by the Key Projects in the Guangzhou Science & Technology Pillar Program (Grant No. 2008Z1-D501) and by the Guangdong Key Technologies R&D Program (Grant No. 2007B010400009).

† Corresponding author. E-mail: jindongw@126.com