基于弱相干态光源的非正交编码被动诱骗态量子密钥分配*

周媛媛† 周学军

(海军工程大学电子工程学院通信工程系,武汉 430033)

(2010 年 9 月 29 日收到;2010 年 12 月 10 日收到修改稿)

基于改造的弱相干态光源,提出了一种非正交编码被动诱骗态量子密钥分配方案. 该方案不主动制备诱骗态,而是根据发送端探测器是否响应,将接收端的探测结果分为响应集合和未响应集合,以此分别作为信号态和诱骗态,并利用这两个集合来估计参量和生成密钥. 数值仿真表明,非正交编码被动诱骗态方案的密钥生成效率和安全传输距离都优于现有的被动诱骗态方案,且性能非常接近主动无穷诱骗态方案的理论极限值;未响应集合对密钥生成的参与使方案性能免受发送端探测效率的影响,弥补了实际探测器探测效率低下的缺陷;由于不需要主动制备诱骗态,该方案实现非常简单,适用于高速量子密钥分配的场合.

关键词: 量子光学, 量子密钥分配, 被动诱骗态, 密钥生成效率

PACS: 03.67.Dd, 03.67.Hk

1. 引 言

理论和实验都已证明诱骗态方案[1—8]可以显著改善采用实际光源的量子密钥分配(QKD)[9]系统的性能. 在诱骗态方案中,发送者(Alice)除信号态之外还要随机发送不同强度的诱骗态. 诱骗态和信号态在物理本质上没有任何区别,只是强度不同而已,所以窃听者(Eve)无法区分. 根据对诱骗态信号的检测结果,Alice 和接收者(Bob)可以更加准确地估计量子信道的特性,监测 Eve 是否存在,从而改善实际 QKD 的密钥生成效率和安全传输距离.

目前,诱骗态方案可分为两类:1)主动诱骗态方案[10—16],即 Alice 需要主动制备诱骗态. 该方案有两个方面的缺点:一是需要主动调制光强,操作比较复杂,从而降低了量子密钥分配的速度;二是 Alice 在制备诱骗态的过程中难免引入一些边信息,Eve 利用这些信息即可分辨信号态和诱骗态,使得诱骗态方案的安全基础难以保证. 2)被动诱骗态方案[17—19],即 Alice 不需要主动准备诱骗态,信号态和诱骗态是由系统根据 Alice 端探测器的检测结果,靠被动选择的方式来产生. 由于不需要主动制备诱骗态,便克服了以上主动诱骗态方案的缺点.

光源能产生光子数分布概率相关的两路信号是实现被动诱骗态方案的前提. 参数下转换光源(PDCS)的双模式特性给被动诱骗态方案的产生提供了土壤,2007 年之后,基于 PDCS 的被动诱骗态方案相继提出[17—19]. 因为弱相干态(WCS)光源只能产生一路信号,所以 WCS QKD 系统一直被认为不能实现被动诱骗态方案[20]. 但是 Curty 研究小组在 2009 年对 WCS 光源进行了改造[21],提出了基于 WCS QKD 系统的 BB84 被动诱骗态方案,并于 2010 年将这一思想进行了完善和推广[22].

本文将考虑非正交编码协议(SARG04)[23],其量子传输和量子测量部分都和 BB84 协议相同,区别仅存在于编码方法. SARG04 协议采用四态非正交编码的方法,使得 Eve 无法在不扰动系统的情况下区分 2 光子态,因此 2 光子态也可以产生安全密钥,这使得 SARG04 协议具有比 BB84 协议更高的安全性. 既然 SARG04 协议和 BB84 协议在量子传输和量子测量部分都相同,那么不难证明能实现 BB84 协议的实验设备也同样可以实现 SARG04 协

* 国家高技术研究发展计划(批准号: 2009AAJ128)资助的课题.

† E-mail: zyy_hjgc@yahoo.com.cn

议[24],所以研究 SARG04 协议的性能就显得非常必要和有意义. 本文提出了一种基于改造的 WCS 光源的 SARG04 被动诱骗态方案,并对方案的性能进行了详细的分析.

2. 被动诱骗态 QKD 系统模型

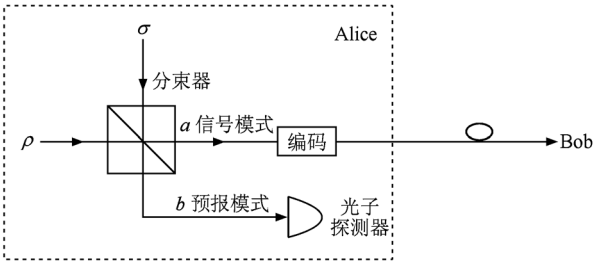

图 1 基于改造的 WCS 光源的被动诱骗态量子密钥分配

2.1. 改造的 WCS 光源模型

Curty 研究小组通过对硬件的改造使 WCS 光源最终输出的两路信号的光子数分布概率具有了相关性,其基本思路[21]如图 1 所示:采用两个 WCS 光源,它们分别产生相位随机的相干态 σ 和 ρ,输入到分束器并发生干涉,则输出的两路信号 a 和 b 的光子数分布概率将具有相关性. 只要对 b 路信号进行检测,就能确定 a 路信号的光子数分布概率.

设相干态 σ 和 ρ 为

$$\rho = \mathrm{e}^{-u_1}\sum_{n=0}^{\infty}\frac{u_1^n}{n!}|n\rangle\langle n|,$$

$$\sigma = \mathrm{e}^{-u_2}\sum_{n=0}^{\infty}\frac{u_2^n}{n!}|n\rangle\langle n|, \qquad (1)$$

式中 u_1 和 u_2 表示两路信号的强度. 此时输出的 a 模式是 n 光子态,b 模式是 m 光子态的联合概率为[21]

$$p_{n,m} = \frac{v^{n+m}\mathrm{e}^{-v}}{n!m!}\frac{1}{2\pi}\int_0^{2\pi} r^n(1-r)^m\mathrm{d}\theta,$$

$$v = u_1 + u_2,$$

$$r = \frac{u_1 t + u_2(1-t) + \xi\cos\theta}{v},$$

$$\xi = 2\sqrt{u_1 u_2(1-t)t}, \qquad (2)$$

其中 θ 代表相位,t 为分束器的分光比. 可以看出 $p_{n,m}$ 是两个泊松分布的乘积,只要 Alice 检测得到 b 模式光子数的分布概率,则 a 模式输出 n 光子态的概率可确定为

$$p_n = \sum_{n=0}^{\infty} p_{n,m} = \frac{v^n}{n!}\frac{1}{2\pi}\int_0^{2\pi} r^n\mathrm{e}^{-vr}\mathrm{d}\theta. \qquad (3)$$

a 模式中 n 光子态未被 Alice 端探测器检测到的概率为

$$p_n^{nt} = (1-d_A)\sum_{m=0}^{\infty}(1-\eta_A)^m p_{n,m}$$

$$= (1-d_A)\frac{v^n\mathrm{e}^{-\eta_A v}}{n!}\frac{1}{2\pi}\int_0^{2\pi} r^n\mathrm{e}^{-(1-\eta_A)vr}\mathrm{d}\theta, \qquad (4)$$

式中 d_A 为 Alice 端探测器的暗计数率,η_A 为其探测效率.

则 a 模式中 n 光子态被 Alice 端探测器检测到的概率为 $p_n^t = p_n - p_n^{nt}$,可以看出 p_n^{nt} 和 p_n^t 不再服从泊松分布.

未响应事件发生的总概率为

$$S^{nt} = \sum_{n=0}^{\infty} p_n^{nt} = (1-d_A)\mathrm{e}^{-\eta_A[u_1(1-t)+u_2 t]} I_{0,\eta_A\xi}, \qquad (5)$$

式中 $I_{0,\eta_A\xi}$ 为一类修正贝塞尔函数.

2.2. 信道模型

设 Y_n 为 n 光子态的计数率,即 Alice 发送一个 n 光子态而 Bob 端探测器又检测到这一事件的概率.

$$Y_n = 1 - (1-d_B)(1-\eta)^n, \qquad (6)$$

式中 d_B 为 Bob 探测系统的暗计数率;η 为 Alice 和 Bob 之间的全局传输效率,是信道传输效率 t_{AB} 和 Bob 端探测效率 η_B 的乘积.

$$t_{AB} = 10^{-\alpha l/10},$$

$$\eta = t_{AB}\eta_B, \qquad (7)$$

式中 α(dB/km)为光纤衰减系数,l(km)为光纤传输距离.

Alice 发送 n 光子态的误码率为

$$e_n Y_n = e_d Y_n + (e_0 - e_d)d_B, \qquad (8)$$

式中 $e_0 = 1/2$,为背景噪声产生的误码率;e_d 是光子击中错误探测器的概率.

3. 基于 WCS 光源的 SARG04 被动诱骗态 QKD 新方案

3.1. 方案描述

本文提出的新方案基于改造的 WCS 光源. 如图 1 所示,将光源输出的模式 a 进行非正交编码,作为信号模式发送给 Bob,而模式 b 被 Alice 端探测器检测来预报模式 a 的光子数和到达时间,这样可以减

少长距离量子密钥分配过程中暗计数的影响. 本文设 Alice 和 Bob 都采用门限探测器. 根据 Alice 端探测器是否响应,可以将 Bob 的探测结果分为两类:响应集合和未响应集合,我们将响应集合用作信号态,未响应集合用作诱骗态. 在本文方案中,信号态和诱骗态的功能没有严格的界限,因为未响应集合不仅监测 Eve 的存在,还将参与密钥生成. 我们利用响应集合和未响应集合对单光子和 2 光子态计数率的上限和误码率的下限进行估计,如果得到的结果与理论安全值相差太大,就认为此次量子通信过程中有 Eve 窃听,便放弃此次通信,重新进行密钥分配. 如果结果证明是安全的,便可按照 ILM-GLLP[25] 公式来提取密钥.

设 Q_n 为 n 光子态的全局计数率,为 a 模式输出 n 光子态的概率 p_n 与 Y_n 的乘积. 设 Q 为光子源的总计数率. 如上所述,Q_n 和 Q 都可以分为响应集合(Q_n^t, Q^t)和未响应集合(Q_n^{nt}, Q^{nt}).

$$Q = \sum_{n=0}^{\infty} p_n Y_n,$$

$$Q^{nt} = \sum_{n=0}^{\infty} p_n^{nt} Y_n. \tag{9}$$

与上相同,光子源的量子比特误码率(QBER)也可写为

$$EQ = \sum_{n=0}^{\infty} p_n e_n Y_n,$$

$$E^{nt}Q^{nt} = \sum_{n=0}^{\infty} p_n^{nt} e_n Y_n. \tag{10}$$

且有 $Q^t = Q - Q^{nt}$, $E^tQ^t = EQ - E^{nt}Q^{nt}$.

Bob 探测到的所有信号都可以根据 Alice 的探测情况被分到不同的集合,每个集合都可用 ILM-GLLP 的思想来进行分析. 则最终密钥生成效率可以看成是响应集合和未响应集合各自密钥生成效率的总和,即 $R = R^t + R^{nt}$.

$$\begin{aligned} R^{nt} \geqslant \frac{1}{4}\{ & -Q^{nt} f(E^{nt}) H_2(E^{nt}) \\ & + p_1^{nt} Y_1 [1 - H_2(e_1)] \\ & + p_2^{nt} Y_2 [1 - H_2(e_2)]\}, \\ R^t \geqslant \frac{1}{4}\{ & -Q^t f(E^t) H_2(E^t) \\ & + p_1^t Y_1 [1 - H_2(e_1)] \\ & + p_2^t Y_2 [1 - H_2(e_2)]\}, \end{aligned} \tag{11}$$

式中 1/4 为 SARG04 协议的筛选效率;$f(x)$ 是以误码率为变量的双向纠错效率函数;$H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$. 其中,$Q^{nt}$, Q^t, E^{nt} 和 E^t 可在实验中直接观测得到,为了对现实 QKD 系统的密钥生成效率进行估算,还需求得 Y_1 和 Y_2 的下限以及 e_1 和 e_2 的上限.

3.2. 参数估计

我们首先求取 Y_0 的上下限,为下面估计 Y_1 和 Y_2 的下限以及 e_1 和 e_2 的上限做好准备.

根据(10)式可得

$$\begin{aligned} E^{nt}Q^{nt} &= \sum_{n=0}^{\infty} p_n^{nt} e_n Y_n \geqslant p_0^{nt} e_0 Y_0, \\ E^tQ^t &= \sum_{n=0}^{\infty} p_n^t e_n Y_n \geqslant p_0^t e_0 Y_0. \end{aligned} \tag{12}$$

则可以简单估计 Y_0 的上限为

$$Y_0 \leqslant Y_0^U = \min\left\{\frac{E^{nt}Q^{nt}}{p_0^{nt}e_0}, \frac{E^tQ^t}{p_0^t e_0}\right\}. \tag{13}$$

因为当 $n \geqslant 2$ 时, $p_1 p_0^{nt} - p_1^{nt} p_0 \leqslant 0$,

$$\begin{aligned} p_1 Q^{nt} - p_1^{nt} Q &= (p_1 p_0^{nt} - p_1^{nt} p_0) Y_0 \\ &\quad + \sum_{n=2}^{\infty} (p_1 p_0^{nt} - p_1^{nt} p_0) Y_0 \\ &\leqslant (p_1 p_0^{nt} - p_1^{nt} p_0) Y_0. \end{aligned} \tag{14}$$

可得

$$Y_0 \geqslant Y_0^L = \max\left\{\frac{p_1 Q^{nt} - p_1^{nt} Q}{p_1 p_0^{nt} - p_1^{nt} p_0}, 0\right\}. \tag{15}$$

现在利用 $p_2 Q^{nt} - p_2^{nt} Q$ 来估计 Y_1 的下限.

由于 $n \geqslant 2$ 时, $p_2 p_n^{nt} - p_2^{nt} p_n \leqslant 0$, 而 $n \leqslant 1$ 时, $p_2 p_n^{nt} - p_2^{nt} p_n \geqslant 0$, 于是得

$$\begin{aligned} p_2 Q^{nt} - p_2^{nt} Q &= \sum_{n=0}^{\infty} (p_2 p_n^{nt} - p_2^{nt} p_n) Y_n \\ &\leqslant (p_2 p_0^{nt} - p_2^{nt} p_0) Y_0 \\ &\quad + (p_2 p_1^{nt} - p_2^{nt} p_1) Y_1. \end{aligned} \tag{16}$$

即可得 Y_1 的下限为

$$Y_1 \geqslant Y_1^L = \max\left\{\frac{p_2^{nt} Q - p_2 Q^{nt} - (p_2^{nt} p_0 - p_2 p_0^{nt}) Y_0^U}{p_1 p_2^{nt} - p_1^{nt} p_2}, 0\right\}. \tag{17}$$

同理可利用 $p_3 Q^{nt} - p_3^{nt} Q$ 来估计 Y_2 的下限为

$$Y_2 \geqslant Y_2^L = \max\left\{\frac{p_3 Q^{nt} - p_3^{nt} Q - (p_3 p_0^{nt} - p_3^{nt} p_0) Y_0^U - (p_3 p_1^{nt} - p_3^{nt} p_1) Y_1^u}{p_3 p_2^{nt} - p_3^{nt} p_2}, 0\right\}. \tag{18}$$

式中 $Y_1^u = \min\left\{\frac{Q^{nt} - p_0^{nt}Y_0^L}{p_1^{nt}}, \frac{Q^t - p_0^tY_0^L}{p_1^t}\right\}$ 为 Y_1 的简单上限.

因为

$$E^tQ^t = \sum_{n=0}^{\infty} p_n^t e_n Y_n \geqslant p_0^t e_0 Y_0 + p_1^t e_1 Y_1,$$

$$E^{nt}Q^{nt} = \sum_{n=0}^{\infty} p_n^{nt} e_n Y_n \geqslant p_0^{nt} e_0 Y_0 + p_1^{nt} e_1 Y_1. \quad (19)$$

可推导 e_1 的上限为

$$e_1 \leqslant e_1^U = \min\left\{\frac{E^tQ^t - p_0^tY_0^Le_0}{p_1^tY_1^L}, \frac{E^{nt}Q^{nt} - p_0^{nt}Y_0^Le_0}{p_1^{nt}Y_1^L}\right\}. \quad (20)$$

同理可得 e_2 的上限为

$$e_2 \leqslant e_2^U = \min\left\{\frac{E^tQ^t - p_0^tY_0^Le_0}{p_2^tY_2^L}, \frac{E^{nt}Q^{nt} - p_0^{nt}Y_0^Le_0}{p_2^{nt}Y_2^L}\right\}. \quad (21)$$

4. 数值仿真与分析

将上述估计的 Y_1 和 Y_2 的下限以及 e_1 和 e_2 的上限代入(11)式,根据 $R = R^t + R^{nt}$ 便可估算实际 QKD 的安全密钥生成效率. 本文仿真采用的实验参数主要来源于 GYS 实验[26]和文献[22]:$a = 0.21$ (dB/km), $d_A = 3.2 \times 10^{-7}$, $\eta_A = 0.12$, $d_B = 1.7 \times 10^{-6}$, $\eta_B = 0.045$, $e_d = 0.033$, $f = 1.22$.

以下仿真都根据传输距离选取了最优信号态强度. 本文方案的 u_1 和 u_2 的最优强度取值几乎不随传输距离的变化而改变,u_1 的值约取 1,u_2 的值大约取在 0.002. u_1 和 u_2 强度相差如此之大的原因为:当一信号强度非常弱时,相比于 u_1 和 u_2 强度数量级相同的情况,a 模式输出的光子数分布更接近泊松分布(如图 2 所示),这更利于准确估计 Y_0, Y_1, Y_2, e_1 和 e_2 的限值. 但需要说明的是:u_1 和 u_2 的这种取值方式在实际实验中不一定是最优的,特别是在通信数据有限,且考虑统计波动时,p^{nt} 和 p^t 会因为太相近而不能被分辨.

从图 3 可以看出:

1)采用 WCS 光源时,SARG04 主动无穷诱骗态方案的安全传输距离达到约 165 km,这也是利用 SARG04 方案进行量子密钥分配所能达到的理论极限;SARG04 被动诱骗态方案的安全传输距离可达约 159 km,密钥生成效率较无穷诱骗态的理论极限

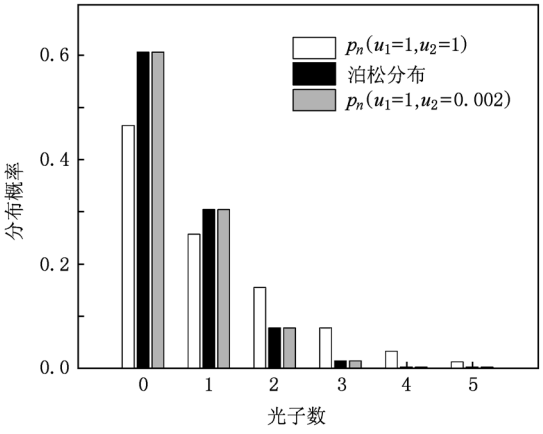

图 2 信号态取不同强度时光子数的分布情况

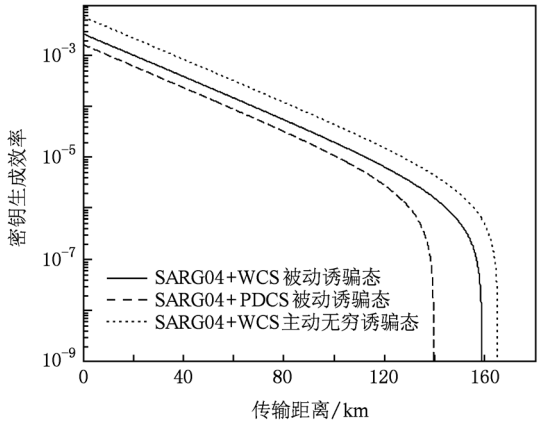

图 3 不同 SARG04 诱骗态方案的性能比较

要稍低,这是因为被动诱骗态方案只利用了响应集合和未响应集合进行参数估计,估计值会稍偏离真实值,所以导致了密钥生成效率的下降,但是性能还是比较接近理论极限值的. 实际上,无穷诱骗态方案是无法实现的,主动诱骗态方案采用有限数目的诱骗态虽然可趋近理论极限,但是实现复杂,量子密钥分配速度下降,且会引起边信息的泄露. 而被动诱骗态不需调制光强,实现简单,可提高密钥分配速度,也避免了边信息的泄露.

2)在图 3 中,我们依次取 Alice 端探测器探测效率 $\eta_A = 0.12, 0.3, 0.6, 0.9$ 对本文方案的密钥生成效率进行了计算和仿真,四条曲线重叠在一起,几乎无法分辨. 在主动诱骗态方案中[14,15],只用响应集合来估计参量和生成密钥. 这种情况下,当 η_A 越低时,Alice 端探测器响应的门限就越高,可以用来生成密钥的数据就减少,最终造成了主动诱骗态方案的性能好坏严重依赖 η_A 的现象. 而在本文提

出的方案中,响应集合和未响应集合都参与密钥生成. 当 η_A 降低时,虽然响应集合对密钥生成所做的贡献减小,但是未响应集合对密钥生成所做的贡献增大;反之,响应集合的贡献增大,未响应集合的贡献减小. 两个集合的作用总是此消彼长,最终维持总的密钥生成效率不变. 这说明未响应集合的加入弥补了实际探测器探测效率低下的缺陷.

3)基于 WCS 光源的 SARG04 被动诱骗态方案的性能优于基于 PDCS 光源的 SARG04 被动诱骗态方案,原因为 PDCS 产生的信号中多光子脉冲所占比例要大于 WCS 光源,导致了密钥生成效率的降低.

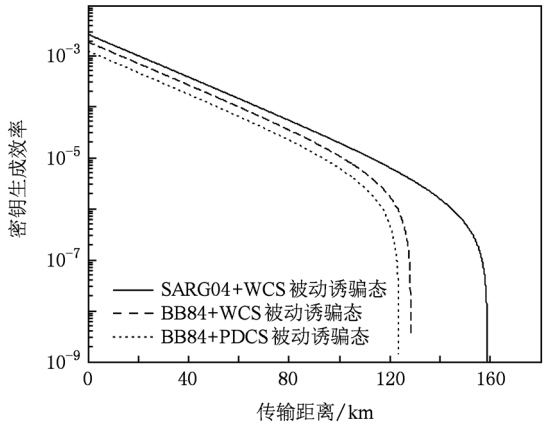

图 4 SARG04 被动诱骗态方案和 BB84 被动诱骗态方案的性能比较

从图 4 可以看出,SARG04 被动诱骗态方案的性能总体优于 BB84 被动诱骗态方案[18,22]. 在都采用改造的 WCS 光源时,两个方案实际操作难易程度相当,但是 SARG04 被动诱骗态方案的密钥生成效率和传输距离都优于 BB84 被动诱骗态方案. 这是因为 BB84 只允许单光子脉冲生成密钥,而 SARG04 协议还允许 2 光子脉冲参与密钥生成.

在实际光源有涨落[27—30]的情况下,本文方案可以按照文献[30]的方法进行分析.

5. 结 论

本文基于改造的 WCS 光源,提出了一种 SARG04 被动诱骗态方案. 改造的 WCS 光源可以输出的两路光子数分布概率相关的信号,因此该方案使其中一路信号承载信息发送给 Bob,而将另外一路信号送给 Alice 端探测器进行检测. 根据 Alice 端探测器是否响应,将 Bob 端的探测结果分为响应集合和未响应集合,利用这两个集合来估计参量和生成密钥. 本文方案有三个方面的优势:1)相对于已有的被动诱骗态方案性能更优,安全传输距离可达 159 km,非常接近主动无穷诱骗态的理论极限;2)与主动诱骗态方案不同,没有舍弃未响应集合,而是将未响应集合应用到参数估计和密钥生成中,克服了主动诱骗态方案性能严重依赖发送端探测器探测效率的问题,弥补了实际探测器探测效率低下的缺陷;3)不需要主动制备诱骗态,实现非常简单,适合应用于高速量子密钥分配的场合,且不会引起边信息的泄露. 因此本文提出的 SARG04 被动诱骗态方案是一种简单有效且可行的量子密钥分配方案.

[1] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901

[2] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503

[3] Wang X B 2005 *Phys. Rev.* A **72** 012322

[4] Lo H K, MA X F, Chen K 2005 *Phys. Rew. Lett.* **94** 230504

[5] Zhang S L, Zou X B, Li K, Jin C H, Guo G C 2007 *Phys. Rev.* A **76** 044304

[6] 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 *Phys. Rev. Lett.* **98** 010505

[7] Yin Z Q, Han Z F, Chen W, Xu F X, Wu Q L, Guo G C 2008 *Chin. Phys. Lett.* **25** 3547

[8] Wang Q, Chen W, Xavier G, Swillo M, Zhang T, Sauge S, Tengner M, Han Z F, Guo G C, Karlsson A 2008 *Phys. Rew. Lett.* **100** 090501

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

[10] MA X F, Qi B, ZhaoY, Lo H K 2005 *Phys. Rew.* A **72** 012326

[11] Li J B, Fang X M 2006 *Chin. Phys. Lett.* **23** 775

[12] Wang Q, Wang X B, Guo G C 2007 *Phys. Rew.* A **75** 012312

[13] Yin Z Q, Han Z F, Sun F W, Guo G C 2007 *Phys. Rev.* A **76** 014304

[14] Mi J L, Wang F Q, Lin Q Q, Liang R S 2008 *Chin. Phys.* B **17** 1178

[15] Hu H P, Wang J D, Huang Y X, Liu S H, Lu W 2010 *Acta Phys. Sin.* **59** 287 (in Chinese) [胡华鹏、王金东、黄宇娴、刘颂豪、路 巍 2010 物理学报 **59** 287]

[16] Mi J L, Wang F Q, Lin Q Q, Liang R S, Liu S H 2008 *Acta Phys. Sin.* **57** 678 (in Chinese) [米景隆、王发强、林青群、梁瑞生、刘颂豪 2008 物理学报 **57** 678]

[17] Mauerer W, Silberhorn C 2007 *Phys. Rew.* A **75** 050305

[18] Adachi Y, Yamamoto T, Koashi M, Imoto N 2007 *Phys. Rev. Lett.* **99** 180503

[19] Quan D X, Pei C X, Zhu C H, Liu D 2008 *Acta Phys. Sin.* **57** 5600 (in Chinese) [权东晓、裴昌幸、朱畅华、刘 丹 2008 物理学报 **57** 5600]
[20] Ma Xiongfeng, Lo H K 2008 *New Journal of Physics* **10** 073018
[21] Curty M, Moroder T, Ma X F, Lütkenhaus N 2009 *Opt. Lett.* **34** 3238
[22] Curty M, Ma X F, Qi B, Moroder T 2010 *Phys. Rew.* A **81** 022310
[23] Scarani V, Acin A, Ribordy G, Gisi N 2004 *Phys. Rev. Lett.* **92** 057901
[24] Fung C H F, Tamaki K, Lo H K 2006 *Phys. Rew.* A **73** 012337
[25] Gottesman D, Lo H K, Lütkenhaus N, Preskill J 2004 *Quantum Inform. Comput.* **4** 325
[26] Gobby C, Yuan Z L, Shields A J 2004 *Phys. Rew. Lett.* **84** 3762
[27] Wang X B 2007 *Phys. Rew.* A **75** 052301
[28] Wang X B, Peng C Z, Zhang J, Yang L, Pan J W 2008 *Phys. Rew.* A **77** 042311
[29] Zhao Y, Qi Bing, Lo H K 2008 *Phys. Rew.* A **77** 052327
[30] Hu J Z, Wang X B 2010 *Phys. Rew.* A **82** 012331

Nonorthogonal passive decoy-state quantum key distribution with a weak coherent state source*

Zhou Yuan-Yuan† Zhou Xue-Jun

(*Department of Communication Engineering, School of Electronic Engineering, Naval University of Engineering, Wuhan* 430033, *China*)

(Received 29 September 2010; revised manuscript received 10 December 2010)

Abstract

A nonorthogonal passive decoy-state method is presented with a reconstructive weak coherent state source. The method dose not prepare decoy states actively and divides the receiver detection events into two groups, i. e., triggered components and nontriggered components, according to triggering situation of the sender detector. Both triggered and nontriggered components, as signal states and decoy states, are used to do some estimations and to generate secure key. The simulation results show that a better key generation rate and a longer secure transmission distance can be obtained with the nonorthogonal passive decoy-state method than with the existing passive methods, and that the performance is comparable to the theoretical limit of an active infinite decoy-state protocol. Furthermore, the nontriggered component contribution to key generation offsets the limitation of the detector low efficiency, and the performance of the method dose not depend on the detector efficiency of sender. Because decoy states need not be prepared actively, and our protocol is easy to implement and apply to quantum key distribution at high transmission rates.

Keywords: quantum optics, quantum key distribution, passive decoy state, key generation rate
PACS: 03.67.Dd, 03.67.Hk

* Project supported by the National High Technology Research and Development Program of China (Grant No. 2009AAJ128).

† E-mail: zyy_hjgc@yahoo.com.cn