基于标记配对相干态光源的诱骗态量子密钥分配性能分析*

周媛媛[1)†] 张合庆[2)] 周学军[1)] 田培根[1)]

1) (海军工程大学电子工程学院, 武汉 430033)

2) (北京航空航天大学电子信息工程学院, 北京 100191)

(2013年5月30日收到; 2013年6月27日收到修改稿)

从有效性、稳定性和可行性三个方面, 对基于标记配对相干态光源的诱骗态量子密钥分配的性能进行了全面分析. 采用四组实验数据对基于标记配对相干态光源的三强度诱骗态方案的密钥生成效率、量子比特误码率和最优信号态强度与安全传输距离之间的关系进行了仿真和分析; 考虑到光源涨落, 对方案的稳定性进行了讨论和仿真; 并对基于标记配对相干态光源设计简单易实现方案的可行性进行了分析. 结论表明: 基于标记配对相干态光源的诱骗态方案性能在安全传输距离和密钥生成效率两方面都优于现有基于弱相干态光源和预报单光子源的诱骗态方案; 在光源强度涨落相同条件下, 标记配对相干态光源的稳定性逊于预报单光子源, 而优于相干态光源. 但是标记配对相干态光源在有效性上的优势可弥补其在稳定性上的不足; 且标记配对相干态光源的双模特性为设计简单易实现的被动诱骗态方案提供了条件.

关键词: 量子光学, 量子密钥分配, 标记配对相干态光源, 性能

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.62.200302

1 引 言

由于量子密钥分配 (QKD)[1] 可以实现经典密码学不能达到的无条件安全性, 所以人们为之倾注了极大的探索热情并取得了令人惊叹的成就. 但QKD 无条件安全性的理论证明都是基于理想的单光子源, 而这以目前的技术水平还无法达到, 所以实验中多以准单光子源来代替. 此类光源产生的脉冲中除了单光子脉冲, 还有空脉冲和多光子脉冲, 这使得 Eve 可以采用光子数分离攻击 (PNS)[2] 获得 Alice 和 Bob 之间的全部信息而不留下任何痕迹. 幸运的是, 2003 年 Hwang[3] 提出了可以抵抗 PNS 攻击的诱骗态方案, 此方案在密钥分配过程中通过改变光脉冲的强度 (诱骗信号) 来监测量子信道是否存在 PNS 攻击, 从而保证实际 QKD 的安全.

目前, 尝试将诱骗态技术应用在基于不同光源的 QKD 系统之中成为了提高量子密钥分配性能最有效的途径之一 [4−13]. 诱骗态方案和弱相干态光源 (WCS) 的结合使得 BB84 QKD 的安全传输距离从 30 km (无诱骗态) 延长到了 140 km[4,5]. 随后预报单光子源 (HSPS) 又进一步将安全传输距离提升至 170 km[6]. 目前, WCS 和 HSPS 已成为 QKD 实验中最常用的光源 [14−17].

作为一种优质的 QKD 光源应具有以下三个特点. 首先, 基于该光源的 QKD 方案的密钥生成效率和安全传输距离要有优势, 即有效性高. 第二, 诱骗态方案成立的基本假设是发送者 Alice 能对光源输出的光子数进行完美的控制. 然而, 这在实际实验中是一项不可能完成的任务, 因为光源强度实际存在着一定程度的涨落. 这虽然不会致命性地颠覆 QKD 的原理, 但会严重降低系统的安全性能. 因此, 光源的强度涨落对 QKD 性能的影响要尽量小, 即稳定性好. 第三, 基于该光源要能设计出简单易实

* 国家高技术研究发展计划 (批准号: 2011AA7014061) 资助的课题.

† 通讯作者. E-mail: zyy_hjgc@aliyun.com

现的 QKD 方案, 即可行性强.

在有效性方面, HSPS QKD 虽可获得较 WCS QKD 更远的传输距离, 但是 HSPS QKD 和 WCS QKD 的密钥生成效率随安全传输距离变化的曲线有一交点, 在交点之前 WCS QKD 的密钥生成效率高于 HSPS QKD; 而在交点之后, HSPS QKD 的密钥生成效率又高于 WCS QKD, 即两种光源在有效性上都不占绝对优势. 在稳定性方面, Wang 等 [18,19] 就一般的光源强度误差对诱骗态编码密钥生成效率的影响进行了研究, 但是此方法要求对量子态的一些参量进行监测. Wang 等 [20] 运用此分析方法对 HSPS 光源和 WCS 光源进行了分析, 结论表明强度涨落情况下, 前者比后者更稳定. 后来, Hu 和 Wang[21] 又提出了强度涨落条件下更严格的密钥生成效率计算公式, 且无需对光源参量进行监测. 在可行性方面, Alice 主动制备的诱骗态数量越多, 参数估计越精确, QKD 方案的性能就越好 (此类方案也被称为主动诱骗态方案). 但是诱骗态数目越多, 实验光源装置的改造就越复杂. 学者们便力图寻找实现尽可能简单的方案. 2007 年之后, 基于 HSPS 的被动诱骗态方案相继提出 [22,23], 即 Alice 不需要主动准备诱骗态, 信号态和诱骗态靠被动选择的方式来产生. 此类方案可在常规量子密钥分配系统上直接实现, 无需对硬件做任何改动, 实现非常简单. 随后, 文献 [24—26] 基于改造的 WCS 光源, 也提出了被动诱骗态方案.

Zhang 等 [27] 首次使用标记配对相干态 (HPCS) 光源进行诱骗态编码, 相比于 WCS 和 HSPS 光源, 在密钥生成效率和安全传输距离方面都有优势. 虽然现在还没有关于 HPCS QKD 实验的报道, 但 HPCS 完全有希望成为更优的 QKD 光源. 目前, 对于 HPCS QKD 性能的研究并不全面. 因此, 本文将从有效性、稳定性和可行性三方面出发, 对基于 HPCS 光源的诱骗态量子密钥分配性能进行了深入的分析. 有效性方面, 基于无条件安全的 Gottesman-Lo-Lütkenhaus-Preskill (GLLP)[28] 数据后处理方法, 采用四组实验数据对 HPCS QKD 三强度诱骗态方案的密钥生成效率、量子比特误码率和最优信号态强度与安全传输距离之间的关系进行了仿真和分析; 在稳定性方面, 采用文献 [21] 的分析方法, 对 HPCS 强度涨落和 QKD 方案性能变化之间的关系进行了仿真和分析; 在可行性方面, 对基于 HPCS 可设计出简单有效 QKD 方案的可行性进行了分析论证.

2 基于 HPCS 光源的诱骗态量子密钥分配

2.1 HPCS 光源

配对相干态 (PCS) 最初由 Agarwal 提出 [29]. 该光源的工作原理是: 共振双光子激发中四波混频和放大自发辐射之间的综合作用可以产生具有压缩和反聚束特性的辐射场, 其属于一种新型的相干态. 这种相干态是与两个模式中光子同时湮灭相应算符的本征态. 因此 PCS 产生的两个模式具有对称性, 且每个模式的光子数分布服从 sub-Poisson 分布.

$$\rho=\sum_{k=0}^{\infty}a_k|k\rangle\langle k|=\sum_{k=0}^{\infty}\frac{1}{\mathrm{I}_0(2x)}\frac{x^{2k}}{(k!)^2}|k\rangle\langle k|, \quad (1)$$

式中 $|k\rangle$ 为 k- 光子态; a_k 是光源产生 k- 光子态的概率; x 为一个模式的信号强度; $\mathrm{I}_0(\mathrm{X})$ 为修正的第一类 Bessel 函数.

所谓 HPCS 光源, 是指将 PCS 光源输出的模式之一进行编码, 作为信号模式发送给接收方 Bob, 而另外一个模式被发送方 Alice 端探测器检测来预报信号模式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. 本文只考虑 Alice 和 Bob 都采用门限探测器的情况.

2.2 信道模型

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

$$Y_k=1-(1-d_{\mathrm{B}})(1-\eta)^k, \quad (2)$$

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; $t_{\mathrm{AB}}=10^{-al/10}$, 其中 α (dB/km) 为光纤衰减系数; l (km) 为光纤传输距离.

Alice 发送 k- 光子态的误码率为

$$e_kY_k=e_dY_k+(e_0-e_d)d_{\mathrm{B}}, \quad (3)$$

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.

设 G_k 为 k- 光子态的全局计数率, 为 Alice 发送一个 k- 光子态且检测到的概率与 Y_k 的乘积:

$$G_k=Y_k[1-(1-\eta_{\mathrm{A}})^k+d_{\mathrm{A}}]\frac{1}{\mathrm{I}_0(2x)}\frac{x^{2k}}{(k!)^2}, \quad (4)$$

式中 $\eta_{\rm A}$ 为 Alice 端探测器的探测效率; $d_{\rm A}$ 为 Alice 端探测器的暗计数率.

设 Q_x 是信号强度为 x 的光子源的总计数率,

$$Q_x = \frac{Y_0 d_{\rm A}}{{\rm I}_0(2x)} + \sum_{k=1}^{\infty} G_k. \tag{5}$$

与上相同, 信号强度为 x 的光子源的量子比特误码率 (quantum bit error rate, QBER) 也可写为

$$E_x Q_x = \frac{Y_0 e_0 d_{\rm A}}{{\rm I}_0(2x)} + \sum_{k=1}^{\infty} G_k e_k. \tag{6}$$

3 有效性分析

目前, 比较成熟的数据后处理方法有 Lütkenhaus[30] 和 GLLP. 其中 Lütkenhaus 方法是为抵制个体攻击而提出的, 而 GLLP 方法面临任何攻击都可提供无条件安全性. 有研究表明: 采用两种方法所获得的 QKD 性能非常相近 [31]. 既然 QKD 所追求的是无条件安全性, 那本文性能分析时选取 GLLP 方法.

GLLP 方法的密钥生成效率为

$$\begin{aligned} R \geqslant \max(q\{&-Q_u f(E_u) H_2(E_u) \\ &+ G_1[1 - H_2(e_1)]\}, 0), \end{aligned} \tag{7}$$

式中 q 为量子密钥分配协议的筛选效率, BB84 协议的筛选效率为 1/2; $f(x)$ 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_u 和 E_u 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 下限和 e_1 的上限.

本文考虑三强度诱骗态方案, 发送者 Alice 采用三个光源, 分别为: 真空源 $S^{\rm v}$, 信号源 $S^{\rm s}$ 和诱骗源 $S^{\rm d}$, 分别随机发送强度为 0, v 和 u 的光子态, 其中 0 和 v 作为诱骗态, u 作为信号态. 设定若 Alice 端探测器响应, Bob 端探测器将对相应时间接收到的光子态进行测量; 反之, Bob 端探测器将放弃检测.

因为有真空态, 可精确估计 $Y_0 = d_{\rm B}$. 按照文献 [27] 中的思路可推出 Y_1 下限和 e_1 的上限.

$$\begin{aligned} Y_1 &\geqslant Y_1^L \\ &= \frac{{\rm I}_0(2v) Q_v - \dfrac{v^4}{u^4} {\rm I}_0(2u) Q_u - Y_0 d_{\rm A} \dfrac{u^4 - v^4}{u^4}}{(\eta_{\rm A} + d_{\rm A})\left(\dfrac{v^2 u^2 - v^4}{u^2}\right)}, \end{aligned} \tag{8}$$

$$e_1 \geqslant e_1^U = \frac{{\rm I}_0(2v) E_v Q_v - Y_0 d_{\rm A} e_0}{(\eta_{\rm A} + d_{\rm A}) Y_1 v^2}. \tag{9}$$

将以上估计所得的相关参数代入 (7) 式, 便可获得最终的安全密钥生成效率.

本文采用表 1 列出的 T8[32], G13[33], KTH[34] 和 GYS[35] 四组实验参数对上述方案进行数值模拟. 其他参数设置如下: $d_{\rm A} = 3.2 \times 10^{-7}$, $\eta_{\rm A} = 0.12$. 信号态 u 根据传输距离选取了最优信号强度.

表 1 量子密钥分配方案四组实验参数

	T8	G13	KTH	GYS
λ/nm	830	1300	1550	1550
α/dB·km^{-1}	2.5	0.32	0.2	0.21
e_d/%	1	0.14	1	3.3
Y_0/pulse	10^{-7}	0.64×10^{-4}	4×10^{-4}	1.7×10^{-6}
$\eta_{\rm B}$/%	7.92	8.14	14.30	4.5

从图 1 可以看出:

1) 在采用相同数量诱骗态, 即实现难度相同的条件下, 基于 HPCS 的诱骗态方案性能在安全传输距离和密钥生成效率两方面都优于基于 WCS 和 HSPS 光源的诱骗态方案;

2) 四组实验参数的仿真结果均显示, WCS QKD 和 HSPS QKD 的性能曲线都有一个交点, 这是因为 HSPS 具有双模态, 可采用光子数标记技术来降低系统暗计数的影响, 从而延长安全传输距离; 但是 HSPS 发出的多光子脉冲比例大于 WCS, 便导致了密钥生成效率上的差距; 因此, 如果系统想获得最优的传输性能, 就必须在交点距离之前采用 WCS 光源, 在交点距离之后切换成 HSPS 光源; 但在实际应用中, 经常性地切换光源并不是很容易实现的; 而 HPCS 光源在有效性上的绝对优势可避免这样的尴尬.

从图 2 中以看出, 在最大传输距离范围内, 基于三种光源诱骗态方案的 QBER 都低于安全门限值 11%. 其中, WCS QKD 的 QBER 最高, HPCS QKD 和 HSPS QKD 的 QBER 较低, 且非常的相近, 这主要是因为 HPCS QKD 和 HSPS QKD 可采用光子数标记技术消除暗计数的影响.

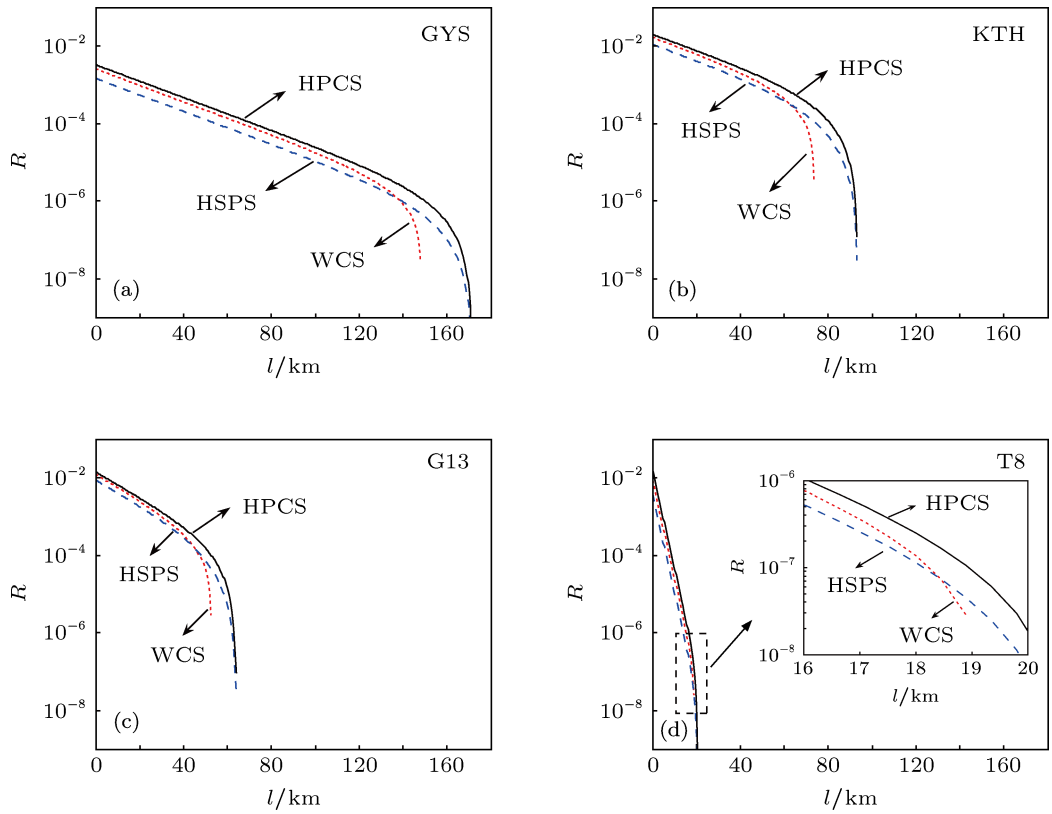

图 1 采用不同实验数据时基于不同光源三强度诱骗态方案的密钥生成效率随传输距离的变化

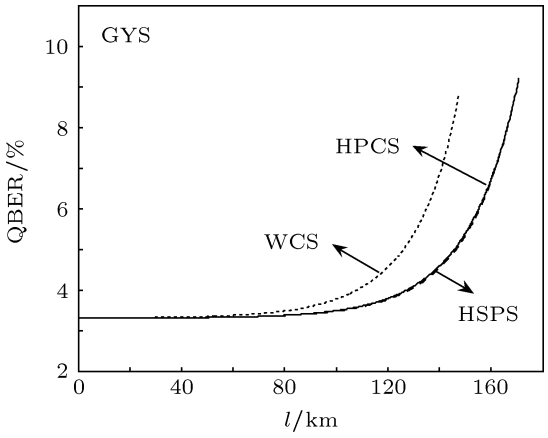

图 2 基于不同光源三强度诱骗态方案的 QBER 随传输距离的变化

图 3(a) 呈现的是在 GYS 实验参数条件下, 在每一点传输距离获得最大密钥生成效率而须选择的最优信号态强度 μ. 从图中可以看出, 三种光源中, HPCS 光源的最优信号态强度最接近于 1, 这也是 HPCS QKD 方案性能优越的主要原因. 图 3(b) 进一步说明了这一点: 最优信号态的选取原则之一是保证单光子态全局计数率 G_1 的最大化, 因为它是 BB84 协议密钥生成的惟一的有效来源; 原则之二是控制多光子态的全局计数率, 以保证 QKD 的安全性和有效性, 即使 G_1/Q_u 取到最大值. 从图 3(b) 中可以看出, HPCS QKD 的 G_1/Q_u 的比值最高, 而 HSPS QKD 和 WCS QKD 的 G_1/Q_u 曲线交点也正好是图 1 中性能曲线存在交点的原因. 可见 HPCS QKD 的有效性和安全性较 WCS QKD 和 HSPS QKD 都要优越.

4 稳定性分析

诱骗态方案成立的基本假设是发送者 Alice 能对光源输出的光子数进行完美的控制, 以保证下式的成立:

$$Y_k^{\rm d} = Y_k^{\rm s}, \quad e_k^{\rm d} = e_k^{\rm s}. \tag{10}$$

但在光源存在涨落的情况下, (10) 式便不再成立, QKD 的有效性和安全性也必定受到影响.

本文稳定性分析依然采用三强度诱骗态方案, 为了简化分析, 文中假定 $S^{\rm v}$ 所输出的量子态为精确的真空态, 但是 $S^{\rm s}$ 和 $S^{\rm d}$ 所输出的脉冲强度会在期望值左右有一定的涨落. 信号态和诱骗态可分别记为 $\rho_i^{\rm s} = \sum_{k=0}^{J} a_{ki}^{\rm s}|k\rangle\langle k|$, $\rho_i^{\rm d} = \sum_{k=0}^{J} a_{ki}^{\rm d}|k\rangle\langle k|$, 其中 a_{ki} 为光源在 i- 时刻产生 k- 光子态的概率, J 可以是有限值或是无限值.

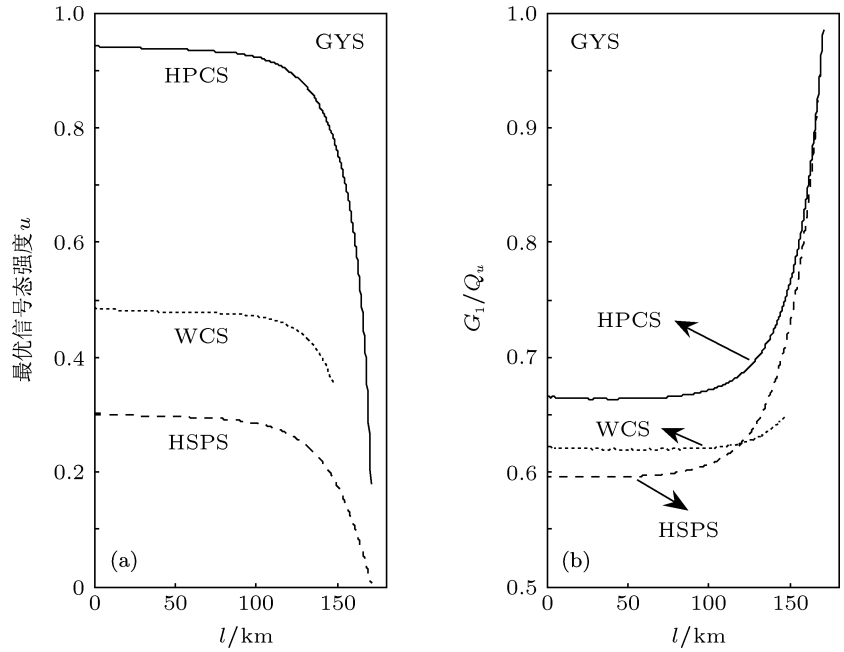

图 3 基于不同光源三强度诱骗态方案的最优信号强度和 G_1/Q_u 随传输距离的变化

假设 Alice 随机采用光源 $\{S^{\rm v}, S^{\rm s}, S^{\rm d}\}$的概率分别为 $p^{\rm v}$, $p^{\rm s}$, $p^{\rm d}$, 且 $p^{\rm v}+p^{\rm s}+p^{\rm d}=1$. 记 $\mathcal{P}^{\rm v}_{i|0}$, $\mathcal{P}^{\rm s}_{i|k}$, $\mathcal{P}^{\rm d}_{i|k}$ 为 i- 时刻产生的 k- 光子态是来源于真空源、信号源或诱骗源的概率, 可分别记为 $\mathcal{P}^{\rm v}_{i|0}=p^{\rm v}d_{ki}$, $\mathcal{P}^{\rm d}_{i|k}=p^{\rm d}a^{\rm d}_{ki}d_{ki}$ 和 $\mathcal{P}^{\rm s}_{i|k}=p^{\rm s}a^{\rm s}_{ki}d_{ki}$. 其中当 $k=0$ 时, $d_{ki}=1/(p^{\rm v}+p^{\rm d}a^{\rm d}_{ki}+p^{\rm s}a^{\rm s}_{ki})$, 当 $k>0$ 时, $d_{ki}=1/(p^{\rm d}a^{\rm d}_{ki}+p^{\rm s}a^{\rm s}_{ki})$.

设 Alice 向接收者 Bob 逐一发送 M 个脉冲, Bob 则要检测 M 次. 定义集合 $\Gamma=\{i|i=1,2,\cdots,M\}$ 包含所有发送的脉冲. 本文忽略第 i 个脉冲在发送后产生的变化. 我们记集合 C 包含所有引起计数的脉冲, 集合 c_k 包含引起计数的 k- 光子态脉冲. 显然, $C=c_0\cup c_1\cup\cdots\cup c_k\cdots\cup c_J$. k- 光子态脉冲引起的计数数目 n_k 就是集合 c_k 中的元素个数. 记 $n^{\rm s}_k$ 和 $n^{\rm d}_k$ 分别为 k- 信号态和 k- 诱骗态所产生的计数个数, 这些参数是无法在实验中直接观测到的. 另记 $N^{\rm v}$, $N^{\rm s}$ 和 $N^{\rm d}$ 分别为真空源、信号源和诱骗源引起的总的计数个数, 因此有 $N^{\rm s}=\sum_{k=0}^{J}n^{\rm s}_k$, $N^{\rm d}=\sum_{k=0}^{J}n^{\rm d}_k$. $N^{\rm v}$, $N^{\rm s}$ 和 $N^{\rm d}$ 可以在实验中直接观测得到. 现在需要在 (10) 式不成立的情况下, 推导出单光子信号态产生的计数个数 $n^{\rm s}_1$ 的下限和单光子信号态的误码率 $e^{\rm s}_1$ 的上限, 以此得到最终的密钥生成效率. 在此之前, 我们必须首先推导真空诱骗态和真空信号态产生的计数个数 $n^{\rm d}_0$ 和 $n^{\rm s}_0$ 的限值.

根据上述定义, 可得 $N^{\rm v}=\sum_{i\in c_0}\mathcal{P}^{\rm v}_{i|0}$, 且 $n^{\rm d}_0$ 可写为

$$n^{\rm d}_0=\sum_{i\in c_0}\mathcal{P}^{\rm d}_{i|0}=\sum_{i\in c_0}p^{\rm d}a^{\rm d}_{0i}d_{0i}=\sum_{i\in c_0}\frac{p^{\rm d}a^{\rm d}_{0i}}{p^{\rm v}}\cdot p^{\rm v}d_{0i}. \quad (11)$$

因此, 可得 $n^{\rm d}_0$ 的限值为

$$\min_{j\in c_0}\left(\frac{p^{\rm d}a^{\rm d}_{0j}}{p^{\rm v}}\right)N^{\rm v}=n^{\rm dL}_0\leqslant n^{\rm d}_0 \leqslant n^{\rm dU}_0=\max_{j\in c_0}\left(\frac{p^{\rm d}a^{\rm d}_{0j}}{p^{\rm v}}\right)N^{\rm v}. \quad (12)$$

采用同样的方法, 我们可以得到 $n^{\rm s}_0$ 的限值为

$$\min_{j\in c_0}\left(\frac{p^{\rm s}a^{\rm s}_{0j}}{p^{\rm v}}\right)N^{\rm v}=n^{\rm sL}_0\leqslant n^{\rm s}_0 \leqslant n^{\rm sU}_0=\max_{j\in c_0}\left(\frac{p^{\rm s}a^{\rm s}_{0j}}{p^{\rm v}}\right)N^{\rm v}. \quad (13)$$

下面将推导 $n^{\rm s}_1$ 的下限. 根据前面的定义有 $n^{\rm d}_k=\sum_{i\in c_k}\mathcal{P}^{\rm d}_{i|k}$, $n^{\rm s}_k=\sum_{i\in c_k}\mathcal{P}^{\rm s}_{i|k}$.

根据文献 [36] 对 HPCS 性质的刻画, 可得

$$\max_{j\in c_k}\left(\frac{p^{\rm d}a^{\rm d}_{kj}}{p^{\rm s}a^{\rm s}_{kj}}\right)\leqslant\max_{j\in c_2}\left(\frac{p^{\rm d}a^{\rm d}_{2j}}{p^{\rm s}a^{\rm s}_{2j}}\right) <\max_{j\in c_1}\left(\frac{p^{\rm d}a^{\rm d}_{1j}}{p^{\rm s}a^{\rm s}_{1j}}\right)\quad k\geqslant 2. \quad (14)$$

根据文献 [21] 的方法, 可得 $n_1^{\rm s}$ 的下限为

$$n_1^{\rm s} \geqslant n_1^{\rm sL} = \frac{1}{\max\limits_{j\in C}\left(\dfrac{p^{\rm d}a_{1j}^{\rm d}}{p^{\rm s}a_{1j}^{\rm s}}\right) - \max\limits_{j\in C}\left(\dfrac{p^{\rm d}a_{2j}^{\rm d}}{p^{\rm s}a_{2j}^{\rm s}}\right)} \times \left[N^{\rm d} - n_0^{\rm dU} - \max_{j\in C}\left(\frac{p^{\rm d}a_{2j}^{\rm d}}{p^{\rm s}a_{2j}^{\rm s}}\right)N^{\rm s} + \max_{j\in C}\left(\frac{p^{\rm d}a_{2j}^{\rm d}}{p^{\rm s}a_{2j}^{\rm s}}\right)n_0^{\rm sL}\right]. \tag{15}$$

即可得单光子信号态的计数率为: $Y_1^{\rm s} \geqslant Y_1^{\rm sL} = \dfrac{n_1^{\rm s}}{N^{\rm s}}$.

记 $N_e^{\rm s}$ 和 $N_e^{\rm d}$ 分别为信号脉冲和诱骗脉冲量子比特翻转的个数, 这两个参数都可通过错误检测得到. 则 $e_1^{\rm s}$ 的上限为

$$e_1^{\rm s} \leqslant e_1^{\rm sU} = \frac{\max\limits_{j\in C}\left(\dfrac{p^{\rm d}a_{1j}^{\rm d}}{p^{\rm s}a_{1j}^{\rm s}}\right)}{\min\limits_{j\in C}\left(\dfrac{p^{\rm d}a_{1j}^{\rm d}}{p^{\rm s}a_{1j}^{\rm s}}\right)} \cdot \frac{N_e^{\rm d} - n_0^{\rm d}2}{\min\limits_{j\in C}\left(\dfrac{p^{\rm d}a_{1j}^{\rm d}}{p^{\rm s}a_{1j}^{\rm s}}\right)Y_1^{\rm sL}}. \tag{16}$$

由于 HPCS 光源目前还没有在 QKD 实验中得到实际应用, 因此还不能获得 $Q^{\rm s}$, $Q^{\rm d}$, $E^{\rm s}$ 和 $E^{\rm d}$ 的实验观测数据, 因此本文用理论计算值来代替. 这部分数值仿真采用 GYS 实验数据. 设在任何发送信号的 i- 时刻, 实际信号脉冲的强度为 $u_i = u(1+\tau_i)$, τ 为信号强度涨落的上限值, 即 $|\tau_i| \leqslant \tau$. 仿真中 $\mu = 0.936$, $v = 0.2$.

在图 4 中, $R(\tau)$ 表示强度涨落为 τ 时的密钥生成效率, $R(0)$ 表示光源无强度涨落时的密钥生成效率. 图 4(a) 截取传输距离 30 km 点处三种光源 $R(\tau)/R(0)$ 的比值, 可见 $R(\tau)/R(0)$ 随着强度涨落参数 τ 的增大而下降, 即 QKD 性能随之降低. 其中, τ 增长对 QKD 性能影响最小的是 HSPS QKD, 即 HSPS QKD 的稳定性最好, HPCS QKD 的稳定性次之, WCS QKD 最差. 图 4(b) 显示在 τ 相同的条件下, 同样光源涨落对 WCS QKD 性能影响最大, HPCS QKD 次之, 对 HSPS QKD 的影响最小. 这说明 HPCS 光源对强度涨落的稳定性没有 HSPS 好, 但明显优于 WCS 光源.

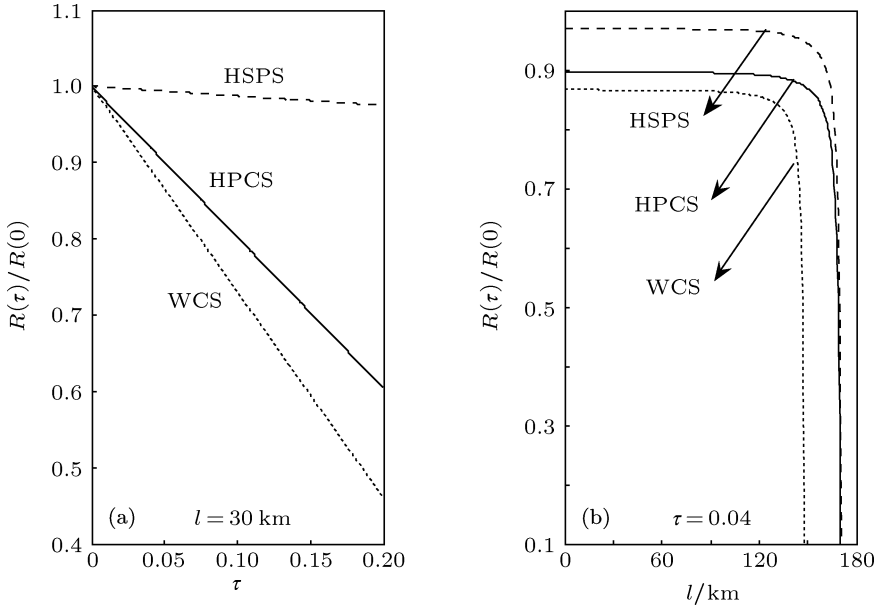

图 4 基于不同光源三强度诱骗态方案的 $R(\tau)/R(0)$ 随信号强度涨落上限 τ 和传输距离的变化

从图 5 中可以看出: 当 HPCS 光源的涨落 $\tau = 0.01$ 时, 其方案性能依然优于 WCS 和 HSPS 无强度涨落, 即 $\tau = 0$ 时的性能. 当 HPCS 光源的涨落 $\tau = 0.02$ 时, 其性能稍逊于无涨落的 WCS 和 HSPS, 但是差别不是很大. 虽然基于 HPCS 的 QKD 方案对于光强涨落的稳定性比 HSPS 稍差, 但是由于 HPCS QKD 的性能较其他两种光源 QKD 方案的性能优异, 一定程度上弥补了稳定性的不足.

5 可行性分析

被动诱骗态方案由于可在标准的 QKD 系统上直接实现, 无需对其光源装置进行改动, 且性能与理论极限的差距也较小, 而成为目前实现最容易、可行性最强的方案选择.

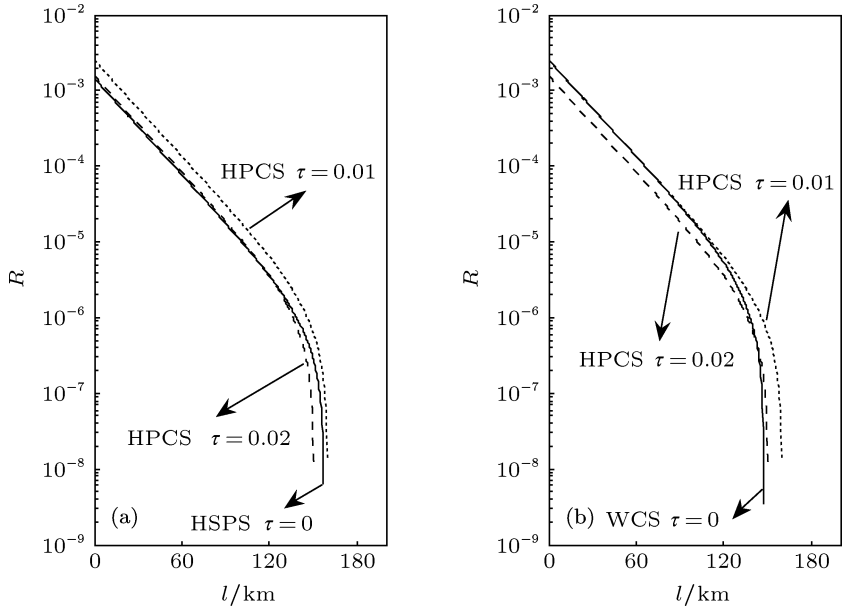

图 5 基于 HPCS 三强度诱骗态方案性能随信号强度涨落的变化

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. 与 HSPS 类似, HPCS 光源也能同时产生两个特性完全相同的模式, 具有实现被动诱骗态 QKD 的条件. 被动诱骗态方案的实施与以上的三强度诱骗态有三点不同: 第一, Alice 只需产生一个强度为 μ 的信号态; 第二, 无论 Alice 端探测器是否响应, Bob 端探测器都需对相应时间接收到的光子态进行测量; 第三, 根据 Alice 端探测器是否响应, 将 Bob 的探测结果分为两类, 即响应集合和未响应集合, 并分别作为信号态, 未响应集合用作诱骗态. 可见, 被动诱骗态相当于主动二强度诱骗态方案. 具体基于 HPCS 的被动诱骗态方案可参见本小组的研究成果 [37], 其仿真表明基于 HPCS 被动诱骗态的有效性依旧优于基于 HSPS 和 WCS 的被动诱骗态方案.

基于 WCS 也可实现被动诱骗态, 但需对光源进行改造 [24,25]: 采用两个 WCS 光源, 将其随机产生的量子态输入到分束器并发生干涉, 则输出的两路信号的光子数分布概率将具有相关性. 其改造行为在一定程度上抹杀了被动诱骗态实现简单的优势.

因此, 在实现的简易程度上, HPCS 和 HSPS 比较有优势, 但 HPCS 被动诱骗态方案的性能依旧优于基于 HSPS 和 WCS 的被动诱骗态方案 [37].

6 结 论

本文从有效性、稳定性和可行性三方面出发, 对基于 HPCS 光源诱骗态量子密钥分配的性能进行了全面深入的分析. 得出如下结论: 有效性方面, 基于 HPCS 的诱骗态方案性能在安全传输距离和密钥生成效率两方面都优于基于 WCS 和 HSPS 光源的诱骗态方案; 在稳定性方面, HPCS 光源稍逊于 HSPS 光源, 而优于 WCS 光源, 但是 HPCS 有效性上的优势可在一定程度上弥补其在稳定性上的不足; 在可行性方面, 基于 HPCS 可设计实现简单的被动诱骗态方案, 且其有效性依旧优于基于 HSPS 和 WCS 的被动诱骗态方案. 因此, HPCS 是一种非常适合诱骗态量子密钥分配实验的光源.

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

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

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

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

[5] Ma X F, Qi B, Zhao Y, Lo H K 2005 *Phys. Rev.* A **72** 012326

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

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

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

044304

[9] 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]

[10] 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]

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

[12] 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]

[13] Zhou Y Y, Zhou X J, Tian P G, Wang Y J 2013 *Chin. Phys.* B **22** 010305

[14] Zhao Y, Qi B, Ma X F, Lo H K, Qian L 2006 *Phys. Rev. Lett.* **96** 070502

[15] Tobias S M, Henning W, Martin F, Rupert U, Felix T, Thomas S, Josep P, Zoran S, Christian K, John G R, Anton Z, Harald W 2007 *Phys. Rev. Lett.* **98** 010504

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

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

[18] Wang X B 2007 *Phys. Rev.* A **75** 052301

[19] Wang X B, Peng C Z, Zhang J, Yang L, Pan J W 2008 *Phys. Rev.* A **77** 042311

[20] Wang S, Zhang S L, Li H W, Yin Z Q, Zhao Y B, Chen W, Han Z F, Guo G C 2009 *Phys. Rev.* A **79** 062309

[21] Hu J Z, Wang X B 2010 *Phys. Rev.* A **82** 012331

[22] Mauerer W, Silberhorn C 2007 *Phys. Rev.* A **75** 050305

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

[24] Curty M, Moroder T, Ma X F, Lütkenhaus N 2009 *Opt. Lett.* **34** 3238

[25] Curty M, Ma X F, Qi B, Moroder T 2010 *Phys. Rev.* A **81** 022310

[26] Zhou Y Y, Zhou X J 2011 *Acta Phys. Sin.* **60** 100301 (in Chinese) [周媛媛, 周学军 2011 物理学报 **60** 100301]

[27] Zhang S L, Zou X B, Li C F, Jin C H, Guo G C 2009 *Chin. Sci. Bull.* **54** 1863

[28] Gottesman D, Lo H K, Lütkenhaus N, Preskill J 2004 *Quantum Inf. Comput.* **4** 325

[29] Agarwal G S 1986 *Phys. Rev. Lett.* **57** 827

[30] Lütkenhaus N 2000 *Phys. Rev.* A **61** 052304

[31] Ma X F 2006 *Phys. Rev.* A **74** 052325

[32] Townsend P D 1998 *IEEE Photonics Technol. Lett.* **10** 1048

[33] Ribordy G, Gautier J D, Gisin N, Guinnard O, Zbinden H 1998 *Electron. Lett.* **34** 2116

[34] Bourennane M, Gibson F, Karlsson A, Hening A, Jonsson P, Tsegaye T, Ljunggren D, Sundberg E1999 *Opt. Express* **4** 383

[35] Gobby C, Yuan Z L, Shields A J 2004 *Appl. Phys. Lett.* **84** 3762

[36] Zhou C, Bao W S, Fu X Q 2011 *Sci. China* **41** 1136

[37] Zhang H Q, Zhou Y Y, Zhou X J, Tian P G 2013 *Optoelectron. Lett.* **9** 389

Performance analysis of decoy-state quantum key distribution with a heralded pair coherent state photon source*

Zhou Yuan-Yuan[1)†] Zhang He-Qing[2)] Zhou Xue-Jun[1)] Tian Pei-Gen[1)]

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

2) (*School of Electronic and Information Engineering, Beihang University, Beijing* 100191*, China*)

(Received 30 May 2013; revised manuscript received 27 June 2013)

Abstract

A comprehensive analysis is made on the performance of decoy-state quantum key distribution with a heralded pair coherent state photon source from the effectiveness, stability and feasibility. The key generation rate, quantum bit error rate, and optimal signal intensity each as a function of secure transmission distance are simulated and analyzed by the three-intensity decoy-state method based on a heralded pair coherent state photon source with four groups of experimental data. Considering the intensity fluctuation, the stability of this method is simulated and discussed. Furthermore, the feasibility of the simple and easy method that is proposed with a heralded pair coherent state photon source is analyzed. The simulation results show that the key generation rate and secure transmission distance obtained from the decoy-state method with a heralded pair coherent state photon source are better than those obtained from the methods with a weak coherent state source and heralded single photon source. With the same intensity fluctuation, the heralded pair coherent state photon source is less stable than the heralded single photon source, but more robust than the weak coherent state source. However, the advantage in the effectiveness of the heralded single photon source can give rise to the shortage of the stability. Moreover, the two same modes of the heralded single photon source provide the feasibility to design a simple and easy passive decoy-state method.

Keywords: quantum optics, quantum key distribution, heralded pair coherent state photon source, performance

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.62.200302

* Project supported by the National High Technology Research and Development Program of China (Grant No. 2011AA7014061).

† Corresponding author. E-mail: zyy_hjgc@aliyun.com