基于不可信光源的量子密钥分配的统计特性研究*

焦荣珍† 丁天 王文集 马海强

(北京邮电大学理学院, 北京 100876)

(2013年3月10日收到; 2013年5月31日收到修改稿)

通过比较被动系统与主动系统的特性, 得出可信光源、不可信光源主动系统和不可信光源被动系统的密钥生成率随距离的变化关系; 采用标准误差分析法, 得到相应变量的偏离量; 基于诱骗态方案分析不可信光源被动系统暗计数率和光源强度参数波动对系统安全特性的影响, 得出在 1310 nm 和 1550 nm 通信窗口下, 系统最大安全通信距离范围分别为 [73.2 km, 96.5 km] 和 [104.5 km, 137.9 km]. 这可为实用量子通信实验提供重要的理论参数.

关键词: 量子密钥分配, 不可信光源, 被动系统, 统计波动

PACS: 03.67.Dd **DOI:** 10.7498/aps.62.180302

1 引 言

量子密钥分配 (QKD) 结合 "一次便签" 式加密方法, 让通信双方 (Alice 和 Bob) 共享一个无条件安全密钥. 自 BB84 协议 [1] 提出以来, QKD 理论迅速发展, 国内外学者完成相关理论的验证工作 [2−9]. 在实用化的量子密钥分配实验中, 一般采用弱相干光源, 这将无法避免窃听者 (Eve) 的分光束攻击 (PNS), QKD 的安全传输距离及密钥生成率会受到极大限制, 为解决 PNS 攻击, Hwang[10] 提出诱骗态方案. 然而对于实际的商用 QKD 系统, 由于其双向传输的特性, 导致 Eve 很容易控制该系统的光源, 此光源被称为不可信光源, 研究人员对其安全性已进行了研究 [11−13], 针对高速量子随机数生成器目前还未实现, 会导致系统主动抽样的过程难于实现的问题, 本文采用被动分束装置代替主动光开关装置, 针对两个通信窗口 (1550 nm 和 1310 nm) 在理论上改变不可信光源系统的装置, 并在此基础上研究了系统光源强度波动和暗计数率的统计波动对安全性的影响, 得到实验所允许出现的最大安全通信距离的范围, 这将为相关实验提供重要的理论依据.

2 理论与计算公式

在实用量子密钥分配实验中, 诱骗态方案是引入一组仅在强度上与信号源不同的光源作为诱骗光源, 通过测定两光源的增益和误码率, 得出系统密钥生成率随距离的变化关系. 在真空 + 弱相干诱骗态方案中, 设信号源的平均光子数为 μ, 诱骗源的平均光子数为 ν_1, ν_2, 信号光源的 n 光子脉冲的计数率和误码率分别为 Y_n 和 e_n, n 光子脉冲的误码率为

$$e_n = \frac{e_0 Y_0 + e_d \eta_n}{Y_n}, \tag{1}$$

n 光子脉冲的增益为

$$Q_n = P_n(\mu) Y_n = \frac{\mu^n}{n!} \mathrm{e}^{-\mu} Y_n. \tag{2}$$

对于诱骗态光源, 其增益和误码率为

$$\begin{aligned} Q_d &= \sum_{n=0}^{\infty} P_n(\nu) Y_n, \\ Q_d E_d &= \sum_{n=0}^{\infty} P_n(\nu) Y_n e_n. \end{aligned} \tag{3}$$

设光源光强的波动参数为 δ, 脉冲光子数在 $[(1-\delta)N, (1+\delta)N]$ 的脉冲为单光子脉冲, 其增益

* 国家重点基础研究计划 (批准号: 2010CB923202) 资助的课题.

† 通讯作者. E-mail: rzjiao@bupt.edu.cn

Q 和误码率 QE 的上下界分别为

$$\overline{Q}=\frac{Q_e}{1-\Delta-\varepsilon},$$
$$\underline{Q}=\max\left(0,\frac{Q_e-\Delta-\varepsilon}{1-\Delta-\varepsilon}\right),$$
$$\overline{QE}=\frac{Q_eE_e}{1-\Delta-\varepsilon},$$
$$\underline{QE}=\max\left(0,\frac{Q_eE_e-\Delta-\varepsilon}{1-\Delta-\varepsilon}\right),$$

其中,

$$\Delta=1-erf\left(\sqrt{\frac{N}{2}}\delta\right). \tag{4}$$

公式中其他参数的取值参见文献 [13], 在满足条件

$$\frac{\lambda_s}{\lambda_d}>\frac{(1+\delta)N-2}{(1-\delta)N-2}\left(\frac{(1+\delta)N-2}{2\delta N}\right)^{\frac{2\delta N}{[(1-\delta)N-2]}}\times\left(\frac{(1+\delta)N-2}{(1-\delta)N-2}\frac{e^2}{2\delta N}\right)^{\frac{1}{2[(1-\delta)N-2]}} \tag{5}$$

时, 单光子脉冲增益下限和误码率上限可表示为

$$Q_1^{L,v,0}=\frac{\underline{P_1^S}}{\overline{P}_1^D\underline{P_2^S}-\underline{P_1^S}\overline{P}_2^D}\left[\underline{Q^DP_2^S}-\overline{Q^SP_2^D}+\left(\underline{P_0^S}\overline{P}_2^D-\overline{P}_0^D\underline{P_2^S}\right)\overline{Q}^V-\frac{2\delta N(1-\lambda_{\rm D})^{2\delta N-1}\underline{P_2^S}}{[(1-\delta)N+1]!}\right],$$
$$e_1^S\leqslant\overline{e_1^S}=\frac{\overline{E^SQ^S}-\underline{P_0^S}E^VQ^V}{\underline{Q_1^S}}. \tag{6}$$

不可信光源系统的密钥生成率下限为

$$R\geqslant\frac{1}{2}\left\{-Q_sf(E_s)H_2(E_s)+Q_1^{L,v,0}\left[1-H_2\left(e_1^{U,v,0}\right)\right]\right\}. \tag{7}$$

对于不可信光源, 在速度高达 10 GHz 的 QKD 系统, 该系统的光开关的时域控制很难实现, 系统脉冲抽样过程中所需的高速量子随机数生成器 (QRNG) 还未实现, 且理想的脉冲强度检测器并不存在. 鉴于以上原因, 本文采用分束器代替光开关, 其分束参数为 q, 改进后的装置不需要主动施加时域控制系统和 QRNG, 同时分束器也不改变脉冲的数目, 此装置我们称之为被动系统. 本文采用的实用不可信光源下的被动测量系统示意图如图 1 所示.

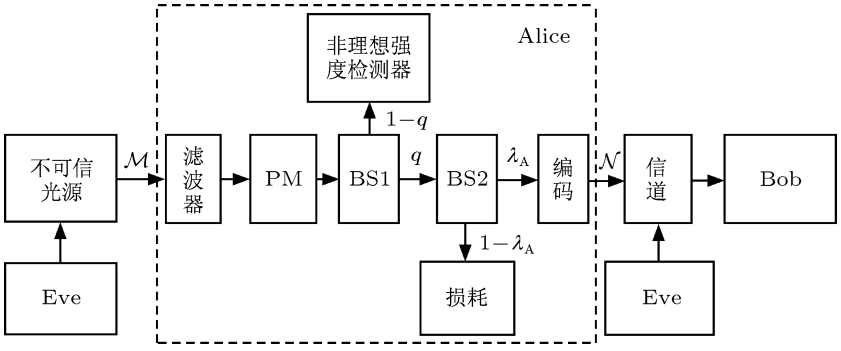

图 1 实用不可信光源下的被动测量系统结构示意图

3 结果与讨论

本文基于图 1 所示的不可信光源下的被动测量系统, 采用真空 + 弱相干态方案, 根据 (1)–(6) 式计算出单光子脉冲增益下限和误码率上限, 由 (7) 式得出系统的密钥生成率随距离的变化关系, 如图 2 所示. 在计算过程中设 $N=10^{12}$, 并采用文献 [13] 的实验参数, 令 $q=0.01$, $\omega=0.015$, 设系统最大安全通信距离为 l, 在 1550 nm 窗口, 不可信光源被动系统下 $l=130.5$ km, 这比主动系统的最大安全通信距离高 4.3 km, 比可信光源系统低 18.4 km; 在 1310 nm 窗口, 不可信光源被动系统下 $l=74.1$ km, 这比主动系统最大安全通信距离高 2.4 km, 比可信光源系统低 10.4 km. 可见, 被动系统的安全特性较主动系统有优势

本文针对不可信光源被动系统, 考虑系统暗计数率波动对系统的影响, 如图 3 所示. 在计算过程中设其波动参数为 ΔY_0, 分别令 $\Delta Y_0=\Delta Y_0=-0.3$, $\Delta Y_0=-0.1$, $\Delta Y_0=0.1$, $\Delta Y_0=0.3$. 如在 1550 nm 通信窗口下, 当 $\Delta Y_0=0.3$ 时, $l=124.4$ km; 而在 1310 nm 通信窗口下, 当 $\Delta Y_0=0.3$ 时, $l=70.6$ km. 在图 4 中比较了光源强度波动对系统性能的影响.

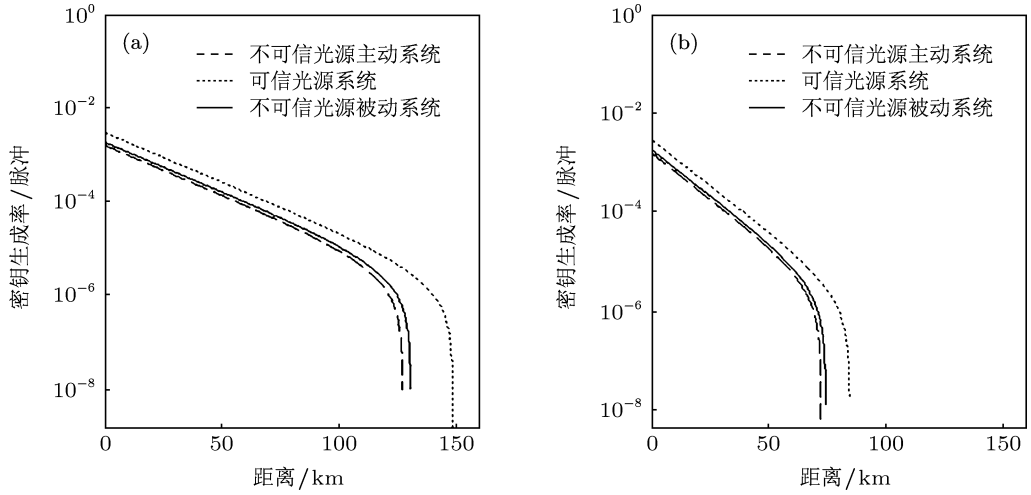

图 2 可信光源、不可信光源主动系统和不可信光源被动系统在 1550 nm 和 1310 nm 通信窗口的性能比较 (a) 1550 nm 窗口; (b) 1310 nm 窗口

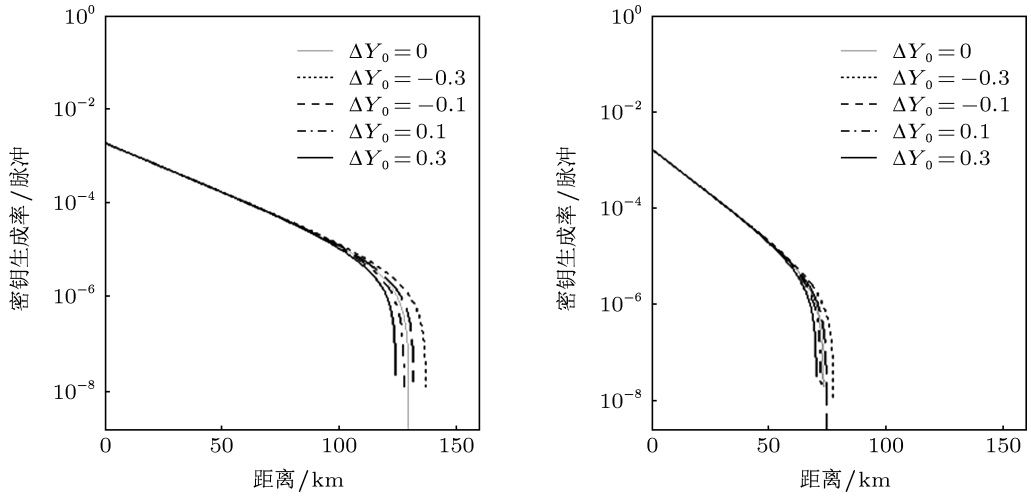

图 3 在 1550 nm 和 1310 nm 通信窗口下参数 Y_0 统计波动对系统性能的影响

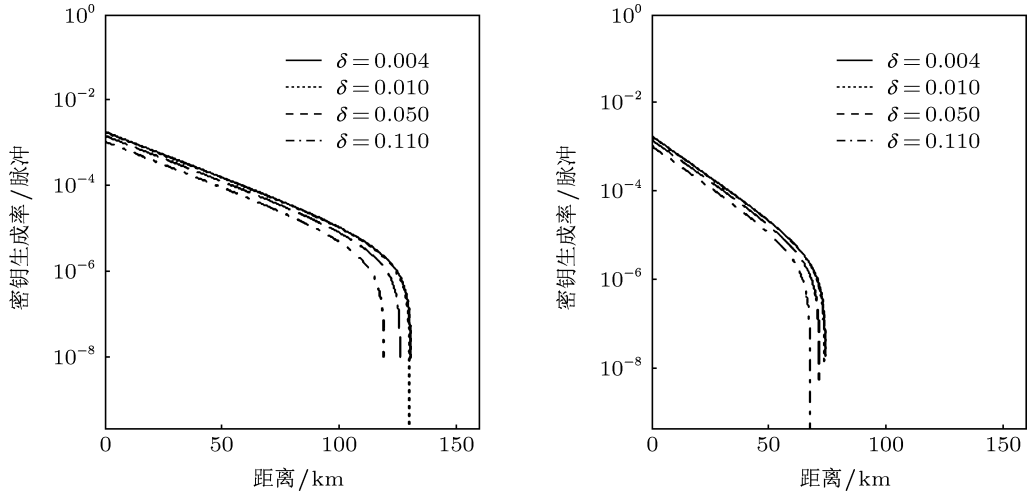

图 4 在 1550 nm 和 1310 nm 通信窗口下参数 δ 统计波动对系统性能的影响

根据以上比较, 得出在合理波动的情况下, 即采取措施将暗计数率波动 ΔY_0 的范围控制在 $(-0.1, 0.1)$ 之间, 将光源强度波动 δ 的范围控制在 $(0.004, 0.05)$ 之间, 可得到实验所允许出现的最大安全通信距离的范围, 即在考虑系统参数波动的情况下, 在 1550 nm 通信窗口下, 系统最大安全通信距离 l 的范围是 [104.5 km, 137.9 km], 在 1310 nm 窗口下, 系统最大安全通信距离 l 的范围是 [73.2 km, 96.5 km], 这将为相关量子通信实验提供重要的理论依据.

[1] Bennett C H, Brassard G 1984 *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing* (Bangalore, New York: IEEE)

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

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

[4] Mao 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]

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

[6] Wang J D, Wei Z J, Zhang H, Zhang H N, Chen S, Qin X J, Guo J P, Liao C J, Liu S H 2010 *Acta Phys. Sin.* **59** 5514 (in Chinese) [王金东, 魏正军, 张辉, 张华妮, 陈帅, 秦晓娟, 郭健平, 廖常俊, 刘颂豪 2010 物理学报 **59** 5514]

[7] Muller A, Herzog T, Hutter B, Tittel W 1996 *Appl. Phys. Lett.* **70** 07793

[8] Zhao Y Qi B, Lo H K 2008 *Phys. Rev.* A **77** 052327

[9] Zhu C H, Pei C X, Quan D X, Gao J L, Chen N, Yi Y H 2010 *Chin. Phys. Lett.* **27** 090301

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

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

[12] Peng X, Jiang H, Xu B J, Ma X F, Guo H 2008 *Opt. Lett.* **33** 2077

[13] Zhao Y, Qi B, Lo H K, Qian L 2010 *New. J. Phys.* **12** 023024

Analysis statistical fluctuation of passive untrusted source for quantum key distribution system*

Jiao Rong-Zhen† Ding Tian Wang Wen-Ji Ma Hai-Qiang

(*Science School, Beijing University of Post and Telecommunication, Beijing* 100876*, China*)

(Received 10 March 2013; revised manuscript received 31 May 2013)

Abstract

The performance of active decoy-state quantum key distribution (QKD) system with an untrusted source is compared with that of passive decoy-state QKD. The key generation rate with the change of the secure transmission distance is shown under the condition of active decoy-state (or passive decoy-state) QKD where we pick the data size to be $N = 10^{12}$. The security characteristics of the passive scheme are studied with statistical fluctuation of the counting rate and the intensity of the practical source. At communication wavelength 1310 nm or 1550 nm, The security range of communication distance is [73.2 km, 96.5 km] or [104.5 km, 137.9 km] respectively. This analysis will provide important theoretical parameters for practical QKD experiment.

Keywords: quantum key distribution, untrusted source, passive scheme, statistical fluctuation

PACS: 03.67.Dd **DOI:** 10.7498/aps.62.180302

* Project supported by National Basic Research Program of China (Grant No. 2010CB923202).

† Corresponding author. E-mail: rzjiao@bupt.edu.cn