基于实用光源的诱惑态量子密钥分配研究*

焦荣珍† 张 弼 马海强

(北京邮电大学理学院,北京 100876)

(2011 年 1 月 17 日收到;2011 年 2 月 24 日收到修改稿)

文章通过比较主动诱惑态和被动诱惑态的特性,假设所有可测量都围绕渐近值上下波动,得到相应变量的偏离量,采用标准误差法分析实用光源条件下,有限脉冲数编码对密钥生成率和传输距离的影响,比较了主动诱惑态、被动诱惑态 、无限长时间极限情况和不同量子效率条件下密钥生成率随传输距离的变化关系,为实用的量子密钥分配实验提供了重要的理论参数.

关键词: 诱惑态, 量子密钥分配, 统计涨落

PACS: 03.67.Dd, 03.67.Hk

1. 引 言

量子密钥分配(QKD)能让通信双方(Alice 和 Bob)共享一个无条件安全密钥,从 1984 年 BB84 协议[1]的提出到现在,量子密钥的理论已基本成熟. 当前,研究低误码率和长距离安全的 QKD 系统成为量子保密通信走向实用化的关键. 实验上 QKD 有两类,一类通过光纤传输[2—5],另一类通过自由空间传输[6,7]. 由于探测效率和光纤损耗的限制,量子密钥通过光纤的分发距离受到很大限制;光子数分束攻击(PNS)也限制了通信双方在实用单光子源条件下 QKD 的传输距离和密钥生成率,而诱惑态协议[8—10]的提出很大程度上解决了这一难题. 然而,在实际通信过程中,通信双方只能交换有限信号脉冲,统计涨落将会对密钥生成率和最大安全传输距离产生影响. 在诱惑态 QKD 研究过程中,虽有研究人员对系统的统计涨落情况进行了分析[11—13],但这些分析只是在 GLLP 公式上简单的修正,没在理论方法上对统计涨落作系统分析. 本文将借助数学工具——标准误差分析法对主动诱惑态和被动诱惑态协议中单光子的计数率、单光子增益和误码率分别进行统计涨落分析,推导出密钥生成率的下限,得出测量样本有限长和无穷长时测量值与真实值之间的误差,分析不同量子效率条件下量子密钥生成率随距离变化的关系,通过比较主动诱惑态和被动诱惑态方案中统计涨落对量子密钥分配实验系统中参数的影响,进而分析统计涨落对成码率的影响.

2. 理论与计算公式

在基于光纤的 QKD 系统中,通信双方的传输系数 t_{AB} 可由下式表示:

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

其中 α 为损耗系数 (单位 dB/km), l 为光纤长度.

i 光子态的计数率、增益和误码率分别为 Y_i, Q_i 和 e_i, 为了比较主动诱惑态和被动诱惑态设置中统计涨落对量子密钥分配系统的影响,考虑单诱惑态方案[12], μ 为信号态, ν 为诱惑态,单光子的计数率 Y_1 下限为

$$Y_1 \geqslant Y_1^{L,\nu_1,\nu_2} = \frac{\mu}{\mu\nu_1 - \mu\nu_2 - \nu_1^2 + \nu_2^2} \times \left(Q_{\nu_1} e^{\nu_1} - Q_{\nu_2} e^{\nu_2} \frac{\nu_1^2 - \nu_2^2}{\mu^2} (Q_\mu e^\mu - Y_0^L) \right), \quad (1)$$

采用标准误差分析,增益 Q_μ, Q_ν, 误码率 E_μ, E_ν 的统计涨落由下式表示:

$$\Delta Q_\mu = u_\alpha \sqrt{Q_\mu / N_\mu},$$

$$\Delta Q_\nu = u_\alpha \sqrt{Q_\nu / N_\nu},$$

* 国家重点基础研究发展计划(批准号:2010CB923202)和中央高校基本科研业务费(批准号:BUPT2009RC0709)资助的课题.

† E-mail: jiao218@sohu.com

$$\Delta Q_\mu E_\mu = u_\alpha \sqrt{2E_\mu Q_\mu / N_\mu},$$
$$\Delta Q_\nu E_\nu = u_\alpha \sqrt{2E_\nu Q_\nu / N_\nu}, \quad (2)$$

这里 $N_\mu(N_\nu)$ 表示 Alice 发出的信号(弱诱惑态)脉冲的数量, u_α 代表偏离中心值的标准差,光源发出的总脉冲数量为 $N = N_\mu + N_\nu$. 信号态的增益在区间 $Q_\mu \pm \Delta Q_\mu$ 内,其他参数 $Q_\nu, Q_\mu E_\mu, Q_\nu E_\nu$ 也类似. 单光子误码率上限 e_1^{U} 的表达式为

$$e_1 \leqslant \frac{B}{Y_1^{\mathrm{L}}}, \quad (3)$$

其中 B 由下式给出:

$$B = \min\left\{\frac{E_\nu Q_\nu e^\nu}{\nu}, \frac{E_\mu Q_\mu e^\mu - E_\nu Q_\nu e^\nu}{\mu - \nu}\right\}. \quad (4)$$

由(1)和(3)式可得

$$Y_1[1 - H(e_1)] \geqslant \frac{A}{1 - 2e_1}\left[1 - H\left(\frac{B(1 - 2e_1)}{A}\right)\right]. \quad (5)$$

式中 A 和 B 的值可直接测量得到. Y_1^{L} 和 e_1^{U} 可以由 A 和 B 表示如下:

$$Y_1^{\mathrm{L}} = A + 2B,$$
$$e_1^{\mathrm{U}} = \frac{B}{A + 2B}, \quad (6)$$

根据标准误差分析过程可得参数 A 和 B 偏离理论值的量为

$$\Delta A = [(c_1\Delta Q_\nu)^2 + 4(c_1\Delta E_\nu Q_\nu)^2 + (c_2\Delta Q_\mu)^2 + 4(c_2\Delta E_\mu Q_\mu)^2]^{\frac{1}{2}},$$
$$\Delta B = \min\left\{\frac{e^\mu \Delta E_\mu Q_\mu}{\mu}, \frac{e^\nu \Delta E_\nu Q_\nu}{\nu}, \frac{\sqrt{(e^\mu \Delta E_\mu Q_\mu)^2 + (e^\nu \Delta E_\nu Q_\nu)^2}}{\mu - \nu}\right\}, \quad (7)$$

式中 c_1 和 c_2 分别为

$$c_1 = \frac{\mu e^\nu}{\nu(\mu - \nu)},$$
$$c_2 = \frac{\nu e^\mu}{\mu(\mu - \nu)}.$$

密钥公式中 $Y_1[1 - H(e_1)]$ 的统计偏差可以写成

$$\Delta Y_1[1 - H(e_1)] = \left\{\left[\Delta A \log_2\left(\frac{2A + 2B}{A + 2B}\right)\right]^2 + \left[\Delta B \log_2\left(\frac{4B(A + B)}{(A + 2B)^2}\right)\right]^2\right\}^{\frac{1}{2}}. \quad (8)$$

综合(1),(6)和(8)式,可得主动诱惑态存在统计涨落情况下的密钥生成率下限公式为

$$R^{\mathrm{L}} \geqslant q\{-Q^{\mathrm{L}} f(E^{\mathrm{L}}) H(E^{\mathrm{L}}) + (p_1^l Y_1^{\mathrm{L}} + p_0^l Y_0)[1 - H(e_1^{\mathrm{U}})]\}. \quad (9)$$

对于被动诱惑态,其装置图如图 1 所示:假设两个 Fock 对角态分别为 ρ 和 σ, 分光镜(BS)的透射率为 t;a 和 b 代表两个输出模式.

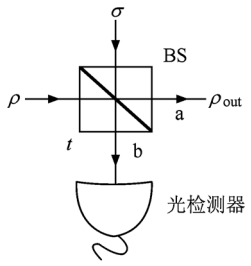

图 1 被动诱惑态 QKD 装置

模式 a 中找到 n 光子的总概率为

$$p_n^t = \frac{1}{1 + \mu t}\left(\frac{\mu t}{1 + \mu t}\right)^n.$$

定义 $p_n^{\bar{c}}$ 为模式 a 中的 n 光子态在阈值探测器中没有产生计数的联合概率,其表达式为

$$p_n^{\bar{c}} = \frac{1 - \varepsilon}{r}\left(\frac{\mu t}{r}\right)^n.$$

式中参数 $r = 1 + \mu[t + (1 - t)\eta_{\mathrm{d}}]$, 则 n 光子在探测器中产生计数的联合概率可以表示成 $p_n^c = p_n^t - p_n^{\bar{c}}$.

模式 a 输出信号的光子数统计依赖于阈值探测器的计数率和误码率,则有

$$N_{\mathrm{th}} = \sum_{n=0}^{\infty} p_n^{\bar{c}} = \frac{1 - \varepsilon}{1 + \mu\eta_{\mathrm{d}}(1 - t)}. \quad (10)$$

同理参数 $Q^{\bar{c}}, E^{\bar{c}}, Q^t$ 和 E^t 分别可以表示为

$$Q^{\bar{c}} = N_{\mathrm{th}} - \frac{(1 - \varepsilon)(1 - Y_0)}{r - (1 - \eta)\mu t},$$
$$Q^{\bar{c}}E^{\bar{c}} = (e_0 - e_{\mathrm{d}})Y_0 N_{\mathrm{th}} + e_{\mathrm{d}}Q^{\bar{c}},$$
$$Q^t = \frac{Y_0 + \mu t\eta}{1 + \mu t\eta},$$
$$Q^t E^t = (e_0 - e_{\mathrm{d}})Y_0 + e_{\mathrm{d}}Q^t,$$

其中 $Q^c = Q^t - Q^{\bar{c}}, Q^c E^c = Q^t E^t - Q^{\bar{c}}E^{\bar{c}}$.

与主动诱惑态 QKD 相似. 参数 A 和 B 的表达式可以表示为

$$A = \frac{p_2^{\bar{c}}Q^t(1 - 2E^t) - p_2^t Q^{\bar{c}}(1 - 2E^{\bar{c}})}{p_2^{\bar{c}}p_1^t - p_2^t p_1^{\bar{c}}},$$
$$B = \min\left\{\frac{E^{\bar{c}}Q^{\bar{c}}}{p_1^{\bar{c}}}, \frac{p_0^{\bar{c}}E^tQ^t - p_0^t E^{\bar{c}}Q^{\bar{c}}}{p_0^{\bar{c}}p_1^t - p_0^t p_1^{\bar{c}}}\right\}, \quad (11)$$

参数 A 和 B 的偏离量的形式为

$$\Delta A = \frac{1}{p_2^c p_1^t - p_2^t p_1^c}\left[(p_2^c \Delta Q^t)^2 + 4(p_2^c \Delta E^t Q^t)^2 + (p_2^t \Delta Q^c)^2 + 4(p_2^t \Delta E^c Q^c)\right]^{\frac{1}{2}},$$

$$\Delta B = \min\left\{\frac{\Delta E^t Q^t}{p_1^t}, \frac{\Delta E^c Q^c}{p_1^c}\right\}, \quad (12)$$

$Y_1[1 - H(e_1)]$ 的偏离量的表示同(8)式. 其他参量的表示参见文献[14].

3. 计算结果与讨论

根据(6)式可以计算出单光子计数率的下限 Y_1^{L} 和单光子误码率上限 e_1^{U}, 然后根据密钥生成率公式可得出最终的成码率与传输距离之间的关系见图2. 在计算过程中假定 Alice 端发射的总脉冲个数为 $N = 6.0 \times 10^9$, 诱惑态和信号态的光强分别为0.01和0.48. 图2中也包含不考虑统计涨落的密钥率情形(粗实线),密钥率降到零的传输距离为 $l = 110.5$ km(考虑统计涨落的主动诱惑态 QKD 装置)和 $l = 141$ km(不考虑统计涨落的主动诱惑态 QKD 装置). 此结果可得出主动诱惑态 QKD 装置有利于对抗统计涨落的影响.

在被动诱惑态 QKD 装置的模拟计算中,假设分光镜(BS)的透射率 $t = 1/2$, $\varepsilon = 0$. 光源发出的光脉冲总数同样选择为 $N = 6.0 \times 10^9$, 根据 Alice 端探测器的效率考虑 $\eta_{\mathrm{d}} = 1$ 和 $\eta_{\mathrm{d}} = 0.4$ 两种情况:其中 $\eta_{\mathrm{d}} = 1$ 为细实线,而 $\eta_{\mathrm{d}} = 0.4$ 为虚线部分. 诱惑态和信号态的光强也是 0.01 和 0.48,图2中还考虑了 $\eta_{\mathrm{d}} = 1$ 且不考虑统计涨落的情况(点线). 密钥率降到零时的传输距离分别为 $l \approx 50$ km(考虑统计涨落的被动 QKD 装置, $\eta_{\mathrm{d}} = 0.4$); $l \approx 80$ km(考虑统计涨落的被动 QKD 装置, $\eta_{\mathrm{d}} = 1$); $l \approx 120.5$ km(不考虑统计涨落的被动 QKD 装置).

在图3中,比较了使用标准差分析法情况下、不同光脉冲编码对量子通信系统的影响. 当 Alice 端探测器效率为 $\eta_{\mathrm{d}} = 0.4$, 分光镜(BS)的透射率 $t = 1/2$. 当 $N = 6.0 \times 10^9$ 时,密钥率降到零时的传输距离 $l \approx 50$ km;当 $N = 6.0 \times 10^{10}$ 时,密钥率降到零时的传输距离 $l \approx 91$ km;当 $N = 6.0 \times 10^{11}$ 时,密钥率降到零时的传输距离 $l \approx 114$ km. 这一趋势也表明:随着编码长度的增加,密钥能够安全传输的距离也相应增加.

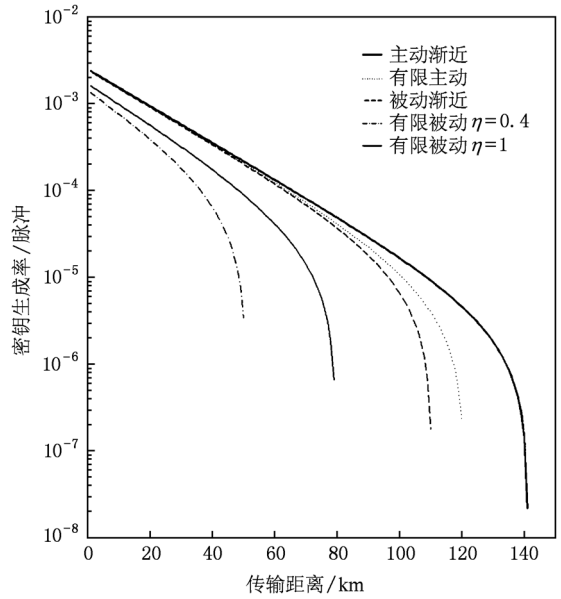

图2 密钥生成率随在不同条件下随传输距离的变化关系

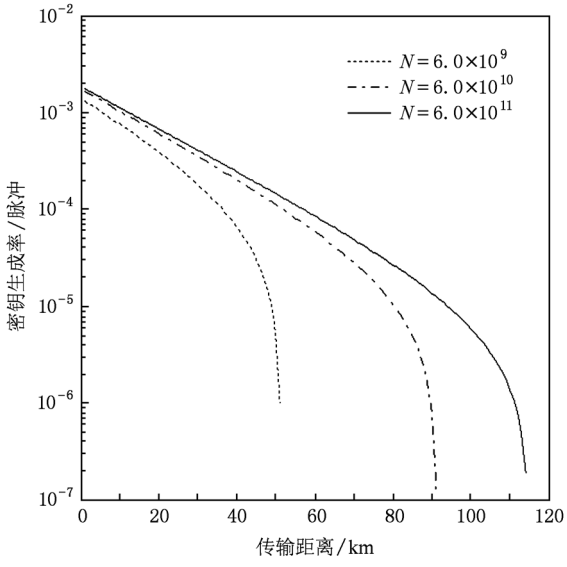

图3 不同的编码长度 N 条件下量子密钥生成率随传输距离的变化关系

[1] Bennet C H, Brassard G 1984 *Proc. IEEE Interna. Conf. Computers, Systems, and Signal Processing* (Bangalore, New York, IEEE)
[2] Boileau J C, Gottesman D, Laflamme R, Poulin D, Spekkens R W 2004 *Phys. Rev. Lett.* **92** 017901
[3] Li M M, Wang F Q, Lu Y Q, Zhao F, Chen X, Liang R S, Liu S H 2006 *Acta Phys. Sin.* **55** 4642 (in Chinese) [李明明、王发强、路轶群、赵 峰、陈 霞、梁瑞生、刘颂豪 2006 物理学报 **55** 4642]
[4] Wang J D, Qin X J, Wei Z J, Liu X B, Liao C J, Liu S H 2010 *Acta Phys. Sin.* **59** 281 (in Chinese) [王金东、秦晓娟、魏正军、刘小宝、廖常俊、刘颂豪 2010 物理学报 **59** 281]
[5] 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]
[6] Hughes R J 2002 *New J. Phys.* **4** 431
[7] Kurtsiefer C, Zarda P, Halder M, Weinfurter H, Corman P, Tapster P R, Parity J C 2002 *Nature* **419** 450
[8] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[9] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[10] Ma X F, Qi B, Zhao Y, Lo H K 2005 *Phys. Rev.* A **72** 012326
[11] Meyer T, Kampermann H, Kleinmamm M, Brub. D 2007 *Phys. Rev.* A **74** 042340
[12] Hayashi M 2007 *Phys. Rev.* A **76** 012329
[13] Lo H K, Ma X F, Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[14] Curty M, Ma X F, Qi B, Moroder T 2010 *Phys. Rev.* A **81** 022310

Decoy-state quantum key distribution with practical light source*

Jiao Rong-Zhen† Zhang Chao Ma Hai-Qiang
(*Science School, Beijing University of Post and Telecommunication, Beijing* 100876, *China*)
(Received 17 January 2011; revised manuscript received 24 Feburary 2011)

Abstract

The performance of active decoy-state quantum key distribution (QKD) system with a practical light source is compared with that of passive decoy-state QKD. The effect of statistical fluctuation due to a finite data size on final secret key rate is analyzed. This procedure is based on the standard error analysis on the assumption that all the variables measured in the experiment fluctuate around their asymptotic values. The relation between key generation rate and secure transmission distance is shown with exchanged quantum efficiency of threshold detector ($\eta_d = 1$ and $\eta_d = 0.4$) under the condition of active decoy-state (or passive decoy-state) QKD which we pick the data size to be $N = 6.0 \times 10^9$. This analysis will provide important parameters for practical QKD experiment.

Keywords: decoy state ,quantum key distribution ,statistical fluctuation
PACS: 03.67.Dd, 03.67.Hk

* Project supported by the State Key Development Program for Basic Research of China (Grant No. 2010CB923202) and the Fundamental Research Funds for the Central Universities of Ministry of Education of China (Grant No. BUPT2009RC0709).

† E-mail: jiao218@sohu.com