诱惑态量子密钥分配系统中统计涨落的研究*

焦荣珍† 唐少杰 张弼

(北京邮电大学理学院, 北京 100876)

(2011 年 6 月 9 日收到; 2011 年 6 月 20 日收到修改稿)

针对实用的量子密钥分配 (QKD) 系统是基于强衰减的弱激光脉冲作为单光子源, 光子数分束攻击极大限制了通信双方在非理想条件下 QKD 的传输距离和密钥生成率, 采用大数定律对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, 利用双诱惑态比较了 1310 nm 和 1550 nm 条件下, 编码脉冲的长度为 ($N = 10^6$—$N = 10^{12}$) 实际 QKD 协议中密钥的生成率与安全传输距离之间的关系、安全传输距离随编码长度的变化的关系, 得出脉冲编码长度增大到 $N = 10^{12}$ 时, 密钥的最大安全传输距离为 135 km.

关键词: 诱惑态, 量子密钥分配, 统计涨落

PACS: 03.67.Dd

1 引 言

量子保密通信是量子信息科学的重要分支, 其关键在于量子密钥分配 (QKD), QKD 能让通信双方 (Alice 和 Bob) 共享一个无条件安全密钥. 早在 1984 年 Bennett 等提出了第一个 QKD 协议 —— BB84 协议, 随后提出了基于两个非正交态的 QKD 协议 ——B92 协议 [1,2], 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 [3−7]. 针对实用的 QKD 系统是基于强衰减的弱激光脉冲作为单光子源, 窃听者 Eve 可用光子数分束攻击 (PNS) 获取信息. 光子数分束攻击极大限制了通信双方在非理想条件下 QKD 的传输距离和密钥生成率, 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, 通信双方由于计算能力和存储能力等原因只能交换有限个信号脉冲, 这种情形下必定会引入统计涨落的因素, 进而降低安全密钥生成率和最大安全传输距离. 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 公式上简单的修订, 没在理论方法上对统计涨落做系统分析. 本文将借助数学工具 —— 大数定律对诱惑态方案中单光子的计数率、单光子增益和误码率分别进行统计涨落分析, 并给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, 得出量子密钥成码率随距离变化的关系; 通过分析量子密钥分配实验中光源的多光子特性和编码长度来估计系统中参数的涨落情况, 进而分析统计涨落对成码率的影响.

2 理论与计算公式

在实验条件不变的情况下, 有规律的随机事件大量重复出现时往往会呈现出必然的统计特性, 这就是大数定律的表现形式. 采用 λ 表示对全体事件测量的一个样本值, d 为测量值有可能的测量结果 (对于比特误码率, $d = 2$ 是因为存在 “Alice = Bob” 和 “Alice≠Bob” 两种情况), 假设用 M 个测量样本来估计事件 σ(σ 为经典事件或量子态), 在实验精度范围内存在下面的表达式

$$\begin{aligned}\left|\lambda^M - \lambda^\infty\right| &\leqslant \frac{1}{2}\xi(M,\varepsilon)\\ &= \frac{1}{2}\sqrt{\frac{2[\ln(1/\varepsilon) + d\ln(M+1)]}{M}},\end{aligned} \tag{1}$$

这里 λ^M 表示对 σ 的 M 个样本测量后得到的测量值, λ^∞ 表示进行无穷次测量后得到事件的真实值;

* 国家重点基础研究发展计划 (973 计划) (批准号: 2010CB923202)、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

ε 为系统最大的失误概率, 根据这一定义, 对于 "一次便签密码" 这样的加密方法来说, 可认为密钥在精度 ε 范围内是安全的, 而攻击者猜对信息的概率也只有 ε.

在实际系统中使用有限长密钥进行编码时, 信号态和诱惑态的单光子计数率 Y_1 和误码率 e_1 存在相对统计涨落. 由于激光器产生 $m \geqslant 11$ 脉冲的概率非常小, 本文对信号态和诱惑态 $1 \leqslant m \leqslant 10$ 光子进行分析, 分别考虑其对通信系统中单光子计数率和误码率的贡献.

本文采用双诱惑态的方案进行研究, ν_1 和 ν_2 为 Alice 和 Bob 选择的两个诱惑态, μ 为信号态, 并满足: $\nu_1+\nu_2 \leqslant \mu \leqslant 1, \nu_1 \leqslant \nu_2$. 根据大数定律, x 光子态的计数率 Y_x^M 满足下面的统计涨落不等式:

$$\left|Y_x^M - Y_x^\infty(\sigma)\right| \leqslant \frac{1}{2}\xi(M,\varepsilon), \tag{2}$$

式中的 Y_x^M 代表 Alice 使用 M 个脉冲对密钥编码时测得的 x 光子态的计数率, Y_x^∞ 代表 Alice 使用无穷多个脉冲对密钥编码时测得的 x 光子态的计数率. 下面分别对信号态和诱惑态 x 光子的计数率的统计涨落进行分析:

$$\left|Y_{x\mu}^{n_{x\mu}} - Y_{x\mu}^\infty\right| \leqslant \frac{1}{2}\xi(n_{x\mu},\varepsilon) = \frac{1}{2}\xi(N_\mu p_{x\mu},\varepsilon), \tag{3}$$

$$|Y_{x\nu}^{n_{x\nu}} - Y_{x\nu}^\infty| \leqslant \frac{1}{2}\xi(n_{x\nu},\varepsilon) = \frac{1}{2}\xi(N_\nu p_{x\nu},\varepsilon), \tag{4}$$

其中 $n_{x\mu}$ 和 $n_{x\nu}$ 表示用来估计信号脉冲和诱惑态脉冲里 x 光子态计数率的样本脉冲. N_μ 和 N_ν 分别表示信号态和诱惑态的脉冲数量, 脉冲中 x 光子态的概率服从 Poisson 分布. 结合 (3) 式, 可以得到在有限长密钥情况下 x 光子信号态和 x 光子诱惑态之间计数率的相对统计涨落表达式:

$$\begin{aligned}\delta_{Y_{x\nu}} &= \left|Y_{x\nu}^{n_{x\nu}} - Y_{x\mu}^{n_{x\mu}}\right| \\ &\leqslant \frac{1}{2}\xi(N_\mu p_{x\mu},\varepsilon) + \frac{1}{2}\xi(N_\nu p_{x\nu},\varepsilon).\end{aligned} \tag{5}$$

同样, 对 x 光子态的误码率进行统计涨落考虑, 可以得到 x 光子态的信号光和诱惑态误码率的相对统计涨落表达式:

$$\begin{aligned}\delta_{e_{x\nu}} &= \left|e_{x\nu}^{n'_{x\nu}} - e_{x\mu}^{n'_{x\mu}}\right| \leqslant \frac{1}{2}\xi(N_\mu p_{x\mu} Y_{x\mu}^{n_{x\mu}},\varepsilon) \\ &\quad + \frac{1}{2}\xi(N_\nu p_{x\nu} Y_{x\nu}^{n_{x\nu}},\varepsilon),\end{aligned} \tag{6}$$

在考虑 (4) 式情况下, 两诱惑态的计数率分别为

$$\begin{aligned}Q_{\nu 1} &= Y_{0\nu_1}^{n_{0\nu_1}} e^{-\nu_1} + Y_{1\nu_1}^{n_{1\nu_1}} \nu_1 e^{-\nu_1} + \sum_{i=2}^{\infty} Y_{i\nu_1}^{n_{i\nu_1}} \frac{\nu_1^i}{i!} e^{-\nu_1} \\ &\leqslant Y_{0\nu_1}^{n_{0\nu_1}} e^{-\nu_1} + \left(Y_{1\mu}^{n_{1\mu}} + \delta_{Y_{1\nu_1}}\right)\nu_1 e^{-\nu_1} \\ &\quad + \sum_{i=2}^{10}\left(Y_{i\mu}^{n_{i\mu}} + \delta_{Y_{i\nu_1}}\right)\frac{\nu_1^i}{i!}e^{-\nu_1} \\ &\quad + \sum_{i=11}^{\infty} Y_{i\nu_1}^{n_{i\nu_1}} \frac{\nu_1^i}{i!} e^{-\nu_1} \\ &= Y_{0\nu_1}^{n_{0\nu_1}} e^{-\nu_1} + Y_{1\mu}^{n_{1\mu}} \nu_1 e^{-\nu_1} + \sum_{i=2}^{10} Y_{i\mu}^{n_{i\mu}} \frac{\nu_1^i}{i!} e^{-\nu_1} \\ &\quad + \sum_{i=1}^{10} \delta_{Y_{i\nu_1}} \frac{\nu_1^i}{i!} e^{-\nu_1} + \sum_{i=11}^{\infty} Y_{i\nu_1}^{n_{i\nu_1}} \frac{\nu_1^i}{i!} e^{-\nu_1}\end{aligned}$$

$$\begin{aligned}Q_{\nu 2} &= Y_{0\nu_2}^{n_{0\nu_2}} e^{-\nu_2} + Y_{1\nu_2}^{n_{1\nu_2}} \nu_2 e^{-\nu_2} + \sum_{i=2}^{\infty} Y_{i\nu_2}^{n_{i\nu_2}} \frac{\nu_2^i}{i!} e^{-\nu_2} \\ &\geqslant Y_{0\nu_2}^{n_{0\nu_2}} e^{-\nu_2} + \left(Y_{1\mu}^{n_{1\mu}} - \delta_{Y_{1\nu_2}}\right)\nu_2 e^{-\nu_2} \\ &\quad + \sum_{i=2}^{10}\left(Y_{i\mu}^{n_{i\mu}} - \delta_{Y_{i\nu_2}}\right)\frac{\nu_2^i}{i!}e^{-\nu_2} \\ &\quad + \sum_{i=11}^{\infty} Y_{i\nu_2}^{n_{i\nu_2}} \frac{\nu_2^i}{i!} e^{-\nu_2} \\ &= Y_{0\nu_2}^{n_{0\nu_2}} e^{-\nu_2} + Y_{1\mu}^{n_{1\mu}} \nu_2 e^{-\nu_2} + \sum_{i=2}^{10} Y_{i\mu}^{n_{i\mu}} \frac{\nu_2^i}{i!} e^{-\nu_2} \\ &\quad - \sum_{i=1}^{10} \delta_{Y_{i\nu_2}} \frac{\nu_2^i}{i!} e^{-\nu_2} + \sum_{i=11}^{\infty} Y_{i\nu_2}^{n_{i\nu_2}} \frac{\nu_2^i}{i!} e^{-\nu_2},\end{aligned} \tag{7}$$

因: $Q_i = Y_i \dfrac{\mu^i}{i!} e^{-\mu}$, 根据单光子计数率的下限可得出单光子增益的下限为

$$\begin{aligned}Q_{1\mu} \geqslant Q_{1\mu}^{L,\nu_1,\nu_2} &= \frac{\mu^2 e^{-\mu}}{\mu\nu_1 - \mu\nu_2 - \nu_1^2 + \nu_2^2} \\ &\quad \left[Q_{\nu_1} e^{\nu_1} - Q_{\nu_2} e^{\nu_2} - \frac{\nu_1^2 - \nu_2^2}{\mu^2}\left(Q_\mu e^\mu - Y_{0\mu}^{n_{0\mu}}\right)\right. \\ &\quad \left. - \left(e^{\nu_1} - \sum_{i=0}^{10}\frac{\nu_1^i}{i!}\right) - A\right],\end{aligned} \tag{8}$$

这里 $A = \sum\limits_{i=1}^{10}\left(\delta_{Y_{i\nu_1}}\dfrac{\nu_1^i}{i!} + \delta_{Y_{i\nu_2}}\dfrac{\nu_2^i}{i!}\right)$. 与计数率的分析类似, 可得出信号态的单光子误码率上限为

$$\begin{aligned}e_{1\mu} &\leqslant e_{1\mu}^{U,\nu_1,\nu_2} \\ &= \frac{E_{\nu_1} Q_{\nu_1} e^{\nu_1} - E_{\nu_2} Q_{\nu_2} e^{\nu_2} - \frac{1}{2}\left(Y_{0\nu_1}^{n_{0\nu_1}} - Y_{0\nu_2}^{n_{0\nu_2}}\right) + \mathrm{B}}{Y_{1\mu}^{n_{1\mu}}(\nu_1 - \nu_2)},\end{aligned} \tag{9}$$

其中:

$$B = \sum_{i=1}^{10}\left(\delta_{Y_{i\nu_1}}\frac{\nu_1^i}{i!} + \delta_{Y_{i\nu_2}}\frac{\nu_2^i}{i!} + \delta_{e_{i\nu_1}}\frac{\nu_1^i}{i!} + \delta_{e_{i\nu_2}}\frac{\nu_2^i}{i!}\right).$$

综合单光子增益的下限和误码率的上限, 可得修正后的安全密钥生成率的公式, R^L 表示最终安全密

钥生成率的下限:

$$R^L = \frac{N_\mu}{2(N_\mu + N_\nu)}\left\{ -1.2Q_\mu H\left(E_\mu\right) + Q_{1\mu}^{L,\nu_1,\nu_2}\left[1 - H\left(e_{1\mu}^{U,\nu_1,\nu_2}\right)\right]\right\}. \quad (10)$$

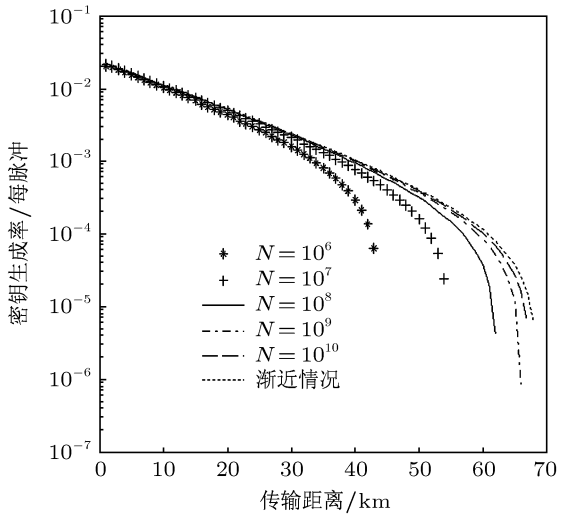

图 1 在 1310 nm 通信窗口, 不同脉冲长度编码的密钥生成率与安全传输距离之间的关系

3 结果与讨论

考虑实际 QKD 协议中使用的密钥长度都是有限的, 为了数值计算的简便, 这里采用真空态 + 弱相干态的双诱惑态协议, 让 $\nu_2 \to 0$, 结合以上方程, 可得到信号态的单光子计数率的下限 Y_1, 单光子增益下限 $Q_{1\mu}$ 和误码率上限 $e_{1\mu}$. 选择波长和光强分别为 $\lambda = 1310$ nm, $\mu = 0.48$ 的弱激光相干脉冲作为通信光源, $\nu_2 \to 0$ 前提下, 可以得到采用不同脉冲长度编码的密钥生成率与安全传输距离之间的关系, 见图 1. 由图可知, 随着密钥编码长度的不断增加, 密钥的安全传输距离也逐渐变大; 当编码脉冲的长度为 $N = 10^6$ 时, 安全密钥的传输距离是 43 km; 当编码脉冲的长度增大到 $N = 10^{10}$ 时, 安全密钥的传输距离已经达到了 68 km, 与无穷多诱惑态的渐近情况只相差 1 km. 选择波长和光强分别为 $\lambda = 1550$ nm, $\mu = 0.48$ 的弱激光相干脉冲作为通信光源, 在 $\nu_2 \to 0$ 前提下, 可得到采用不同脉冲长度编码的密钥生成率与安全传输距离之间的关系, 见图 2. 从图中可以明显看出, 密钥的安全传输距离与密钥编码采用的脉冲个数之间成正比, 随着编码长度的不断增加, 密钥的安全传输距离逐渐接近极限情况. 使用 1550 nm 的单模光纤, 当脉冲编码长度为 $N = 10^8$ 时, 密钥的最大安全传输距离是 74 km; 若脉冲编码长度增大到 $N = 10^{12}$ 时, 密钥的最大安全传输距离就增加到 135 km.

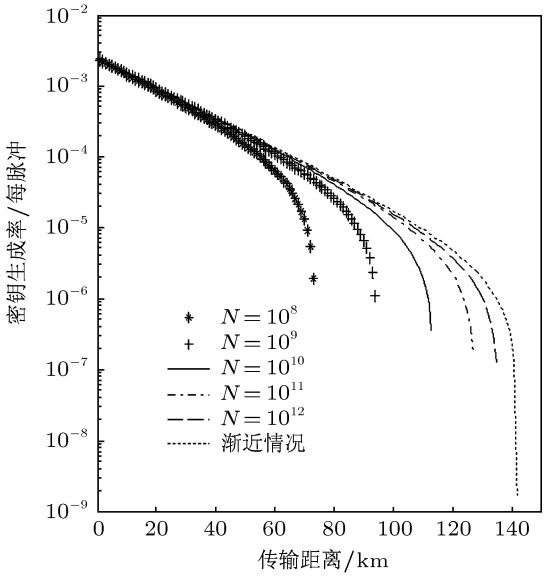

图 2 在 1550 nm 通信窗口, 不同脉冲长度编码的密钥生成率与安全传输距离之间的关系

[1] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121

[2] Bennet C H, Brassard G 1984 *Proc. IEEE International Conference Computers, Systems*, and *Signal Processing* Bangalore, New York, IEEE

[3] 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]

[4] Ma H Q, Li Y L, Zhao H, Wu L A 2005 *Acta Phys. Sin.* **54** 5014 (in Chinese) [马海强, 李亚玲, 赵环, 吴令安 2005 物理学报 **54** 5014]

[5] Jiao R Z, Zhang W H 2009 *Acta Phys. Sin.* **58** 2189 (in Chinese) [焦荣珍, 张文翰 2009 物理学报 **58** 2189]

[6] 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]

[7] 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]

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

Analysis of statistical fluctuation in decoy state quantum key distribution system*

Jiao Rong-Zhen† Tang Shao-Jie Zhang Chao

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

(Received 9 June 2011; revised manuscript received 20 June 2011)

Abstract

Decoy state has proven to be a very useful method of significantly enhancing the performance of a quantum key distribution (QKD) system with practical light sources. The data-set size in practical QKD protocol is always finite, which will cause statistical fluctuations. The gain and the error rate of the quantum state are analyzed by considering absolutely statistical fluctuation. The relation between key generation rate and the secure communication distance is shown with exchanged quantum signal ($N = 10^6 - 10^{12}$) by the method of two-decoy-state protocol under the condition that communication wavelength is 1310 nm (or1550 nm). The result indicates that the minimal number of exchanged quantum signals increases obviously with the increase of transmission distance. The secure transmission distance is 135 km under the condition that quantum signal is 10^{12}.

Keywords: decoy state, quantum key distribution, statistical fluctuation

PACS: 03.67.Dd

* Project supported by National Basic Research Program of China (Grant No. 2010CB923202) and Chinese Universities Scientific Fund (Grant No. BUPT2009RC0709).

† E-mail: jiao218@sohu.com