基于两种光源的诱发态量子密钥分配性能分析*

王 涵† 闫连山‡ 潘 炜 罗 斌 郭 振 徐明峰

(西南交通大学信息科学与技术学院信息光子与通信研究中心,成都 610031)

(2010 年 1 月 30 日收到;2010 年 5 月 20 日收到修改稿)

单光子的衰减特性及其易受干扰的缺点限制了纯单光子量子系统的传输码率及距离. 弱相干光脉冲(WCP)光源和准单光子源(HSPS)则具有更高的实用价值. 本文将这两种光源和诱发态方案相结合并采用 Lütkenhaus 和 Gottesman-Lo- Lütkenhaus-Preskill (GLLP)两种数据后处理方法进行性能分析. 仿真结果表明:HSPS 在传输距离上要优于 WCP,对应相同传输距离时系统量子误码率(QBER)要小些,但相对密钥生成率低.

关键词: 量子密钥分配, 诱发态, WCP 光源, HSPS 光源

PACS: 03. 67. Dd

1. 引 言

量子密码通信是最近 20 年发展起来的一种新的通信技术,它利用量子特性来得到或提高通信的保密性[1]. 近年来,人们提出了许多量子密钥分配协议,主要是点对点量子密钥分配协议[2]和网络中量子密钥分配协议[3]. 单光子量子密钥分配(QKD)利用量子力学原理对信息进行编码,通信双方密切地监察量子误码率(QBER)的异常增加,从而判断有没有被偷听. 一旦发现被偷听,立即摒弃,重新进行通信.

单光子 QKD 的主要缺点是光强太弱,易衰减及受干扰,从而限制了它的码率及传送距离. 目前尚没有简单可靠的真正单光子源,绝大多数都是利用激光源经过衰减来得到单光子. 泊松光源的光子数服从泊松分布,除了含有单光子脉冲外还含有多光子脉冲. 实际 QKD 系统采用的泊松光源一般是弱相干光脉冲(WCP)光源[4]. 但在相干态光源系统中,当密钥传输距离超 100 km 时暗计数就会严重影响系统的密钥生成率. Waks 等[5]证明在实际的 QKD 实验中亚泊松光源如准单光子源(HSPS),相对泊松光源性能有较大的改进. HSPS 是由参量下转换触发机理所产生的,它能有效减少长距离量子密钥分配过程中暗计数的影响,从而增大 QKD 的安全距离[6,7]. 实际系统中光源输出的光脉冲含有多光子,窃听者 Eve 会对输出脉冲实行光子数分裂(PNS)攻击[8]. 针对这种攻击,Hwang[9]提出了基于诱发态的 QKD 方案. 其核心思想是 Alice 随机地将信号脉冲转换成多光子脉冲(诱发脉冲),然后检查诱发脉冲的计数率. 如果诱发脉冲的计数率比其他信号脉冲要异常高些,Alice 就中断通信,否则继续通信,并通过诱发脉冲来估计脉冲信号的计数率. 根据上述方案,Lo 研究小组提出了实际可行的诱发态 QKD 方案[10,11]. Yin 等[12]提出的双强度诱发态 QKD 方案,其安全传输距离可超过 120 km. 焦荣珍等[13]提出的真空 + 弱诱发态 QKD 方案,其安全传输距离可超过 140 km. Li 等[14]提出了一种采用 SARG04 协议的相干态诱发态 QKD 方案,其传输距离可超过 160 km. 胡华鹏研究小组提出了一种基于泊松分布的参量下转化光子对的 SARG04 协议诱发态 QKD 方案,其安全传输距离可达 167 km[15]. 米景隆研究小组提出的采用 HSPS 和 SARG04 协议的诱发态 QKD 方案,其安全传输距离可达 192 km[16]. 该研究小组提出的“双探测器”HSPS 诱发态 QKD 方案可使系统的安全传输距离达到 221. 5 km[17].

本文利用文献[18]中所采用的反对个体攻击的 Lütkenhaus[19]和无条件安全的 GLLP[20]两种数据

* 国家自然科学基金(批准号:60972003)和教育部新世纪优秀人才资助项目(批准号:NCET-08-0821)资助的课题.

† E-mail:whyhooqis@ gmail. com

‡ E-mail: lsyan@ home. swjtu. edu. cn

后处理方法,在真空 + 诱发态方案下比较了采用两种光源(WCP 和 HSPS)在量子密码通信中密钥生成率和传输距离之间的关系.

2. 理论模型

2.1. WCP 诱发态

在光纤 QKD 系统中,假设 Alice 使用弱相干光进行密钥传输,且每个光脉冲的相位是随机的,脉冲平均光子数目 μ 服从泊松分布. 相位随机性对于保证 QKD 的安全性至关重要. Alice 发出的光子态的密度矩阵为

$$\rho_{\mathrm{A}} = \sum_{i=0}^{\infty} \frac{\mu^i}{i!} e^{-\mu} |i\rangle\langle i|, \quad (1)$$

$|0\rangle\langle 0|$ 为空态, $|i\rangle\langle i|$ 为 i 光子态, $i = 1,2,\cdots$. $i = 1$ 对应的光子态称为单光子态, $i \geqslant 2$ 的光子态称为多光子态. i 光子态的增益 Q_i 为

$$Q_i = Y_i \frac{\mu^i}{i!} e^{-\mu}. \quad (2)$$

当 $i = 1$, Q_1 和 e_1 分别为单光子态的增益和误码率.

Lütkenhaus 方法在反对个体攻击时是安全的,而 GLLP 方法则是无条件安全的. GLLP 方法中引入了标记量子比特的概念,Eve 可以获得标记量子比特的信息,因此其对 QKD 来说是不安全的. 在 GLLP 中,Alice 和 Bob 从原理上将量子比特分成两部分,标记和未标记量子比特,因此只需对未标记量子比特进行密性放大. 基于标记量子比特想法,数据后处理程序如下:首先,Alice 和 Bob 对数据进行纠错,若成功的话二者共享相同的密钥,然后他们计算有多少数据需进行密性放大. 其次,他们使用随机散列函数(或其他的密性放大程序)来得到最终安全密钥. 由于 PNS 攻击,我们将单光子态量子比特看作是未标记量子比特而其他光子态(空态和多光子态)看作是标记量子比特. 下面我们来比较 Lütkenhaus 和 GLLP 两种数据后处理方法的密钥生成率.

Lütkenhaus 方法的密钥生成率为

$$R \geqslant q\{-Q_\mu f(E_\mu) H_2(E_\mu) + Q_1[1 - \log_2(1 + 4e_1 - 4e_1^2)]\}, \quad (3)$$

而 GLLP 方法的密钥生成率为

$$R \geqslant q\{-Q_\mu f(E_\mu) H_2(E_\mu) + Q_1[1 - H_2(e_1)]\}. \quad (4)$$

其中 Q_μ 为总增益, E_μ 为系统总的 QBER 值,BB84 协议中 $q = 1/2$, 纠错效率 $f(E_\mu) = 1.16$. $H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$ 是二进制香农熵函数. Alice 和 Bob 需要从 QKD 实验数据中估计 Q_1 和 e_1.

在方程(3)和(4)中,大括号里前半部分用于纠错,后半部分用于密性放大. 密性放大只用于单光子部分. 实际上文献[21]中 Lütkenhaus 已经使用了标记量子比特概念.

当我们采用真空 + 弱诱发态方案时,考虑 Alice 和 Bob 使用 Q_{vac} 作为真空态的增益, Q_v 和 E_v 分别对应弱诱发态 v (光强)的增益和量子误码率. 由此可估计出真空诱发态的背景计数率为 $Y_0 = Q_{\mathrm{vac}}$, 而 Q_1 和 e_1 的估计值分别为

$$Q_1 \geqslant \frac{\mu^2 e^{-\mu}}{\mu v - v^2}\left(Q_v e^v - Q_\mu e^\mu \frac{v^2}{\mu^2} - \frac{\mu^2 - v^2}{\mu^2} Y_0\right), \quad (5)$$

$$e_1 \leqslant \frac{E_v Q_v e^v - e_0 Y_0}{Q_1 e^\mu v/\mu}. \quad (6)$$

其中 $e_0 = 1/2$ 为真空诱发态的误码率.

我们比较了 Lütkenhaus 和 GLLP 两种数据后处理方法的密钥生成率,采用表 1 四组实验参数 T8[21], G13[22], KTH[23], GYS[24] 对上述模型进行数值模拟. 我们得到了图 1 中 Lütkenhaus 和 GLLP 两种方法在 WCP 光源和真空 + 弱诱发态协议下系统密钥生成率和传输距离之间的关系. 从图 1 中可看出 GLLP 方法的密钥生成率要比采用 Lütkenhaus 方法稍微低些. 我们得到了四条 GLLP 曲线在最大传输距离时的 QBER 分别为 6.56%, 6.89%, 6.76% 和 6.39%, 很明显要远低于文献[25]中提到的 QBER 可接受值 11%. 这是由于本文分析采用的 QKD 光源是弱相干态光源,而文献[26]假设的光源是完美的单光子源.

表 1 量子密钥分配四组实验参数

实验	T8[16]	G13[17]	KTH[18]	GYS[19]
λ /nm	830	1300	1550	1550
α /(dB/km)	2.5	0.32	0.2	0.21
e_{d} /%	1	0.14	1	3.3
Y_0 /pulse	10^{-7}	1.64×10^{-4}	4×10^{-4}	1.7×10^{-6}
η_{Bob} /%	7.92	8.14	14.30	4.5

2.2. HSPS 诱发态

HSPS 一般由单模自发参量下转换触发机理所

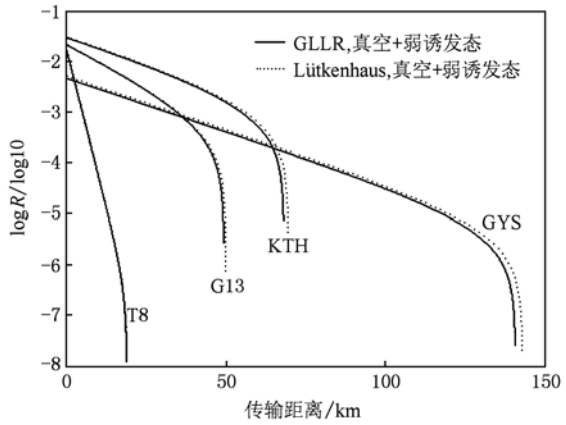

图1 WCP 诱发态数值模拟

产生,参量下转换产生的单模热态光子数分布为

$$p(\mu,n) = \frac{\mu^n}{(1+\mu)^{n+1}}, \tag{7}$$

式中μ为脉冲平均光子数. 在量子通信过程中,为了进一步减少暗计数和散射光的影响,在 Alice 端要加一个阈值检测器,以下称之为"触发检测器". 只有当触发检测器产生回应,同步脉冲才确认被发送给了接收者——告知 Bob 已经发送了一个脉冲[22]. 设 η_A 和 d_A 分别为检测效率和触发检测器的暗计数率,则我们可得到准单光子源的光子数分布为

$$\begin{aligned} P(\mu,n) &= p(\mu,n)[1-(1-\eta_A)^n + d_A] \\ &= \frac{\mu^n}{(1+\mu)^{n+1}}[1-(1-\eta_A)^n + d_A], \end{aligned} \tag{8}$$

很容易验证光子数服从亚泊松分布. 光子态密度矩阵为

$$\begin{aligned} \rho_\mu &= \frac{1}{P_{\mathrm{post}(\mu)}} \sum_{n=0}^{\infty} P(\mu,n) \,|n\rangle\langle n| \\ &= \frac{1}{P_{\mathrm{post}(\mu)}} \sum_{n=0}^{\infty} \frac{\mu^n}{(1+\mu)^{n+1}} \\ &\quad \times [1-(1-\eta_A)^n + d_A] \,|n\rangle\langle n| \\ &= \frac{1}{P_{\mathrm{post}(\mu)}} \left\{ \frac{d_A}{1+\mu} |0\rangle\langle 0| \right. \\ &\quad + \sum_{n=1}^{\infty} \frac{\mu^n}{(1+\mu)^{n+1}}[1-(1-\eta_A)^n \\ &\quad \left. + d_A] \,|n\rangle\langle n| \right\}, \end{aligned} \tag{9}$$

$$P_{\mathrm{post}}(\mu) = \frac{d_A}{1+\mu} + \frac{\mu\eta_A}{1+\mu\eta_A}. \tag{10}$$

信号光的总增益为

$$\begin{aligned} Q_\mu &= \sum_n Y_n P(\mu,n) \\ &= \sum_{n=0}^{\infty} Y_n \frac{\mu^n}{(1+\mu)^{n+1}}[1-(1-\eta_A)^n + d_A] \\ &= Y_0 \frac{d_A}{1+\mu} + \sum_{n=1}^{\infty} Y_n \frac{\mu^n}{(1+\mu)^{n+1}} \\ &\quad \times [1-(1-\eta_A)^n + d_A]. \end{aligned} \tag{11}$$

与前面采用 WCP 光源类似,采用真空态 + 弱诱发态方案,Alice 和 Bob 使用 Q_{vac} 作为真空态的增益,Q_v 和 E_v 分别为弱诱发态 v (光强)的增益和量子误码率,而真空态背景计数率 $Y_0 = Q_{\mathrm{vac}}$,则弱诱发态光的总增益为

$$\begin{aligned} Q_v &= \sum_n Y_n P(v,n) \\ &= \sum_{n=0}^{\infty} Y_n \frac{v^n}{(1+v)^{n+1}}[1-(1-\eta_A)^n + d_A] \\ &= Y_0 \frac{d_A}{1+v} + \sum_{n=1}^{\infty} Y_n \frac{v^n}{(1+v)^{n+1}} \\ &\quad \times [1-(1-\eta_A)^n + d_A], \end{aligned} \tag{12}$$

相应的真空态 + 弱诱发态情况下单光子计数率 Y_1 的下限为

$$\begin{aligned} Y_1 \geqslant & \left\{ \frac{\mu}{v}(1+v)^3 Q_v - \frac{v}{\mu}(1+\mu)^3 Q_\mu \right. \\ & \left. - Y_0 d_A \left[\frac{\mu}{v}(1+v)^2 - \frac{v}{\mu}(1+\mu)^2 \right] \right\} \\ & \times [\eta_A(\mu - v)]^{-1}, \end{aligned} \tag{13}$$

单光子增益的下限为

$$\begin{aligned} Q_1 &= Y_1 P(\mu,1) \geqslant \frac{\mu(\eta_A + d_A)}{\eta_A(\mu - v)(1+\mu)^2} \\ &\quad \times \left\{ \frac{\mu}{v}(1+v)^3 Q_v - \frac{v}{\mu}(1+\mu)^3 Q_\mu - Y_0 d_A \right. \\ &\quad \left. \times \left[\frac{\mu}{v}(1+v)^2 - \frac{v}{\mu}(1+\mu)^2 \right] \right\}, \end{aligned} \tag{14}$$

单光子误码率的上限为

$$e_1 \leqslant \frac{(1+v)^2 E_v Q_v - (1+v) e_0 Y_0 d_A}{Y_1 \eta_A v}, \tag{15}$$

系统总的 QBER 为

$$\begin{aligned} E_\mu Q_\mu &= \sum_{n=0}^{\infty} e_n Y_n P(\mu,n) \\ &= \frac{e_0 Y_0 d_A}{1+\mu} + \sum_{n=1}^{\infty} e_d [Y_0 + 1 - (1-\eta)^n] \\ &\quad \times \frac{\mu^n}{(1+\mu)^{n+1}}[1-(1-\eta_A)^n + d_A], \\ E_\mu &= E_\mu Q_\mu / Q_\mu. \end{aligned} \tag{16}$$

与 WCP 类似,我们可得到 HSPS 下 Lütkenhaus 和 GLLP 方法的密钥生成率.

Lütkenhaus 方法的密钥生成率为

$$R \geqslant \frac{P_{\mathrm{post}}(\mu)}{2}\left\{-Q_{\mu}f(E_{\mu})H_2(E_{\mu}) + Y_1\frac{\mu(\eta_{\mathrm{A}}+d_{\mathrm{A}})}{(1+\mu)^2}[1-\log_2(1+4e_1-4e_1^2)]\right\}, \quad (17)$$

GLLP 方法的密钥生成率为

$$R \geqslant \frac{P_{\mathrm{post}}(\mu)}{2}\left\{-Q_{\mu}f(E_{\mu})H_2(E_{\mu}) + Y_1\frac{\mu(\eta_{\mathrm{A}}+d_{\mathrm{A}})}{(1+\mu)^2}[1-H_2(e_1)]\right\}. \quad (18)$$

纠错效率 $f(E_{\mu}) = 1.16$. $H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$ 是二进制香农熵函数.

同样,我们采用上述四组实验参数 T8, G13, KTH, GYS 对模型进行数值模拟,得到了图 2 中 Lütkenhaus 和 GLLP 两种数据后处理方法在 HSPS 光源和真空 + 弱诱发态方案下系统密钥生成率和传输距离之间的关系. 我们得到四条 GLLP 曲线在图 1 同样截断距离时对应的 QBER 分别为 3.12%, 3.37%, 3.82% 和 4.8%. 这比图 1 中采用 WCP 光源在相同传输距离下的 QBER 值要小些,这是由于 HSPS 光源发出的非空信号脉冲强度越大,QBER 值越小. 与图 1 中采用 WCP 光源相比,HSPS 光源的成码率要低些,这是因为在非空信号脉冲中多光子脉冲越多,密钥生成率越低. HSPS 诱发态的密钥传输距离要比 WCP 诱发态的密钥传输距离更长些. 例如在 GYS 实验参数下最大传输距离可延长 30km,这是因为 HSPS 光源能有效减少长距离量子密钥分配过程中暗计数的影响,从而增大 QKD 的安全传输距离.

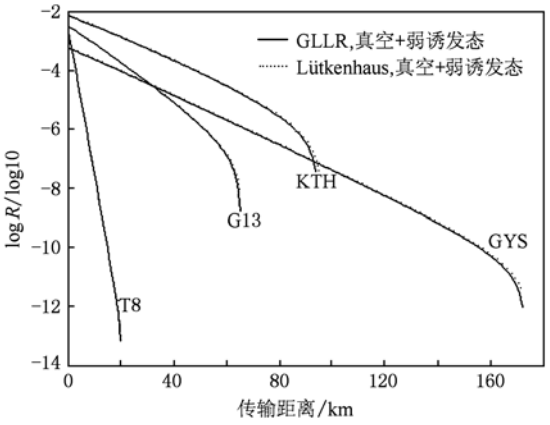

图 2 HSPS 诱发态数值模拟

3. 结 论

本文采用了反对个体攻击的 Lütkenhaus 和无条件安全的 GLLP 两种数据后处理方法,在真空 + 诱发态协议下,我们比较了 WCP 和 HSPS 两种不同光源在量子密码通信中密钥生成率和传输距离之间的关系. 我们的仿真结果显示 HSPS 在传输距离上要优于 WCP,对应相同传输距离时系统量子误码率(QBER)要小些,但相对密钥生成率则略低.

[1] Gisin N, Ribordy G, Tittel W, Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

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

[3] Tao Y, Pan W, Luo B, Li F 2008 *Acta Electron. Sin.* **30** 2588 (in Chinese)[陶 原、潘 炜、罗 斌、李 丰 2008 电子学报 **30** 2588]

[4] Rosenberg D, Harrington J W, Rice P R, Hiskett P A, Peterson C G, Hughes R J, Lita A E, Nam S W, Nordholt J E 2007 *Phys. Rev. Lett.* **98** 010503

[5] Waks E, Santori C, Yamamoto Y 2002 *Phys. Rev.* A **66** 042315

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

[7] 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]

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

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

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

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

[12] Yin Z Q, Han Z F, Chen W, Xu F X, Wu Q L, Guo G C 2008 *Chin. Phys. Lett.* **10** 3547

[13] 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]

[14] Li J B, Fang X M 2006 *Chin. Phys. Lett.* **6** 1375

[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 *Chin. Phys.* B **17** 1178

[17] 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]

[18] Ma X F 2006 *Phys. Rev.* A **74** 052325
[19] Lütkenhaus N 2000 *Phys. Rev.* A **61** 052304
[20] Gottesman D, Lo H K, Lütkenhaus N, Preskill J 2004 *Quantum Inf. Comput.* **4** 325
[21] Townsend P D 1998 *IEEE Photonics Technol. Lett.* **10** 1048
[22] Ribordy G, Gautier J D, Gisin N, Guinnard O, Zbinden H 1998 *Electron. Lett.* **34** 2116
[23] Bourennane M, Gibson F, Karlsson A, Hening A, Jonsson P, Tsegaye T, Ljunggren D, Sundberg E1999 *Opt. Express* **4** 383
[24] Gobby C, Yuan Z L, Shields A J 2004 *Appl. Phys. Lett.* **84** 3762
[25] Shor P W, Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[26] Zhang S L, Zou X B, Li K, Jin C H, Guo G C 2007 *Phys. Rev.* A **76** 044304

Performance analysis of decoy state quantum key distribution using two kinds of photon sources*

Wang Han† Yan Lian-Shan‡ Pan Wei Luo Bin Guo Zhen Xu Ming-Feng
(*Center for Information Photonics and Communications, School of Information Science and Technology, Southwest Jiaotong University, Chengdu* 610031, *China*)
(Received 30 January 2010; revised manuscript received 20 May 2010)

Abstract

Since the single photon is easy to attenuate and be disturbed, its key generation rate and transmission distance in quantum communication systems are generally limited. In contrast, weak coherent pulse (WCP) and heralded single photon source (HSPS) exhibit higher feasibility than the single photon source in quantum key distributions (QKD). We compare the performances of QKD using these two kinds of photon sources and decoy state method, incorporating data-postprocessing methods including the Lütkenhaus scheme and Gottesman-Lo-Lütkenhaus- Preskill (GLLP) scheme. Simulation results indicate that QKD using HSPS can transmit longer distance than using WCP with lower overall quantum bit error rate (QBER) at the same transmission distance, albeit with relatively low key generation rate.

Keywords: quantum key distribution, decoy state, weak coherent pulse, heralded single photon source
PACS: 03.67.Dd

* Project supported by the National Natural Science Foundation of China (Grant No. 60972003) and the Program for New Century Excellent Talents in University (Grant No. NCET-08-0821).

† E-mail: whyhooqis@gmail.com
‡ E-mail: lsyan@home.swjtu.edu.cn