

单光子量子密钥分发系统中干涉稳定性分析*

郑力明^{1,2} 王发强² 刘伟平¹ 廖常俊² 刘颂豪²

(1 暨南大学电子工程系, 广州 510632)

(2 华南师范大学信息光电子科技学院, 广州 510631)

摘 要 为了研究位相编码量子密钥分发系统中的干涉稳定性, 运用解析和数值计算方法详细研究了光纤双折射、温度变化、非对称性以及耦合器分光比对量子密钥分发系统干涉条纹可见度的影响, 结果表明光纤双折射、温度变化和非对称性都将影响系统的干涉可见度, 调整接收端的调制位相能消除温度变化的影响, 并减小非对称性对系统的影响, 但不能改善光纤双折射对系统干涉的影响. 另外, 耦合器分光比影响系统的效率.

关键词 量子密钥分发; 干涉; 双折射; 非对称性; 温度漂移

中图分类号 TN253 **文献标识码** A

0 引言

1964 年 Bell 不等式的提出开创了量子理论的技术应用, 是近代量子信息论的基础. 1982 年发现的量子不可克隆原理激发了量子密码术的研究. 随着 1984 年第一个实现量子密码术协议的提出^[1], 量子密钥分发很快就在实验上实现了. 目前关于单光子量子保密通信系统, 美国的 MagiQ 公司和瑞士的 id Quantique 公司已经开始有产品进入市场^[2]. 2003 年 Lightwave 报道日本 NEC、TAO 和 JST 三家通信公司已合作进行了通过廉价光纤传输单光子量子密码 100 km 的实验^[3], 传输码率为每秒几个比特, 误码率小于 10%, 并在 2004 年将这一距离延长到 150 km^[4]. 与此同时, 国内同行也开展了许多相关的理论和技术研究^[5-7].

单光子量子密钥分发系统中一般采用的编码方式有: 偏振编码^[8]和相位编码^[9]. 偏振编码系统的优势在于结构简单、易于理解. 其缺点在于由于光纤的双折射使光的偏振状态在传输过程中很难保持以致造成误码, 因此, 其传输距离受到很大的限制. 而相位编码系统的优点在于相位调制器的响应速度快, 可实现快速编码, 传输距离比较远. 但是由于: 1) 发送端和接收端的环境温度以及温度变化不一致; 2) 光纤的弯曲和扭转等因素引起的双折射; 3) 发送端和接收端干涉仪光程差的不对称性, 都会使接收端的干涉可见度下降. 本文详细分析了上述因素对单光子量子密钥分发系统中干涉稳定性的影响.

1 干涉稳定性的理论计算

采用 Mach-Zehnder 干涉仪实现相位编码的单光子量子密钥分发系统的原理图如图 1^[9], 其工作过程为: 激光器经脉冲调制, 发出的光经强衰减器 A 强衰减得到的单光子脉冲经耦合器 1, 可能走 Mach-Zehnder 干涉仪上臂路径, 也可能走下臂路径, 走下臂的被位相调制器 Φ_1 位相调制. 由于干涉仪两臂的长度不等, 所以从耦合器 2 出来的光脉冲有两个, 经光纤传播后到达接收端 Bob 的耦合器 3 干涉仪, 每个光脉冲通过干涉仪都有两种可能的路径, 所以在耦合器 4 处将有四个光脉冲. 如果 Alice 和 Bob 的干涉仪的两臂光程差完全相同, 则中间的两个脉冲将发生重叠, 并产生干涉, 由单光子探测器 D_1 、 D_2 探测到.

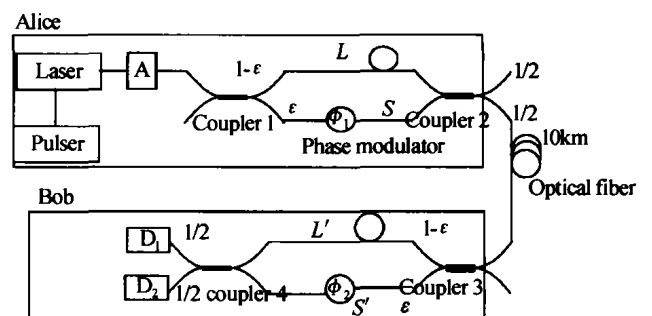


图 1 Mach-Zehnder 干涉仪实现相位编码实验系统
Fig. 1 Phase code experimental system based on Mach-Zehnder interferometer

设耦合器 1 和耦合器 3 的分光比为 $(1 - \epsilon) : \epsilon$, 耦合器 2 和耦合器 4 的分光比为 1:1, 初始输入的任意偏振态高斯光脉冲为

$$E_x = A_x \exp \left\{ -t^2/2T^2 \right\} e^{i\phi_x}$$

$$E_y = A_y \exp \left\{ -t^2/2T^2 \right\} e^{i\phi_y}$$

式中: A_x 和 A_y 分别为 X、Y 方向偏振分量的振幅, ϕ_x 和 ϕ_y 分别为 X、Y 方向偏振分量的位相, T 为高斯脉

*国家重点基础研究发展计划(973)项目(2001CB3093)和广州市科技攻关计划项目(1999-Z-035-01)资助
Tel:020-85226228 Email:qitworld@126.com
收稿日期:2005-01-05

冲的全宽.

经过烦琐而不复杂的运算,可以得到 D_1 端的两个重叠相干脉冲的光强为

$$I = \frac{\varepsilon(1-\varepsilon)}{4} \exp(-t^2/T^2) \{ A_x^2 |\exp\{i\varphi + i(\theta_x - \theta'_x) + i(\phi_1 - \phi_2) - i\kappa_A \Delta L + i\kappa_B \Delta L'\} + \exp\{[t^2 - (t - \Delta t)^2]/2T^2\}|^2 + A_y^2 |\exp\{i\varphi + i(\theta_y - \theta'_y) + i(\phi_1 - \phi_2) - i\kappa_A \Delta L + i\kappa_B \Delta L'\} + \exp\{[t^2 - (t - \Delta t)^2]/2T^2\}|^2 \} \quad (1)$$

式中: $\varphi = \phi_s + \phi_{L'} - \phi_L - \phi_{s'}$, ϕ_s 、 ϕ_L 、 $\phi_{L'}$ 和 $\phi_{s'}$ 分别是光通过 Alice 和 Bob 的干涉仪长短臂产生的位相, θ_x 、 θ_y 和 θ'_x 、 θ'_y 分别是相互重叠的两个脉冲的两个偏振分量因光纤双折射而产生的不同相移, κ_A 和 κ_B 分别是 Alice 和 Bob 端的干涉仪因温度漂移而使单位长度光纤产生的相移, $\Delta L = L - S\Delta L' = L' - S'$, $\Delta t = t_L + t_{s'} - t_s - t_{L'}$, t_L 、 t_s 、 $t_{s'}$ 和 $t_{L'}$ 分别是光脉冲通过两个干涉仪四条臂的时间.

式(1)比较复杂,因此,对不同因素的影响分别加以考虑. 首先,考虑如果收发两端的干涉仪完全对称,即 $L' = L$, $S' = S$,则有

$$I = \frac{\varepsilon(1-\varepsilon)}{4} \exp(-t^2/T^2) \{ A_x^2 |\exp\{i(\theta_x - \theta'_x) + i(\phi_1 - \phi_2) - i(\kappa_A - \kappa_B)\Delta L\} + 1|^2 + A_y^2 |\exp\{i(\theta_y - \theta'_y) + i(\phi_1 - \phi_2) - i(\kappa_A - \kappa_B)\Delta L\} + 1|^2 \} \quad (2)$$

由式(2)可以看出,光纤双折射引起的位相差以及收发两端不同的温度漂移都将影响光脉冲的干涉,降低可见度. 如果考虑光纤的扭转,则式(2)中的偏振幅度 A_x 、 A_y 的大小将发生变化,结果将更加复杂. 假如在光纤干涉仪的制作时避免扭转,可以避免系统的性能恶化.

其次,如果只考虑干涉仪的非对称性和温度漂移,则

$$I = \frac{\varepsilon(1-\varepsilon)}{4} \exp(-t^2/T^2) |\exp\{i\varphi + i(\phi_1 - \phi_2) - i\kappa_A \Delta L + i\kappa_B \Delta L'\} + \exp\{[t^2 - (t - \Delta t)^2]/2T^2\}|^2 \quad (3)$$

由式(3)可以看出,收发两端干涉仪的非对称性也将使系统的干涉可见度降低. 另外,即使收发两端的温度漂移系数相同 $\kappa_A = \kappa_B$,也因干涉仪的非对称性而使系统的干涉可见度降低.

2 讨论

式(2)、(3)进行数值计算,所取参数为: $T = 500$ ps, $\varepsilon = 0.5$, $\phi_1 = \phi_2 = 0$. 图2是 $(\theta_x - \theta'_x) - (\kappa_A - \kappa_B)\Delta L$ 和 $(\theta_y - \theta'_y) - (\kappa_A - \kappa_B)\Delta L$ 分别取①0、0,②

0、 $\pi/2$,③ $\pi/2$ 、 $\pi/2$,④0、 $\pi/2$ 时根据式(2)作出的干涉脉冲强度曲线,其中曲线1、2、3对应 $A_x = 1/\sqrt{5}$, $A_y = 2/\sqrt{5}$,曲线4对应 $A_x = 2/\sqrt{5}$, $A_y = 1/\sqrt{5}$. 图3中的曲线是 $\varphi - i\kappa_A \Delta L + i\kappa_B \Delta L'$ 和 Δt 分别取①0、0;②0、150 ps;③ $\pi/2$ 、150 ps;④ $\pi/2$ 、250 ps 时根据式(3)作出的干涉脉冲强度曲线.

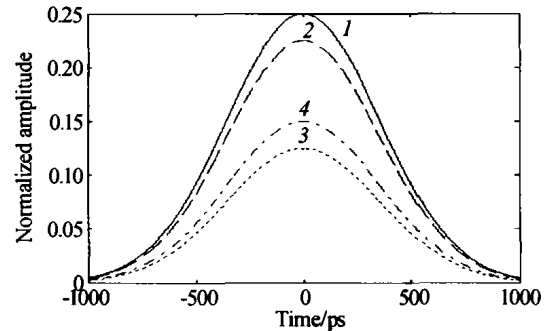


图2 不同偏振状态或温度漂移时的干涉脉冲
Fig. 2 Interference pulse under various polarization states or temperature excursion

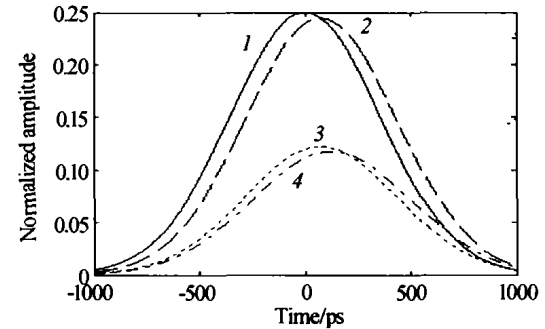


图3 不同非对称状态时的干涉脉冲
Fig. 3 Interference pulse under various asymmetry states

从图2中的曲线可以看出当相互重叠的脉冲之间的偏振状态不一致时或收发两端温度漂移不一致时,相干脉冲的强度下降,影响干涉条纹的可见度. 首先,仅考虑光纤双折射的影响. 通常光脉冲所走的两条路径的双折射是不一样的,因此,两重叠脉冲的各偏振分量因双折射而产生的位相是不同的,即 $\theta_x - \theta'_x$ 、 $\theta_y - \theta'_y$ 都不等于零,且两者的值一般不相等. 图2中的曲线1是无任何干扰的理想干涉曲线,对比曲线1、2和3可知光纤双折射影响系统的干涉可见度. 另外,对比图2中的曲线2和4可以发现,如果在接收端光脉冲偏振状态发生变化,即使光纤双折射引起的位相漂移不变,其最终的干涉脉冲强度也将发生变化. 这些表明如果接收端光脉冲偏振态或光纤的双折射随时间发生变化,这将影响系统的稳定性.

其次,仅讨论温度变化的影响. 由于光纤对温度变化比较灵敏,如通常的单模光纤在波长 $1.31 \mu\text{m}$ 处的位相漂移随温度的变化为 $47.8 \text{ rad}/^\circ\text{C m}$. 因此,收发两端的环境温度及其变化有非常微小的差别都将影响系统的干涉可见度. 尤其是空气流动和

热扩散都将引起温度的变化,造成系统的不稳定.当只考虑温度漂移影响时,两偏振分量的相因子 $(\kappa_A - \kappa_B)\Delta L$ 是相同的,式(2)可以写为

$$I = \frac{\varepsilon(1-\varepsilon)}{4} \exp(-t^2/T^2) |\exp\{i(\phi_1 - \phi_2) - i(\kappa_A - \kappa_B)\Delta L\} + 1|^2 \quad (4)$$

图2中的曲线3就是温度漂移引起的位相变化为 $\pi/2$ 时的干涉脉冲强度曲线.因为温度漂移的影响是随时间变化的慢变过程,由式(4)发现,在系统运行时不断调整接收端的调制位相 ϕ_2 ,可以消除温度对系统的影响.而光纤双折射对两个偏振分量相因子的影响一般情况下是不一样的,因此,光纤双折射对干涉的影响是不能用调整接收端调制位相的方法来消除的.

图3中的曲线1是理想的干涉光脉冲强度曲线,对比曲线1和2可以发现,非对称性引起的两相干脉冲不完全重叠将影响干涉可见度.由曲线3和4可知,收发两端干涉仪的非对称性越大,则干涉可见度越差.对比曲线2和3可知,由非对称性引起的位相不对称也将影响干涉可见度,由此也可以看出,调整接收端的调制位相 ϕ_2 ,可以减小非对称性对系统的影响.

最后,讨论耦合器分光比对系统的影响.由式(1)中的因子 $\varepsilon(1-\varepsilon)$ 可以看出,当 ε 取1/2时,此因子有极大值1/4,因此耦合器分光比可以影响系统的密码产生效率.以上各图中分光比均取在最优值1/2处.

3 结论

本文研究了光纤双折射、温度变化、非对称性以及耦合器分光比对量子密钥分发系统干涉稳定性的影响,结果表明光纤双折射、温度变化和不对称性都将影响系统的干涉可见度,调整接收端的调制位相能消除温度变化的影响,并减小非对称性对系统的影响,但不能改善光纤双折射对系统干涉的影响,关于系统干涉偏振稳定性的解决方案因篇幅所限,将

另文讨论.另外,耦合器分光比将影响系统的密码产生效率.

参考文献

- 1 Bennett C, Brassard G. Quantum cryptography: Public-key distribution and coin tossing. Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (New York:IEEE), 1984. 175 ~ 179
- 2 Mullins J. Quantum physics spins off marketable products. *IEEE Spectrum*, 2002, 5: 21 ~ 22
- 3 Kosaka H, Tomita A, Nambu Y, et al. Single-photon interference experiment over 100 km for quantum cryptography system using a balanced gated-mode photon detector. *Electronics Letters*, 2003, 39(16): 1199 ~ 1201
- 4 Kimura T, Nambu Y, Hatanaka T, et al. Singlephotoninterference over 150-km transmission using silica-based integrated-optic interferometers for quantum cryptography. *Jpn J Appl Phys*, 2004, 43(9AB): L1217 ~ 1279
- 5 刘景锋,梁瑞生,刘伟平,等.量子保密通信的光精密控制强衰减技术.光子学报,2004,33(7):867 ~ 870
Liu J F, Liang R S, Liu W P, et al. *Acta Photonica Sinica*, 2004, 33(7): 867 ~ 870
- 6 刘景锋,梁瑞生,唐志列,等.基于BB84协议的实际QKD系统的窃听问题研究.光子学报,2004,33(11):1356 ~ 1359
Liu J F, Liang R S, Tang Z L, et al. *Acta Photonica Sinica*, 2004, 33(11): 1356 ~ 1359
- 7 陈志新,唐志列,魏正军,等.QKD系统在Brendbart基窃听下BB84协议的信息量研究.光子学报,2004,33(12): 1469 ~ 1472
Chen Z X, Tang Z L, Wei Z J, et al. *Acta Photonica Sinica*, 2004, 33(12): 1469 ~ 1472
- 8 Zbinden H, Gisin N, Huttner B, et al. Practical aspects of quantum cryptographic key distribution. *J Crypto*, 2000, 13: 207 ~ 220
- 9 Townsend P D, Thompson I. A quantum key distribution channel based on optical fibre. *J Mod Opt*, 1994, 41(12): 2425 ~ 2433

Interference Stability Analysis of Quantum Key Distribution System Based on Single Photon

Zheng Liming^{1,2}, Wang Faqiang², Liu Weiping¹, Liao Changjun², Liu Songhao²


1 Department of Electrical Engineering, Jinan University, Guangzhou 510632

2 College for Information and Optoelectronics Science and Engineering, South China Normal University, Guangzhou 510631

Received date:2005-01-05

Abstract In order to study the interference stability in phase coded quantum key distribution (QKD) system, the influence that optical fiber birefringence, temperature variation, asymmetry and coupling ratio have on the interference visibility of the system is studied in details in this paper by using analytic and numerical methods. Further more, the influence of temperature variation and that of asymmetry could be eliminated and depressed respectively by adjusting of phase modulator in receiver. But the influence of birefringence could not be amended. In addition, the influence of the coupling ratio of coupler is limited to system efficiency only.

Keywords Quantum key distribution (QKD); Interference; Birefringence; Asymmetry; Temperature excursion



Zheng Liming was born in Guangdong Province, China, in 1971. He received the M. S. degree of Electronics from Jinan University in 2000. He is now working as an associate professor in the Department of Electrical Engineering, Jinan University. He is currently pursuing the Ph. D. degree of Optics in South China Normal University. His current research interest is in the field of Quantum information.