

文章编号: 0253-2239(2010)11-3328-04

磁光效应对量子相位编码系统的影响分析

韩宝彬 裴昌幸 刘 丹

(西安电子科技大学综合业务网及关键技术国家重点实验室, 陕西 西安 710071)

摘要 受光纤双折射的影响,单光子极化态在光纤中传输时容易发生慢变进而影响到量子密钥分发系统的性能。利用概率波叠加理论分析了法拉第旋转镜的时分复用干涉仪相位编码系统。分析结果表明,利用单光子往返通过同一根光纤可以有效抵消光纤双折射的影响,但容易受到非互易性效应如磁光效应的影响。随着磁光旋转角的增加,成功到达干涉仪的单光子形成正常干涉条纹的概率逐渐减小。旋转角大于 42° 时,形成正常干涉条纹的概率接近于零。

关键词 量子通信;相位编码;概率波;磁光效应

中图分类号 O436.4 文献标识码 A doi: 10.3788/AOS20103011.3328

Analysis of Influence of Magneto-Optical Effect on Quantum Key Distribution System with Phase Coding

Han Baobin Pei Changxing Liu Dan

(State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, Shaanxi 710071, China)

Abstract Being affected by birefringence, the polarization state of single photon is randomly and slowly altered during the transmission in single mode fiber. This influences the performance of quantum key distribution system. The “plug and play” system with Faraday rotation mirror is theoretically analyzed by the use of probability wave superposition. The results show that the bidirectional transmission of a single photon through the same fiber can effectively offset the influence of fiber birefringence, but is vulnerable to nonreciprocity effects such as magneto-optical effect. The probability of normal interference fringes, formed by the single photon reaching the interferometer successfully, decreases with the increase of magneto-optical rotation angle. When the rotation angle is greater than 42° , the probability of forming the normal interference fringes is close to 0.

Key words quantum communications; phase coding; probability wave; magneto-optical effect

1 引 言

自1984年量子密钥分发协议提出和1992年量子密钥分发演示实验成功后^[1,2],量子保密通信有了长足的发展。由于量子密钥分发具有无条件安全的优点,国内外都在积极地开展理论和实验研究^[3~10]。在光纤量子通信方面,通信距离已经达到了 150 km ^[11]。目前,量子通信主要有相位编码和极化编码^[12]两种编码

方案,由于相位编码可以较好地抵消信道对光子极化态的影响,人们认为光纤信道更适合采用相位编码。

本文针对A. Muller等^[13]提出的“即插即用”(“plug and play”)相位编码模型,利用概率波的叠加特性研究了磁光效应对相位编码的影响,结果表明磁光效应极大的影响了密钥分发效率,严重情况下密钥分发无法实施。

收稿日期: 2009-11-06; 收到修改稿日期: 2010-03-22

基金项目: 国家自然科学基金(60572147, 60672119)、国家重点实验室专项基金(ISN02080002)和高等学校创新引智计划(B08038)资助课题。

作者简介: 韩宝彬(1977—),男,博士研究生,讲师,主要从事安全和量子通信等方面的研究。

E-mail: hanbaobin@163.com

导师简介: 裴昌幸(1945—),男,教授,博士生导师,主要从事网络测量和量子通信等方面的研究。

E-mail: chxpei@xidian.edu.cn

2 相位编码密钥分发模型

图 1 为基于法拉第旋转镜的时分复用干涉仪相位编码模型示意图^[13],该模型也被称为“plug and play”型。其中 LD 表示激光源,LD 上方半圆形部件为环形器,PBS 为偏振分束器。 PM_a 和 PM_b 分别为相位调制器,D0,D1 和 D2 为单光子探测器。DL 为防止背向散射的干扰引入的纳秒级延时线,FM 为法拉第反射镜。

Bob 首先发射一个脉冲经过环形器传向 Alice,并在耦合器 1 上分开:一部分通过短臂经偏振分束器 PBS 后传向 Alice(用 S 光表示),经 Alice 端法拉第镜(FM)反射后重新返回 Bob 端;另一部分脉冲经过长臂后通过 PBS 后传向 Alice(用 L 光表示),Alice 利用相位调制器 PM_a 对 L 光进行移相操作引入相移 ϕ_a 。在 FM 作用下,L 光再次通过偏振分束器时将透射通过短臂。S 光则被反射通过长臂到达干涉仪,此时 Bob 利用相位调制器 PM_b 调制对 S 光

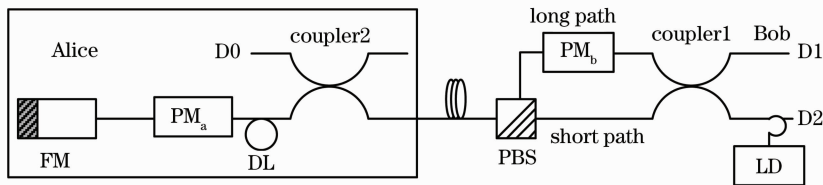


图 1 名为“即插即用”的基于法拉第旋转镜的时分复用干涉仪相位编码模型

Fig. 1 Phase encoded system of time division multiplexing interferometer based on Faraday rotation mirror named “plug and play”

3 性能分析

详细的分析“plug and play”模型的性能,必须利用概率波理论。

设初始时刻 LD 发出的光脉冲用 $E = A\exp[j(\omega t + \varphi)]$ 表示, ω 为光的角频率, t 表示时间, φ 表示初始相位,经 1:1 分束器耦合到两臂上分别为 E_s 和 E_L 。假设 Alice 和 Bob 端引入的延时分别用 $f(\tau_A)$ 和 $f(\tau_B)$ 表示。考虑到光纤中存在双折射,假设光纤水平和垂直折射率分别为 n_x 和 n_y ,水平和垂直方向的相位常数发生变化分别用 β_x 和 β_y 表示。令光纤长为 l ,则光纤传输矩阵为

$$\mathbf{T}_f = \begin{bmatrix} \exp(j\beta_x l) & 0 \\ 0 & \exp(j\beta_y l) \end{bmatrix}. \quad (2)$$

进行移相操作引入相移 ϕ_b 。由于所经路径长度相同,两部分脉冲到达的时间不同,接收端可以探测到这两部分脉冲的干涉。令初始量子态 $|0\rangle$,量子态通过耦合器^[14]既是作一次 Hardmard 变换,用 H 表示。移相器引入的移相用 ϕ 表示。最终在 Bob 端输出的量子态^[14]为

$$H\phi H|0\rangle = \frac{1}{2} \{ [\exp(i\Delta\phi + 1)]|0\rangle + [\exp(i\Delta\phi - 1)]|1\rangle \}, \quad (1)$$

式中 $\Delta\phi = \phi_a - \phi_b$ 。可以看出,探测器 D1 和 D2 探测到单光子的概率完全由移相器引入的相位差决定。当 Alice 控制的 ϕ_a 取 0 或 π 时,Bob 控制的 ϕ_b 只有取 0 或 π 时,D1 或 D2 才能得到确定的输出;如果 ϕ_b 取值范围为 $(\pi/2, 3\pi/2)$,则 D1 或 D2 得到确定输出的概率为 1/2,反之亦然。所以该模型可以按照 BB84 协议的要求进行工作。

理想情况下 FM 的矩阵模型为

$$\mathbf{F}_M = \begin{bmatrix} \cos(\pi/2) & \sin(\pi/2) \\ -\sin(\pi/2) & \cos(\pi/2) \end{bmatrix}. \quad (3)$$

S 路光经 PBS 进入 Alice,又经 FM 处理并延时再次经过公共光纤后耦合至长臂,设此时信号为

$$\mathbf{E}'_s = f(\tau_A) \mathbf{T}_f \mathbf{F}_M \mathbf{T}_f \mathbf{E}_s \exp(j\phi_b). \quad (4)$$

同样对 L 路光分量,设回到 PBS 后为 \mathbf{E}'_l ,有:

$$\mathbf{E}'_l = f(\tau_B) \mathbf{T}_f \mathbf{F}_M \mathbf{T}_f \mathbf{E}_l \exp(j\phi_a), \quad (5)$$

$f(\tau)$ 仅仅是提供延时,去除该因子后再比较两式可知,无论是 S 光路还是 L 光路都经过两次光纤和一次 FM。相应的传递函数用 T 表示。考虑任意 $\mathbf{E} = \begin{bmatrix} E_x \\ E_y \end{bmatrix}$,设经 T 后为 \mathbf{E}' 。

$$\mathbf{E}' = \mathbf{T}_f \mathbf{F}_M \mathbf{T}_f \mathbf{E} = \begin{bmatrix} \exp(j\beta_x l) & 0 \\ 0 & \exp(j\beta_y l) \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} \exp(j\beta_x l) & 0 \\ 0 & \exp(j\beta_y l) \end{bmatrix} \cdot \begin{bmatrix} E_x \\ E_y \end{bmatrix} = \begin{bmatrix} \exp[j(\beta_x + \beta_y)l] E_y \\ -\exp[j(\beta_x + \beta_y)l] E_x \end{bmatrix}. \quad (6)$$

Bob 端干涉电场强度值为

$$E = E'_1 + E'_s = A \exp[j(\omega t + \varphi)] \times \exp\left[\frac{1}{2}j(\phi_a + \phi_b)\right] \cos \frac{1}{2}(\Delta\varphi), \quad (7)$$

式中 $\Delta\varphi = \phi_a - \phi_b$ 决定了探测器 D1 和 D2 检测到单光子的概率。(7) 式中没有包含光纤的长度因子 l , 意味着判决概率不受光纤双折射的影响。

根据法拉第效应^[3,15,16], 当线偏振光传播方向和磁场方向相同时, 振动面向左旋; 而线偏振光逆着磁场方向传播时, 振动面将向右旋。假设公共光纤

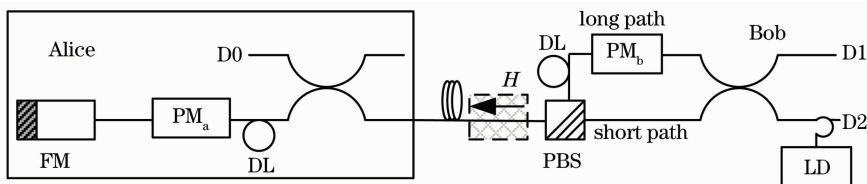


图 2 磁场中的“plug and play”模型
Fig. 2 “Plug and play” in magnetic field

(9)和(10)式表明 E_s 和 E_l 的极化态被旋转了 2θ 的角度。由于经过 PBS 相当于对概率波做量子测量, 根据量子力学半正定算子值 (POVM) 测量定义, 再次通过 PBS 后, E_s 将有 $\sin^2 2\theta$ 的概率水平通过 PBS 进入短臂, 同样 E_l 则以概率 $\sin^2 2\theta$ 被 PBS 反射而进入长臂。从而得到

$$E'_s = f(\tau_A) \mathbf{T}_i \mathbf{F}_M \mathbf{T}_i E_s, \quad (11)$$

$$E'_l = f(\tau_B) \mathbf{T}_i \mathbf{F}_M \mathbf{T}_i E_l \exp[j(\phi_a + \phi_b)]. \quad (12)$$

(12) 式意味着到达 Bob 端的概率波已经不再包含 Alice 和 Bob 的相位差信息, 从而无法实现密钥的分发。在存在磁场时, 时分复用干涉仪仍能形成正常干涉条纹的概率为

$$p = p(E_s \rightarrow L, E'_l \rightarrow S) = \cos^4 2\theta. \quad (13)$$

将(8)式代入, 有

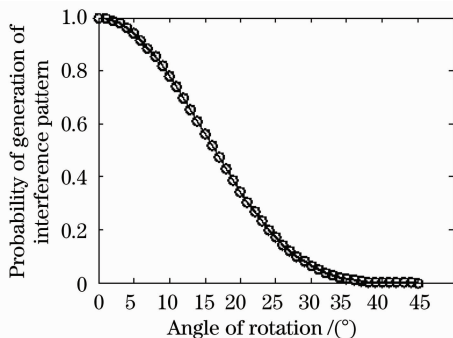


图 3 旋转角和干涉条纹形成概率的关系

Fig. 3 Relation between angle of rotation and the probability of generation of interference pattern

存在磁场强度为 H , 作用长度 l , 那么由磁场引起偏振旋转角为

$$\theta = V \oint H dl. \quad (8)$$

如图 2 为磁场中的“plug and play”模型图, 由于 E_s 和 E_l 需要两次往返经过磁场作用区, 则在重新回到 PBS 后有

$$E_s \mathbf{x} \rightarrow E_s \overline{(y + 2\theta)}, \quad (9)$$

$$E_l \mathbf{y} \rightarrow E_l \overline{(x + 2\theta)}. \quad (10)$$

$$p = \cos^4(2V \oint H dl). \quad (14)$$

根据(13)式, 可以得到旋转角和干涉条纹正常形成的关系如图 3 所示。从图 3 中可以看到, 在旋转角度大于 30° 时, 正常产生干涉条纹的概率在 0.06 以下, 旋转角大于 37° 时, 干涉条纹形成的概率小于 0.01, 旋转角大于 42° 后, 生成概率已经接近 0, 这意味着相位编码密钥分发系统无法正常工作。

4 结 论

光纤虽然具有抗干扰性好等特点, 但直击雷或是附件的磁场都将会使光信号的极化面发生旋转。从前面分析来看, 光纤特性的不理想不会影响到基于法拉第旋转镜的时分复用干涉仪相位编码模型方案, 但磁光效应会使该方案密钥分发效率下降, 在磁致旋转角在 $42^\circ \sim 45^\circ$ 时, 该方案已经无法正常工作。因此, 在实施密钥分发时必须要考虑磁场等因素的影响。

参 考 文 献

- 1 C. H. Bennett, G. Brassard. Quantum cryptography: public key distribution and coin tossing[C]. IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India, 1984. 175~179
- 2 C. H. Bennett. Quantum cryptography: uncertainty in the service of privacy[J]. *Science*, 1992, **257**(5071): 752, ~753
- 3 Han Baobin, Pei Changxing, Chen Nan *et al.*. Analysis of the effect of magneto-optic effect on BB84 protocol[J]. *Chinese J. Quant. Electron.*, 2007, **24**(5): 575~578

- 韩宝彬, 裴昌幸, 陈南等. 磁光效应对 BB84 协议的影响分析[J]. 量子电子学报, 2007, **24**(5): 575~578
- 4 C. Gobby, Z. L. Yuan, A. J. Shields. Quantum key distribution over 122 km standard telecom fiber[J]. *Appl. Phys. Lett.*, 2004, **84**(19): 3762~3764
- 5 C. Kurtsiefer, P. Zarda, M. Halder *et al.*. A step towards global key distribution [J]. *Nature*, 2002, **419**(6906): 450
- 6 T. Kimura, Y. Nambu, T. Hatanaka *et al.*. Single-photon interference over 150 km transmission using silica-based integrated-optic interferometers for quantum cryptography[J]. *Japan J. Appl. Phys.*, 2004, **43**(9): 1217~1219
- 7 Guo Zhanying, Zhang Xinhai, Fang Jianxing *et al.*. Probabilistic teleportation of an arbitrary n -particle entangled state and its quantum logic circuit[J]. *Acta Optica Sinica*, 2008, **28**(2): 387~391
- 郭战营, 张新海, 方建兴等. 任意 n 粒子纠缠态的概率传送及其量子逻辑线路[J]. 光学学报, 2008, **28**(2): 387~391
- 8 S. J. Qin, Q. Y. Wen, L. M. Meng *et al.*. High efficiency of two efficient QSDC with authentication is at the cost of their security[J]. *Chin. Phys. Lett.*, 2009, **26**(2): 020312
- 9 Chen Yan, Deng Ke, Hu Yu *et al.*. Effect of fiber coupling on photon-detection probability of quantum key distribution systems [J]. *Acta Optica Sinica*, 2007, **27**(8): 1401~1404
- 陈彦, 邓科, 胡渝等. 光纤耦合对量子密钥分配系统光子探测的影响[J]. 光学学报, 2007, **27**(8): 1401~1404
- 10 Yu Yafei, Zhang Zhiming. Analysis on unsecurity of quantum secret sharing based on smolin bound entangled states[J]. *Acta Optica Sinica*, 2008, **28**(3): 556~559
- 於亚飞, 张智明. 束缚纠缠态量子秘密共享的不安全性分析[J]. 光学学报, 2008, **28**(3): 556~559
- 11 T. Kimura, Y. Nambu. Single-photon Interference over 150 km transmission using silica-based integrated-optic interferometers for quantum cryptography[J]. *Japan J. Appl. Phys.*, 2004, **43**(9): 1217~1219
- 12 Han Baobin, Pei Changxing, Chen Nan *et al.*. Analysis of the effect of polarization mode dispersion on QKD[J]. *J. Xidian University*, 2008, **35**(5): 830~833
- 韩宝彬, 裴昌幸, 陈南等. 偏振模色散对量子密钥分发影响分析[J]. 西安电子科技大学学报(自然科学版), 2008, **35**(5): 830~833
- 13 A. Muller, T. Herzog, B. Huttner *et al.*. "Plug and play" systems for quantum cryptography [J]. *Appl. Phys. Lett.*, 1997, **70**(7): 793~795
- 14 Dirk Bouwmeester, Artur Ekert, Anton Zeilinger. The Physics of Quantum Information[M]. Germany. Springer-Verlag Berlin Heidelberg, 2000. 3~7
- 15 Su Yang, Wang Jiangping, Li Yuquan. Analysis of directionality for spatial electromagnetic field measurement based on Faraday effect[J]. *Acta Optica Sinica*, 2008, **28**(4): 705~709
- 苏洋, 王江平, 李玉权. 基于法拉第效应的空间电磁场测量的方向性研究[J]. 光学学报, 2008, **28**(4): 705~709
- 16 Zhou Yuan, Li Yanqiu. Optimization of topside antireflective coatings for hyper numerical aperture lithography [J]. *Acta Optica Sinica*, 2008, **28**(2): 337~343
- 周远, 李艳秋. 高数值孔径光刻成像中顶层抗反膜的优化[J]. 光学学报, 2008, **28**(2): 337~343