

文章编号: 1001-3806(2015)06-0756-05

量子密钥分配系统中非线性偏振耦合的研究

董颖娣^{1,2}, 彭进业^{1*}

(1. 西北工业大学 电子信息学院, 西安 710072; 2. 西安建筑科技大学 信息与控制工程学院, 西安 710055)

摘要: 受传输光纤非线性偏振影响, 量子密钥分配系统本振光与信号光耦合率下降, 使形成偏振复用信号的抖动增强, 系统的稳定性和安全性下降。为了提高量子光学中偏振编码技术的性能, 经过理论分析和数值模拟, 给出可操作性的实验方案, 解决了光纤非线性偏振耦合导致的偏振抖动问题。结果表明, 在同等条件下, 以分光检测结果反馈控制本振光和信号光的非线性偏振耦合率, 可增强偏振复用信号的稳定性, 将系统传输容量提高 61%。该结果有利于偏振编码技术在量子密钥分配系统的实际应用。

关键词: 量子光学; 量子密钥分配; 反馈控制; 偏振编码; 非线性偏振; 偏振抖动

中图分类号: O431.2 **文献标志码:** A **doi:**10.7510/jgjs.issn.1001-3806.2015.06.005

Investigation on nonlinear polarization coupling in quantum key distribution

DONG Yingdi^{1,2}, PENG Jinye¹

(1. School of Electronics and Information, Northwestern Polytechnical University, Xi'an 710072, China; 2. School of Information and Control Engineering, Xi'an University of Architecture and Technology, Xi'an 710055, China)

Abstract: Because of the effect of nonlinear polarization of transmission fiber, coupling ratio between local oscillator and quantum signal in a quantum key distribution system is decreased, signal jitters which leads to polarization multiplexing is increased, and security and stability of the system are decreased. To enhance technical performance of polarization encoding of quantum optics, after theoretical analysis and numerical simulation, operational experiment scheme was proposed to solve the polarization jitters caused by nonlinear polarization coupling of fiber. The results show that signal stability of polarization multiplexing enhances and transmission capacity of quantum key distribution increases to 61% by using feedback of spectral test results to control fiber nonlinear polarization coupling ratio between local oscillator and quantum signal. The research is helpful for practical application of polarization coding technology in quantum key distribution.

Key words: quantum optics; quantum key distribution; feedback control; polarization encode; nonlinear polarization; polarization jitter

引言

自 1984 年量子密钥分发协议的提出及 1992 年量子密钥分发演示实验成功^[1-2]以来, 量子密钥分发系统已经从实验研究发展到商业应用^[3]阶段, 其相关的技术也相继成熟, 但相位补偿技术和偏振控制技术^[4]仍然是影响密钥分发系统性能的关键。

在量子密钥系统中, 量子态以两个垂直的线偏振模的形式在光纤中传输, 光纤传输性能影响系统的稳定性和安全性^[5-7]。1986 年, WINFUL^[8]指出了由于非线性耦合, 将导致连续光偏振不稳定。MARCUSE 等人

研究了具有随机双折射的非线性偏振模色散, 并将非线性耦合薛定谔方程转换为马尔科夫偏振模色散方程^[9-10]。量子密钥系统中两偏振模耦合率下降即非线性偏振旋转会引起量子态偏振度随机抖动^[11], 从而使稳定的量子密钥分发变得困难, 限制了偏振编码方案在量子保密通信中的应用和发展, 以非线性耦合薛定谔方程分析两偏振模耦合率问题, 并没有开展研究和讨论。本文中分析了非线性偏振耦合对连续变量量子密钥分发 (quantum key distribution, QKD) 系统的影响, 并提出了以非线性偏振耦合反馈控制技术改善系统性能, 并给出了实验方案。

作者以非线性薛定谔方程阐述了光纤非线性偏振耦合; 在非线形偏振耦合条件下分析连续变量量子密钥分配系统中的性能; 采用香农信息论分析了合法通信双方之间的互信息; 给出了非线性偏振耦合反馈的控制理论算法和实验方案。

作者简介: 董颖娣 (1978-), 女, 博士研究生, 讲师, 主要研究方向为量子保密通信、光传输理论。

* 通讯联系人。E-mail: jinyepeng@nwpu.edu.cn

收稿日期: 2014-10-11; 收到修改稿日期: 2014-11-20

1 原理和模型

近年来,量子密钥分配系统向高速化、实用化方向发展,对于速率在 100Gbit/s 以上的量子密钥分配系统,偏振复用^[12]是系统关键。由于非线性偏振耦合使两个偏振方向独立的调制信号偏振复用后抖动增加,非线性偏振耦合过程采用光纤的非线性薛定谔方程^[13]描述:

$$\frac{\partial A}{\partial z} + \frac{i}{2} \frac{\beta}{T_0} \frac{\partial^2}{\partial \tau_1^2} + \frac{\alpha}{2} A = i\gamma AG \quad (1)$$

式中, A 为复振幅, z 为传输距离, β 为传输常数, T_0 为脉冲宽度, τ_1 为传输时间, α 为光纤损耗系数, γ 为光纤非线性系数, G 为 2×2 耦合矩阵, 其决定光纤内的非线性旋转, 计算公式如下所示:

$$G = \begin{bmatrix} |A_x|^2 + \frac{2}{3}|A_y|^2 & \frac{1}{3}|A_x||A_y|e^{-i2\Delta\varphi} \\ \frac{1}{3}|A_x||A_y|e^{-i2\Delta\varphi} & |A_x|^2 + \frac{2}{3}|A_y|^2 \end{bmatrix} \quad (2)$$

式中, A_x, A_y 分别为量子信号和本振信号的复振幅, $\Delta\varphi$ 为两者相位差。在量子密钥分配系统中, 两路参与信号是不断变化的, 当本振信号与量子信号由于非线性偏振旋转发生变化时, 即造成偏振复用信号抖动增加, 从而影响使密钥分发系统的传输性能下降。

1.1 量子密钥系统的非线性偏振旋转分析

量子密钥分发系统偏振复用过程如图 1 所示。量子密钥系统的两路信号, 量子信号和本振信号, 在进入光纤前进行偏振复用, 形成偏振态垂直的复用信号, 在普通低双折射的单模光纤中, 只考虑非线性偏振效应而忽略本征色散影响(假定本征色散已经被补偿)时, 光纤中的圆偏振态将保持不变, 仅产生相移。

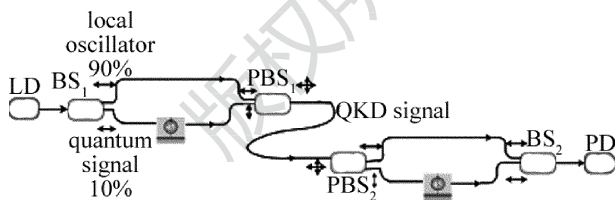


Fig. 1 Principle scheme of polarization multiplexing in a quantum key distribution system (LD: laser device; PBS: polarization beam splitter; BS: beam splitter; PD: pilot detector)

在偏振分束器 PBS_1 处, 相互垂直的线偏振光与圆偏振态之间的关系为:

$$\begin{cases} \dot{A}_+(\tau, z) = \frac{1}{\sqrt{2}}[\dot{S}(\tau, z) + i\dot{L}(\tau, z)] \\ \dot{A}_-(\tau, z) = \frac{1}{\sqrt{2}}[\dot{S}(\tau, z) - i\dot{L}(\tau, z)] \end{cases} \quad (3)$$

式中, $\dot{A}_+(\tau, z), \dot{A}_-(\tau, z)$ 分别表示两个圆偏振光的复振幅向量, $\dot{S}(\tau, z), \dot{L}(\tau, z)$ 分别表示量子密钥分配系

统的线偏振态的信号光和本振光。圆偏振态传输距离至 PBS_2 处, 其偏振态保持不变, 其非线性偏振旋转产生复振幅相位与光纤非线性之间关系^[14]可用下式来描述:

$$\begin{cases} A_+(\tau, z) = \frac{2}{3}\gamma[|T_+(\tau)|^2 + 2|T_-(\tau)|^2]z + A_{0+}(\tau) \\ A_-(\tau, z) = \frac{2}{3}\gamma[2|T_+(\tau)|^2 - |T_-(\tau)|^2]z + A_{0-}(\tau) \end{cases} \quad (4)$$

式中, $|T_+(\tau)|, |T_-(\tau)|$ 分别为 A_+ 和 A_- 的随时间变化的幅度函数。根据圆偏振与线形偏振之间的关系, 可以推出本振信号 $\dot{L}(\tau, z)$ 与量子信号 $\dot{S}(\tau, z)$ 传输至 PBS_2 处量子偏振态与复振幅函数之间的关系为:

$$\begin{cases} \dot{L}(\tau, z) = \frac{1}{\sqrt{2}}[\dot{A}_+(\tau, z) + i\dot{A}_-(\tau, z)] \\ \dot{S}(\tau, z) = \frac{-i}{\sqrt{2}}[\dot{A}_+(\tau, z) - i\dot{A}_-(\tau, z)] \end{cases} \quad (5)$$

经过推导后, 在 PBS_2 信号与 PBS_1 处信号之间的关系用偏振矩阵描述, 如下式所示:

$$\begin{bmatrix} \dot{L}(\tau, z) \\ \dot{S}(\tau, z) \end{bmatrix} = \exp\left[i\gamma z(S_0^2 + L_0^2) - \frac{\alpha z}{2}\right] \times \begin{bmatrix} \cos\theta(\tau) & \sin\theta(\tau) \\ -\sin\theta(\tau) & \cos\theta(\tau) \end{bmatrix} \begin{bmatrix} \dot{L}(\tau, 0) \\ \dot{S}(\tau, 0) \end{bmatrix} \quad (6)$$

式中, $\theta(\tau) = \frac{2}{3}\gamma Z_{\text{eff}} L(\tau) S(\tau) \sin\Delta\varphi_0$ 为系统非线性偏振旋转使本振光和信号光产生的旋转角, $Z_{\text{eff}} = (1 - e^{-\alpha})/\alpha$ 为光纤的有效长度, $\Delta\varphi_0$ 为两线性偏振光的初始相位, 矩阵 $\begin{bmatrix} \cos\theta(\tau) & \sin\theta(\tau) \\ -\sin\theta(\tau) & \cos\theta(\tau) \end{bmatrix}$ 为非线性偏振旋转引入的偏振矩阵。据此可知, 由于光纤的非线性效应使量子密钥分配系统量子偏振态旋转, 旋转角 $\theta(\tau)$ 与光纤的非线性效应、线偏振光的初始相位、光纤的有效长度等因素有关。

1.2 量子密钥系统的非线性偏振旋转分析

量子密钥分配系统偏振复用信号经过光纤长距离传输后, 因光纤非线性作用, 其偏振方向与分束器的偏振方向发生分离, 如图 2 所示。

由于光纤的非线性效应影响, 本振光偏振态与水平轴产生了角度为 $\theta(\tau)$ 的偏转。根据马吕斯定律, 通过偏振分束器后, 本振光在水平方向的强度分量为 $I_{10} \times \cos^2\theta(\tau)$, 信号光在垂直方向的偏振分量为 $I_{0s} \sin^2\theta(\tau)$ 。根据偏振失配原理, 本振光在垂直方向的分量大小即为引起系统误比特率的附加噪声。当信源符号为 X 、输出 Y 为高斯分布时, 通信双方之间互信息量可用香农定理描述。在此定义带宽 $B = 1\text{Mbit}$, σ_x^2/n_0^2 为

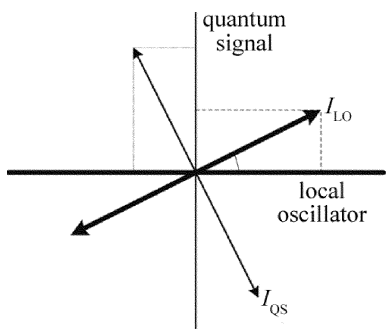


Fig. 2 Sketch diagram of nonlinear polarization after rotating (I_{LO} : optical field of local oscillator; I_{QS} : optical field of quantum signal)

量子信号的信噪比, σ_x^2 和 n_0^2 分别量子信号及高斯噪声的概率密度分布函数方差。当非线性偏振旋转角为 $\theta(\tau)$ 时, 信源分布函数为 $X-N(0, \sigma_x^2 \cos^2 \theta(\tau))$, 噪声分布函数为 $Y-N(0, n_0^2 (1 + \sin^2 \theta(\tau)))$, 由此可知传输系统的非线性偏振旋转后密钥分配系统信息容量为:

$$C = \frac{1}{2} \log_2 \left\{ 1 + \frac{\sigma_x^2}{n_0^2} \frac{\cos^2 \theta(\tau)}{1 + \sin^2 \theta(\tau)} \right\} \quad (7)$$

由于非线性偏转旋转角 $\theta(\tau)$ 使系统互信息量下降程度如图 3 所示。

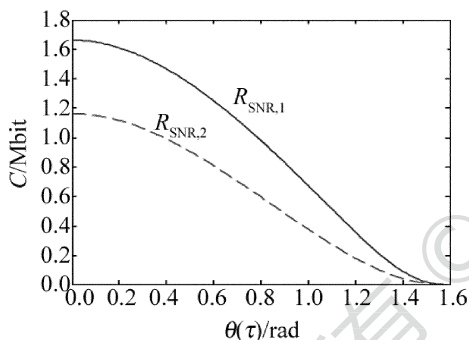


Fig. 3 Relationship between nonlinear polarization rotating angle $\theta(\tau)$ and transmission capacity C

在此设计传输光纤长度为 20km 条件下, 光纤非线性系数为 2.2/km、损耗系数为 0.2dB/km 时, 本振光与信号光的初始相位差 $\pi/2$ 、本振光与信号光比值为 9:1、信号服从均值为 0、方差为 20 的高斯分布, 量子密钥分配系统的信道传输率与非线性偏振旋转角之间关系如图 3 所示, 信噪比 1 ($R_{SNR,1}$) 设置为 9, 信噪比 2 ($R_{SNR,2}$) 设置为 4, 由图 3 可知, 随着非线性偏振旋转角 $\theta(\tau)$ 逐渐增加, 传输信道的信息容量 C 下降, 当非线性偏振旋转角增至 1.58 左右时, 传输容量下降为 0。

由此可见, 在量子密钥分配系统由于非线性偏振旋转角增加了信道的偏振抖动程度, 从而引起量子密钥系统信息容量下降; 抖动越剧烈, 系统传输效率越低, 这一问题成为制约量子密钥系统稳定工作的瓶颈。

2 非线性偏振耦合反馈控制技术方

为了减小非线性偏振耦合对量子密钥信号的影响, 本文中提出了反馈控制的方法, 以最大似然估计法计算出非线性偏振旋转角均值, 并根据均值对系统的非线性偏振旋转角进行修正, 对比同等条件下修正后系统传输容量; 并给出非线性偏振耦合补偿技术的实验方案。

2.1 非线性偏振耦合反馈控制的理论分析

以最大似然估计法计算非线性偏振耦合的均值 $\langle \theta(\tau) \rangle$:

$$\langle \theta(\tau) \rangle = \frac{1}{m} \sum_{\tau=1}^m \left[\frac{2}{3} \gamma Z_{\text{eff}} L(\tau) S(\tau) \sin \Delta \varphi_0(\tau) \right] \quad (8)$$

其补偿角大小 $\Delta \theta(\tau)$ 为:

$$\Delta \theta(\tau) = | \theta(\tau) - \langle \theta(\tau) \rangle | \quad (9)$$

式中, m 采样时间的极值, τ 为系统采样时间内采样参量。经过反馈补偿后系统接收端偏振控制器的传输矩阵可以描述为:

$$\mathbf{U} = \begin{bmatrix} \cos \Delta \theta(\tau) & \sin \Delta \theta(\tau) \\ -\sin \Delta \theta(\tau) & \cos \Delta \theta(\tau) \end{bmatrix} \quad (10)$$

接收端量子偏振态为:

$$\begin{bmatrix} \dot{\mathbf{L}}(\tau, z) \\ \dot{\mathbf{S}}(\tau, z) \end{bmatrix} = \exp \left[i \gamma z (S_0^2 + L_0^2) - \frac{\alpha z}{2} \right] \times \begin{bmatrix} \cos \Delta \theta(\tau) & \sin \Delta \theta(\tau) \\ -\sin \Delta \theta(\tau) & \cos \Delta \theta(\tau) \end{bmatrix} \begin{bmatrix} \dot{\mathbf{L}}(\tau, 0) \\ \dot{\mathbf{S}}(\tau, 0) \end{bmatrix} \quad (11)$$

由 (9) 式可知, 通过反馈补偿后量子密钥分配系统的信息容量为:

$$C_1 = \frac{1}{2} \log_2 \left\{ 1 + \frac{\sigma_x^2}{n_0^2} \frac{\cos^2 \Delta \theta(\tau)}{1 + \sin^2 \Delta \theta(\tau)} \right\} \quad (12)$$

与图 3 相同条件下, 仿真结果如图 4 所示, 经过反馈补偿后, 非线性偏振耦合值变化范围逐渐缩小至 0~0.8, 说明量子密钥分配系统中量子态的抖动幅值下降, 信道传输容量变化量逐渐变小, 以信噪比 1 为例, 经过非线性偏振反馈补偿后, 随着修正后的非线性

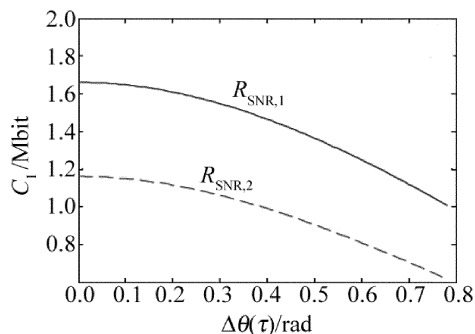


Fig. 4 Relationship between nonlinear polarization rotating angle $\Delta \theta(\tau)$ and transmission capacity C_1 after amendment

偏振旋转角 $\Delta\theta(\tau)$ 增加, 传输容量 C_1 由 1.62 下降至 1.00, 下降的抖动程度小于没有补偿的系统的传输性能, 且系统的传输容量比没有进行反馈补偿条件下提高了 61%。

2.2 非线性偏振反馈矫正的实验方案分析

量子密钥系统非线性偏振反馈控制如图 5 所示, 其中反馈控制部分用分束器将本振光按照 50:50 比例分束, 经探测器转化为电流, 计算得到其幅值大小为 $\frac{1}{2}I_{10}\sin^2\theta(\tau)$ (幅值通过计算的机采样获取), 计算采样点的均值, 将计算均值作为矫正依据, 对系统的非线性偏振耦合偏振角进行及时矫正, 以改善系统的稳定性。

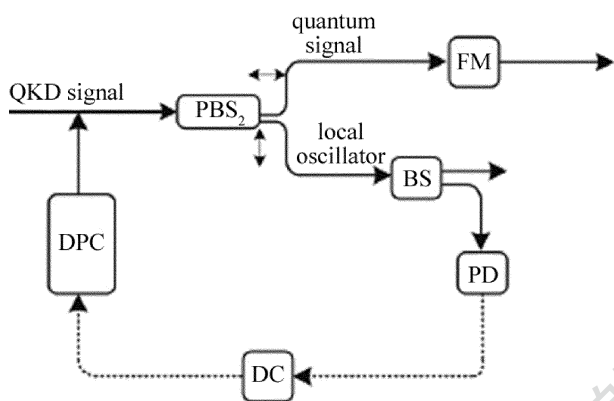


Fig. 5 Sketch diagram of feedback control of nonlinear polarization in quantum key distribution (FM: Faraday mirror; DC: dynamic controller; DPC: dynamic polarization controller)

反馈控制的具体实施过程通过以下两个阶段完成。

2.2.1 分光检测阶段 量子密钥分发的接收方将量子信号通过偏振分束器, 根据光的偏振理论及偏振耦合器的性质, 如果偏振无漂移, 那么本振光将会和信号光完全分开。在存在偏振漂移的情况下, 本振光会泄露一部分光到信号光端, 使得本振光自身的能量降低, 通过分出一部分本振光来进行检测, 可以得知偏振漂移程度。在偏振匹配的情况下, 本振光的强度达到最大。此时即为无偏振的状态。在此电流检测之前需要直流转换器将其转化为直流信号, 并将其放大, 以保证检测准确性。

2.2.2 非线性偏振矫正阶段 反馈控制电路将输出的直流电压反馈给接收方的动态偏振控制器内的单片机, 单片机对反馈电压进行采样, 并通过下述反馈控制算法来持续调节动态控制器, 使得直流反馈电压最大。

动态控制器^[15]通过改变其内部的 4 个光纤挤压器上的电压 V_1, V_2, V_3, V_4 对偏振复用信号的偏振态进行控制, 电压调节范围从 $-12V$ 到 $+12V$ 之间。光的偏振态用邦加球上的点来描述, 斯托克斯参量 $S_1, S_2,$

S_3 对应着邦加球相应的坐标轴。倘若改变电压 V_1 或 V_3 , 则偏振态会在邦加球上以 S_1 为中心转动; 改变电压 V_2 或 V_4 , 则偏振态会在邦加球上以 S_2 为中心转动。基于以上讨论, 偏振反馈算法的具体流程如下: (1) 动态偏振控制器的单片机对直流反馈电压采样并记录数据; (2) 4 个控制电压都置为 0V, 选择第 1 个控制电压; (3) 根据均值电流大小增加电压, 此时偏振态会在邦加球上绕着对的矢量轴做顺时针转动, 采集直流反馈电压, 如果电压已经达到了 $+12V$, 进入步骤 (7); (4) 根据均值电流大小增加电压, 此时偏振态会在邦加球上绕着对应的量轴做顺时针转动, 采集直流反馈电压, 如果电压已经达到了 $+12V$, 进入步骤 (7); (5) 根据均值电流大小减小电压, 此时偏振态会在邦加球上绕着对应矢量轴做逆时针转动, 采集直流反馈电压, 如果电压已经达到了 $-12V$, 进入步骤 (7); (6) 如果直流反馈电压增大, 那么继续步骤 (5) 否则, 进入步骤 (7); (7) 选择下一个电压控制器, 继续步骤 (3)。

可以将直流反馈电压一直保持在一个最大值的状态。根据以上分析, 这时对应的本振光的强度最强, 本振光没有发生泄露, 偏振复用信号与偏振分束器之间没有偏振旋转, 信号光与本振光之间的非线性偏振效应可以得到相应的改善。

3 结论

偏振编码方案在量子保密通信中有着广泛的应用, 非线性偏振耦合将引起偏振复用信号的偏振抖动增加, 从而降低了量子密钥分配系统的安全性和稳定性。量子密钥系统非线性偏振耦合导致偏振复用信道抖动增加, 将偏振控制的思想运用于量子密钥分发系统的非线性偏振耦合, 通过对非线性偏振偏移量监测提供反馈电压, 补偿了由于偏振随机抖动引起的偏振漂移。数值仿真表明, 系统经过反馈后, 量子态偏振抖动度下降, 量子密钥分配系统的传输效率增强, 系统稳定性得以改善, 从而实现了基于偏振编码的长距离高稳定性的量子密钥分发实验。

参 考 文 献

[1] BENNETT C H, BRASSARD G. Quantum cryptography: public key distribution and coin tossing[C]//Computer Systems and Signal Processing, Proceedings of IEEE International Conference and Signal Processing. New York, USA: IEEE, 1984: 175-179.
 [2] EKERT A K. Quantum cryptography based on bell's theorem[J]. Physical Review Letters, 1991, 67(6): 661-663.
 [3] JOUGUET P, KUNZ-JACQUES S, LEVERRIER A, et al. Experimental demonstration of long distance continuous-variable quantum key distribution [J]. Nature Photonics, 2013, 7(5): 378-381.
 [4] CHEN J, LI Y, WU G, et al. Stable quantum key distribution with polarization control[J]. Physica Sinica, 2007, 56(9): 5243-5246

- (in Chinese).
- [5] JOUGUET P, KUNZ-JACQUES S, DIAMANTI E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution[J]. *Physical Review*, 2013, A87(9): 2313-2317.
- [6] LEVERRIER A, GRANGIER P. Long distance quantum key distribution with continuous variables[M]. Madrid, Spain: *Theory of Quantum Computation, Communication, and Cryptography*, 2014: 143-152.
- [7] HAN B B, PEI Ch X, CHEN N, *et al.* Analysis of the effect of polarization mode dispersion on QKD[J]. *Journal of Xidian University*, 2008, 35(5): 830-833 (in Chinese).
- [8] WINFUL H G. Polarization instabilities in birefringent nonlinear media: application to fiber-optic devices[J]. *Optics Letters*, 1986, 11(1): 33-35.
- [9] MARCUSE D, MANYUK C R, WAI P K A. Application of the Manakov-PMD equation to studies of signal propagation in optical fibers with randomly varying birefringence [J]. *IEEE Journal of Lightwave Technology*, 1997, 15(9): 1735-1746.
- [10] MARCUSE D. Derivation of analytical expressions for the bit-error probability in lightwave systems with optical amplifiers[J]. *IEEE Journal of Lightwave Technology*, 1990, 8(12): 1816-1823.
- [11] WANG J, MIAO H L. Compensation of polarization mode dispersion by in-line synchronous modulation [J]. *Laser Technology*, 2002, 26(3): 211-213 (in Chinese).
- [12] FOURSAD, CAI Y, CAI J X, *et al.* Coherent 40Gbit/s transmission with high spectral efficiency over transpacific distance [C]// *OSA Library Resource Center*. Los Angeles, USA: *OSA Library Resource Center*, 2011: 657-672.
- [13] AGRAWAL G. Applications on nonlinear fiber optics [M]. 2nd ed. Pittsburgh, USA: *Academic Press*, 2013: 468-470.
- [14] LIU L L, WU Ch Q. Investigation on decreasing of DOP in PM systems caused by nonlinear polarization coupling in fibers[J]. *Journal of Beijing Jiaotong University*, 2013, 37(6): 118-201 (in Chinese).
- [15] FANG J. Continuous-variable quantum key distribution: optical system design and improved schemes[D]. Shanghai: *Shanghai Jiaotong University*, 2014: 48-50 (in Chinese).