

基于 DWDM 的量子经典融合通信系统噪声处理技术

冉攀¹, 胡敏¹, 郭邦红^{2*}

(1. 华南师范大学 信息光电子科技学院, 广州 510006; 2. 深圳大学 计算机与软件学院, 广东 深圳 518060)

摘要:为提高系统容量和光纤的利用率,降低网络建设成本,提出了基于密集波分复用(DWDM)技术的量子经典融合通信系统。为消除或降低系统中经典信号对量子信号的影响,设计一种非等间隔波长选取方法和采用光隔离器分别处理融合系统中的四波混频噪声和喇曼散射噪声。仿真结果表明:经过噪声处理后,量子经典融合通信系统中的因四波混频和喇曼散射噪声导致的量子误码率(QBER)下降约 33.3%。

关键词:量子密钥分发;密集波分复用;量子经典融合通信;四波混频;喇曼散射

中图分类号:TN256 **文献标志码:**A **文章编号:**1002-5561(2020)08-0022-05

DOI:10.13921/j.cnki.issn1002-5561.2020.08.006

开放科学(资源服务)标识码(OSID):



Noise processing technology of quantum and classical fusion communication system based on DWDM

RAN Pan¹, HU Min¹, GUO Banghong^{2*}

(1. School of Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou 510006, China;

2. College of Computer Science and Software Engineering, Shenzhen University, Shenzhen Guangdong 518060, China)

Abstract: To improve the system capacity, the utilization rate of optical fiber and reduce the cost of network construction, this paper proposes a quantum and classical fusion communication system based on dense wavelength division multiplexing (DWDM) technology. To eliminate or reduce the impact of classical signal on quantum signal in the system, it designs an unequal wavelength allocation method and an optical isolator are to deal with the four wave mixing noise and Raman scattering noise of the fusion system respectively. The simulation results show that the quantum bit error rate (QBER) of the quantum and classical fusion communication system is reduced by 33.3% due to four wave mixing and Raman scattering noise after noise processing.

Key words: quantum key distribution; dense wavelength division multiplexing; quantum classical fusion communication; four wave mixing; Raman scattering

0 引言

量子算法及量子计算的快速发展对以非对称加密(RSA)算法为代表的现行主流公钥密码机制构成了巨大的威胁。一旦量子计算取得突破,现有的密码体

收稿日期:2020-03-16。

基金项目:国家自然科学基金(61572203)资助;广东省重点领域研发计划(2018B030325002)资助;瞬态光学与光子技术国家重点实验室开放基金(SKLSST201602)资助。

作者简介:冉攀(1991—),男,硕士研究生,现就读于华南师范大学信息光电子科技学院光学专业,参与国家自然科学基金项目1项、广东省重点领域研发计划项目1项,主要研究方向为量子信息与光通信技术、量子保密通信与经典通信融合网络。

*通信作者:郭邦红(E-mail: guobangh@163.com)。



系将形同虚设。量子密钥分发(QKD)技术的出现为信息安全与通信保密提供了一种新的解决方案。QKD^[1]是基于量子不可克隆定理和海森堡测不准原理等物理定理保证安全性的密钥分发方法,结合一次一密(OTP)体制,提供了理论上的绝对安全性。

自首个 QKD 协议 BB84^[2]被提出以来,QKD 在理论、实验等方面取得了巨大的进步。尤其是基于光纤量子信道的 QKD 系统,已经有部分公司可以提供商用产品。同时,将光子作为信息载体的经典光网络技术也取得了重大发展,采用密集波分复用(DWDM)技术实现量子与经典信号在同一光纤中同时传输,可以提高系统容量和光纤利用率,并降低网络建设成本,是量子通信系统实际应用的关键技术^[3]。然而,在传输过

程中,主要由四波混频和喇曼散射 2 种效应产生的经典信号噪声会严重干扰量子信号,如何降低甚至消除噪声影响是亟待解决的问题。文献[3]采用较大的波长间隔(经典通信波长为 1550 nm,量子通信波长为 1310 nm)减小四波混频噪声的影响,但是 O 波段的信道衰减(0.33 dB/km)比 C 波段(0.2 dB/km)大,将导致 QKD 的安全距离和成码率下降。因此,本文提出采用非等间隔波长选取方法和光隔离器(OI)分别处理这 2 种噪声。

1 基于 DWDM 的量子经典融合通信系统

1.1 融合通信系统方案

目前,在 QKD 系统应用中,为避免量子信号受经典信号的干扰,通常使用暗光纤(已铺设但未使用)的商用光纤进行信号传输,即量子信号独占光纤资源,但是该方法会导致光纤利用率低和网络建设成本增加。为此,本文提出一种基于 DWDM 的量子经典融合通信系统,系统方案如图 1 所示。

融合通信系统包括脉冲激光源(PLS)、随机数发生器(RNG)、相位调制器(PM)、电压检测装置(VC)、光衰减器(VOA)、OI、窄带滤波器(NBF)、非平衡马赫-曾德尔干涉仪(MZI)和雪崩光电二极管(APD)。PLS 根据 RNG 的设置,产生特定条件的量子信号和经典信号通过左侧 DWDM 复用传输到光网络,在脉冲信号到达右侧 DWDM 进行解复用,经过解复用的量子信号通过 OI 后进行滤波,量子信号由非平衡 MZI 接收,经典信号由经典信号收发器接收。

量子信号的编解码过程如下:在量子信号发送端,PM 将脉冲相位随机调制为 0 或者 π 。经过光网络传输后,在量子信号接收端组成非平衡 MZI 的左侧分束器(BS)等概率将量子信号脉冲分为 2 路,MZI 上、下臂之间的光脉冲时延与 PLS 的重复周期相等。2 路

相邻脉冲在非平衡 MZI 右侧的 BS 合束发生干涉。根据 2 路相邻量子信号脉冲分别由 PM 施加的相位差是 0 或 $\pm\pi$,APD1 或 APD2 发生响应,通信双方完成信息交换。另外,经典信号发送端的 VOA 用于降低光功率,减小其对量子信号的干扰;在量子信号接收端前的 NBF 用于提高隔离度,滤除带外噪声。

图 1 中,经典信号是双向的,经典信号包括数据信号和同步信号等;量子信号是单向传输的,即量子信号从发送端到接收端,量子信号发送端与量子信号接收端组成 QKD 系统。本方案采用差分相移(DPS)协议^[4],同时也可以采用其它的量子编码系统,如法拉第-迈克尔逊干涉仪方案等。

1.2 系统安全性

原始的 BB84 协议要求 Alice 使用理想的单光子源进行量子态制备。当前单光子技术尚不成熟,实际应用中常使用强衰减脉冲激光——弱相干态脉冲(WCP)。然而,WCP 有一定概率包含多光子,使得 BB84 协议易受光子数分束攻击^[5],限制了安全通信距离和密钥产生率。因此,本文采用基于 BB84 诱骗态协议,通过在量子信号发送端发射的信号光中随机掺杂不同强度的诱骗光来监测信道和窃听者对光脉冲的影响,从而提高系统的安全码率。真空态+弱诱骗态^[6,7]协议方法是发射 3 种不同平均光子数的光脉冲(分别称为信号态、诱骗态和真空态),并且每次发送哪种脉冲是随机的,全部探测完成后再统计各不同平均光子数总的探测率,然后求出单光子探测率的下限 $Q_{1,\mu}^L$ 和误码率的上限 e_1^U ,结合 GLLP 公式^[8]可以得到基于 BB84 诱骗态协议下的安全码率公式:

$$R \geq q[-Q_{\mu}f(E_{\mu})H_2(E_{\mu}) + Q_{1,\mu}^L[1 - H_2(e_1^U)]] \quad (1)$$

其中, q 为协议效率, Q_{μ} 和 E_{μ} 分别为信号态的增益和误码率, μ 为信号脉冲的平均光子数, $f(E_{\mu})$ 为双边归

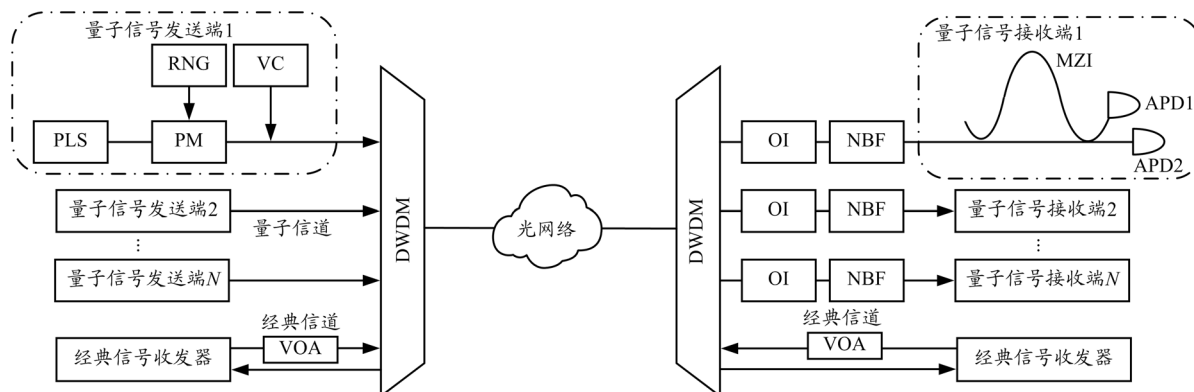


图 1 融合通信系统示意图

错效率, $H_2(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ 为二元香农熵函数。通过仿真得到安全码率与传输距离的对应关系如图 2 所示。可以看出,在不考虑探测器攻击的情况下,当传输距离超过 130 km 后,安全码率急剧下降。如果窃听者采用以相位重映射攻击为代表的探测器攻击方法,则安全码率将进一步降低。因此我们设计了电压检测装置对抗该攻击。

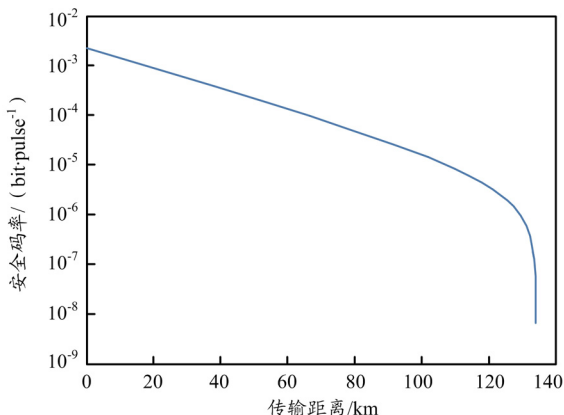


图 2 基于 BB84 诱骗态协议仿真结果

对于基于相位编码的 BB84 诱骗态协议,理论安全分析总是假设光源的加载相位为 $(0, \pi)$ 。在相位编码的 QKD 系统中,电压脉冲驱动信号控制 PM。驱动信号分为上升沿、稳定区和下降沿三部分,调制相位正比于加载到 PM 上的电压。

正常情况下量子信号在稳定区进行调相,加载相位 $(0, \pi)$ 。实际情况是窃听者可在信道上控制信号脉冲使得 PM 在驱动信号上升沿时进行调相,从而加载相位变为 $(0, \sigma)$,实现相位重映射攻击^[9],窃取信息。

为了克服相位重映射攻击,本文采用改进型差分相位编码,在 PM 的右端设置 VC(如图 1 所示)。当 VC 检测到脉冲电压和调制相位电压超过设定范围时,就可以发现有窃听者存在,只有当电压检测符合要求时,系统才编解码信息。这样就保证了光脉冲是在稳定区加载的相位而非脉冲上升沿或下降沿,从而进一步提高系统的安全性。

2 融合通信系统的噪声处理

2.1 四波混频噪声处理方法

四波混频^[10]源于 2 个或多个光场之间的相互作用和光纤的三阶非线性效应。在典型的 DWDM 系统中,信道是被等间隔分配在频率网络上,间隔为 50 GHz、100 GHz 或 200 GHz 等。由于周期性间隔,产生的新频率落在 DWDM 信道频率本身上或在 DWDM 系统使用

的频率之上或之下的其它网格频率上。当产生的新频率波与量子信道频率相同时,四波混频成为量子信号的带内噪声,无法用滤波器消除。

目前,量子经典融合通信系统中四波混频噪声处理方法有降低经典光功率^[10,12]、时频域滤波技术等^[13,13],但是这些方法有的受制于滤波器件或者由于噪声的特殊性,因此需要进一步研究以降低噪声干扰。本文提出非等间隔波长选取方法,找出能减小或者消除四波混频噪声的波长信道,以下面波长为例进行说明。 $\lambda_k, \lambda_{k+1} = \lambda_k + \Delta\lambda, \lambda_{k+2} = \lambda_k + \Delta 2\lambda, \lambda_{k+3} = \lambda_k + \Delta 3\lambda \dots$ 为符合国际电信联盟 (ITU-T) 波长标准, λ_k 与 $\lambda_{k+1}, \lambda_{k+3}$ 和 λ_{k+6} 产生的新频率光波长分别为 $\lambda_{k+2}, \lambda_{k+6}$ 和 $\lambda_{k+12}, \lambda_{k+1}$ 与 λ_{k+3} 和 λ_{k+6} 产生的新频率光波长分别为 λ_{k+5} 和 $\lambda_{k+11}, \lambda_{k+3}$ 与 λ_{k+6} 产生的新频率光波长为 λ_{k+9} 。由于 λ_{k+1} 与 λ_{k+3} 的间隔较大,产生的新频率光波 λ_{k+5} 相对较弱。故可以采用波长 $\lambda_k, \lambda_{k+1}, \lambda_{k+3}$ 和 λ_{k+10} 等作为信号波长,实验数据表明^[10],当经典信号波长大于 1550 nm 时对量子信道的影响更小。因此将 1550 nm 作为波段分界值,将量子信号规划在低于 1550 nm 波段,经典信号规划在高于 1550 nm 波段,如图 3 所示。

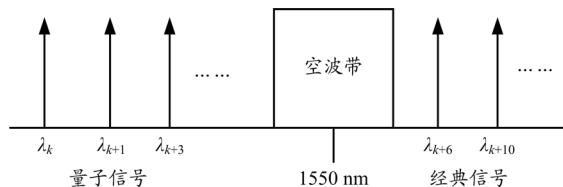


图 3 非等间隔信道波长规划示意图

2.2 喇曼散射噪声处理方法

当喇曼散射噪声^[10]的传播方向与激励信号(经典信号)同向传输时称为前向喇曼散射,与激励信号反向时称为后向喇曼散射。本文采用反向同传,即量子信号与经典信号的传播方向相反,因此需要考虑后向喇曼散射导致的噪声影响。于是,本文提出在融合通信系统中引入 OI,利用其单向性消除后向喇曼散射噪声,其原理如图 4 所示。

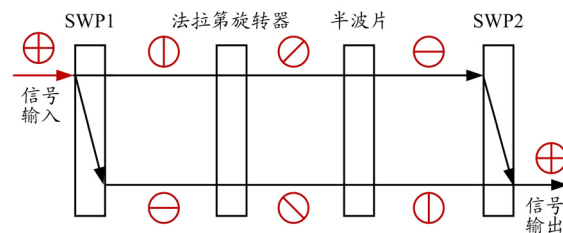


图 4 OI 正向输入示意图

当具有任意偏振态的入射光正向输入时首先通过空间分离偏振器(SWP1), SWP1 的作用是将入射光分解为 2 个正交偏振分量, 让垂直分量投射通过和水平分量折射通过。2 个分量通过法拉第旋转器后, 偏振态旋转 45° 。法拉第旋转器后面跟随一块半波片, 半波片的作用是将从左向右传播的光的偏振态顺时针旋转 45° , 将从右向左传播的光的偏振态逆时针旋转 45° , 因而法拉第旋转器与半波片的组合可以使垂直偏振光变为水平偏振光, 反之亦然。最后 2 个分量的光在输出端由 SWP2 合在一起输出, 保留有用信号(量子信号)。

当光信号反向输入时, 如图 5 所示, 半波片和法拉第旋转器的旋转方向正好相反, 当 2 个分量的光通过这 2 个器件时, 其旋转效果相互抵消, 偏振态维持不变, 在光纤输入端不能被 SWP 再组合在一起, 于是起到隔离作用, 从而消除后向喇曼散射。

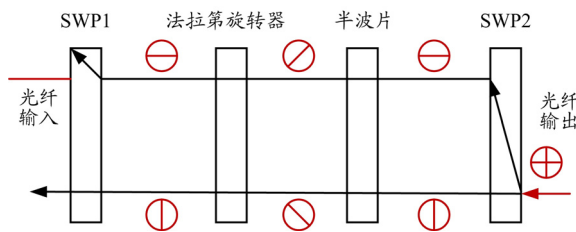


图 5 OI 反向输入示意图

3 数值仿真

3.1 仿真原理

为了评估本噪声处理方法对融合通信系统性能的影响, 本文对图 1 所示系统的量子误码率(QBER)进行了计算并仿真。探测器探测到的喇曼散射和四波混频噪声的光子数分别为^[14]:

$$D_{\text{ram}} = \frac{1}{2} \cdot \frac{P_{\text{ram}} \lambda_q}{hc} \tau_{\text{gate}} \eta_{\text{spd}} f_{\text{rep}} \cdot 10^{-0.1IL} \quad (8)$$

$$D_{\text{fwm}} = \frac{1}{2} \cdot \frac{P_{\text{fwm}} \lambda_q}{hc} \tau_{\text{gate}} \eta_{\text{spd}} f_{\text{rep}} \cdot 10^{-0.1IL} \quad (9)$$

其中, P_{ram} 为喇曼散射噪声功率, P_{fwm} 为四波混频噪声功率, λ_q 为信号光波长, c 为光速, τ_{gate} 为探测器的门宽, η_{spd} 为探测器的效率, f_{rep} 为系统的重复频率, IL 为系统光器件以及光纤引入的总插入损耗。为了更直观体现四波混频和喇曼散射噪声对系统性能的影响, 本文分别计算 2 种噪声带来的 QBER。QBER 作为错误检测数 F 和总检测数 $R+F$ 之间的比率, 其表达式为:

$$QBER = \frac{F}{R+F} \quad (10)$$

喇曼散射噪声和四波混频噪声带来的量子误码

率 $QBER_{\text{ram}}$ 和 $QBER_{\text{fwm}}$ 分别为:

$$QBER_{\text{ram}} = \frac{1}{2} \cdot \frac{q D_{\text{ram}}}{R_{\text{sift}} + 2q f_{\text{rep}} p_{\text{dark}} + q D_{\text{fwm}} + q D_{\text{ram}}} \quad (11)$$

$$QBER_{\text{fwm}} = \frac{1}{2} \cdot \frac{q D_{\text{fwm}}}{R_{\text{sift}} + 2q f_{\text{rep}} p_{\text{dark}} + q D_{\text{fwm}} + q D_{\text{ram}}} \quad (12)$$

其中, R_{sift} 为筛选码速率, q 为 DPS 的协议效率, p_{dark} 为探测器的暗计数率。本文以 1 个量子信道和 3 个经典信道为例, 就采用等间隔、非等间隔波长 2 种情况对四波混频产生的新频率光波长落到量子信道引起的 QBER 的噪声光子数进行仿真, 同时增加了 OI 隔离后向噪声, 主要仿真参数如表 1 所示。其中系统采用标准单模光纤, 取频率间隔为 100 GHz, OI 引入 0.2 dB 的插损, 得到四波混频噪声光子数仿真结果如图 6 所示, 喇曼噪声光子数仿真结果如图 7 所示。

表 1 主要仿真参数

参数名称	数值	参数名称	数值
量子通信波长	1549.32 nm	IL	8 dB
经典光功率	0 dBm	η_{spd}	10%
量子信道滤波器带宽	0.12 nm	f_{rep}	10 MHz
OI 插入损耗	0.2 dB	τ_{gate}	125 ps
光纤损耗系数	0.21 dB/km	—	—

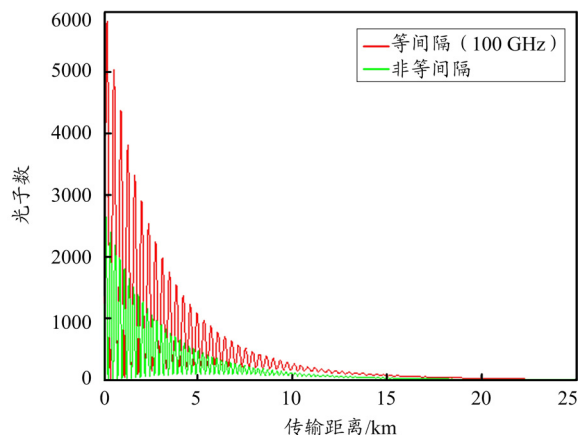


图 6 四波混频噪声光子数对比

3.2 仿真结果与讨论

从图 6 可以看出, 在传输距离一定的情况下, 量子接收端探测器在采用非等间隔波长划分方法探测到的光子数约为等间隔波长划分方法检测到的光子数的 1/2, 即非等间隔信道划分方法产生的四波混频噪声只占波长信道等间隔选取方法的噪声的 1/2, 明显降低了四波混频噪声光子对量子信号的干扰, 增加了安全通信距离。

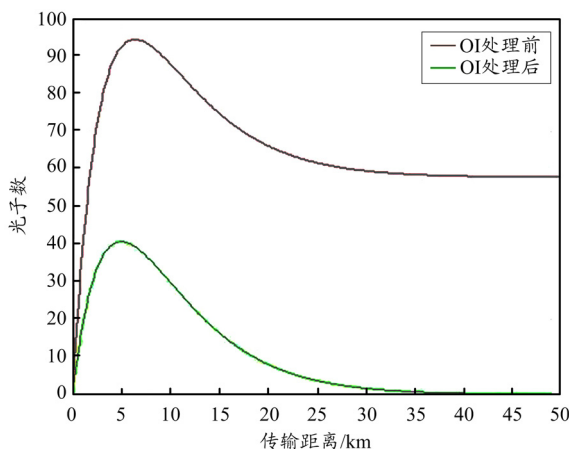


图7 喇曼散射噪声光子数对比

从图7可以看出,在传输距离为5 km时,消除的后向喇曼散射光子是经过OI处理后剩余光子的约1.4倍,大大减小了喇曼散射噪声。同时,对比图6和图7可以看出,在相同传输距离下,四波混频噪声对系统的干扰更大。

为了从整体上更直观地评估采用本方法进行噪声处理后系统性能的提升,本文对比了在噪声处理前和噪声处理后的QBER,结果如图8所示。可以看出,采用本方法进行噪声处理后,四波混频和喇曼散射噪声产生的QBER将降低约33.3%,显著提高了系统性能。

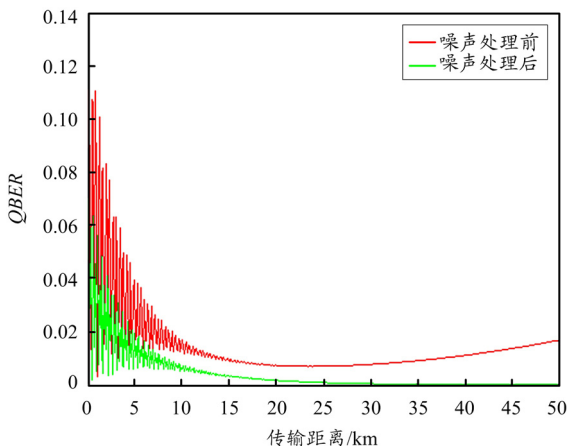


图8 噪声处理前后系统中QBER的对比情况

4 结束语

本文提出了基于DWDM的量子经典融合通信系统,量子信号和经典信号共用现有光纤基础设施,可以有效节约光纤资源和网络建设成本。同时,提出针对融合通信系统中出现的噪声处理方法;采用非等间隔波长划分方法可以有效降低四波混频产生的噪声

对量子信号的干扰;采用OI处理可以降低喇曼散射噪声,显著提高了系统性能。本文的设计对于加快推动量子经典融合通信商业化、产业化发展具有重要的参考价值。

参考文献:

- [1] GISIN N, RIBORDY G, TITTEL W, et al. Quantum cryptography[J]. Reviews of Modern Physics, 2002, 74(1): 145-195.
- [2] BENNETT C H, BRASSARD G. Quantum Cryptography: Public Key distribution and coin tossing [C]//Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, December 9-12, 1984, Bangalore, India. IEEE, 1984: 175-179.
- [3] MAO Y, WANG B X, ZHAO C, et al. Integrating quantum key distribution with classical communications in backbone fiber network[J]. Optics Express, 2018, 26(5): 6010-6020.
- [4] INOUE K, WAKS E, YAMAMOTO Y. Differential Phase Shift Quantum Key Distribution [J]. Physical Review Letters, 2002, 89(3): 037902-1-037902-3.
- [5] BRASSARD G, LÜTKENHAUS N, MOR T, et al. Limitations on practical quantum cryptography [J]. Physical Review Letters, 2000, 85(6): 1330-1333.
- [6] LO H K, MA X, CHEN K. Decoy State Quantum Key Distribution[J]. Physical Review Letters, 2005, 94(23): 230504-1-230504-4.
- [7] MA X, QI B, ZHAO Y, et al. Practical decoy state for quantum key distribution[J]. Physical Review A, 2005, 72(1): 012326-1-012326-15.
- [8] GOTTESMAN D, LO H-K, LUTKENHAUS N, et al. Security of quantum key distribution with imperfect devices[C]//International Symposium on Information Theory (ISIT), June 27-July 2, 2004, Chicago, USA. IEEE, 2004: 325-360.
- [9] XU F, QI B, LO H K. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system [J]. New Journal of Physics, 2010, 12(11): 113026-1-113026-14.
- [10] ERAERDS P, WALENTA N, LEGRE M, et al. Quantum key distribution and 1 Gbps data encryption over a single fibre [J]. New Journal of Physics, 2010, 12(6): 063027-1-063027-15.
- [11] PETERS N A, TOLIVER P, CHAPURAN T E, et al. Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments[J]. New Journal of Physics, 2009, 11(4): 045012-1-045012-17.
- [12] PATEL K A, DYNES J F, LUCAMARINI M, et al. Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks [J]. Applied Physics Letters, 2014, 104(5): 051123-1-051123-4.
- [13] MORA J, AMAYA W, RUIZ-ALBA A G, et al. Simultaneous transmission of 20 x2 WDM/SCM-QKD and 4 bidirectional classical channels over a PON[J]. Optics Express, 2012, 20(15): 16358-16365.
- [14] SUN Y, LU Y, NIU J, et al. Reduction of FWM noise in WDM-based QKD systems using interleaved and unequally spaced channels [J]. Chinese Optics Letters, 2016, 14(6): 060602-060607.