第 59 卷 第 5 期/2022 年 3 月/激光与光电子学进展 研究论文

激光与光电子学进展

波分复用量子密钥分发拉曼噪声分析及最佳波段选择算法

周晓东[1]，张松磊[1]，方晓明[1]，卞宇翔[2,3*]，冯宝[2,3]，刘志昊[4**]

[1]国网福建省电力有限公司信息通信分公司，福建 福州 350003；

[2]南京南瑞信息通信科技有限公司，江苏 南京 210003；

[3]南京南瑞国盾量子技术有限公司，江苏 南京 210003；

[4]东南大学计算机科学与工程学院，江苏 南京 211189

摘要 经典-量子信道复用技术旨在提升量子保密通信的信道利用率，但噪声串扰会严重制约量子信道的传输效率。基于对信道拉曼噪声干扰的分析，使用组合优化方法对信道分配策略进行优化，提出了一种适用于量子密钥分发(QKD)系统的最佳波段选择算法。所提波段选择算法基于噪声与信道相对位置间的相关联性，利用组合优化方法优化经典及量子信道的分配，从而得到最小化噪声的多波段复用方案。与传统双波段复用方案相比，所得最佳多波段复用方案可有效降低不同频段间经典光对量子光的干扰，从而提高信道传输的密钥率。

关键词 量子光学；量子通信；量子密钥分发；信道复用；波分复用

中图分类号 TP3 **文献标志码** A **doi**：10.3788/LOP202259.0527001

Raman Noise Analysis and Optimal Band Selection Algorithm for Wavelength Division Multiplexing Quantum Key Distribution

Zhou Xiaodong[1], Zhang Songlei[1], Fang Xiaoming[1], Bian Yuxiang[2,3*], Feng Bao[2,3], Liu Zhihao[4**]

[1]*Information and communication branch of State Grid Fujian Electic Power Co., Ltd., Fuzhou, Fujian* 350003, *China*;

[2]*Nanjing NARI Information & Communication Technology Co., Ltd., Nanjing, Jiangsu* 210003, *China*;

[3]*Nanjing NRGD Quantum Technology Co., Ltd., Nanjing, Jiangsu* 210003, *China*;

[4]*School of Computer Science and Engineering, Southeast University, Nanjing, Jiangsu* 211189, *China*

Abstract Although classical-quantum channel multiplexing technology attempts to improve the channel use of quantum secure communication, noise crosstalk severely limits the quantum channel transmission efficiency. A combined optimisation method is used to optimise the channel allocation strategy based on channel Raman noise interference analysis, and an optimal band selection algorithm suited for the quantum key distribution system is proposed. The allocation of classical and quantum channels is adjusted and optimised using the proposed combinatorial optimisation algorithm based on the correlation between the noise and channel relative position to obtain a multi-band multiplexing scheme that minimises noise. Compared with the traditional dual band multiplexing scheme, the optimal multi band multiplexing scheme can effectively reduce the interference of classical light to quantum light between different frequency bands, so as to improve the key rate of channel transmission.

Key words quantum optics; quantum communication; quantum key distribution; channel multiplexing; wavelength division multiplexing

收稿日期：2021-03-16；**修回日期**：2021-04-15；**录用日期**：2021-05-27

基金项目：国网福建省电力有限公司科技项目(52130M19000Y)

通信作者：*nrgd_lw@163.com；**liuzhtopic@163.com

1 引 言

量子密钥分发(QKD)技术是基于量子力学基础,利用量子态不可克隆原理和海森堡不确定性原理,从而协商出安全共享密钥的技术。随着量子通信的快速发展,由于较成熟的技术手段和光量子易制备、易传输的特点,基于光量子的QKD技术[1-3]的实用化逐渐趋于成熟,实现了超远程的安全通信。经过多年发展,QKD技术逐渐从实验阶段转向实用阶段[4],但实用化的量子通信网络面临许多技术障碍。在多用户量子通信网络的建设中,信道的低利用率会严重增加铺设和维护光纤的经济成本。因此,关于光纤QKD复用技术的研究是促进量子通信网络实用化的关键一环。

作为重要的国家基础设施,电力系统的安全关系国计民生。随着能源互联网的发展,电力系统对于数据传输的安全性与传输效率的要求日益提升。一方面,能源互联网对通信网络的开放性、互动性、智能化提出了更高要求;另一方面,这些数据的传输也正在经受多方面的安全考验。在这种背景下,国家电网公司自2016年起,在北京、江苏、安徽、上海、新疆等地建设了电力量子保密通信示范工程。然而,现有量子保密通信系统中,量子信道、协商信道和业务信道独立占用纤芯资源,存在量子信道利用率低、维护成本高等问题,迫切需要开展经典-量子信道复用技术的研究。经典的光路复用技术如波分复用(WDM)技术,可以很好地移植到经典-量子复用技术中。然而量子光[5]作为单光子或准单光子信号,能量极低,和能量相对很高的经典光复合传输时会受到很大的噪声影响。

现阶段,在离散变量QKD(DV-QKD)框架下解决经典-量子复用信道噪声问题的技术大致有3种:波段检测技术、主动避让技术及被动分波技术。波段检测技术是指通过对光路中的几种波段进行检测,主要检测不同波长下的光纤放大器(EFDA)自发辐射干扰和拉曼效应噪声程度,从而确定合适的信号传输波长的技术。主动避让技术是指主动采取系统的措施对经典光进行预处理或后处理,避开拉曼噪声和光线的非线性效应影响的技术。例如,通过降低经典光功率、对接收信号进行时域频域滤波等方式降低噪声,或者正交频分复用配合固有的滤波方式可以有效减少串扰,然而这种方式通常是造成密钥率低下的主要原因[6]。被动分波技术是指通过提前采取措施,将量子光和经典光进行有效分离的技术。例如,通过采取高隔离度的复用器加大经典光和量子光的波长差距,该方法可以有效滤除噪声,或者优化经典光的传输方向,减小信号反向传播中由于衰减产生的干扰。此外,采用连续可变QKD(CV-QKD)[7-8]或多模光纤复用[9-11]来减小拉曼噪声的影响也具有一定的可行性。

基于粗波分复用(CWDM)的QKD复用技术[12-14]很早就被人们研究,该技术利用量子信道和经典信道的较大波长间隔减少了由于拉曼噪声对量子信道的影响。但是CWDM-QKD有几个局限性:由于1300 nm波长处QKD的衰减严重,CWDM-QKD只能适应更短距离的传输;并且由于通道间的波长间隔较大,复用的波长数比较少。因此,CWDM-QKD只适合接入网等环境使用。要想在长距离链路(广域网)上传输经典量子复用信号,密集波分复用(DWDM)是必要的。

基于被动分波技术的思路,本文提出一种改进的波段分配模式。针对某些特定的QKD系统,已有研究解决了单量子多经典信道集成量子经典密集波分复用系统的最优波段复用问题[13]。然而,在更一般的情况下,多个量子和多个经典信号的传输问题还没有得到充分的研究。考虑到拉曼光谱的形状,这个问题的传统解决方案是将高波长分配给经典信道,将低波长分配给量子信道。已经有关于在具有两个独立的量子和经典波段的约束下的适当波段选择[15]的研究,然而最佳波段复用不一定遵循这种双波段形式[16]。本文研究了更具有广泛实用意义的多波段最佳波段复用模式,分析了在特定DWDM设置下经典信道对量子信道造成的串扰影响,还验证了优化的波段选择方案在提高QKD链路性能上的表现。

2 经典信号-量子信号共纤传输的波分复用QKD系统

区别于经典加密通信,量子密钥协商过程中,QKD通过随机制备偏振态和随机选取测量基的方式,利用量子力学特性保证了密钥的完全随机性。本实验组以BB84协议为例对DWDM-QKD的噪声源进行分析。发送方Alice随机选取正基(|0°〉和|90°〉代表0/1)或斜基(|45°〉和|135°〉代表0/1)之一,将随机生成的二进制代码制备为对应的偏振态。接收方Bob接收到对应偏振态光子后,同样随机选

取基进行测量，当且仅当双方选取一致的基时，Bob得出正确的结果。测量后双方交换得出共同选取的基，即Bob公布测量基后Alice回复其中双方选取一致的基，保留正确的测量结果，最后双方可以得到一段共享的密钥。

考虑一个载有数个经典信道和量子信道的DWDM链路，一般地，将其中M个信道分配给QKD使用，而N个前向经典信道（从Alice到Bob）和N个后向经典信道（从Bob到Alice）传输经典数据。在实际的线路中，一般有单模光纤和双光纤上两种情况，由于现有的绝大部分量子经典信号复用方案都是基于已有铺设的经典光纤线路，本实验组也采取基于第1种单模光纤的全双工DWDM系统，经典信道起始端经由EFDA加强，量子信道末端通过NBF（窄带滤波器）进行滤波，如图1所示。在第1种情况下，假设每个经典通道都配备了光环行器，以实现在相同波长的两个方向上的信号传输。除了现有的这两种方式，未来还可能出现具有经典链路和量子链路的大容量全双工DWDM系统。值得注意的是，通常来说共向传输的拉曼噪声小于在相反方向上传输量子信号和经典信号的情况下产生的噪声[17]，这使得不同情况下波长的最优分配模式有稍许的不同。

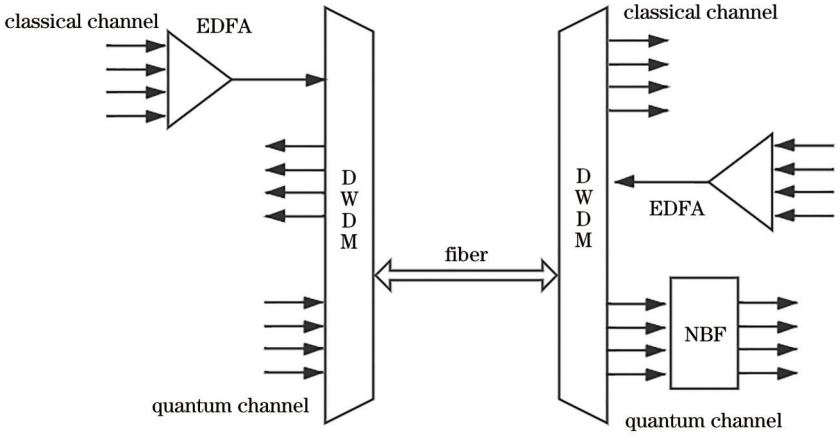

图1　全双工的经典-量子复用信道

Fig. 1　Full-duplex classical-quantum multiplexing channel

经典信号和量子信号共纤传输时，强度较大的经典光会对强度较小的量子光造成较大的串扰，直接导致复用信道的传输效率大幅下降。串扰主要来源拉曼噪声和邻道串扰，在本实验中，假设QKD解码器中配备的窄带滤波器很好地过滤了邻道串扰带来的噪声，因此仅考虑拉曼噪声带来的影响。

理论计算和实验验证都表明，在长途的经典光-量子光共纤传输情境中，特别是在DWDM环境中，自发拉曼散射（SRS）[2]是主要噪声源。SRS是一种非弹性散射过程，在此过程中，散射的光子被转换为波长更长或更短的光子，分别称为Stokes散射和反Stokes散射，其中后者的影响小于前者。拉曼噪声的光谱很宽，因此很容易泄漏到量子信道中，影响量子信号的传输。根据这个特性，一般地，为了使由于拉曼散射引起的噪声最小，有时会将量子通道的波长设置得比经典通道的波长低。在此规则下，只需要考虑自发Stokes拉曼散射光子的影响。这种波段复用模式也叫作双波段形式，该分配模式简单地从噪声方向上选取了较小的一侧，虽然有效地减小了拉曼噪声的影响，但是从信道利用率上来看却十分低效。

3　拉曼噪声分析及波段选择算法

3.1　经典-量子复用信道的拉曼噪声分析

拉曼噪声根据传播方向可以分为两类，与数据信号共同传播的拉曼噪声称为前向散射，反向传播的拉曼噪声称为后向散射。在典型光纤长度下，后向拉曼散射比前向拉曼散射强。对于一条经典信号与量子信号混合传输的光纤来说，正向传输波长为λ_{f}与反向传输波长为λ_{b}的经典信号对于波长为λ_{q}的量子信号分别产生前向拉曼噪声和后向拉曼噪声，噪声强度的表达式分别为

$$I_{\mathrm{F}}=I\cdot\exp(-\alpha L)\cdot L\rho(\lambda_{\mathrm{f}},\lambda_{\mathrm{q}})\Delta\lambda,\tag{1}$$

$$I_{\mathrm{B}}=I\cdot\frac{1-\exp(-2\alpha L)}{2\alpha}\cdot\rho(\lambda_{\mathrm{b}},\lambda_{\mathrm{q}})\Delta\lambda,\tag{2}$$

式中：I是输入光的强度；α是平均近似后的光纤衰减系数；L是光纤长度；$\Delta\lambda$是影响通道的频带宽度；ρ是相应参数条件下的拉曼噪声系数。经典信号在

1550 nm 波长下的 λ_q-ρ 图[18]如图 2 所示。从图中可以看出，拉曼噪声的强度以 1550 nm 为界可以分为前后两部分，离界太近的部分因波长间隔限制不能选取，其中后半部分波长较大的一段噪声强度平均要高于前半部分波长较小的一段。因此，如果使用双波段形式（也就是复用信道中仅包含经典信号和量子信号各仅占一个波段的形式），那么将量子通道的波长设置得比经典通道低的模式将会是波段复用的最佳方案。

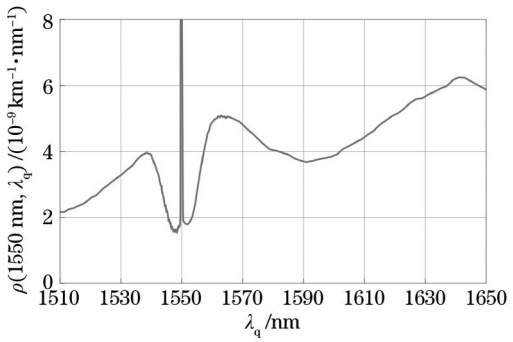

图 2　不同波段信道受拉曼噪声影响的系数[18]

Fig. 2　Coefficients of different band channels affected by Raman noise[18]

为了便于后续和量子通道结合计算，把噪声强度转换为量子接收器的探测器检测通过的平均光子数，并提取出与波长无关的参数，有

$$p_{\mathrm{F}}=K_{\mathrm{F}}\lambda_{\mathrm{q}}\rho\left(\lambda_{\mathrm{f}},\lambda_{\mathrm{q}}\right),\tag{3}$$

$$p_{\mathrm{B}}=K_{\mathrm{B}}\lambda_{\mathrm{q}}\rho\left(\lambda_{\mathrm{b}},\lambda_{\mathrm{q}}\right),\tag{4}$$

$$K_{\mathrm{F}}=I\exp\left(^{-\alpha L}\right)L\Delta\lambda T_{\mathrm{d}}\eta_{\mathrm{d}}/(2hc),\tag{5}$$

$$K_{\mathrm{B}}=I\left[1-\exp\left(-2\alpha L\right)\right]\Delta\lambda T_{\mathrm{d}}\eta_{\mathrm{d}}/(4\alpha hc),\tag{6}$$

式中：K_{F} 和 K_{B} 是与波长无关的参数；T_{d} 和 η_{d} 分别是探测器时间间隔和量子效率；h 为普朗克常数；c 为真空中的光速。

实验的最终目的是提高复用信道中传输时的密钥生成率，还需要将噪声强度和密钥生成率联系到一起。对于一个周期为 T 的 QKD 系统的某一个信道，用 μ 表示主信号状态下的平均光子数，密钥生成率 R[19]的表达式为

$$R=q\left\{-Q_{\mu}f\left(E_{\mu}\right)H_2\left(E_{\mu}\right)+Q_1\left[1-H_2\left(e_1\right)\right]\right\}/T,\tag{7}$$

式中：q 仅与采取的协议相关；Q_{μ} 和 E_{μ} 分别指信道传输的总增益和量子比特出错概率（QBER）；Q_1 和 e_1 指单光子态的增益和 QBER；f 为错误检验效率；H_2 是二元香农熵函数。4 个参数与噪声光子数 p 的关系分别为

$$Q_{\mu}=1-(1-p)\exp\left(-\eta\mu\right),\tag{8}$$

$$E_{\mu}=\left\{e_{\mathrm{detector}}\left[1-\exp\left(-\eta\mu\right)\right]+\frac{p}{2}\right\}/Q_{\mu},\tag{9}$$

$$Q_1=(\eta+p-\eta p)\mu\exp\left(-\mu\right),\tag{10}$$

$$e_1=\left(e_{\mathrm{detector}}\eta+\frac{p}{2}\right)/(\eta+p-\eta p),\tag{11}$$

$$p_m=p_{\mathrm{F}}+p_{\mathrm{B}},\tag{12}$$

式中：η 是单光子的总传输概率；e_{detector} 是探测器的错误率。

3.2　多波段复用 QKD 噪声分析

本实验组构建一个具体的多波段复用 DWDM 模型来进行噪声分析。考虑一个经典与量子的混合信道，信道的可用波长范围由以下集合表示：$G=\left\{\lambda_1,\cdots,\lambda_D\right\}$，DWDM 系统的信道间隔用 Δ 表示。将 G 分配给经典信道的波长集 $A=\left\{\lambda_{\mathrm{A}_1},\cdots,\lambda_{\mathrm{A}_N}\right\}$、$B=\left\{\lambda_{\mathrm{B}_1},\cdots,\lambda_{\mathrm{B}_N}\right\}$ 和量子信道波长集 $U=\left\{\lambda_{\mathrm{q}_1},\cdots,\lambda_{\mathrm{q}_M}\right\}$，即把 D 个信道分配给 N 个经典信道和 M 个量子信道。表示前向经典信道的集合 A 和反向的经典信道集合 B 可能重叠，量子信道 U 可以是双向的。假定所有经典信号具有相等的发射功率，用 I 表示。考虑到接收器的灵敏度，假定该发射功率被最小化以满足目标误码率（BER）。

关于量子信道，所用 QKD 通道将采用 BB84 协议的诱骗态版本[20]与主要适用于光纤通道的时间相位编码[21]，以允许在 QKD 编码器上使用弱激光脉冲。在时间相位编码中，量子位是根据马赫-曾德尔干涉仪（MZI）产生的两个连续脉冲 r 和 s 的相位差编码的。

在图 1 所示的 DWDM 系统中，每个经典信号在每个量子链路的接收器处诱导一定量的拉曼串扰噪声。考虑波长为 $\lambda_{\mathrm{q}_m}(m=1,2,\cdots,M)$ 的量子信道，计算由第 $n(n=1,2,\cdots,N)$ 个数据信道引起的拉曼噪声量。数据信道可以包括沿着与信道 m 中的量子信号相同的方向或者相反的方向传播的信号。前者的波长使用 λ_{f_n} 表示，后者用 λ_{b_n} 表示。有 $\lambda_{\mathrm{f}_n}=\lambda_{\mathrm{A}_n}$ 和 $\lambda_{\mathrm{b}_n}=\lambda_{\mathrm{B}_n}$。

根据第 1 节中关于拉曼噪声的内容可知，经典信道对量子信道的串扰噪声取决于它们对应波长之间的差异。因此，量子密钥分配信道的密钥率取决于量子信道和经典信道在波长网格中的相对位置。文献[22-23]也研究了单波段及多波段复用信

道下拉曼噪声对密钥生成率的影响，但并未考虑多经典信道复用的情况，也并未考虑经典信道与量子信道的波段选择的相对位置不同对总噪声大小的影响。在此符号定义系统下，原问题可以描述为一个优化问题，即在图1所示的DWDM系统中，在每个信道的最小密钥率约束下，最大化QKD密钥率的最佳波段选择找到集合U、A和B，使得QKD信道的总密钥率最大化。这个问题可以表述为

$$\max_{A,B,U}\sum R_m,\ \text{s.t.}\ R_m>R_{\min},\tag{13}$$

式中：R_m是根据(7)式计算的第m个量子信道的密钥率；$R_{\min}$是R_m所需的最小值。参数$R_{\min}$的定义考虑了QKD链路的服务质量。在多用户设置中，需要保证每个QKD用户的最小密钥率，$R_{\min}$将指定该最小密钥率。如果只对最大化总密钥率的结果感兴趣，而不受单个密钥率的约束，可以简单地在(13)式中使用$R_{\min}$的负值。根据定义，$R_{\min}$是非负的，为$R_{\min}$选择一个负值将消除每个信道的最小密钥率的任何约束。这只是为了便于注释，否则负阈值没有物理含义。

首先尝试简化(13)式中的优化问题，由于采取的是有效BB84协议，q的值近似于1，之后就取$q=1$，因为这并不影响不同信道分配方案下密钥率R值的相对大小判断。

因此对于某一个信道来说，密钥率的下限为

$$R=Q_1\left[1-H_2\left(e_1\right)-f\left(E_\mu\right)Q_\mu H_2\left(E_\mu\right)\right]。\tag{14}$$

为了解决(13)式中的优化问题，可以通过研究R_m与p_m的关系来进行简化。R_m是p_m的下降函数，可以用一条直线以合理的精度近似拟合该曲线。在这个近似下，(13)中的优化问题可以表示为

$$\min_{A,B,U}\sum p_m,\ \text{s.t.}\ p_m<p_{\max},\tag{15}$$

式中：$p_{\max}$表示使R_m达到最小值的串扰光子数量，取决于光纤长度和QKD系统参数。负的R_m值可以用无限大的$p_{\max}$值来建模，这相当于消除了对p_m的任何约束。原则上，(15)式的最优解可以用来表示(13)式的近似最优解。在该模型下，(12)式可以重写为

$$p_m=\sum_{n=1}^{N}\left(p_{\mathrm{F}}^{nm}+p_{\mathrm{B}}^{nm}\right)。\tag{16}$$

针对图1所示的DWDM结构检查这个优化问题。根据(3)、(4)式，可以将(16)式中的成本函数重写为

$$C=K_{\mathrm{F}}\sum_{n,m}\lambda_{\mathrm{q}_m}\rho\left(\lambda_{\mathrm{f}_m},\lambda_{\mathrm{q}_m}\right)+K_{\mathrm{B}}\sum_{n,m}\lambda_{\mathrm{q}_m}\rho\left(\lambda_{\mathrm{b}_m},\lambda_{\mathrm{q}_m}\right)。\tag{17}$$

容易证明，当$A=B$时，(17)式才能取得最优解，否则可以用得到较小噪声的前向(后向)经典信道波长集合代替另外一个，从而产生更小的噪声。因此问题可以描述为

$$\min_{A,U}\sum_{n}\sum_{m}\lambda_{\mathrm{q}_m}\rho\left(\lambda_{\mathrm{f}_n},\lambda_{\mathrm{q}_m}\right),\ \text{s.t.}\sum_{n}\lambda_{\mathrm{q}_m}\rho\left(\lambda_{\mathrm{f}_n},\lambda_{\mathrm{q}_m}\right)<p,\tag{18}$$

式中：$p=p_{\max}/\left(K_{\mathrm{F}}+K_{\mathrm{B}}\right)$。该优化问题可以通过线性规划来求解。

3.3　波段选择算法

算法1是波段选择算法的一种具体实现方式，可以解决(18)式中的优化问题。对于给定总信道数量D，分别分配N个经典信道和M个量子信道的波段选择任务，p为允许串扰光子数的临界值，算法1遍历了所有选择情况的组合，并计算所有信道噪声，进而进行相互比较，得到最终的波段选择方案。由于一般情况下，进行分配的信道数量并不会很多，这种算法可以很高效地实现。且在忽略误差的情况下，该算法可以得到理论最佳的波段选择方案。通过算法1对(18)式中的优化问题进行求解，可以找到相应初始情况下的最佳波段复用方案。算法1的具体步骤如下所示。

Algorithm 1　Wavelength selection algorithm

Input: N, M, D, p, $S(i,j)=\lambda_j\rho(\lambda_i,\lambda_j)$
Output:
Set A contains the label assigned to the channel by the classical channel
Set U contains the label assigned to the channel by the quantum channel
$c=+\infty$
for t in size$-N$ subsets of $\{1,2,\cdots,D\}$
　$y=\sum_{j\in t}S(j,:)$
　$I=\mathrm{sort}(y)$
　$s=\mathrm{sum}(y)$
　if $s<c$ and $\max(y)<p$ then
　　$c=s$
　　$A=$ First M elements in I
　　$U=t$
　end if
end for

4　数值模拟

由所提波段选择算法得到的波段选择方案经

理论验证具有最优性，此小节将用数值模拟的方式将波段选择算法和传统双波段选择的分配结果进行拉曼噪声对比分析，并展示不同参数下两种波段选择算法在进行拉曼噪声对比分析时的运行效果。表 1 列出了 QKD 系统的标称值，表 2 总结了基于实际考虑的其他系统参数。假设在全双工 DWDM 系统中，经典信道采用开关键控，数据速率为 10 GHz 数据激光器的发射功率由接收器灵敏度控制，该灵敏度假定为±28 dBm，对应于 10^{-12} 的误码率。

表 1　QKD 系统实验参数

Table 1　Experimental parameters of QKD system

Parameter	Value
Average number of photons per signal pulse	0.48
Quantum efficiency of single-photon detectors	0.3
Error correction inefficiency	1.2
Phase-distortion error probability, e_d	0.01
Time gate interval /ms	0.1
Channel loss coefficient /km^{-1}	0.046

表 2　DWDM 系统实验参数

Table 2　Experimental parameters of DWDM system

Parameter	Value
NBF bandwidth /GHz	15
Channel spacing, Δ /GHz	200
Directivity of DWDM module /dB	50

将所提多波段方法与传统的双波段方法（将波长的较低的部分分配给量子信道、较长的波长分配给经典信道）进行拉曼噪声对比分析。以双波段方法为基准，算法的改进效率 RI 为

$$I_{\mathrm{RI}}=\frac{R-R_0}{R}\times 100\%, \tag{19}$$

式中：R_0 是双波段方法的密钥率。依据第 2 节的方法进行了 12 个经典信道和 1 个量子信道混合的实验，不同光纤长度下的密钥率及改进效率如表 3 所示。表 3 中的实验数据表明，光纤长度越长，多波段分配模式的改进效率 RI 越高，这意味着该波段复用方式具有较强的抗衰减能力。

表 3　不同光纤长度的密钥生成率及改进效率（N=12, M=1）

Table 3　Key generation rate and improved efficiency of different fiber lengths (N=12, M=1)

Fiber length /km	R_0 /(10^6 bit·s^{-1})	R /(10^6 bit·s^{-1})	RI
40	14.1	14.9	5.50
45	9.33	10.1	9.69
50	5.27	6.29	19.4
55	1.79	2.93	63.0

为了进一步研究多波段分配方法的性能，定义另一个度量 $N_{\max}$，即可以与 M 个量子信道集成的最大可能数目的经典信道，使得所有信道都具有正密钥率。与传统方法进行比较，数值结果表明，根据光纤长度的不同，$N_{\max}$ 通常可以提高一到两个通道。这意味着通过使用最佳波段复用，可以支持更高的数据传输。

图 3 和图 4 分别为 M=1 和 M=4 时模拟计算得到的最优波段复用方案，其中星星代表经典信道，圆点代表量子信道。图 3 和图 4 具体展现了该分配方案下量子信道和经典信道的分布情况，从图中可以看出，信道得到很有效的利用。因此，多波段分配下的 QKD 可以在保证降低经典信道-量子信道的拉曼噪声串扰影响的同时，充分利用信道复用，从而提高 QKD 的传输能力。

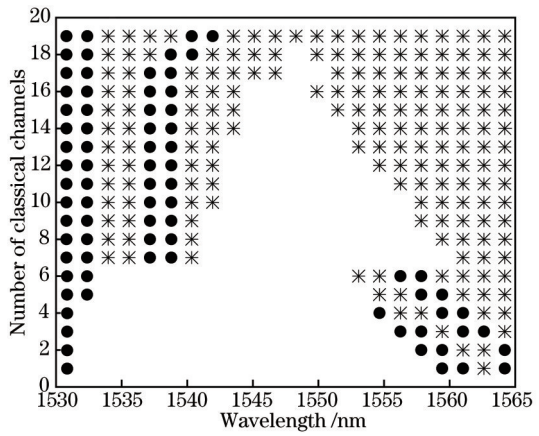

图 3　M=1 时模拟计算得到的最优波段复用方案

Fig. 3　Optimal band multiplexing scheme obtained by simulation calculation when M=1

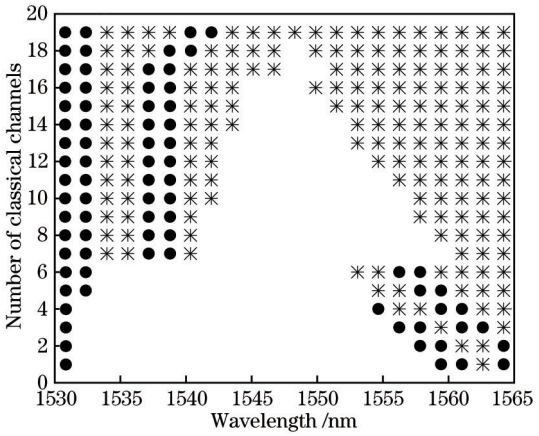

图 4　M=4 时模拟计算得到的最优波段复用方案

Fig. 4　Optimal band multiplexing scheme obtained by simulation calculation when M=4

5 结 论

研究了量子密钥分发系统中，混合经典-量子网络中的波段复用问题，利用光网络的可重构性，提出了一种通过适当的波段选择来提高链路性能的QKD方案。在全双工系统的设置下，研究了使QKD信道的总密钥率最大化的最佳波段复用方法。数值结果表明，传统的两个量子带和经典带的波段复用方法不一定是最佳的解决方案，这进一步验证了文献[16]的理论工作。在大多数情况下，所提多波段选择方法与最佳优化方法几乎相同。除了所采用的诱骗版本的BB84协议以外，由于多波段复用使总串扰噪声最小化，波段选择算法还可以适用于不同的QKD协议。

组合优化方法在通信模型的构建和参数选择中都可以起到实际有效的作用。受限于单光子传输场景下QKD的噪声抑制能力，本实验组对密钥率的优化止步于尽可能降低拉曼噪声产生的影响。另一方面，CV-QKD抑制串扰噪声的能力更为出色，组合优化方法在CV-QKD上的应用值得进一步关注。

参 考 文 献

[1] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing[J]. Theoretical Computer Science, 2014, 560: 7-11.

[2] Ekert K A. Quantum cryptography based on Bell's theorem[J]. Physical Review Letters, 1991, 67(6): 661-663.

[3] Wang S, Chen W, Guo J F, et al. 2 GHz clock quantum key distribution over 260 km of standard telecom fiber[J]. Optics Letters, 2012, 37(6): 1008-1010.

[4] Berthold J, Saleh A A M, Blair L, et al. Optical networking: Past, present, and future[J]. Journal of Lightwave Technology, 2008, 26(9): 1104-1118.

[5] Aleksic S, Winkler D, Poppe A, et al. Distribution of quantum keys in optically transparent networks: perspectives, limitations and challenges[C]//2013 15th International Conference on Transparent Optical Networks (ICTON), June 23-27, 2013, Cartagena, Spain. New York: IEEE Press, 2013: 1-6.

[6] Agrawal G P. Fiber-optic communication systems [M]. 4th ed. Hoboken: John Wiley & Sons, Inc., 2011.

[7] Bacco D, Da Lio B, Cozzolino D, et al. Boosting the secret key rate in a shared quantum and classical fibre communication system[J]. Communications Physics, 2019, 2: 140-141.

[8] Karinou F, Brunner H H, Fung C H F, et al. Toward the integration of CV quantum key distribution in deployed optical networks[J]. IEEE Photonics Technology Letters, 2018, 30(7): 650-653.

[9] 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.

[10] Ureña M, Gasulla I, Fraile F J, et al. Modeling optical fiber space division multiplexed quantum key distribution systems[J]. Optics Express, 2019, 27(5): 7047-7063.

[11] Huang C, Li Y X, Meng W, et al. Effect of mode coupling on quantum bit error rate in mode division multiplexing simultaneous transmission system[J]. Acta Optica Sinica, 2020, 40(4): 0406002.
黄超, 李云霞, 蒙文, 等. 模式耦合对模分复用同传系统中量子误码率的影响[J]. 光学学报, 2020, 40(4): 0406002.

[12] Huang C, Li Y X, Meng W, et al. Performance analysis of quantum key distribution system based on mode division multiplexing[J]. Laser & Optoelectronics Progress, 2020, 57(15): 150604.
黄超, 李云霞, 蒙文, 等. 基于模分复用的量子密钥分发系统性能分析[J]. 激光与光电子学进展, 2020, 57(15): 150604.

[13] Bian Y X, Li Y, Zhang G Z, et al. Key technologies and future prospects of power quantum secure communication[J]. Information and Communications Technology and Policy, 2019(10): 26-32.
卞宇翔, 李勇, 张国志, 等. 电力量子保密通信关键技术及未来展望[J]. 信息通信技术与政策, 2019(10): 26-32.

[14] Kumar R, Qin H, Alléaume R. Coexistence of continuous variable QKD with intense DWDM classical channels[J]. New Journal of Physics, 2015, 17(4): 043027.

[15] Renner R, Cirac J I. De Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography[J]. Physical Review Letters, 2009, 102(11): 110504.

[16] Bahrani S, Razavi M, Salehi J A. Crosstalk reduction in hybrid quantum-classical networks[J]. Scientia Iranica, 2016, 23(6): 2898-2907.

[17] Bahrani S, Razavi M, Salehi J A. Optimal

wavelength allocation in hybrid quantum-classical networks[C]//2016 24th European Signal Processing Conference (EUSIPCO), August 29-September 2, 2016, Budapest, Hungary. New York: IEEE Press, 2016: 483-487.

[18] Eraerds P, Walenta N, Legré M, et al. Quantum key distribution and 1 Gbps data encryption over a single fibre[J]. New Journal of Physics, 2010, 12(6): 063027.

[19] Patel K A, Dynes J F, Choi I, et al. Coexistence of high-bit-rate quantum key distribution and data on optical fiber[J]. Physical Review X, 2012, 2(4): 041010.

[20] Lo H K, Ma X F, Chen K. Decoy state quantum key distribution[J]. Physical Review Letters, 2005, 94 (23): 230504.

[21] Lo H K, Chau H F, Ardehali M. Efficient quantum key distribution scheme and a proof of its unconditional security[J]. Journal of Cryptology, 2005, 18(2): 133-165.

[22] Ma X F, Razavi M. Alternative schemes for measurement-device-independent quantum key distribution[J]. Physical Review A, 2012, 86(6): 062319.

[23] Cheng K, Zhou Y Y, Wang H. Scheme of measurement-device-independent classical-quantum signal transmission in shared fiber[J]. Laser & Optoelectronics Progress, 2019, 56(8): 082701.
程康, 周媛媛, 王欢. 测量设备无关的经典-量子信号共纤传输方案[J]. 激光与光电子学进展, 2019, 56(8): 082701.