DOI: 10.3969/j.issn.1007-5461.2023.04.014

基于BP神经网络的经典-量子信号共纤同传系统参数预测

孙一石， 孙 弋*

(西安科技大学通信与信息工程学院， 陕西 西安 710054)

摘 要: 光纤量子密钥分发的应用推广取决于与现有光网络的兼容性, 而利用波分复用技术将经典数据和量子信号进行共纤传输兼备安全性、经济性和实用性等优势。针对经典 - 量子信号共纤同传系统中信号态平均光子数、诱骗态种类数量等参数最优取值处理困难、运行速度缓慢等影响其实用化的突出问题, 建模分析了主要噪声成分, 并在考虑统计波动影响下对有限长效应和诱骗态方法进行了评估。进而利用原始信号数据集对反向传播 (BP) 神经网络进行训练, 以实现不同信道噪声条件下的信号态平均光子数等系统参数的预测。结果表明, 该网络输出的预测平均光子数取值与原始曲线取值结果基本一致, 训练误差小于 10^{-3}。该网络可作为一种有效模型用于实用化诱骗态经典-量子共纤同传系统参数预测, 对量子保密通信向着高速率、大容量、智能化发展具有潜在的应用价值。

关 键 词: 量子光学; 量子密钥分发; 波分复用; 机器学习; 神经网络

中 图 分 类 号： TN918 **文 献 标 识 码：** A **文章编号:** 1007-5461(2023)04-00546-14

Parameter prediction of classical-quantum signals co-fiber transmission system based on BP neural network

*SUN Yishi, SUN Yi**

(College of Communication and Information Technology, Xi'an University of Science and Technology, Xi'an 710054, China)

Abstract: The application of fiber-based quantum key distribution (QKD) depends on the compatibility with existing optical networks. The use of wavelength division multiplexing (WDM) technology for co-fiber transmission of classical data and quantum signals has the advantages of security, economy, and practicality. Aiming at the prominent problems that affect the application of the classical-quantum signal co-fiber transmission system, such as the difficulty in optimizing and calculating the average photon number of signal states, the number of decoy states and other parameters, and the slow running speed, the channel noise components are modelel and analyzed, and the finite-length effect and the decoy state method are evaluated considering the statistical fluctuations. Furthermore, based on the experimental data

基金项目: 国家自然科学基金 (61971436, 61803382)

作者简介: 孙一石 (2002 -), 河北丰润人, 主要从事量子通信、智能算法方面的研究。E-mail: 1527482049@qq.com

导师简介: 孙 弋 (1972 -), 陕西泾阳人, 博士, 教授, 主要从事智能算法、通信网络方面的研究。E-mail: sunyi@xust.edu.cn

收稿日期: 2022-10-09; **修改日期:** 2022-12-28

*通信作者。

set, the back propagation (BP) neural network is trained to predict the system parameters such as the average photon number of signal states under different channel noise conditions. The results show that the predicted average photon number by the BP network is basically consistent with the original curve, and the training error is less than 10^{-3}. It is indicated that the network can be used as an effective model for practical prediction of the parameters of the decoy-state classical-quantum co-fiber transmission system, which is of great practical significance for the development of quantum-secure communication towards high speed, large capacity and intelligence.

Key words: quantum optics; quantum key distribution; wavelength division multiplexed; machine learning; neural network

0　引　言

量子密钥分发 (QKD) [1−3]能够在相距较远的通信双方间共享安全密钥, 确保合法用户能察觉任何企图窃听传送中密钥的行为, 在信息理论上保证密钥传输的安全性, 其结合一次一密 (OTP) 的加密机制可以确保电信领域经典加密方式安全可靠。经过研究人员三十多年的探索, QKD技术已经发展成熟并广泛应用[4, 5], 目前光纤QKD传输距离能够达到833 km[6]。然而, 微弱量子信号单独占用一根光纤会引发资源浪费, 利用波分复用 (WDM) 技术将经典光信号和量子光信号合并在一根光纤中进行共纤传输是解决此问题的主要方法之一, 可以大大提升量子通信网络的灵活性和可拓展性。

在共纤同传系统的实际应用过程中, QKD信号容易受到来自经典强光信号的干扰。QKD信号的劣化主要归咎于光纤中的损耗、色散和非线性效应。1997年, 英国电信实验室的Townsend[7]首次实现了QKD与经典光信号的波分复用实验。二十多年来, 经典 - 量子信号共纤同传系统先后经历了降低信道串扰[8−13]、克服传输损耗[14−18]、提高频谱利用率[19−23]、增加通信容量等阶段[24−27], 目前正朝着大容量、高速率的方向发展[28−30], 而如何高效快捷地对系统内的复杂参数进行处理成为量子保密通信实用化进程中的关键一环。

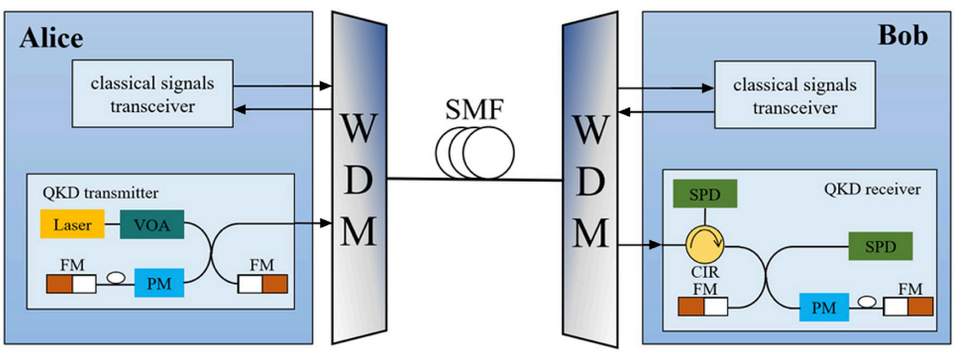
针对影响实用化经典 - 量子信号共纤同传系统的参数 (如信号态平均光子数、诱骗态种类数量等) 最优取值上处理困难、运行速度缓慢的突出问题, 基于机器学习在数据特征分析和数据处理方面的优越性, 将其应用于光纤量子通信系统以处理海量数据、优化实验参数[31−35], 从而加速QKD技术的实用化进程。特别地, 相比于传统的QKD系统, 经典 - 量子信号共纤同传系统噪声成分更加复杂, 采用神经网络算法提高系统运算速度, 对系统参数进行优化处理, 从而实现关键参数快速估计和预测, 可推动量子保密通信向着智能化、自动化发展。

本文基于经典 - 量子信号共纤同传系统的应用背景, 搭建了系统模型, 对系统内的三种主要噪声成分进行了理论分析, 并推导了有限长效应下的系统安全码率, 最后, 选用反向传播 (BP) 神经网络对共纤同传系统的数据集进行训练, 实现对信号态平均光子数的预测和优化, 有效提高了QKD系统的性能。

1　系统建模与噪声分析

经典—量子信号共纤同传系统主要由光源、信道和探测器三部分组成。与经典的QKD系统不同, 共纤同传系统有两种光源: 一种是用于经典通信和数据传输的光纤激光源, 另一种是用于单光子编码的弱相干

光源。数据信息在经典信道中传输; 量子信号经过光衰减器 (VOA) 后, 基于法拉第-迈克尔逊干涉结构对单光子的相位、偏振等物理量进行编码[28−30], 在量子信道中传输。随后经典信号和量子信号通过波分复用器 (WDM) 耦合到单模光纤 (SMF) G.652 中。信号到达接收端先进行解复用, 经典信号和量子信号分别被发送到光接收机和单光子探测器 (SPD), 对 QKD 信号实现探测解码以及后处理操作后完成量子密钥的安全分发。



VOA: variable optical attenuator; PM: phase modulator; FM: Faraday mirror; CIR: circulator; SPD: single-photon detector

图 1 WDM-QKD 系统结构框图

Fig. 1 Structure diagram of WDM-QKD system

图 1 所示的经典-量子信号共纤同传系统基于文献 [36], 此文献中模型的信道间隔设置为 400 GHz, 在 DWDM 广泛部署的今天, 这样的信道间隔不利于系统的实际应用。考虑到频谱利用率和信道需求, 本模型将信道间隔设置为 200 GHz, 在提高系统性能的同时, 系统内的噪声也相应地发生了变化。其中, 主要的噪声成分为信道串扰、自发拉曼散射噪声和四波混频噪声。

信道串扰噪声是由于解波分复用器件隔离度的不完美性导致经典光子泄露到量子信道中产生的一种带外噪声, 其在探测端的计数率为

$$Y_{\text{leak}}=\frac{Pt_{\text{mux}}t_{\text{demux}}10^{-\frac{\alpha L}{10}}10^{-\frac{\xi}{10}}\tau_{\text{D}}t_{\text{filter}}\eta_{\text{D}}}{hf}, \tag{1}$$

式中: P 表示经典光信号的发射功率, t_{mux}、t_{demux} 分别表示波分复用器和波分解复用器产生的插入损耗, α 表示光纤损耗系数, L 表示传输距离, ξ 表示解波分复用器件的隔离度, τ_{D} 表示单光子探测器的门宽, t_{filter} 表示滤波器件产生的损耗, η_{D} 表示探测效率, f 表示噪声频率。

自发拉曼散射噪声是由于经典光信号与光纤非线性相互作用产生的一种弹性噪声, 根据量子信号与经典信号的不同传输方向, 其分为前向自发拉曼散射噪声和后向自发拉曼散射噪声, 在探测端的计数率分别表示为

$$Y_{\text{ram}}^{\text{f}}=\frac{\beta PLB\tau_{\text{D}}t_{\text{mux}}t_{\text{demux}}10^{-\frac{\alpha L}{10}}t_{\text{filter}}\eta_{\text{D}}}{hf}, \tag{2}$$

$$Y_{\text{ram}}^{\text{b}}=\frac{5\beta PB\tau_{\text{D}}t_{\text{mux}}t_{\text{demux}}(1-10^{-\frac{\alpha L}{5}})t_{\text{filter}}\eta_{\text{D}}}{\alpha hf\ln 10}, \tag{3}$$

式中: β 表示标准自发拉曼散射系数, B 表示窄带滤波器的带宽。

四波混频噪声是指当两个及以上光信号复用时由于光纤三阶非线性效应产生的一种带内噪声, 其在探

测端的计数率可表示为

$$Y_{\mathrm{fwm}}=\frac{\eta_{\mathrm{ijk}}D^2\chi^2P_{\mathrm{i}}P_{\mathrm{j}}P_{\mathrm{k}}t_{\mathrm{mux}}{}^3 10^{-\frac{\alpha L}{10}}\left(1-10^{-\frac{\alpha L}{10}}\right)^2\tau_{\mathrm{D}}t_{\mathrm{demux}}t_{\mathrm{filter}}\eta_{\mathrm{D}}}{9\left(\frac{\alpha\ln 10}{10}\right)^2 hf}, \tag{4}$$

式中: η_{ijk}表示四波混频效率, 受发射光的频率间隔、色散、色散频率等因素影响; D表示简并因子; χ表示光纤的非线性系数; P_{i}、P_{j}和P_{k}分别表示三个经典信号的发射功率。

在不同场景下, 以上三类噪声造成的劣化影响也在变化, 探究不同传输距离各类噪声的计数率分布情况, 有利于针对性开展噪声抑制技术, 提高密钥分发效率。

2　有限长效应下的安全密钥率分析

一个基 (Z基) 下的量子密钥公式可以表示为[37]

$$R^Z\geq q\left\{Q_1^Z\left[1-H_2(e_1^Z)\right]-Q_\mu^Z f(E_\mu^Z)H_2(E_\mu^Z)\right\}, \tag{5}$$

式中: q表示BB84协议中的选基概率, Q_1^Z和e_1^Z为单光子态的增益和误码率, Q_μ^Z表示信号态的增益, E_μ^Z表示全局的量子误码率, $H_2(x)$表示二进制熵函数。Q_μ^Z、E_μ^Z都可以在实验中测得, 而Q_1^Z和e_1^Z的边界值需要通过诱骗态方法进行估计。

在进行有限长效应分析前, 首先对经典-量子信号合纤进行建模分析。(5) 式平均光子数为μ的光脉冲在接收端的增益Q_μ^Z和量子误码率 (QBER) E_μ^Z分别表示为

$$Q_\mu^Z=\sum_0^\infty \mathrm{e}^{-\mu}\frac{\mu^n}{n!}Y_n=Y_0+1-\mathrm{e}^{-\eta\mu}, \tag{6}$$

$$E_\mu^Z=\frac{1}{Q_\mu^Z}\sum_{i=0}^{\infty}e_iY_i\frac{\mu^i}{i!}\mathrm{e}^{-\mu}=\frac{1}{Q_\mu^Z}\left[e_0Y_0+e_{\mathrm{d}}(1-Y_0)(1-\mathrm{e}^{\eta\mu})\right], \tag{7}$$

式中: e_0是背景噪声产生的误码率, 由于背景噪声是随机的, 因此$e_0=0.5$; e_{d}是光子击中错误探测器的概率; η是总的传输效率; Y_n表示Alice发送n个光子信号Bob端探测的相应概率, 其中Y_0为真空态计数率, 由背景噪声决定, 包括探测器的暗计数率P_{d}以及来自经典信号的噪声计数率Y_{leak}、Y_{ram}和Y_{fwm}。

在渐进情况下, (5) 式中所要求的单光子态参数可以通过经典-量子信号共纤同传的实测值准确估计, 并收敛成一个准确的数值, 这样就可以安全地得到共纤同传系统的最终密钥长度。然而, 在实际经典-量子信号共纤同传系统中, 传输的量子态数量是有限的, 导致测量值在统计上产生波动, 被称为有限密钥效应, 在估计最终安全密钥长度时这一效应不能忽略。本节在进行诱骗态经典-量子信号共纤同传有限长密钥安全性分析前, 首先介绍用于分析统计波动的切诺夫界方法。

在失信概率ε下, 对于观测值$\zeta>0$的期望值的置信区间$C[\zeta]$可以被表示为

$$\begin{cases}C^{\mathrm{L}}[\zeta]=\dfrac{\zeta}{1+\delta^{\mathrm{L}}}\\[2ex] C^{\mathrm{U}}[\zeta]=\dfrac{\zeta}{1-\delta^{\mathrm{U}}}\end{cases}, \tag{8}$$

式中: $C^{\mathrm{L}}[\zeta]$和$C^{\mathrm{U}}[\zeta]$分别表示$C[\zeta]$的上界和下界, δ为统计涨落的大小, 用于表示对物理量期望值的估计区间, 并且δ^{L}和δ^{U}可以通过

$$\begin{cases}\left[\dfrac{\mathrm{e}^{\delta^{\mathrm{L}}}}{(1+\delta^{\mathrm{L}})^{1+\delta^{\mathrm{L}}}}\right]^{\frac{\zeta}{1+\delta^{\mathrm{L}}}}=\dfrac{\varepsilon}{2}\\ \left[\dfrac{\mathrm{e}^{-\delta^{\mathrm{U}}}}{(1-\delta^{\mathrm{U}})^{1-\delta^{\mathrm{U}}}}\right]^{\frac{\zeta}{1-\delta^{\mathrm{U}}}}=\dfrac{\varepsilon}{2}\end{cases} \tag{9}$$

得到。运用Lambert W函数, (9) 式可以表示为

$$\begin{cases}\dfrac{1}{1+\delta^{\mathrm{L}}}=-W_0\left(-\mathrm{e}^{\left[\ln(\frac{\varepsilon}{2})-\zeta\right]/\zeta}\right)\\ \dfrac{1}{1-\delta^{\mathrm{U}}}=-W_{-1}\left(-\mathrm{e}^{\left[\ln(\frac{\varepsilon}{2})-\zeta\right]/\zeta}\right)\end{cases}, \tag{10}$$

如果$\zeta=0$, 那么可以得到$C^{\mathrm{L}}[\zeta]=0$和$C^{\mathrm{U}}[\zeta]=-\ln(\dfrac{\varepsilon}{2})$。

通过 (8)～(10) 式, Q_m^{γ}和$E_m^{\gamma}Q_m^{\gamma}$期望值的置信区间分别可以用$C^{\mathrm{L}}[Q_m^{\gamma}]$和$C^{\mathrm{U}}[Q_m^{\gamma}]$、$C^{\mathrm{L}}[E_m^{\gamma}Q_m^{\gamma}]$和$C^{\mathrm{U}}[E_m^{\gamma}Q_m^{\gamma}]$来表示, 其中$Q_m^{\gamma}$和$E_m^{\gamma}Q_m^{\gamma}$分别是$\gamma$基下筛后密钥的数量和量子比特误码率。假设传输量子态总数为N, 那么, 这些置信区间可以用来计算信号态和诱骗态整体增益和QBER的上下界, 分别表示为

$$\begin{cases}C^{\mathrm{L}}[Q_m^{\gamma}]=\dfrac{C^{\mathrm{L}}[M_m^{\gamma}]}{N_m^{\gamma}}\\ C^{\mathrm{U}}[Q_m^{\gamma}]=\dfrac{C^{\mathrm{U}}[M_m^{\gamma}]}{N_m^{\gamma}}\\ C^{\mathrm{L}}[E_m^{\gamma}Q_m^{\gamma}]=\dfrac{C^{\mathrm{L}}[E_m^{\gamma}M_m^{\gamma}]}{N_m^{\gamma}}\\ C^{\mathrm{U}}[E_m^{\gamma}Q_m^{\gamma}]=\dfrac{C^{\mathrm{U}}[E_m^{\gamma}M_m^{\gamma}]}{N_m^{\gamma}}\end{cases}, \tag{11}$$

式中$N_m^{\gamma}=q_m q_{\gamma}^2 N$表示Alice和Bob在相同基$\gamma$、平均光子数$m$情况下的量子态数量。此外, γ基下单光子态筛后密钥数的下界为

$$Q_1^{\gamma\mathrm{L}}=Y_1^{\gamma\mathrm{L}}q_{\gamma}^2N(q_{\mu}e^{-\mu}\mu+q_{\nu}e^{-\nu}\nu), \tag{12}$$

式中: $Y_1^{\gamma\mathrm{L}}$是Y_1^{γ}的下界, 可以结合 (8)～(11) 式的诱骗态方法进行推导。$Q_1^{\gamma\mathrm{L}}$由来自信号态和诱骗态的单光子增益共同组成。单光子信号态增益的下界可以通过切诺夫界方法的反向形式给出, 即

$$Q_{1\mu}^{\gamma\mathrm{L}}=(1-\delta)p_1^{\mu}Q_1^{\gamma\mathrm{L}}, \tag{13}$$

式中: $\delta=\dfrac{-\ln(\varepsilon/2)+\sqrt{[\ln(\varepsilon/2)]^2-8\ln(\varepsilon/2)p_1^{\mu}Q_1^{\gamma\mathrm{L}}}}{2p_1^{\mu}Q_1^{\gamma\mathrm{L}}}$, $p_1^{\mu}=\dfrac{q_{\mu}e^{-\mu}\mu}{q_{\mu}e^{-\mu}\mu+\sum_{m\neq\mu}q_m e^{-m}m}$为光源强度泊松分布条件下对应的单光子信号态的比例。

在有限长效应情况分析中, 单光子态的相位误码率与QBER之间的关系(即$e_{1\mu}^{pZ}=e_1^{bX}$) 不再正确, 受到统计波动的影响, 两类误码率之间存在偏差θ。偏差的上界θ^{U}可以用随机抽样定理表示, 其失效概率为

$$\varepsilon=\frac{\sqrt{Q_1^{X\mathrm{L}}+Q_{1\mu}^{Z\mathrm{L}}}}{\sqrt{e_1^{bX\mathrm{U}}(1-e_1^{bX\mathrm{U}})Q_1^{X\mathrm{L}}Q_{1\mu}^{Z\mathrm{L}}}}2^{-(Q_1^{X\mathrm{L}}+Q_{1\mu}^{Z\mathrm{L}})\xi(\theta^{\mathrm{U}})}, \tag{14}$$

式中: $\xi(\theta^{\mathrm{U}})=h(e_1^{bX\mathrm{U}}+\theta^{\mathrm{U}}-q^x\theta^{\mathrm{U}})-q^x h(e_1^{bX\mathrm{U}})-(1-q^x)h(e_1^{bX\mathrm{U}}+\theta)$, $q^x=\dfrac{Q_1^{X\mathrm{L}}}{Q_1^{X\mathrm{L}}+Q_{1\mu}^{Z\mathrm{L}}}$。因而相位误码率的上界表示为

$$e_{1\mu}^{pZU}=e_1^{bXU}+\theta^{U}, \tag{15}$$

式中e_1^{bXU}为e_1^{bX}的上界, 可以通过诱骗态方法进行推导。

3　基于机器学习的系统参数优化算法

为了优化不同条件下的信号态强度, 本研究提出了一种利用人工神经网络进行自适应光源选择的方法。选择使用最广泛的误差反向传播(BP) 神经网络作为预测μ值的模型。BP神经网络是一种多层前馈神经网络, 采用误差反向传播算法进行训练, 该算法利用输出后的误差来估计输出层直接前导层的误差, 再用这一误差估计前一层的误差, 如此一层一层地反传下去, 就获得了其他各层的误差估计。BP神经网络的传播算法伪代码如表1所示。

表1 BP神经网络传播算法

Table 1 Propagation algorithm of BP neural network

输入: 训练集$D=\{(x_k,y_k)\}_{k=1}^{m}$; 学习率 η

输出: 连接权值或阈值确定的多层前馈神经网络

1: **function** $BP(D,\eta)$

2: 在 (0, 1) 范围内随机初始化网络中的所有连接权值和阈值

3: **repeat**

4: **for all** $(x_k,y_k)\in D$ **do**

5: 计算当前样本输出 $\hat{y}^k=f(\beta_j-\theta_j)$

6: 计算输出神经元梯度

$$\begin{aligned}g_j&=-\frac{\partial E_k}{\partial \hat{y}^k}\cdot\frac{\partial \hat{y}^k}{\partial \beta_j}\\&=-(\hat{y}_j^k-y_j^k)f'(\beta_j-\theta_j)\\&=\hat{y}_j^k(1-\hat{y}_j^k)(\hat{y}_j^k-y_j^k)\end{aligned}$$

7: 计算隐层的神经元梯度项

$$\begin{aligned}e_h&=-\frac{\partial E_k}{\partial b_h}\cdot\frac{\partial b_h}{a_h}\\&=-\sum_{j=1}^{t}\frac{\partial E_k}{\partial \beta_j}\cdot\frac{\partial \beta_j}{b_h}f'(a_h-\gamma_h)\\&=\sum_{j=1}^{t}w_{hj}g_j f'(a_h-\gamma_h)\\&=b_h(1-b_h)\sum_{j=1}^{t}w_{hj}g_j\end{aligned}$$

8: 更新权值

$$\Delta w_{hj}=ng_jb_h$$

$$\Delta v_{ih}=\eta e_h x_i$$

9: 更新阈值

$$\Delta\theta_j=-\eta g_j$$

$$\Delta\gamma_h=-\eta e_h$$

10: **end for**

11: **until** 达到停止条件

12: **end function**

4 仿真结果及分析

为便于开展系统性能研究, 采用第2节系统模型构建和理论分析过程进行数值模拟仿真。通过分析数值仿真结果来确定信号态最优光子数、量子光脉冲以及诱骗态方法选择等影响共纤同传系统性能的关键参数, 并将采集到的有效数据保存, 便于利用数据集对人工神经网络展开训练, 从而实现系统相关参数的准确预测功能。主要仿真参数如表2所示。

表2 WDM−QKD数值仿真选用参数

Table 2 Parameters used for the numerical simulation of WDM−QKD

Parameter	Value
I (波分复用器的插入损耗)/dB	1.5
α_c (光纤衰减系数)/(dB·km^{-1})	0.21
ξ (波分复用器的隔离度)/dB	80
τ_D (单光子探测器门宽)/ps	100
η_D (单光子探测器探测效率)	0.045
h (普朗克常数)/(J·s)	6.63×10^{-34}
c (光速)/(m·s^{-1})	299792458
t_F^c (滤波后带外噪声的透过率)	0.01
t_F (滤波后带内噪声的透过率)	0.95
t_{Bob} (来自内部光学器件的透过率)	0.9
β (自发拉曼散射系数)/(km·nm)	2×10^{-9}
$\Delta\lambda$ (滤波器带宽)/pm	35.23
χ (光纤非线性系数)/(W·km)	1.2
D_{ijk} (简并因子)	3
D_c (光纤色散系数)/(ps·nm^{-1}·km^{-1})	18
dD_c/dλ (光纤色散斜率)/(ps·nm^{-2}·km^{-1})	0.056
e_d (未对准引起的误码率)	0.033
P_d (探测器的暗记数率)	3×10^{-6}
$f(E_\mu)$ (纠错系数)	1.22

4.1 噪声计数及安全密钥率仿真

选取带宽35.23 pm窄带滤波器和门宽100 ps单光子探测器, 设置经典光发射功率为0 dBm。结合噪声计数率公式, 三种噪声计数随传输距离的变化如图2所示。

通过对比可知, 经典噪声的干扰在不同的滤波和探测条件下是不同的, 20 km以内四波混频噪声对系统干扰较大, 呈现周期式振荡浮动, 但整体强度趋于减弱; 超过20 km自发拉曼散射噪声起主导作用, 后向自发拉曼散射噪声呈现先上升后趋于饱和状态, 前向自发拉曼散射噪声呈现先上升后下降的趋势; 系统内信道串扰噪声受到窄带滤波抑制明显。因此, 可以根据实际传输距离条件选用不同方法来抑制主要噪声。

此外, 统计波动情况下诱骗态方法的选择对于系统性能的提升至关重要。采用弱+真空诱骗态方法[34]来估计Y_1^L和e_1^U的取值, 改进后的切诺夫界方法可用于有限长密钥安全性分析。为了便于对比, 同样对单诱骗态方法进行了仿真。统计波动下实用化经典—量子信号共纤同传系统的安全密钥率传输关系如图3所示,

图中实线表示弱+真空诱骗态方法, 虚线表示单诱骗态方法。

由图 3 可知, 弱+真空诱骗态方法的性能优于单诱骗态方法。随着发送量子脉冲数的增加, 量子密钥率和最大安全传输距离也相应地增加。当量子脉冲数 N 达到 10^{13} 时, 仿真产生的曲线与无穷脉冲情况基本一致。考虑到实际环境和成本, 可以选择弱+真空诱骗态方法且设置 $N=10^{13}$ 作为实际系统诱骗态方案来实现系统性能参数的优化。

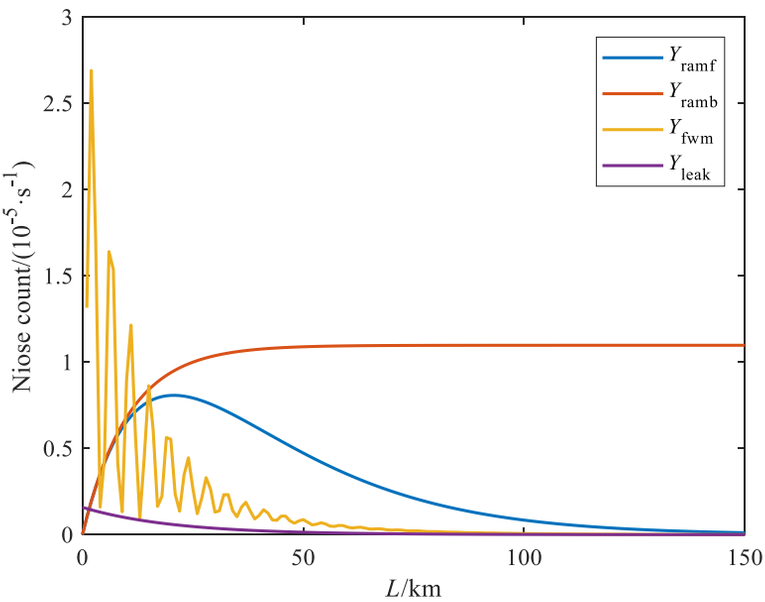


图2　自发拉曼散射噪声、四波混频噪声和带外噪声探测端噪声计数率曲线

Fig. 2　Comparison of the detection rates of SRS noise, FWM noise and out-band noise

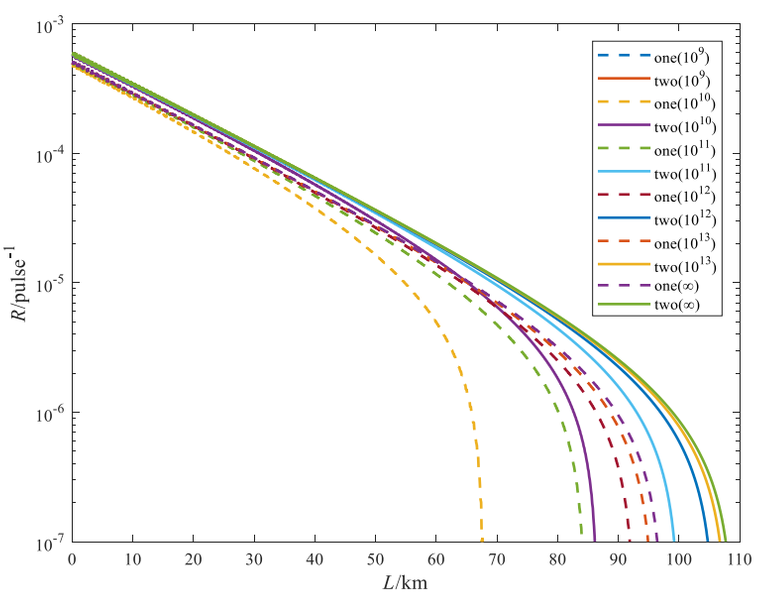


图3　统计波动下采用不同诱骗态方法的安全密钥率传输关系

Fig. 3　The secure key transmission relationship under different decoy state methods with statistical fluctuations

4.2 网络训练及参数预测

由密钥率分析和安全码率曲线可知, 信号态平均光子数的取值在将密钥生成率最优化过程中发挥着重要的作用, 如何选择最优的信号态平均光子数成为提高共纤同传系统性能的关键因素。结合应用场景, 在传输距离为10～110 km、经典发射功率为0～2 mW的范围内建立2121个样本的最优信号态强度μ的数据集。利用神经网络对该数据集进行训练, 测试不同条件下信号态的最优强度。在进行预测前首先确定神经网络中的关键指标。

4.2.1 超参数分析测试神经元分布

BP神经网络包括三层, 分别是输入层、隐含层和输出层。根据输入的数据集, 设置网络模型的输入层为2, 输出层为1, 对隐含层进行超参数分析以测试神经元的分布。设置隐含层为三层结构, 其采用tansig传递函数;输出层采用线性传递函数, 网络的训练性能函数采用MSE均方误差函数, 分别对不同神经元分布情况下的网络性能进行测试, 设置训练次数为2000次, 学习速率为0.01, 结果如图4所示。

由图4(a)～(c) 可知, 当设置神经元个数分别为 (3, 2, 1) 、(6, 4, 1) 、(15, 10, 1) 时, 神经元数量越少, 迭代次数越多, 收敛速度越慢; 但神经元数量增多时, 每次迭代所需要的时间增长, 同样导致收敛速度变慢。一般情况下, 随着训练能力提高, 预测能力也增强。但这种趋势到达极限时, 增加神经元数量反而将导致预测能力下降, 如图4(d) 所示, 即出现所谓 "过拟合" 现象。因此, 需要综合衡量以选择一个合适的神经元分布。因此, 本实验选取三层神经元个数为 (15, 10, 1) 。

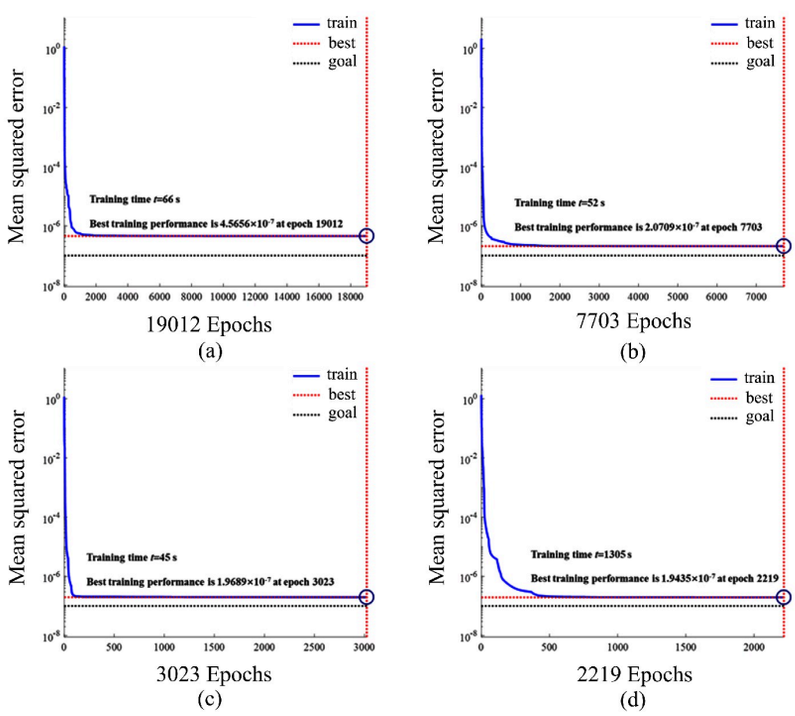


图4 不同神经元分布下神经网络的训练性能。(a) 神经元设置 (3, 2, 1)；(b) 神经元设置 (6, 4, 1)；(c) 神经元设置 (15, 10, 1)；(d) 神经元设置(48, 24, 1)

Fig. 4 Training performance of neural network with different distribution of neurons. (a) Neuron setup (3, 2, 1); (b) Neuron setup (6, 4, 1); (c) Neuron setup (15, 10, 1); (d) Neuron setup (48, 24, 1)

4.2.2　选用合适的学习函数

在本网络模型中, 隐含层采用 tansig 传递函数, 输出层采用线性传递函数, 网络的训练性能函数采用 MSE 均方误差函数, 接下来将从 Levenberg-Marquardt (LM) 变梯度算法、Bayesian 正则化算法、Scaled Conjugate Gradient (SCG) 算法中选择适当的学习函数。首先, 通过神经网络对几种学习函数的性能进行测试, 选用隐含层神经元为 10 个, 训练、确认、测试样本分布为 14: 3: 3 (70%、15%、15%), 训练结果如图 5～7 所示。

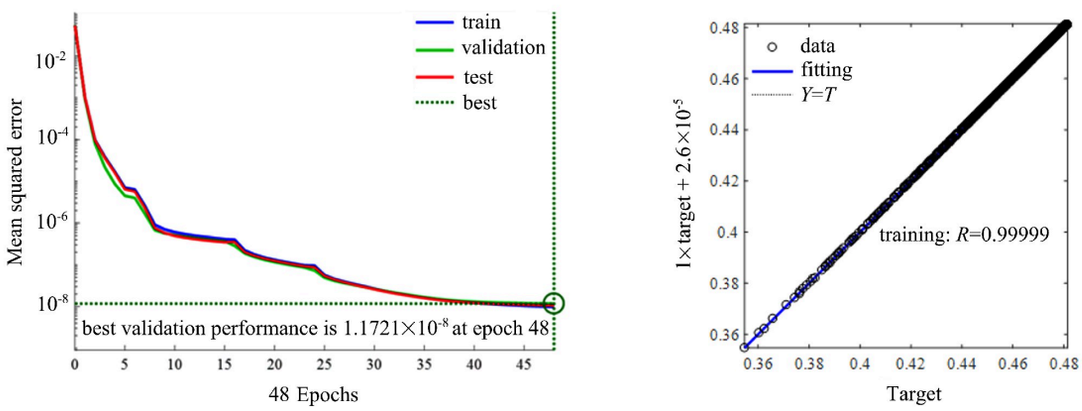


图 5　神经网络选用 LM 变梯度算法的训练性能

Fig. 5　Training performance of neural network with LM variable gradient algorithm

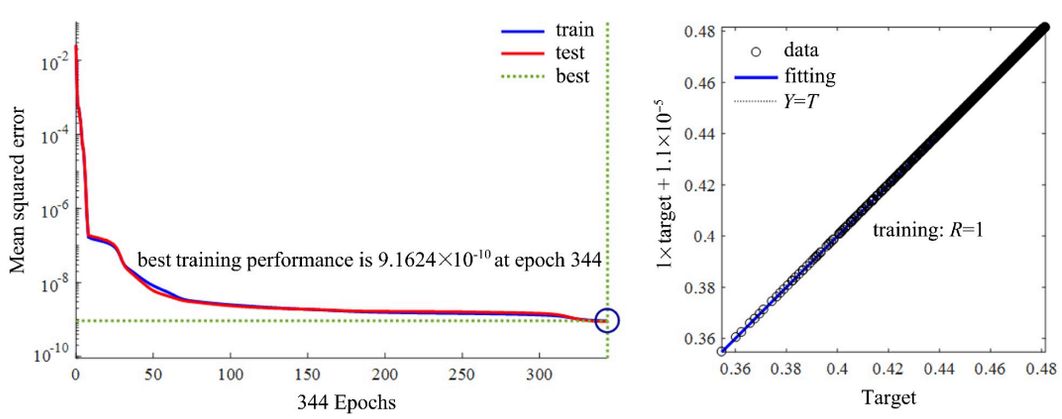


图 6　神经网络选用 Bayesian 正则化算法的训练性能

Fig. 6　Training performance of neural network with Bayesian regularization algorithm

首先选用 Levenberg-Marquardt (LM) 变梯度算法, 结果如图 5 所示, 当迭代不再改进时, 训练自动停止, 这表明验证样本的均方误差达到标准; 当选择 Bayesian 正则化算法时, 结果如图 6 所示, 数据的拟合效果较好, 但达到收敛需要更多次迭代; 当选用量化共轭梯度 (SCG) 算法时, 结果如图 7 所示, 相比于前两种算法, 数据的拟合效果下降。

综上所述, 选择 LM 变梯度算法和 Bayesian 正则化算法时, 数据的拟合效果明显优于选用 SCG 算法。相同条件下, LM 变梯度算法达到收敛所需要的迭代次数更短, 训练性能与 Bayesian 正则化算法相近。出于对算力和资源的考虑, 本实验选用 LM 变梯度算法作为学习函数。

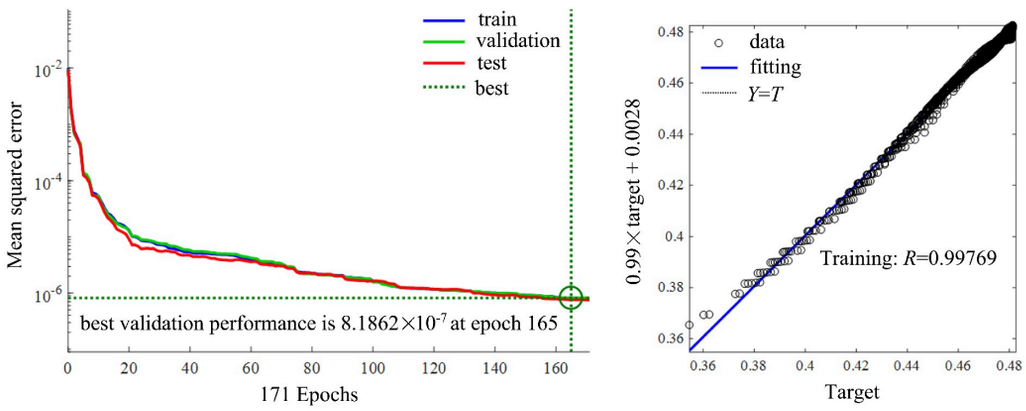


图7 神经网络选用量化共轭梯度算法的训练性能

Fig. 7 Training performance of neural network with SCG algorithm

4.2.3 测试模型效果

通过超参数分析, 选用 (15, 10, 1) 的神经元分布, 选用学习函数为Levenberg-Marquardt (LM) 变梯度算法。BP神经网络构建的模型如图8所示。其中$X=A^{[0]}$表示输入层输入的训练数据; 隐含层指神经网络中的权重矩阵, 共包含三层, $A^{[1]}$、$A^{[2]}$、$A^{[3]}$分别表示每层的神经元个数; $A^{[4]}$表示经过反复学习训练得到的与最小误差相对应的权值和阈值。通过该BP神经网络模型对数据集进行训练, 预测得到不同条件下信号态的最优强度。BP神经网络对光源的预测结果如图9所示。

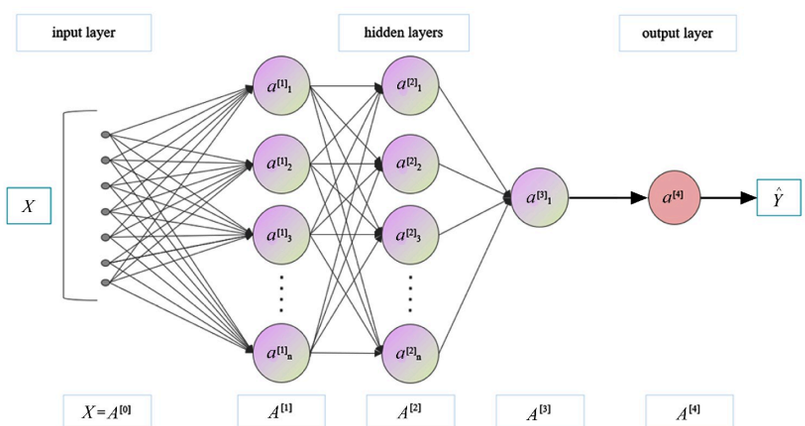


图8 BP神经网络模型

Fig. 8 BP neural network model

图9(a) 为拟合效果曲线, 横坐标为样本数, 纵坐标为归一化数值, 归一化是为了归纳训练集样本的统计分布性, 便于数据处理, 保证程序运行时收敛加快。图中原始数据曲线为对最优信号态强度μ选取的101 × 21数据集, 原始数据曲线与预测数据点呈现类似周期的变化规律, 是由于在原始数据选取过程中, 按照同一发射功率下传输距离递增的顺序进行最优信号态强度选取, 即每当同一发射功率下101个传输距离点选择完毕后, 又要对下一个发射功率下的101个传输距离点进行选择, 直到21个发射功率点选择完毕为止。图9(b)为训练误差曲线, 纵坐标表示在训练集中模型预测值与原始数据值之间的误差。由图8、9可知, 通过BP神经网络生成的预测数据的拟合效果与原始数据曲线基本一致, 样本集的训练误差小于10^{-3}, 说明该神经网络

具有较高的预测精度, 可作为一种有效模型用于实用化诱骗态经典-量子信号共纤同传系统的参数估计和预测, 对系统参数优化具有一定的指导意义。

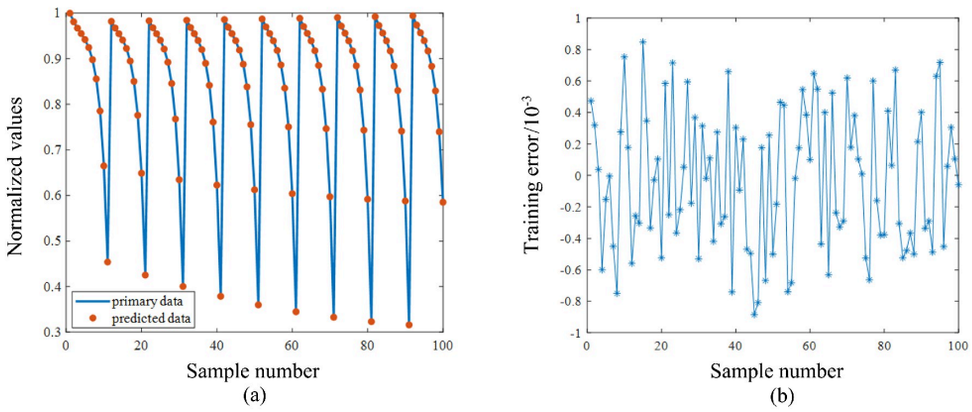


图9　使用BP神经网络的光源预测结果。(a) 拟合效果; (b) 训练误差

Fig. 9　Light source prediction results using BP neural network. (a) Imitative effect; (b) Training error

5　结　论

经典光网络与量子通信设备的高效融合是推动现代保密通信体制变革的关键一环, 经典-量子信号共纤同传技术在降低系统成本的同时, 大大提高了网络的灵活性与可拓展性。针对共纤同传系统内的复杂参数和海量数据的估计、处理、预测问题, 在对QKD系统进行噪声分析和有限长效应分析后, 利用一种BP神经网络来预测光源中的信号态平均光子数。结果显示原始数据曲线和预测数据基本拟合, 训练误差小于10^{-3}, 表明该模型能够实现智能参数预测功能, 提高了系统的运行速度和密钥分发性能, 为量子保密通信的智能化发展提供了一种可行性方案。

参考文献:

[1] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing [C]. *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, 1984: 175-179.

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

[3] Gisin N, Ribordy G, Tittel W, *et al*. Quantum cryptography [J]. *Reviews of Modern Physics*, 2002, 74(1): 145-195.

[4] Chen Y A, Zhang Q, Chen T Y, *et al*. An integrated space-to-ground quantum communication network over 4, 600 kilometres [J]. *Nature*, 2021, 589(7841): 214-219.

[5] Li Y, Liao S K, Cao Y, *et al*. Space-ground QKD network based on a compact payload and medium-inclination orbit [J]. *Optica*, 2022, 9(8): 933-938.

[6] Wang S, Yin Z Q, He D Y, *et al*. Twin-field quantum key distribution over 830-km fibre [J]. *Nature Photonics*, 2022, 16(2): 154-161.

[7] Townsend P D. Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing [J]. *Electronics Letters*, 1997, 33(3): 188-190.

[8] Runser R J, Chapuran T E, Toliver P, *et al*. Demonstration of 1.3 μm quantum key distribution (QKD) compatibility with 1.5 μm metropolitan wavelength division multiplexed (WDM) systems [C]. *OFC/NFOEC Technical Digest. Optical Fiber Communication Conference*, 2005.

[9] Nweke N I, Toliver P, Runser R J, *et al*. Experimental characterization of the separation between wavelength-multiplexed quantum and classical communication channels [J]. *Applied Physics Letters*, 2005, 87(17): 174103.

[10] Chapuran T E, Toliver P, Peters N A, *et al*. Optical networking for quantum key distribution and quantum communications [J]. *New Journal of Physics*, 2009, 11(10): 105001.

[11] Li J H, Shi L, Zhang Q F, *et al*. Noise analysis and performance optimization of experiments in classical-quantum signals co-channel transmission [J]. *Chinese Journal of Quantum Electronics*, 2021, 38(3): 365-373.
李佳豪, 石 磊, 张启发, 等. 经典-量子信号共信道传输实验噪声分析及性能优化 [J]. 量子电子学报, 2021, 38(3): 365-373.

[12] Wang Y S, Li Y X, Shi L, *et al*. Scheme of multiplexed classical and quantum transmission system with heralded single-photon source [J]. *Chinese Journal of Quantum Electronics*, 2015, 32(4): 445-451.
王宇帅, 李云霞, 石 磊, 等. 预报单光子源下的经典-量子信息共信道同传系统研究 [J]. 量子电子学报, 2015, 32(4): 445-451.

[13] Cheng K, Zhou Y Y, Wang H. Performance analysis of classical-quantum signals simultaneous transmission sharing a same fiber schemes [J]. *Chinese Journal of Quantum Electronics*, 2019, 36(3): 336-341.
程 康, 周媛媛, 王 欢. 经典-量子信号共纤同传方案性能分析 [J]. 量子电子学报, 2019, 36(3): 336-341.

[14] 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.

[15] Choi I, Young R J, Townsend P D. Quantum key distribution on a 10 Gb/s WDM-PON [J]. *Optics Express*, 2010, 18(9): 9600-9612.

[16] Mora J, Amaya W, Ruiz-Alba A, *et al*. Simultaneous transmission of 20x2 WDM/SCM-QKD and 4 bidirectional classical channels over a PON [J]. *Optics Express*, 2012, 20(15): 16358-16365.

[17] Wang L J, Chen L K, Ju L, *et al*. Experimental multiplexing of quantum key distribution with classical optical communication [J]. *Applied Physics Letters*, 2015, 106(8): 081108.

[18] Wang B X, Mao Y Q, Shen L, *et al*. Long-distance transmission of quantum key distribution coexisting with classical optical communication over a weakly-coupled few-mode fiber [J]. *Optics Express*, 2020, 28(9): 12558-12565.

[19] Yoshino K I, Fujiwara M, Tanaka A, *et al*. High-speed wavelength-division multiplexing quantum key distribution system [J]. *Optics Letters*, 2012, 37(2): 223-225.

[20] Ferreira da Silva T, Xavier G B, Temporão G P, *et al*. Impact of Raman scattered noise from multiple telecom channels on fiber-optic quantum key distribution systems [J]. *Journal of Lightwave Technology*, 2014, 32(13): 2332-2339.

[21] 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.

[22] Sun Y M, Lu Y S, Niu J N, *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.

[23] Niu J N, Sun Y M, Cai C, *et al*. Optimized channel allocation scheme for jointly reducing four-wave mixing and Raman scattering in the DWDM-QKD system [J]. *Applied Optics*, 2018, 57(27): 7987-7996.

[24] 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.

[25] Dynes J F, Tam W W S, Plews A, *et al*. Ultra-high bandwidth quantum secured data transmission [J]. *Scientific Reports*, 2016, 6: 35149.

[26] Wang L J, Zou K H, Sun W, *et al*. Long distance co-propagation of quantum key distribution and terabit classical optical data channels [J]. *Physical Review A*, 2017, 95(1): 012301.

[27] Eriksson T A, Hirano T, Puttnam B J, *et al*. Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels [J]. *Communications Physics*, 2019, 2: 9.

[28] Geng J Q, Fan-Yuan G J, Wang S, *et al*. Coexistence of quantum key distribution and optical transport network based on standard single-mode fiber at high launch power [J]. *Optics Letters*, 2021, 46(11): 2573-2576.

[29] Geng J Q, Fan-Yuan G J, Wang S, *et al*. Quantum key distribution integrating with ultra-high-power classical optical communications based on ultra-low-loss fiber [J]. *Optics Letters*, 2021, 46(24): 6099-6102.

[30] Geng J Q, Fan-Yuan G J, Li K J, *et al*. Integration in the C-band between quantum key distribution and the classical channel of 25 dBm launch power over multicore fiber media [J]. *Optics Letters*, 2022, 47(12): 3111-3114.

[31] Liu W Q, Huang P, Peng J Y, *et al*. Integrating machine learning to achieve an automatic parameter prediction for practical continuous-variable quantum key distribution [J]. *Physical Review A*, 2018, 97(2): 022316.

[32] Lu F Y, Yin Z Q, Wang C, *et al*. Parameter optimization and real-time calibration of a measurement-device-independent quantum key distribution network based on a back propagation artificial neural network [J]. *Journal of the Optical Society of America B*, 2019, 36(3): B92-B98.

[33] Wang W Y, Lo H K. Machine learning for optimal parameter prediction in quantum key distribution [J]. *Physical Review A*, 2019, 100(6): 062334.

[34] Ding H J, Liu J Y, Zhang C M, *et al*. Predicting optimal parameters with random forest for quantum key distribution [J]. *Quantum Information Processing*, 2020, 19(2): 60.

[35] Niu J N, Sun Y M, Jia X L, *et al*. Key-size-driven wavelength resource sharing scheme for QKD and the time-varying data services [J]. *Journal of Lightwave Technology*, 2021, 39(9): 2661-2672.

[36] Zhao L Y, Wu Q J, Qiu H K, *et al*. Practical security of wavelength-multiplexed decoy-state quantum key distribution [J]. *Physical Review A*, 2021, 103(2): 022429.

[37] Ma X F, Qi B, Zhao Y, *et al*. Practical decoy state for quantum key distribution [J]. *Physical Review A*, 2005, 72(1): 012326.