基于 BP 神经网络的测量设备无关协议参数预测

周江平[1]，周媛媛[1*]，周学军[1]，李洁琼[2]

（1. 海军工程大学 电子工程学院，武汉 430000；2. 92682 部队，湛江 524000）

摘要 针对传统参数优化方法计算开销大，不能满足实时性要求高、计算量大等应用场景的问题，结合当今主流的机器学习方法，提出了一种改进的基于 BP 神经网络的参数优化方法，利用本地搜索算法的数据训练网络并对参数进行预测，替代传统的查找算法，从而获得更好的实时性和更低的计算复杂度，随后与基于随机森林和 XGBoost 的方法进行了比较。仿真结果表明，BP 神经网络预测所得各参数的均方误差数量级为 10^{-6} 或更小，由该参数计算所得密钥生成率与最优密钥生成率比值的均值为 0.998 8，且该应用中 BP 神经网络相对随机森林和 XGBoost 具有更好的预测性能。

关键词 量子光学；量子密钥分发；BP 神经网络；参数优化；测量设备无关

中图分类号 TN918; O431.2 **文献标志码** A DOI 10.12178/1001-0548.2023011

Measurement Device Independent Protocol Parameter Prediction Based on BP Neural Network

ZHOU Jiangping[1], ZHOU Yuanyuan[1*], ZHOU Xuejun[1], and LI Jieqiong[2]

(1. College of Electronic Engineering, Naval University of Engineering, Wuhan 430000, China; 2. Unit 92682, Guangdong 524000, China)

Abstract The traditional parameter optimization algorithm cannot meet the requirements of the application scenarios with high real-time, large amount of calculation. Combining with the current mainstream machine learning methods, an improved parameter optimization method based on back-propagation BP neural network is proposed. Using the data of the local search algorithm to train the network and predict the parameters, the proposed methods can obtain better real-time performance and lower computational complexity for the traditional search algorithm is replaced. The proposed method is compared with random forest and XGBoost methods. The simulation results show that the order of magnitude of the mean square error of each parameter predicted by BP neural network is 10^{-6} or less. The average value of the ratio between the key generation rate calculated by the predicted parameter and the optimal key generation rate is 0.9988. And BP neural network in this application has better prediction performance than random forest and XGBoost.

Key words quantum optics; quantum key distribution; BP neural network; parameter optimization; measurement device independent

量子密钥分发（Quantum Key Distribution, QKD）基于量子力学基本原理，可实现远距离双方无条件安全通信[1]。由于实际应用中，光源、检测器等设备非理想性，系统存在诸多安全漏洞。为此，诱骗态协议[2]、测量设备无关（Measurement Device Independent, MDI）协议[3]等相继被提出，有效解决了窃听者针对光源和测量设备的攻击。尽管双场（Twin Field, TF）量子密钥分发协议[4]被提出，突破了密钥生成率的 PLOB 界[5]，但其离实际应用还有较长的路要走。测量设备无关协议作为一种更加成熟的协议，其多种变种协议[6-9]的性能仍然较好，是量子密钥分发领域重要的协议分支。

在量子密钥分发的实际应用中，为提升密钥生成率和最大传输距离，需要根据实际应用环境参数，如数据长度、失调误差、传输距离等，优化系统参数的选择，如信号态强度、诱骗态强度等。传统的方法主要有全局搜索和本地搜索两种[10]，但这两种方法耗时均较长。随着量子网络的发展，接入网络的设备越来越多，网络单元变化导致的参数优化计算量激增[11]，为满足实时通信要求，须将搜索

收稿日期：2023−01−06；修回日期：2023−03−22

作者简介：周江平，博士，主要从事量子通信方面的研究。

*通信作者 E-mail: EPJZYY@aliyun.com

时间控制在毫秒级，针对这种计算量大、实时性要求高的应用场景，传统方法无法实现。

随着机器学习的发展，已有多个结合机器学习的方法实现了最优参数的实时预测。文献 [12] 利用 BP 神经网络（Back-Propagation Neural Network, BPNN）对基于 MDI 协议的量子密钥分发网络进行参数优化和误差校准，证明了 BP 神经网络的有效性；文献 [13] 将随机森林（Random Forest, RF）应用于 MDI 协议的参数预测，取得了较 BPNN 更好的效果；文献 [14] 将 XGBoost 应用于 TF 协议的参数预测，取得了较 RF 和 BPNN 更好的效果。然而，上述 3 种方法均为基于单个参数的预测，即分别针对每一个参数来构建和训练不同的网络，而实际中，密钥生成率由参数的组合来决定，参数之间可能存在特定联系，因而将参数以整体的形式进行预测更加合理。

本文基于 BP 神经网络对参数整体进行预测，并与随机森林和 XGBoost 方法进行对比。

1 三强度诱骗态 MDI 协议

不失一般性，本文考虑基于统计波动的三强度诱骗态 MDI 协议进行分析。MDI 协议的密钥生成率公式[3] 为：

$$R \geqslant P_{11}^{\mathrm{Z}} Y_{11}^{\mathrm{Z}}\left[1-H\left(e_{11}^{\mathrm{X}}\right)\right]-Q_{\mu\mu}^{\mathrm{Z}} f_e H\left(E_{\mu\mu}^{\mathrm{Z}}\right) \tag{1}$$

式中，11 表示通信双方发送的光子数均为 1；μ表示信号态强度；Z 和 X 表示基矢的选择；Y_{11}^{Z}为计数率；e_{11}^{X}表示错误计数率；$Q_{\mu\mu}^{\mathrm{Z}}$为总增益；f_e为纠错效率；$E_{\mu\mu}^{\mathrm{Z}}$表示量子比特误码率；$H(x)$为熵函数，其表达式为$H(x)=-x\log_2(x)-(1-x)\log_2(1-x)$；$P_{11}^{\mathrm{Z}}$为信源产生 Z 基下 11 光子态的概率。

在三强度诱骗态 MDI 协议中，通过对不同信源强度$\{\mu,\nu,\omega\}$下总增益和量子比特误码率的测量，可以估计Y_{11}^{Z}和e_{11}^{X}，从而得到最终密钥生成率[15-16]。考虑统计波动、真实值和实验值之间存在偏差，采用标准差分析法[17]：

$$\begin{gathered} Q_{q_{\mathrm{a}}q_{\mathrm{b}}}^{\lambda}\left(1-\beta_q\right) \leqslant Q_{q_{\mathrm{a}}q_{\mathrm{b}}}^{\lambda} \leqslant Q_{q_{\mathrm{a}}q_{\mathrm{b}}}^{\lambda}\left(1+\beta_q\right) \\ E_{q_{\mathrm{a}}q_{\mathrm{b}}}^{\lambda} Q_{q_{\mathrm{a}}q_{\mathrm{b}}}^{\lambda}\left(1-\beta_{eq}\right) \leqslant E_{q_{\mathrm{a}}q_{\mathrm{b}}}^{\lambda} Q_{q_{\mathrm{a}}q_{\mathrm{b}}}^{\lambda} \leqslant E_{q_{\mathrm{a}}q_{\mathrm{b}}}^{\lambda} Q_{q_{\mathrm{a}}q_{\mathrm{b}}}^{\lambda}\left(1+\beta_{eq}\right) \end{gathered} \tag{2}$$

式中，$\lambda \in \{\mathrm{X},\mathrm{Z}\}$表示基的选择；$q_{\mathrm{a}},q_{\mathrm{b}}$分别表示通信双方的信源强度选择；$Q_{q_{\mathrm{a}}q_{\mathrm{b}}}^{\lambda},E_{q_{\mathrm{a}}q_b}^{\lambda}$分别表示总增益和量子比特误码率；波动率$\beta_q,\beta_{eq}$可分别表示为：

$$\begin{gathered} \beta_q=\min\left(\frac{n_\alpha}{\sqrt{N_{q_{\mathrm{a}}q_{\mathrm{b}}}^{\lambda} Q_{q_{\mathrm{a}}q_{\mathrm{b}}}^{\lambda}}},1\right) \\ \beta_{eq}=\min\left(\frac{n_\alpha}{\sqrt{N_{q_{\mathrm{a}}q_{\mathrm{b}}}^{\lambda} E_{q_{\mathrm{a}}q_{\mathrm{b}}}^{\lambda} Q_{q_{\mathrm{a}}q_{\mathrm{b}}}^{\lambda}}},1\right) \end{gathered} \tag{3}$$

式中，n_α为标准差，与置信度相对应；$N_{q_{\mathrm{a}}q_{\mathrm{b}}}^{\lambda}$为选择对应的信源强度和基底时，发送的总脉冲个数。

不同的信源强度概率和基选概率会影响$N_{q_{\mathrm{a}}q_{\mathrm{b}}}^{\lambda}$的值，从而影响最终密钥的生成率。假设选择$\{\mu,\nu,\omega\}$的概率分别为$P_\mu,P_\nu,P_\omega$，3 个概率之间存在关系$P_\omega=1-P_\mu-P_\nu$，确定信源强度后选择 X 基的条件概率为$P_{\mathrm{X}|\mu},P_{\mathrm{X}|\nu},P_{\mathrm{X}|\omega}$，那么选择 Z 基的条件概率分别为$1-P_{\mathrm{X}|\mu},1-P_{\mathrm{X}|\nu},1-P_{\mathrm{X}|\omega}$。

假设$\mu>\nu>\omega\geqslant 0$，直接使用文献 [18] 中的结论，根据式 (2)，Y_{11}^{Z}和e_{11}^{X}可用如下公式进行估计：

$$\begin{gathered} Y_{11}^{\mathrm{Z}} \geqslant Y_{11}^{\mathrm{Z,L}}=\frac{1}{(\mu-\omega)^2(\nu-\omega)^2(\mu-\nu)}\times \\ \left(\begin{array}{l} \left(\mu^2-\omega^2\right)(\mu-\omega)\left(Q_{\nu\nu}^{\mathrm{Z,L}}\exp(2\nu)+Q_{\omega\omega}^{\mathrm{Z,L}}\exp(2\omega)-Q_{\nu\omega}^{\mathrm{Z,U}}\exp(\nu+\omega)-Q_{\omega\nu}^{\mathrm{Z,U}}\exp(\omega+\nu)\right)- \\ \left(\nu^2-\omega^2\right)(\nu-\omega)\left(Q_{\mu\mu}^{\mathrm{Z,U}}\exp(2\mu)+Q_{\omega\omega}^{\mathrm{Z,U}}\exp(2\omega)-Q_{\mu\omega}^{\mathrm{Z,L}}\exp(\mu+\omega)-Q_{\omega\mu}^{\mathrm{Z,L}}\exp(\omega+\mu)\right) \end{array}\right) \\ e_{11}^{\mathrm{X}} \leqslant e_{11}^{\mathrm{X,U}}=\frac{1}{(\nu-\omega)^2 Y_{11}^{\mathrm{X,L}}}\times \\ \left(E_{\nu\nu}^{\mathrm{X,U}} Q_{\nu\nu}^{\mathrm{X,U}}\exp(2\nu)+E_{\omega\omega}^{\mathrm{X,U}} Q_{\omega\omega}^{\mathrm{X,U}}\exp(2\omega)-E_{\nu\omega}^{\mathrm{X,L}} Q_{\nu\omega}^{\mathrm{X,L}}\exp(\nu+\omega)-E_{\omega\nu}^{\mathrm{X,L}} Q_{\omega\nu}^{\mathrm{X,L}}\exp(\omega+\nu)\right) \end{gathered} \tag{4}$$

式 (4) 中上标 U 和 L 分别表示根据测量值估计出真实值区间的上下边界，该边界可由式 (2) 直接得到。$Y_{11}^{\mathrm{X,L}}$的估计公式与$Y_{11}^{\mathrm{Z,L}}$相似，仅仅只有基的差别。

假设光源为相干态光源，那么脉冲中光子数分布满足泊松分布，生成密钥的 11 光子态概率为：

$$P_{11}^{\mathrm{Z}}=P_\mu^2\left(1-P_{X|\mu}\right)^2\mu^2\exp(-2\mu) \tag{5}$$

综合来看，密钥生成率与如下 8 个独立参数的选择有关：$\mu,\nu,\omega,P_\mu,P_\nu,P_{\mathrm{X}|\mu},P_{\mathrm{X}|\nu},P_{\mathrm{X}|\omega}$。

2 基于 BP 神经网络的参数优化模型

2.1 BP 神经网络

BP 神经网络[19] 是机器学习中一种被广泛应用的人工神经网络。如果有足够的训练数据以及合理

的超参数设定，它可以逼近十分复杂的函数关系，具有非线性映射、良好的自适应性以及较好的泛化能力。

BP 神经网络中，基本单元是“神经元”。它模仿生物大脑的神经元，将所有的输入进行线性组合并根据激活函数计算输出：

$$y=\sigma\left(\sum w_i x_i+b\right) \tag{6}$$

式中，y是神经元的输出；x_i是神经元的输入；w_i是每一个输入对应的权重；b是偏置；$\sigma(x)$为激活函数，可以选择 sigmoid 函数、ReLU 函数等。

BP 神经网络一般包括输入层、隐藏层和输出层。隐藏层可以是单层或者多层。每一层由多个神经元组成，同一层神经元互不连接，相邻层的神经元相互连接。

在输入层输入一组数据后，经过神经网络的处理会在输出层得到一组输出，该输出与真实值之间可能存在一定的误差，可以定义损失函数来描述这种误差，通过“反向传播”算法调整神经网络中连接的权值，使得损失函数最小，这样就可以使得神经网络的输出更加接近真实值。这也说明神经网络可以很好地近似输入与输出之间的映射关系。从而对新的输入可通过神经网络较准确地预测其输出。

2.2　参数优化模型

密钥生成率R除了与用户选择的参数$\boldsymbol{x}=[\mu,\nu,\omega,P_\mu,P_\nu,P_{X|\mu},P_{X|\nu},P_{X|\omega}]$有关外，还与系统环境有关，如失调误差$e_\mathrm{d}$、暗计数率$p_\mathrm{d}$、检测效率$\eta_\mathrm{d}$、纠错效率$f$、置信度$\varepsilon$、传输距离$L$、总脉冲数$N$等。其中，纠错效率和置信度为系统算法级的参数，一般不会改变，检测效率可以转换至系统传输率中进行计算，因此等效于L的变化。因此，系统环境特征可表示为$\boldsymbol{s}=[e_\mathrm{d},p_\mathrm{d},L,N]$。参数优化问题可表述为对于一组已知的系统环境特征$\boldsymbol{s}$，寻找一组最优参数$\boldsymbol{x}_\mathrm{opt}$，使得密钥生成率$R$最大，即：

$$\boldsymbol{x}_\mathrm{opt}(\boldsymbol{s})=\arg\max_{\boldsymbol{x}\in\boldsymbol{X}}R(\boldsymbol{s},\boldsymbol{x}) \tag{7}$$

式中，$\boldsymbol{X}$为参数$\boldsymbol{x}$的取值空间。

$\boldsymbol{x}$关于$\boldsymbol{s}$的函数难以求解解析表达式，目前常用的方法是全局搜索、本地搜索或者神经网络算法。构建图 1 所示神经网络来解决这一问题。

神经网络共 4 层，输入层用 4 个神经元，两个隐藏层分别用 400 和 200 个神经元，输出层用 8 个神经元，层之间全连接。激活函数用 ReLU 函数。

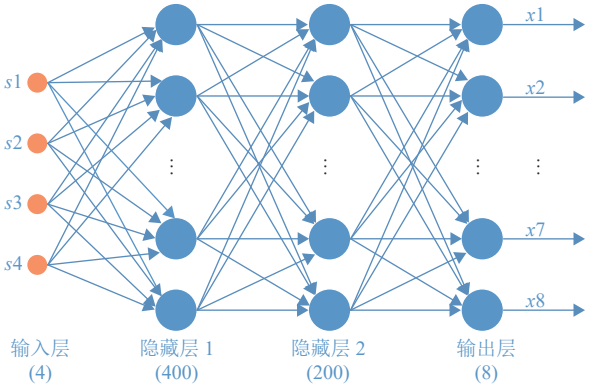


图 1　神经网络模型

3　仿真及分析

3.1　数据准备

实验中相关参数主要来源于文献 [20]，是 QKD 实验中常用参数。固定参数$f=1.15$，$\eta_\mathrm{d}=14.5\%$，$\varepsilon=1-10^{-7}$，光纤衰减系数$\alpha=0.2$，其余参数取值范围见表 1。

表 1　仿真中用到的部分实验参数

e_d/%	p_d	N	L/km
1～5	10^{-10}～10^{-6}	10^{8}～10^{15}	1～250

其中e_d、p_d和N，在其取值范围内均匀选取 12 个值，在L的取值范围内均匀选取 250 个值，共得到 432 000 组不同的数据。对不同的取值利用本地搜索算法[10] 求解最优参数$\boldsymbol{x}$，并根据式 (1) 求解密钥生成率R。

从表 1 中可以看出，不同的输入参数之间取值差异很大，需对数据进行归一化，以便更好地适应 BPNN 的特点。密钥生成率为 0 的数据并没有包含有效的参数优化信息，因而过滤掉该部分数据。将剩余数据按照 2:1 随机分为训练集和测试集。

3.2　基于 BP 神经网络的参数优化

考虑常见的一组环境参数：数据长度为2.7×10^{14}，暗计数为4.5×10^{-7}，失调误差为 1.4%。在不同距离时，预测用户选择的各参数情况如图 2 所示。

图 2 中，实线和虚线均为利用 LSA 算法求取的参数值，圆点和×型点为利用 BP 神经网络预测得到的参数值，为更清晰地显示预测值，对 BP 神经网络得到的所有预测值按照等间隔抽样，仅将样本以点的形式展示在图中。从图中可以看出，8 个

参数在距离小于 220 km 时，BP 神经网络与 LSA 算法得到的最优参数几乎相同，超过 220 km 后，二者的差距越来越明显。特别是P_μ和$P_{X|\mu}$，BP 神经网络的预测值甚至超出其取值范围。这是因为当距离超过 220 km 时，LSA 算法无法得到有效的参数使得密钥生成率大于 0，这部分数据对系统没有意义，因而没有用于 BP 神经网络的训练，故 BP 神经网络对这部分参数的预测与 LSA 算法会存在较大的差异。

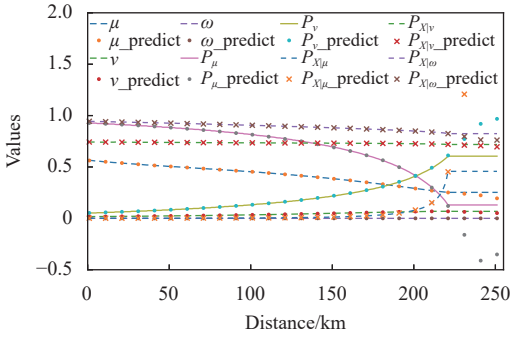


图 2　固定环境参数下 BP 神经网络参数预测结果

分别将基于 BP 神经网络预测与基于 LSA 算法得到的参数代入密钥生成率公式，密钥生成率图像如图 3 所示。图中，实线为基于 LSA 算法得到的密钥生成率曲线，×型点为基于 BP 神经网络得到的密钥生成率，二者图像几乎重叠，说明 BP 神经网络对最优参数预测的准确性与 LSA 算法相近，证明了其有效性。

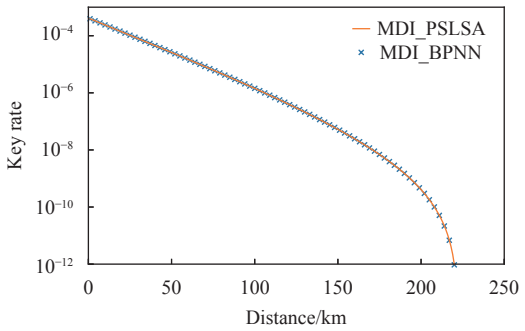


图 3　基于 BP 神经网络预测参数计算的密钥生成率

3.3　BPNN、RF 和 XGBoost 预测性能比较

除 BPNN 外，基于机器学习的预测模型还有很多，比较典型的有随机森林和 XGBoost 等[21-22]。实际上其他小组在量子密钥分发的参数预测中也应用过上述两种模型。

首先基于均方误差（Mean Square Error, MSE）比较不同模型对参数预测的准确性。以前面准备的数据集为基础，排除掉密钥生成率为 0 的数据，如$L>220$ km的相关数据。主要是因为该部分数据在实际应用中没有意义，预测的准确性不会影响系统性能。3 个模型分别基于此数据集进行训练和参数预测，计算 MSE，具体结果见表 2。

表 2　不同模型对相关参数预测的均方误差

模型	参数							
	μ	ν	ω	P_μ	P_ν	$P_{X\|\mu}$	$P_{X\|\nu}$	$P_{X\|\omega}$
BPNN	2.0×10^{-6}	4.4×10^{-8}	3.0×10^{-24}	6.2×10^{-6}	3.3×10^{-6}	3.1×10^{-6}	2.1×10^{-7}	3.0×10^{-7}
RF	3.7×10^{-6}	6.6×10^{-8}	4.4×10^{-25}	2.1×10^{-4}	8.6×10^{-5}	2.9×10^{-4}	4.6×10^{-6}	7.8×10^{-5}
XGBoost	3.9×10^{-5}	1.2×10^{-5}	3.2×10^{-19}	2.3×10^{-4}	1.6×10^{-4}	4.8×10^{-4}	1.8×10^{-5}	2.6×10^{-5}

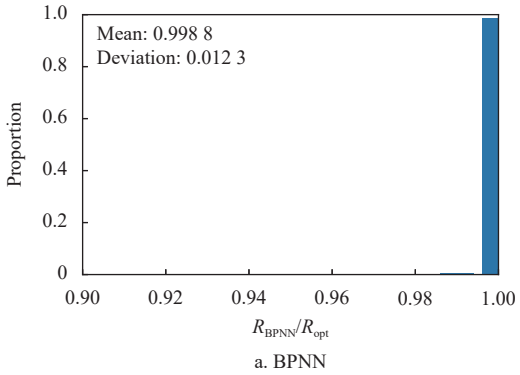
由表 2 中数据可知，3 种方法预测所得结果都较为准确，MSE 都在10^{-4}量级或更小。根据经验，ω取值很小，通常为 0，故其 MSE 都很小。相比 RF 和 XGBoost，BPNN 预测结果中除ω外，其余参数的 MSE 均最小，且P_μ、$P_{X|\mu}$、$P_{X|\omega}$这 3 个参数对应的 MSE 相较要小 2 个数量级，因而其预测结果相对更加准确；RF 和 XGBoost 预测性能相当，仅在对ν和ω两个参数的预测中，RF 要明显优于 XGBoost，而在剩余参数中二者具有相近的 MSE。总体来看，3 种模型对各参数预测的准确性，BPNN 要明显优于 RF 和 XGBoost，RF 要略优于 XGBoost。需要进一步说明的是，BPNN 和 RF 对ω的预测结果 MSE 分别为10^{-24}和10^{-25}量级，RF 相对更优，但是ω在$[0,10^{-4}]$范围内变化时，对密钥生成率的影响不大[10]，从对密钥生成率影响大小的角度看，RF 在该处的优势并无明显意义。

从时间和计算复杂度方面看，对 80 000 个数据进行优化，利用 LSA 所花的时间约为 369 ms，利用 BPNN 所花的时间约为 1.06 ms，利用 XGBoost 所花时间约为 1.17 ms，利用 RF 所花时间约为 9.93 ms。可以看出，利用机器学习的 3 种方法所

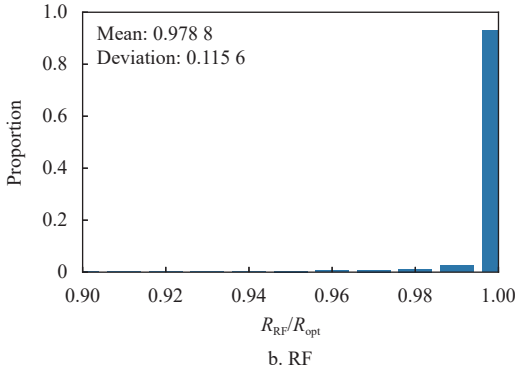
花时间在同一个数量级上，比利用 LSA 算法快两个数量级。不可否认，机器学习在前期训练时，需要花费大量的时间来训练，本实验中通常在 10 h 以上，但是这个时间是在系统工作之前，不会对系统的实时性产生影响。且实际应用中可以利用神经网络加速芯片进一步提高 BPNN 的预测速度。

一般情况下，所选各参数分量越接近最优值，得到的密钥生成率越大。然而密钥生成率关于 8 个参数的函数并非凸函数，且不同参数的波动对最终密钥的影响大小也不尽相同，因而有必要基于最终密钥生成率对 3 种模型预测性能进行比较。

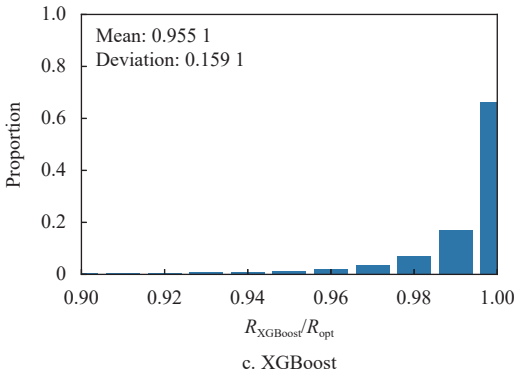
图 4 展示了通过 BPNN、RF 和 XGBoost 预测参数计算得到的密钥生成率与最优密钥生成率的比值情况，横轴表示二者比值，纵轴表示在测试集中该比值所占比例。整体来看，3 种模型密钥生成率预测值和最优值的比值几乎都集中在 0.9 以上，这说明 3 种模型预测性能良好，能得到的较高的密钥生成率。对比来看，BPNN 中密钥生成率预测值和最优值的比值集中在 0.98 以上，RF 主要集中在 0.95 以上，而 XGBoost 在 0.90 处仍有少量值；此外，BPNN 中密钥生成率预测值和最优值的比值具有相对更大的均值 0.998 8 和更小的标准差 0.012 3，因此 BPNN 具有更好的预测性能。



a. BPNN



b. RF



c. XGBoost

图 4　密钥生成率不同模型预测值与最优值的比值

4　结束语

本文首先将环境参数和用户设置参数区分开来，构建了通用的测量设备无关量子密钥分发参数预测模型，随后基于 BP 神经网络，改进对单独参数单独构建网络预测的做法，将用户设置参数作为整体，实现了联合参数预测，从仿真结果可以看出，无论是对各用户设置参数的预测准确性，还是通过预测参数计算得到的最终密钥生成率的准确性，都具有良好的性能。

与机器学习常用的 RF 和 XGBoost 算法比较可知，本文构建的 BP 神经网络无论是在各参数的预测值还是基于预测参数求出的密钥生成率中，都具有更高的准确性。可以作为未来实时量子密钥分发和大型量子密钥分发网络中参数设置和调整优化的有效手段。

参 考 文 献

[1] LO H K, CHAU H F. Unconditional security of quantum key distribution over arbitrarily long distances[J]. Science, 1999, 283(5410): 2050-2056.

[2] 陈小明, 陈雷, 阎亚龙. 诱骗态量子密钥分发中不可区分假设的合理性和安全性验证[J]. 电子科技大学学报, 2022, 51(4): 482-487.
CHEN X M, CHEN L, YAN Y L. Rationality and security verification of indistinguishability assumption in decoy-state quantum key distribution[J]. Journal of University of Electronic Science and Technology of China, 2022, 51(4): 482-487.

[3] LO H K, CURTY M, QI B. Measurement-device-independent quantum key distribution[J]. Physical Review Letters, 2012, 108(13): 130503.

[4] LUCAMARINI M, YUAN Z L, DYNES J F, et al. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters[J]. Nature, 2018, 557(7705): 400-403.

[5] 周江平, 周媛媛, 周学军, 等. 二诱骗态相位匹配量子密钥

分发方案[J]. 电子科技大学学报, 2021, 50(5): 650-655.
ZHOU J P, ZHOU Y Y, ZHOU X J, et al. Two-decoy-state phase matching quantum key distribution method[J]. Journal of University of Electronic Science and Technology of China, 2021, 50(5): 650-655.

[6] YU Z W, ZHOU Y H, WANG X B. Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method[J]. Physical Review A, 2015, 91(3): 032318.

[7] ZHOU Y H, YU Z W, WANG X B. Making the decoy-state measurement-device-independent quantum key distribution practically useful[J]. Physical Review A, 2016, 93(4): 042324.

[8] DING H J, MAO C C, ZHANG C M, et al. Improved statistical fluctuation analysis for measurement-device-independent quantum key distribution[J]. Quantum Information Processing, 2018, 17: 332.

[9] 韩朵, 李志慧, 高菲菲. 几类量子密钥分发协议的比较与分析[J]. 量子光学学报, 2019, 25(4): 380-386.
HAN D, LI Z H, GAO F F. Comparison and analysis of several kinds of quantum key distribution protocols[J]. Journal of Quantum Optics, 2019, 25(4): 380-386.

[10] XU F, XU H, LO H K. Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution[J]. Physical Review A, 2014, 89(5): 052333.

[11] 徐雅斌, 陈淑娟, 李艳平. 量子密钥分发网络的多路径密钥传输方法研究[J]. 电子科技大学学报, 2020, 49(2): 276-282.
XU Y B, CHEN S J, LI Y P. Research on multipath key transmission in quantum key distribution networks[J]. Journal of University of Electronic Science and Technology of China, 2020, 49(2): 276-282.

[12] WANG W, LO H K. Machine learning for optimal parameter prediction in quantum key distribution[J]. Physical Review A, 2019, 100(6): 062334.

[13] 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.

[14] DONG Q, HUANG G, CUI W, et al. Optimization parameter prediction-based XGBoost of TF-QKD[J]. Quantum Information Processing, 2022, 21(7): 1-9.

[15] MA X, FUNG C H F, RAZAVI M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution[J]. Physical Review A, 2012, 86(5): 052305.

[16] SUN S H, GAO M, LI C Y, et al. Practical decoy-state measurement-device-independent quantum key distribution[J]. Physical Review A, 2013, 87(5): 052329.

[17] MA X, QI B, ZHAO Y, et al. Practical decoy state for quantum key distribution[J]. Physical Review A, 2005, 72(1): 012326.

[18] XU F, CURTY M, QI B, et al. Practical aspects of measurement-device-independent quantum key distribution[J]. New Journal of Physics, 2013, 15(11): 113007.

[19] KOHONEN T. An introduction to neural computing[J]. Neural Networks, 1988, 1: 3-16.

[20] MA X, FUNG C H F, RAZAVI M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution[J]. Physical Review A-Atomic, Molecular, and Optical Physics, 2012, 86: 052305.

[21] BREIMAN L. Random forests[J]. Machine Learning, 2001, 45: 5-32.

[22] LIAW A, WIENER M. Classification and regression by randomforest[J]. R News, 2002, 2(3): 18-22.

编 辑 叶 芳