

## 机器学习在量子通信资源优化配置中的应用\*

陈以鹏<sup>1)2)#</sup> 刘靖阳<sup>1)2)#</sup> 朱佳莉<sup>1)2)</sup> 方伟<sup>1)2)</sup> 王琴<sup>1)2)†</sup>

1) (南京邮电大学, 量子信息技术研究所, 南京 210003)

2) (南京邮电大学, 宽带无线通信与传感网教育部重点实验室, 南京 210003)

(2022年5月4日收到; 2022年7月7日收到修改稿)

在未来量子通信网络的大规模应用中, 如何根据当前用户实际情况实现资源优化配置, 比如选择最优量子密钥分发协议 (quantum key distribution, QKD) 和最优系统参数等, 是实现网络应用的一个重要考察指标. 传统的 QKD 最优协议选择以及参数优化配置方法, 大多是通过局部搜索算法来实现. 该方法需要花费大量的计算资源和时间. 为此, 本文提出了将机器学习算法应用到 QKD 资源优化配置之中, 通过回归机器学习的方式来同时进行不同情境下的最优协议选择以及最优协议的参数优化配置. 此外, 将包括随机森林 (random forest, RF)、最近邻 (k-nearest neighbor, KNN)、逻辑回归 (logistic regression) 等在内的多种回归机器学习模型进行对比分析. 数据仿真结果显示, 基于机器学习的新方案与基于局部搜索算法的传统方案相比, 在资源损耗方面实现了质的跨越, 而且 RF 在多个回归评估指标上都取得了最佳的效果. 此外, 通过残差分析, 发现以 RF 回归模型为代表的机器学习方案在最优协议选择以及参数优化配置方面具有很好的环境鲁棒性. 因此, 本工作将对未来量子通信网络实际应用起到重要的推进作用.

**关键词:** 量子通信, 量子密钥分发, 回归机器学习, 资源优化配置**PACS:** 03.65.-w, 03.67.Hk, 42.50.Ex, 42.79.Sz**DOI:** 10.7498/aps.71.20220871

## 1 引言

量子密钥分发 (quantum key distribution, QKD) 是量子保密通信的核心, 其安全性基于物理学基本原理, 原则上能够为远距离通信的双方 (Alice 和 Bob) 提供无条件安全的信息保障. 第一个 QKD 协议由 Bennett 和 Brassard<sup>[1]</sup> 于 1984 年提出, 此后简称 BB84 协议, 其安全性已经得到严格的数学证明<sup>[2,3]</sup>, 也是目前应用最为广泛的一种 QKD 协议. 原始的 BB84 协议需要采用理想的单光子源, 但是在实际应用中, 大多采用弱相干光源 (weak coherent source, WCS), 该类光源中的多光

子成分使得窃听方 (eve) 实施光子数分离攻击 (PNS) 成为可能. 为了解决 PNS 攻击, 科学家提出了诱骗态方法<sup>[4-6]</sup>. 此外, 探测端的测信道漏洞也是 Eve 攻击的对象<sup>[7-10]</sup>. 为了关闭探测器端的诸多侧信道漏洞, 加拿大 Lo 等<sup>[11]</sup> 和英国 Braunstein 等<sup>[12]</sup> 于 2012 年各自独立地提出了测量设备无关量子密钥分发 (measurement-device-independent, MDI) 协议. MDI-QKD 结合诱骗态方案可以免疫所有针对探测段的攻击手段, 因此提出之后受到了广泛的关注<sup>[13-18]</sup>. 在实际应用中, MDI-QKD 的安全密钥率和传输距离受统计起伏效应影响严重. 在此背景下, 双场量子密钥分发协议 (twin-field quantum key distribution, TF-QKD) 于 2018 年

\* 国家重点研究发展计划 (批准号: 2018YFA0306400, 2017YFA0304100)、国家自然科学基金 (批准号: 12074194)、江苏省自然科学基金前沿技术 (批准号: BK20192001) 和江苏省研究生科研创新计划 (批准号: KYCX20\_0726) 资助的课题.

# 同等贡献作者.

† 通信作者. E-mail: qinw@njupt.edu.cn

被 Lucamarini 等<sup>[19]</sup>提出. TF-QKD 保留了 MDI-QKD 的测量设备无关特性, 并打破了无中继量子信道码率-距离限制 (PLOB 界)<sup>[20,21]</sup>, 进一步提高了量子通信的实用性能, 这也使其成为目前关注度最高的 QKD 协议之一<sup>[22–24]</sup>.

在实际执行量子密钥分发之前, 首先需要根据用户实际情况选择合适的密钥分发协议<sup>[25,26]</sup>, 同时对选定的量子密钥分发协议进行相关参数的优化配置<sup>[27]</sup>, 从而确保通信双方之间能够实现最优的安全密钥共享, 本文将这个过程称之为最优协议选择以及最优参数配置. 传统的解决方案可以使用遍历收索方法或维度下降局域收索 (LSA) 优化算法<sup>[28]</sup>. 但是以上方法在实际应用时需要消耗大量的计算资源和计算时间, 无法满足实时量子通信的需求. 另一方面, 由于机器学习在数据处理方面的优势, 其常被用于协助解决量子信息中的部分问题<sup>[29,30]</sup>. 鉴于此, 本文考虑使用机器学习方案替代上述传统方案, 即通过机器学习实现回归模型来建模传统方案. 仿真结果表明, 相较于传统方案, 机器学习方案大幅减少了时间资源消耗, 因而显示出在实时量子通信应用中的巨大应用前景.

## 2 机器学习方案

监督机器学习过程可以简单解释为通过特征数据到标签数据的映射, 去学习一个具有指定数据预测功能的机器学习模型, 即基于某种机器学习算法  $F(x)$  通过  $X \rightarrow Y$  的映射过程去学习获取具有数据预测功能的 ML 模型  $f(x)$ . 以几种主流的量子密钥分发协议: BB84, MDI 以及 TF-QKD 为问题背景, 并主要从数据的获取和机器学习模型的构建两方面来介绍本文工作.

### 2.1 ML 标签数据与特征数据的获取

为简单起见, 本文在评价最优 QKD 协议时暂不考虑系统安全等级等因素, 仅把安全密钥速率 ( $R$ ) 作为评定特定情境下最优 QKD 协议的关键指标. 在实际 QKD 过程中,  $R$  值与下面几种系统因素紧密相关: 探测器的暗记数率 ( $Y_0$ )、探测效率 ( $\eta$ )、本底误码 ( $e_d$ ), 通信发送方发送的光脉冲数 ( $N$ ), 通信双方间的通信距离 ( $L$ ). 将系统参数组合成 5 维向量  $X = [Y_0, e_d, \eta, N, L]$ , 并将其作为 ML 的特征数据格式.

在讨论 ML 所需标签数据格式之前, 首先对获取仿真数据过程中所涉及到的 3 种主流 QKD 协议及其诱骗态方法进行简要论述. 对于 BB84 协议, 使用的是三强度诱骗态方法<sup>[5]</sup>. 在该方案中, 参数优化过程所涉及到的主要配置参数包括: 信号态强度  $\mu$ 、诱骗态强度  $\nu$ 、发送信号态脉冲的概率  $P_\mu$ 、发送诱骗态脉冲的概率  $P_\nu$ 、信号态制备在 Z 基的概率  $P_{z\mu}$ 、诱骗态制备在 X 基的概率  $P_{x\nu}$ . 对于 MDI 协议, 使用的是四强度诱骗态方法<sup>[31]</sup>, 参数优化涉及到的配置参数主要包括: 信号态强度  $\mu$ 、诱骗态强度  $\nu$  和  $\omega$ 、发送信号态  $\mu$  的概率  $P_\mu$ 、发送诱骗态  $\nu$  的概率  $P_\nu$ 、发送诱骗态  $\omega$  的概率  $P_\omega$ . 对于 TF 协议, 使用的是四强度诱骗态方法<sup>[32]</sup>, 对应系统参数包括: 信号态强度  $\mu$ 、诱骗态强度  $\nu$ ,  $\omega$  及其对应选择概率  $P_\mu$ ,  $P_\nu$ ,  $P_\omega$ , 以及失败概率  $\epsilon$  等.

为了在 ML 标签数据格式中表征所选的最优协议, 本工作将 3 种协议对应编号 1, 2, 3, 并将其作为标签向量的一个维度. 则不同协议的标签格式有:  $Y_{\text{BB84}} = [\mu, \nu, P_\mu, P_\nu, P_{z\mu}, P_{x\nu}, 1]$ ,  $Y_{\text{MDI}} = [\mu, \nu, \omega, P_\mu, P_\nu, P_\omega, 2]$ ,  $Y_{\text{TF}} = [\mu, \nu, \omega, P_\mu, P_\nu, P_\omega, \epsilon, 3]$ . 研究发现 BB84 协议和 MDI 协议的标签向量格式均为 6 维, 而 TF 协议的标签向量格式为 7 维. 为了构建统一格式的标签向量, 采用占位法来抹平上述差异, 即  $Y_{\text{BB84}} = [\mu, \nu, P_\mu, P_\nu, P_{z\mu}, P_{x\nu}, \text{NUM}, 1]$ ,  $Y_{\text{MDI}} = [\mu, \nu, \omega, P_\mu, P_\nu, P_\omega, \text{NUM}, 2]$ . 进一步地, 得益于占位方式的使用, 不同协议能够很好的保证参数维度的一致性, 这更有利于本工作推广到其他多种不同的 QKD 协议.

在标签数据格式和特征数据格式构建完成之后, 需要获取通用的特征数据和标签数据. 根据实际经验, 本文将特征数据格式中的 5 个系统参数限制到表 1 所示的特征范围中. 本工作在 5 个系统参数的特征范围内进行等间隔的取值, 以间隔  $n$  为例, 则可以生成  $n^5$  特征数据. 这里需要注意一点, 对于本底误码的取值而言, TF 协议是其他两个协议的 4 倍. 随后利用不同 QKD 协议的密钥生成公式, 并结合 LSA 算法优化不同协议的配置参数, 以获取 3 份数据量大小为  $n^5$  的标签数据. 接着通过比较不同协议的密钥率大小, 将 3 个协议关联起来, 即直接根据密钥率  $R$  将无效数据剔除后的  $Y_{\text{BB84}}$ ,  $Y_{\text{MDI}}$  和  $Y_{\text{TF}}$ , 这 3 份标签数据合并为一份标签数据  $Y$ . 至此, 便得到了 ML 所需的特征数据  $X$  和标签数据  $Y$ .

表 1 系统参数的特征范围

Table 1. Characteristic range of system parameters.

$Y_0$	$e_d$	$\eta$	$N$	$L/\text{km}$
$10^{-10}$ — $10^{-5}$	0.00—0.06	0.1—0.9	$10^6$ — $10^{16}$	1—600

## 2.2 数据集划分及回归模型构建

特征数据和标签数据统称为 ML 数据集, 经过上述的相关操作整个数据集的大小在 10 万量级. 随后本工作采用归一化 (normalization) 操作来加速 ML 模型对数据集的学习拟合, 表示为  $\text{num} = (\text{num} - \text{min}) / (\text{max} - \text{num})$ . 从数据集中随机划分出 80% 用于 ML 模型训练的训练集和 20% 用于 ML 模型性能评估的测试集. 后续, 在训练集上先后进行随机森林、最近邻、逻辑回归等 ML 模型的学习训练. 鉴于 RF 模型取得了最佳的预测效果, 接下来仅以 RF 为例, 介绍其构建的主要过程.

随机森林 (random forests, RF)<sup>[33]</sup> 是基于 Bagging (bootstrap aggregation) 集成算法的典型范例, 其基本单元是决策树 (decision tree)<sup>[34][35]</sup>, 直观理解就是众多决策树构成一片随机森林. 在机器学习任务中, 随机森林既可以用于分类任务又可以用于回归任务, 本文主要是利用 RF 算法训练一个回归模型. RF 回归模型, 是由众多回归决策树集成而来的. 回归树在训练时, 每确定一个节点, 就会将特征数据对应的特征空间进行一次划分, 划分形成的单元会以该单元内的均值作为其输出值. RF 中除了森林这一重要概念之外, 还有随机的概念. 随机主要有两种含义: 其一, 从训练集中随机有放回

的拿取样本数据用于决策树的学习, 有放回的随机抽取就是 Bagging 算法的直观体现; 其二, 随机选取特征向量中的特征用于决策树的学习. 随机的样本数据、随机的特征选择, 导致 RF 中的决策树各不相同, 而 RF 最终输出的结果则取决于不同决策树回归输出的均值. 图 1 展示了本工作中 RF 回归模型的算法框架.

RF 在训练集上进行学习拟合时, 需要对其算法的一些参数进行调优, 才能获取预测效果最好的回归模型. 这里主要使用网格搜索 (GridSearch) 和交叉验证 (CV) 的方法来对 Sklearn 中的随机森林 Regressor 模型进行调参. GridSearch 可以理解为在指定参数范围内按照一定步长将候选参数所有可能的取值进行排列组合, 即生成“网格”. 而交叉验证则是将训练集进一步切分, 以常见的  $K$  折交叉验证法为例, 训练集中的  $K-1$  份使用网格参数进行训练, 训练集中剩余的 1 份则用于评估, 重复  $K$  次并选出  $K$  次平均评分最高时的网格参数, 进而完成参数调优. 本工作中 RF 回归模型的最终调参结果是:  $n\_estimators$  为 90、 $max\_depth$  为 56、 $min\_samples\_split$  为 1. 其中, 第 1 个参数用于指定 RF 原始训练集有放回随机抽取样本数据所生成的子数据集个数; 第 2 个参数用于指定生成决策树的最大深度; 第 3 个参数用于指定决策树节点可分的最小样本数. 在完成 RF 回归模型的构建后, 对特征数据  $X$  中 5 个系统参数的重要性进行评估. 结果表明: 距离  $L$  对 RF 模型的影响最大; 其他几个系统参数的重要性相对较小, 具体的重要性比重如图 2 所示.

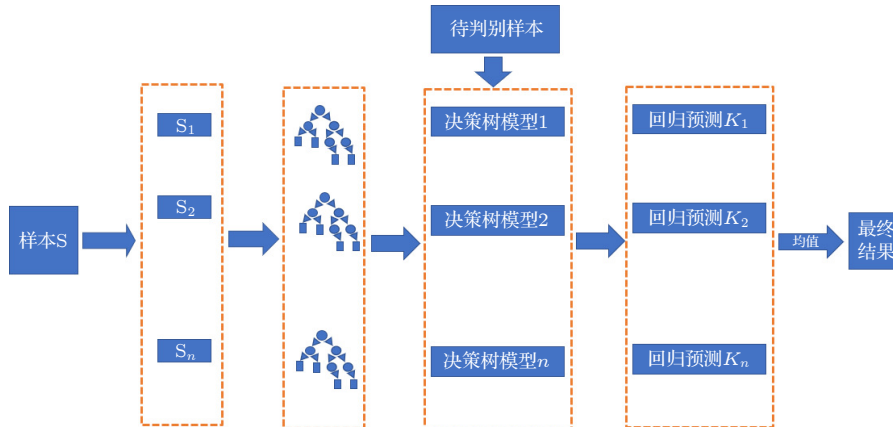


图 1 随机森林回归模型的算法框架.

Fig. 1. The algorithm framework of random forest regression model.



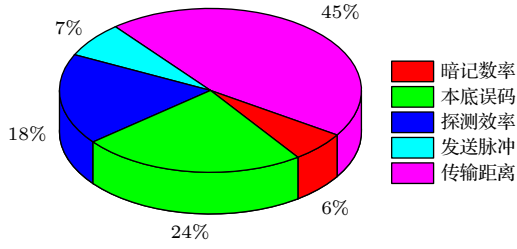


图 2 系统参数对随机森林回归模型的重要性。

Fig. 2. Importance of system parameters to RF regression model.

### 3 方案评估与讨论

在测试集上对已获 ML 模型进行性能评估时, 需要注意标签数据  $Y$  中包含了协议标号和该协议对应的配置参数. 不同于分类模型直接获取协议标号, 本工作的回归模型需要对回归预测的协议标号进行取整操作才能正确的实现协议分类. 下面简要介绍 3 种常用回归模型的性能评估指标, 并对本文的 RF, KNN, LR 模型进行比较分析.

平均绝对误差 (mean absolute error, MAE), 用于评估回归模型预测结果和真实结果差异的平均值, 其值越小说明 ML 模型对数据的拟合效果就越好, 可以表示为:  $MAE = \frac{1}{N} \sum_{i=1}^N |y_i - \tilde{y}_i|$ . 均方误差 (mean squared error, MSE), 用于计算预测结果和真实结果对应样本点误差平方和的均值, 其值越小说明 ML 模型在数据预测方面的性能就越好, 可以表示为:  $MSE = \frac{1}{N} \sum_{i=1}^N (y_i - \tilde{y}_i)^2$ . 决定系数 (coefficient of determination  $R$  squared,  $R$  squared), 一般被认为是衡量线性回归相对较好的指标, 其取值范围在  $0-1$  之间, 越靠近 1 说明 ML 模型对数据的拟合效果就越好, 可以表示为:  $R^2 = 1 - \left( \frac{\sum_{i=1}^N (y_i - \tilde{y}_i)^2}{\sum_{i=1}^N (y_i - \bar{y})^2} \right)$ . 上述表达式中的  $N$  为测试集数据量、 $y_i$  为测试集中的真实结果、 $\tilde{y}_i$  为 ML 模型使用测试集预测出来的结果、 $\bar{y} = \frac{1}{N} \sum_{i=1}^N y_i$ . 这里将回归模型的评估指标以及预测准确率如表 2 所示.

由表 2 可知, 基于相同训练集获取的 RF 回归模型相较于 KNN 和 LR 模型, 在 MAE, MSE,  $R^2$  预测准确率等性能指标上都取得了最好的表现, 这也说明 RF 适用于最优协议选择和参数优化配置的任务. 此外, 将 ML 方案 and 传统方案在个人电脑

上的具体耗时情况如表 3 所示. 个人电脑的硬件配置为: Intel(R) Core(TM) i1-9750H CPU @2.60GHz; NVIDIA GeForce GTX 1650; 16 GB DDR4 2667 MHZ. 具体的时间资源损耗统计过程, 本工作在指定某一用户需求下, 先后使用两种不同方案进行时间统计. 机器学习方案: 在获取训练完成的模型后, 将需求数据输入模型, 模型可以在短短数秒之内给出协议选择以及参数配置. 传统方案: 根据提供的用户需求数据, 采用 LSA 优化并获取 3 个协议的安全码率, 之后对 3 个协议的码率大小进行比对, 将成码率最大的协议作为最优协议. 该过程的时间损耗主要集中在采用 LSA 对协议参数进行优化获取最佳码率这个过程, 耗时超过 24 h. 从表 3 结果来看, 两种方案选择的协议相同且协议配置参数的残差在 0.025 以内, 但是两者的耗时却存在着巨大的差异, 这进一步表明机器学习在很大程度上满足了简化并加速量子通信资源配置的目的.

表 2 不同回归模型的评估对比

Table 2. Evaluation and comparison of different regression models.

	RF	KNN	LR
MAE	0.002	0.012	0.038
MSE	0.016	0.049	0.131
$R^2$	0.978	0.795	0.397
Accuracy	0.977	0.787	0.365

表 3 时间资源损耗记录表

Table 3. Time resource wastage table.

	机器学习方案			传统方案
Model	RF	KNN	LR	LSA
Time	1.23 s	2.95 s	5.43 s	24 h以上

为了更加直观地展示 RF 方案的可行性, 接下来就 RF 的残差和混淆矩阵进行可视化分析. 图 3 为 RF 回归模型在训练集和测试集上的残差图, 这里的残差分析针对的是协议的配置参数, 即标签数据  $Y$  向量中处于第一维的配置参数. 图 3 中的蓝色点为训练集上的残差情况, 绿色点为测试集上的残差情况. 经统计, 多数偏差都低于 0.025, 这表明 RF 机器学习方案具有相对较好的鲁棒性. 图 4 展示了协议选择的混淆矩阵, 主对角线的协议选择为正确的选择情况. 从图 4 可以看出, RF 模型在不同情境下都能以较大的概率做出正确的协议选择. 通过对混淆矩阵可视化数据的相关计算, 可以

求得 RF 回归模型的预测准确率在 98% 左右, 这也与表 2 中通过函数接口计算的准确率基本相当。

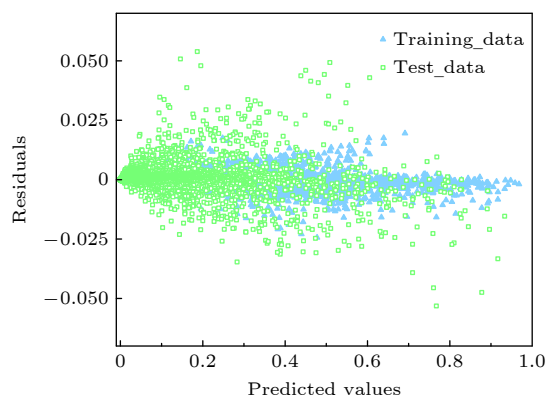


图 3 随机森林回归模型的残差图

Fig. 3. Residual diagram of RF regression model.

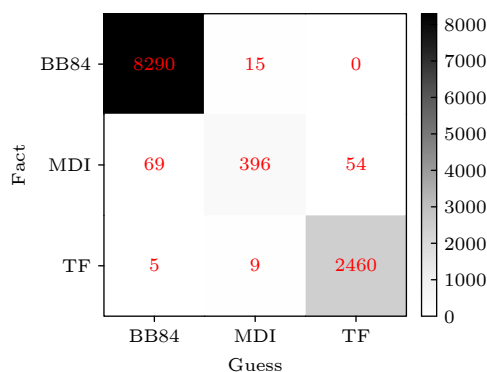


图 4 随机森林回归模型的混淆矩阵

Fig. 4. Residual diagram of RF regression model.

## 4 总结与展望

本文提出了基于机器学习的最优协议选择以及优化参数配置的新方案, 相较于传统方案而言, 新方案大幅度地减少了时间资源损耗, 通过残差分析证明机器学习方案具有较好的鲁棒性. 此外, 本文详细地介绍了机器学习方案的流程, 主要是通过监督学习去实现满足协议选择以及参数配置功能的回归模型. 在构建的多个回归模型中, RF 模型取得了最佳的表现: 均方误差为 0.002、平均绝对误差为 0.016、 $R^2$  为 0.978. 综上, 本工作的研究对未来即时量子通信网络的大规模应用以及多协议高速 QKD 的发展都有很好的参考价值.

感谢南京邮电大学通信与信息工程学院张春辉老师和周星宇老师的帮助与讨论.

## 参考文献

- [1] Bennett C H, Brassard G 1984 *Proceedings of IEEE International Conference on Computers, System and Signal Processing* (Bangalore: IEEE) p175
- [2] Busch P, Heinonen T, Lathi P 2007 *Phys. Rep.* **452** 155
- [3] Wootters W K, Zurek W H 1982 *Nature.* **299** 299
- [4] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
- [5] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
- [6] Lo H K, Ma X F, Chen K 2005 *Phys. Rev. Lett.* **94** 230504
- [7] Makarov V, Hjelme D R 2005 *J. Mod. Optic.* **52** 691
- [8] Qi B, Fung C H F, Lo H K, Ma X F 2007 *Quantum. Inf. Comput.* **7** 73
- [9] Lamas L A, Qin L, Gerhardt I, Makarov V, Kurtsiefer C 2009 *New. J. Phys.* **11** 065003
- [10] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J 2010 *Nat. Photonics.* **4** 686
- [11] Lo H, Curty M, Qi B 2012 *Phys. Rev. Lett.* **108** 130503
- [12] Braunstein S L, Pirandola S 2012 *Phys. Rev. Lett.* **108** 130502
- [13] Wang X B. 2013 *Phys. Rev. A* **87** 012320
- [14] Rubenok A, Slater J A, Chan P, Lucio M I, Tittel W 2013 *Phys. Rev. Lett.* **111** 130501
- [15] Tang Z Y, Liao Z F, Xu F H, Qi B, Qian L, Lo H K 2014 *Phys. Rev. Lett.* **112** 190503
- [16] Liu Y, Chen T Y, Wang L J, Liang H, Shentu G L, Wang J, Cui K, Yin H L, Liu N L, Li L, Ma X F, Pelc J S, Fejer M M, Peng C Z, Zhang Q, Pan J W 2013 *Phys. Rev. Lett.* **111** 130502
- [17] Zhou X Y, Ding H J, Zhang C H, Wang Q 2020 *Opt. Lett.* **45** 4176
- [18] Liu J Y, Zhou X Y, Wang Q 2021 *Phys. Rev. A.* **103** 022602
- [19] Lucamarini M, Yuan Z L, Dynes J F, Shields A J 2018 *Nature* **557** 400
- [20] Takeoka M, Guha S. 2014 *Nat. Commun.* **5** 5235
- [21] Pirandola S, Laurenza R, Ottaviani C 2017 *Nat. Commun.* **8** 15043
- [22] Wang X B, Yu Z W, Hu X L 2018 *Phys. Rev. A.* **98** 062323
- [23] Pittaluga M, Minder M, Lucamarini M, Sanzaro M, Woodward R I, Li M J, Yuan Z L, Shields A J 2021 *Nat. Photonics.* **15** 530
- [24] Wang S, Yin Z Q, Chen W, He D Y, Song X T, Li H W, Zhang L J, Zhou Z, Guo G C, Han Z F 2022 *Nat. Photonics.* **16** 154
- [25] Ren Z A, Chen Y P, Liu J Y, Ding H J, Wang Q 2021 *IEEE Commun. Lett.* **25** 3
- [26] Fan-Yuan G J, Lu F Y, Wang S, Yin Z Q, He D Y, Zhou Z, Teng J, Chen W, Guo G C, Han Z F 2021 *Photon. Res.* **9** 1881
- [27] Ding H J, Liu J Y, Zhang C M, Wang Q 2020 *Quantum. Inf. Comput.* **19** 2548
- [28] Xu F, Xu H, Lo H K. 2014 *Phys. Rev. A.* **89** 052333
- [29] Liu J Y, Ding H J, Zhang C M, Xie S P, Wang Q 2019 *Phys. Rev. Appl.* **12** 014059
- [30] Yang M, Ren C L, Ma Y C, Xiao Y, Ye X J, Song L L, Xun J S, Yung M H, Li C F, Guo G C 2019 *Phys. Rev. Lett.* **123** 190401
- [31] Zhou Y H, Yu Z W, Wang X B. 2016 *Phys. Rev. A.* **93** 042324
- [32] Zhang C H, Zhang C M, Wang Q. 2019 *Opt. Lett.* **44** 1468
- [33] Breiman L 2001 *J. Clin. Microbiol.* **45** 5
- [34] Cover T M, Hart P E 1967 *IEEE Trans. Inf. Theory* **13** 21
- [35] Cox D R 1958 *J. R. Stat. Soc. B* **20** 215

# Application of machine learning in optimal allocation of quantum communication resources\*

Chen Yi-Peng<sup>1)2)#</sup> Liu Jing-Yang<sup>1)2)#</sup> Zhu Jia-Li<sup>1)2)</sup>  
Fang Wei<sup>1)2)</sup> Wang Qin<sup>1)2)†</sup>

1) (*Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*)

2) (*Key Laboratory of Broadband Wireless Communication and Sensor Network of Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*)

( Received 4 May 2022; revised manuscript received 7 July 2022 )

## Abstract

In the application of quantum communication networks, it is an important task to realize the optimal allocation of resources according to the current situation. For example, We need to select the optimal quantum key distribution (QKD) protocol and parameters. Traditionally, the most commonly implemented method is the local search algorithm (LSA), which costs a lot of resources. Here in this work, we propose a machine learning based scheme, in which the regression machine learning is used to simultaneously select the optimal protocol and corresponding parameters. In addition, we make comparisons among a few machine learning models including random forest (RF), K-nearest neighbor (KNN) and logistic regression. Simulation results show that the new scheme takes much less time than the LSA scheme, and the RF achieves the best performance. In addition, through the RF residual analysis, we find that the machine learning scheme has good robustness. In conclusion, this work may play an important role in promoting the practical application of quantum communication networks.

**Keywords:** quantum communication network, quantum key distribution, regression machine learning, optimal allocation of resources.

**PACS:** 03.65.-w, 03.67.Hk, 42.50.Ex, 42.79.Sz

**DOI:** [10.7498/aps.71.20220871](https://doi.org/10.7498/aps.71.20220871)

---

\* Project supported by the National Key R&D Program of China (Grant Nos. 2018 YFA0306400, 2017 YFA0304100), the National Natural Science Foundation of China (Grant No. 12074194), the Leading-edge technology program of Jiangsu Natural Science Foundation (Grant No. BK20192001), and Postgraduate Research & Practice Innovation Program of Jiangsu Province (KYCX20\_0726).

# These authors contributed equally.

† Corresponding author. E-mail: [qinw@njupt.edu.cn](mailto:qinw@njupt.edu.cn)



## 机器学习在量子通信资源优化配置中的应用

陈以鹏 刘靖阳 朱佳莉 方伟 王琴

### Application of machine learning in optimal allocation of quantum communication resources

Chen Yi-Peng Liu Jing-Yang Zhu Jia-Li Fang Wei Wang Qin

引用信息 Citation: *Acta Physica Sinica*, 71, 220301 (2022) DOI: 10.7498/aps.71.20220871

在线阅读 View online: <https://doi.org/10.7498/aps.71.20220871>

当期内容 View table of contents: <http://wulixb.iphy.ac.cn>

---

## 您可能感兴趣的其他文章

### Articles you may be interested in

#### 标记单光子源在量子密钥分发中的应用

Overview of applications of heralded single photon source in quantum key distribution

物理学报. 2022, 71(17): 170304 <https://doi.org/10.7498/aps.71.20220344>

#### 基于量子催化的离散调制连续变量量子密钥分发

Discrete modulation continuous-variable quantum key distribution based on quantum catalysis

物理学报. 2020, 69(6): 060301 <https://doi.org/10.7498/aps.69.20191689>

#### 基于混合编码的测量设备无关量子密钥分发的简单协议

A simple protocol for measuring device independent quantum key distribution based on hybrid encoding

物理学报. 2020, 69(19): 190301 <https://doi.org/10.7498/aps.69.20200162>

#### 光纤偏振编码量子密钥分发系统荧光边信道攻击与防御

Eavesdropping and countermeasures for backflash side channel in fiber polarization-coded quantum key distribution

物理学报. 2019, 68(13): 130301 <https://doi.org/10.7498/aps.68.20190464>

#### 一种基于标记单光子源的态制备误差容忍量子密钥分发协议

State preparation error tolerant quantum key distribution protocol based on heralded single photon source

物理学报. 2022, 71(3): 030301 <https://doi.org/10.7498/aps.71.20211456>

#### 基于峰值补偿的连续变量量子密钥分发方案

Continuous-variable quantum key distribution based on peak-compensation

物理学报. 2021, 70(11): 110302 <https://doi.org/10.7498/aps.70.20202073>