基于回归决策树的测量设备无关型量子密钥分发参数优化*

刘天乐[1)2)] 徐枭[1)2)] 付博玮[1)2)] 徐佳歆[1)2)]
刘靖阳[1)2)] 周星宇[1)2)†] 王琴[1)2)]

1) (南京邮电大学通信与信息工程学院, 南京 210003)

2) (南京邮电大学量子信息技术研究所, 南京 210003)

(2023 年 2 月 8 日收到; 2023 年 3 月 17 日收到修改稿)

量子密钥分发 (quantum key distribution, QKD) 结合一次一密的加密方式, 可以实现无条件安全的量子通信. 双场 (twin-field, TF) QKD 和测量设备无关 (measurement-device-independent, MDI) QKD 具有较高的安全性, 同时适合构建以测量端为中心的网络, 具有广阔的应用前景. 但在实际应用过程中, 参数配置对 QKD 性能有着极大影响, 而实际场景中存在着用户数量大、位置距离中心站点非对称、并且用户大部分处在实时移动中的特点. 面对上述实时的参数配置需求, 传统的参数优化方式将无法满足. 本文提出将监督机器学习算法应用于 QKD 参数优化配置中, 通过机器学习模型预测不同场景下 TF 和 MDI 两种常用协议的最优参数. 将神经网络、最近邻、随机森林、梯度提升决策树和分类回归决策树 (classification and regression tree, CART) 等监督学习模型进行对比, 结果显示 CART 模型在 R^2 等回归评估指标上均有最优表现. 在随机划分训练组、验证组情况下, 预测参数的密钥率与最优密钥率比值的均值在 0.995 以上; 在"超精度"和"超范围"两种极限情况下, 该均值仍能维持在 0.988 左右, 且在残差分析中具有较好的环境鲁棒性, 展现出较好的性能. 此外, 基于 CART 的新方案相较于传统方案在计算实时性表现上有很大提升, 将单次预测时间缩短至微秒量级, 很好地满足了通信方在移动状态下的实时通信需求.

关键词: 量子密钥分发, 测量设备无关, 分类回归决策树, 参数优化

PACS: 03.65.–w, 03.67.Hk, 42.50.Ex, **DOI:** 10.7498/aps.72.20230160

1 引 言

量子通信的根本目标是使共享不安全信道的合法通信方 (Alice 和 Bob) 在窃听者 (Eve) 存在的条件下依然能够进行信息的安全传输. 作为一种理论上无条件安全的密钥分发技术, 量子密钥分发 (quantum key distribution, QKD) 技术被广泛应用于量子保密通信中[1,2], 其安全性由"量子态不可克隆定律"、"测量塌缩定理"和"海森伯不确定性原理"等量子力学基本定律保证[3–5]. 第一个 QKD 协议是由 Bennett 和 Brassard[6] 于 1984 年提出的 BB84 协议, 在理想状态下 BB84 协议中信息载体是单个光子, 但是在实际应用中, 单光子源难以完全实现, 故实验中大多采用弱相干光源[7], 这就使得窃听者 (Eve) 可以使用光子数分离法 (PNS) 进行攻击[8,9]. 此外, 窃听者还有可能攻击探测端的测信道漏洞[10]. 为了免疫所有探测端的可能攻击, 2012 年 Lo 等[11] 和 Braunstein 等[12] 各自独立地提出了测量设备无关量子密钥分发 (measurement-device-independent

* 国家重点研发计划 (批准号: 2018YFA0306400)、国家自然科学基金 (批准号: 12074194, 62101285, 62201276) 和江苏省自然科学基金前沿引领技术 (批准号: BK20192001) 资助的课题.

† 通信作者. E-mail: xyz@njupt.edu.cn

QKD, MDI-QKD) 协议. 2018 年 Lucamarini 等[13]提出了双场量子密钥分发协议 (twin-field QKD, TF-QKD), 不仅保留了 MDI-QKD 的测量设备无关特性, 而且消除了实际应用中 MDI-QKD 协议密钥率受统计起伏影响较大的特性, 并打破了无中继量子信道码率-距离限制 (PLOB 界)[14–16], 提升了 QKD 的实用性.

在量子通信实际应用过程中, MDI-QKD 系统一般采用星状网络进行连接[17,18] (图 1), 而 TF-QKD 和 MDI-QKD 协议也正满足这一特性, 在应用中可以将昂贵的测量设备放置在中心站点, 通信双方只需要持有造价便宜且相对便携的发送设备即可完成密钥分发过程.

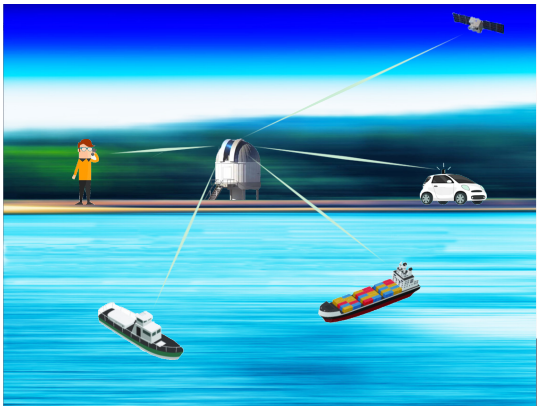

图 1 MDI-QKD 系统示意图
Fig. 1. Schematic diagram of MDI-QKD system.

在量子密钥分发之前, 需要对不同协议 (TF-QKD 或 MDI-QKD) 的参数 (如强度、选择概率等) 配置进行优化[19,20], 从而使通信方能获得相应条件下的最高密钥生成率. 传统的参数配置优化方案一般使用遍历搜索算法或局域搜索算法 (LSA)[21], 传统方案需要计算大量的数据, 容易造成计算资源和计算时间的浪费, 无法满足量子通信系统对实时性的需求. 近年来随着机器学习领域的快速发展, 将机器学习用于 QKD 参数预测成为研究热点. 2018 年, Liu 等[22] 首次将机器学习模型应用于连续变量 QKD 系统, 并提出了一种基于支持向量回归 (SVR) 算法的参数预测模型. 2019 年, Wang 等[23] 在低功耗设备上测试了用于 QKD 参数优化的机器学习算法证明了机器学习模型在低功耗量子通信终端上的适用性. 同年, Lu 等[24] 使用反向传播人工神经网络实现了 MDI-QKD 网络的参数优化与实时标定. 2022 年, Chen 等[25] 将随机森林 (random forest, RF) 模型应用于对称信道量子通信资源优化, 减小了传统方案的时间损耗. 在实际应用场景中, 通信双方一般具有较强的可移动性, 且信道处于非对称状态, 预测参数数量倍增, 因此 QKD 系统在通信实时性上提出了更高的要求. 为了更好地满足实时通信的需求, 本文将多种监督机器学习算法与传统参数优化方案结合, 通过前期采集的数据对机器学习模型进行训练, 最终建立适用于用户处在非对称情况的最优参数预测模型. 本文的仿真结果表明在保证有效密钥率的情况下, 与传统方案对比, 采用机器学习的最优参数预测方案极大地缩短了参数配置所需时间, 在实际 QKD 系统中应用前景广阔.

2 数据格式及特征数据获取

为了获得更高的安全密钥率, 本文使用监督学习的方法构建机器学习模型. 监督学习是机器学习的一个子领域, 监督学习过程需要使用带有正确答案的数据集训练已有算法, 最终获得有数据预测功能的函数[26]. 下面以 QKD 系统中可能用到的 MDI-QKD 和 TF-QKD 协议为例, 介绍训练数据集的输入、输出数据格式及相应数据的获取.

2.1 输入特征数据格式

在 QKD 系统的工作过程中, 安全密钥率 (R) 的大小与系统自身参数有密切关系, 在用户处于非对称的情况下, 影响因素主要包括: 短距离通信方到测量站点的距离 L, 通信双方到测量站点的距离差 ΔL, 本底误码率 $e_{\rm d}$, 探测效率 η, 通信方发送的光脉冲数 N 和暗计数率 Y_0. 将系统参数组合成一个六维向量 $X = [L, \Delta L, Y_0, \eta, e_{\rm d}, N]$, 并令其作为模型训练数据集的输入数据格式, 然后根据实际情况给输入数据划分了相应的范围 (TF-QKD 情况), 见表 1.

表 1 系统参数范围
Table 1. System parameter range.

参数	L /km	ΔL /km	N	η	Y_0	$e_{\rm d}$
范围	0—300	0, 25, 50, 75, 100	10^9—10^{14}	0.1—0.9	10^{-11}—10^{-6}	0.01—0.10

以等间隔取值对所有训练数据进行划分, 最终得到的 TF-QKD 协议待优化数据近 10^5 组; MDI-QKD 除本底误码率 $e_{\rm d}$ 取值范围变为 0.1—0.5 外, 其余处理与 TF-QKD 协议相同, 同样得到近 10^5 组待优化数据.

需要特别说明的是, 本文聚焦于系统中收发端的状态, 而将信道特性归为衰减 (由距离 L 及距离差 ΔL 表征) 与本底误码率 $e_{\rm d}$. 故未特别区分光纤信道与自由空间信道, 对于自由空间信道中的湍流等参量带来的影响则归于额外的衰减与本底误码率的增大[27], 以保证模型的普适性.

2.2 输入标签数据格式

在非对称信道 MDI-QKD 和 TF-QKD 协议中, 本文根据不同协议的原理及其使用的诱骗态方法确定输入标签数据的格式. 其中 TF-QKD 协议使用四强度诱骗态方法[28], 在密钥分发过程中需要优化的配置参数包括: 通信方 Alice (Bob) 的信号态强度 $\mu_1(\mu_2)$、诱骗态强度 $\upsilon_1(\upsilon_2)$ 和 $\omega_1(\omega_2)$、信号脉冲的发送概率 $P_{\mu1}(P_{\mu2})$、诱骗态脉冲的发送概率 $P_{\upsilon1}(P_{\upsilon2})$ 和 $P_{\omega1}(P_{\omega2})$, 以及 Z 窗口下的发送概率 $\varepsilon_1(\varepsilon_2)$. 最终, 将这些配置参数组合成标签向量 $Y_{\rm TF}=[\mu_1,\ \upsilon_1,\ \omega_1,\ P_{\mu1},\ P_{\upsilon1},\ P_{\omega1},\ \varepsilon_1,\ \mu_2,\ \upsilon_2,\ \omega_2,\ P_{\mu2},\ P_{\upsilon2},\ P_{\omega2},\ \varepsilon_2]$; MDI-QKD 协议使用四强度诱骗态方法[29], 其配置参数相较于 TF 缺少了 Z 窗口下的发送概率 ε. 类比 TF-QKD 协议的定义方式, MDI-QKD 协议的输入标签向量定义为 $Y_{\rm MDI}=[\mu_1,\ \upsilon_1,\ \omega_1,\ P_{\mu1},\ P_{\upsilon1},\ P_{\omega1},\ \mu_2,\ \upsilon_2,\ \omega_2,\ P_{\mu2},\ P_{\upsilon2},\ P_{\omega2}]$. 相较于对称信道的方案[20,25], 非对称信道 QKD 系统面对的待优化参数倍增, 预测难度加大. 此外, 由于 MDI-QKD 协议和 TF-QKD 协议在实现难度上各有优缺点, 故不放在一起进行密钥率的评估.

2.3 训练集数据的获取

输入特征数据和输入标签数据统称为输入数据集, 使用 LSA 算法为每一组输入特征数据计算相应的标签数据, 并作为相应条件下的最优参数配置, 随后对所有数据进行了归一化处理. 以较为复杂的 TF-QKD 情况为例, 优化过程的具体说明如下. 这是一个非线性单目标优化问题[21], 可以表示成:

$$\begin{aligned}&\max R_{\rm TF}=f(\mu_1,\upsilon_1,\omega_1,P_{\mu1},P_{\upsilon1},P_{\omega1},\varepsilon_1,\\&\qquad\mu_2,\upsilon_2,\omega_2,P_{\mu2},P_{\upsilon2},P_{\omega2},\varepsilon_2)\\&\text{s.t.}\ \begin{cases}P_{01}+P_{\mu1}+P_{\upsilon1}+P_{\omega1}=1,\\P_{02}+P_{\mu2}+P_{\upsilon2}+P_{\omega2}=1,\\\upsilon_1>\omega_1>0,\\\upsilon_2>\omega_2>0,\end{cases}\end{aligned}\tag{1}$$

其中, $R_{\rm TF}$ 为 TF-QKD 协议下系统的通信密钥率, $P_{01}(P_{02})$ 为 Alice (Bob) 发送光强为 0 的概率.

对于该多维的优化问题, 本文将之转化成 14 个一维优化问题, 再由约束条件及变量间关系进行进一步简化. 对上述一维优化问题使用经典的搜索算法找到局部最优解[21]. 随后, 循环多次以确保结果接近全局最优解.

对于局部搜索算法, 初值的选择尤为重要. 对此本文的处理方法是: 经验赋值与参数继承相结合. 首先, 根据实验经验给出一组满足约束条件的标准值, 以这一标准值作为第一组参数的初值. 随后, 用已得到的有效结果 (满足约束且密钥率 $R_{\rm TF}$ 在合理范围) 作为后续情况的初值; 对于无效结果, 则用标准初值作为后续情况的初值. 需注意的是, 每次优化的输入参数与要继承参数对应的输入参数有且只有一位发生改变, 使得初值设置尽可能合理.

3 机器学习方案选择

本节首先将数据集标准化后随机划分为 70% 的训练集和 30% 的验证集, 随后选取了 3 种不同类别的常用监督学习算法, 并使用训练集的数据对相应算法进行训练. 在获得训练完成的模型后, 将验证集的数据带入并计算不同算法中各个参数的 R^2, 通过综合比较 R^2 的大小初步选定了决策树作为本文参数配置优化的监督学习算法类别. 最后使用分类回归决策树 (classification and regression tree, CART) 算法构建了回归决策树.

3.1 常用监督学习算法选择

选取了监督学习中常用的决策树算法、神经网络算法和 K-最近邻算法 (K-nearest neighbor, KNN) 等 3 种算法进行初步比较, 其中决策树算法是通过训练生成一种树形结构, 其中每个内部节点表示一个属性上的判断值, 每个分支代表一个判断

结果的输出, 最后每个叶节点代表一种输出值[30]. 神经网络是一种模仿生物神经网络结构和功能的计算模型, 常用于对函数进行估计或近似[31]. KNN 算法是通过判断输入数据与已有数据的距离大小来决定输出值的模型. 这 3 种算法代表了监督学习的几个不同方向, 以 TF-QKD 为例, 在数据集随机划分为 70% 的训练集和 30% 的验证集情况下 (下文简写为"标准情况"), 不同算法对验证集输出参数的决定系数 R^2 如图 2 所示.

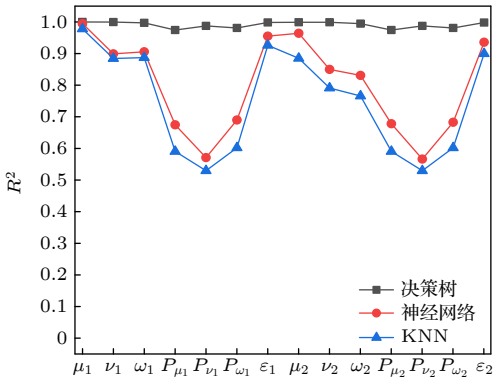

图 2 不同类别监督学习算法 R^2 比较

Fig. 2. Comparison of R^2 of supervised learning algorithms in different categories.

通过对决策树、神经网络与 KNN 算法各个预测参数 R^2 的比较, 发现决策树算法各个预测参数的 R^2 和整体 R^2 均远高于其他两种类型的算法, 对应残差分析如图 3—图 5 所示.

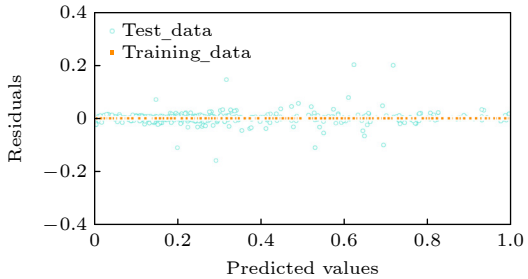

图 3 标准情况决策树模型残差图

Fig. 3. Decision tree model residual plot for standard cases.

图 5 橙色点是训练集的残差分布图, 绿色点是验证集的残差分布图. 从图 5 可知, 决策树模型拥有较强的环境鲁棒性, 且过拟合现象不明显. 另两种模型残差虽与预测值本身相关性较小, 环境鲁棒性同样较好, 但残差绝对值较大, 本文认为在实际系统中是不可接受的. 最后, 各方案时间消耗见表 2.

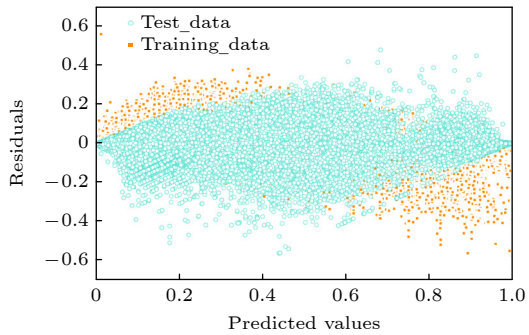

图 4 标准情况神经网络模型残差图

Fig. 4. Neural networks model residual plot for standard cases.

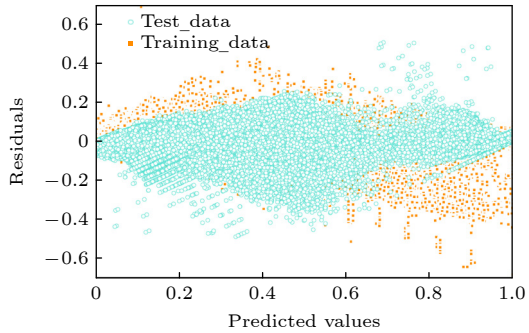

图 5 标准情况 KNN 模型残差图

Fig. 5. KNN model residual plot for standard cases.

表 2 不同方案时间消耗对比

Table 2. Comparison of time loss between different schemes.

协议	决策树/s	神经网络/s	KNN/s	传统/h
TF-QKD	0.713	0.825	1.509	163
MDI-QKD	0.608	0.710	1.301	116

由于决策树模型的单次计算时间在微秒量级, 为了更清楚地展示新方案和传统方案的区别, 对结果进行了放大处理, 即使用同一计算机 (硬件配置: Intel(R) Core(TM) i7-10750 H CPU @ 2.60 GHz, RAM: 16 GB DDR4 2933 MHz) 分别通过不同方案计算多组数据后统计所需时间, 其中 TF-QKD 协议共计算有效数据 55063 组, MDI-QKD 协议共计算有效数据 43741 组, 由表 2 可知, 决策树模型的时间开销最小. 综上所述, 决策树算法对本文所做工作有更好的适用性. 接下来将构建相应的回归决策树.

3.2 决策树的构建过程

CART 算法是一种既能解决离散型分类问题

又能解决连续型回归问题的决策树算法, 最初由 Breiman[32] 于 1984 年提出. CART 回归算法采用平方误差最小化原则选取数据特征, 通过对数据特征的划分建立二叉决策树模型, 最后对生成的决策树进行剪枝处理, 构造出具有泛化和预测能力的回归决策树[33]. 下面开始构建 CART 回归决策树.

3.2.1 数据空间划分及决策树生成

对于 CART 回归决策树的划分, 采用启发式的方法. 首先随机选择训练集特征数据的第 j 个变量 $x^{(j)}$ 作为切分变量, 以该变量的取值 s 作为切分点, 将数据集切分成两个区域:

$$\begin{aligned} R_1(j,s) &= \{x|x^{(j)} \leqslant s\}, \\ R_2(j,s) &= \{x|x^{(j)} \geqslant s\}, \end{aligned} \tag{2}$$

每个区域的输出预测值 c_1 和 c_2 分别为

$$c_m = \frac{1}{N_m} \sum_{x_i \in R_m(j,s)} y_i \quad (m=1,2), \tag{3}$$

其中 y_i 是当前区域第 i 组训练数据的最优值, N_m 是区域内数据量. 然后对变量和切分点的选取做优化, 通过对 j 和 s 的不同取值组合遍历, 使得各个区域的误差平方和最小:

$$\min_{j,s} \left[\sum_{x_i \in R_1(j,s)} (y_i - c_1)^2 + \sum_{x_i \in R_2(j,s)} (y_i - c_2)^2 \right], \tag{4}$$

选取此时的 j 和 s 作为切分变量和切分点[34,35].

对划分后的区域重复上述步骤, 进行多次最优切分, 最终形成一棵完整的决策树.

3.2.2 剪 枝

为了防止决策树出现过拟合的情况, 对决策树进行最小误差剪枝 (minimum error pruning, MEP), MEP 是一种自下而上的剪枝方法[36], 对于已获得决策树的每个非叶子节点, 首先计算该节点的误差 $E_{\mathrm{r}}(t)$, 然后计算该节点下所有叶子结点的误差 $E_{\mathrm{r}}(T_{\mathrm{t}})$ 加权和, 其权重为该节点覆盖的训练样本数量的比例. 如果该子树满足 $E_{\mathrm{r}}(t) < E_{\mathrm{r}}(T_{\mathrm{t}})$, 则剪去该子树, 否则保留. 节点误差的计算公式为

$$E_{\mathrm{r}}(t) = \sum_{i=1}^{N} |y_i - c_i|. \tag{5}$$

最后判断所有节点是否都通过测试, 完成剪枝.

3.2.3 输出值预测

在完成决策树的构建和剪枝后, 输入验证集数据可获得对应的输出预测结果:

$$f(x) = \sum_{m=1}^{M} c_m I, \tag{6}$$

其中, $f(x)$ 为预测输出值, I 为指示函数, 表示为

$$I = \begin{cases} 1, & x \in \mathbb{R}_m, \\ 0, & x \notin \mathbb{R}_m. \end{cases} \tag{7}$$

图 6 为 CART 决策树构建流程图. 最终, 基于这一思路使用 Sklearn 库中的 Decision Tree Regressor 函数训练决策树, 训练参数包括: 树的最大深度“max_depth”为 36, 拆分内部节点所需的最小样本数“min_samples_split”为 2, 叶节点所需的最小样本数“min_samples_leaf”为 1, 损失函数 criterion 选用“squared_error”.

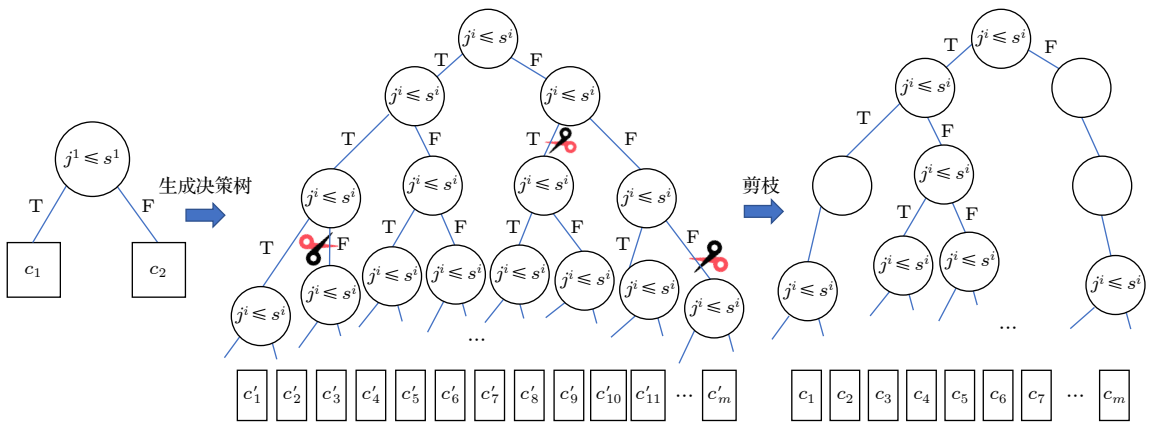

图 6 CART 构建过程

Fig. 6. CART construction process.

4 结果和讨论

4.1 基础结果呈现

首先检验上述决策树模型“标准情况”下的表现. 为此, 引入回归模型中常见的 3 种评价指标, 对 TF-QKD 协议和 MDI-QKD 协议数据训练出的决策树模型分别进行评价.

均方误差 (mean squared error, MSE) 用于计算预测结果与最优结果误差平方和的均值, 其取值越小说明模型性能越强, 计算公式为

$$\mathrm{MSE}=\frac{1}{N}\sum_{i=1}^{N}[y_i-f(x_i)]^2. \tag{8}$$

平均绝对误差 (mean absolute error, MAE) 常用于计算模型预测结果与最优结果误差平均值, 其取值越小说明模型对数据的拟合效果越好, 表达式为

$$\mathrm{MAE}=\frac{1}{N}\sum_{i=1}^{N}|y_i-f(x_i)|. \tag{9}$$

决定系数 (coefficient of determination, R^2) 是模型预测结果准确程度的指标, 可表示为

$$R^2=1-\sum_{i=1}^{N}[y_i-f(x_i)]^2\Big/\sum_{i=1}^{N}(y_i-\bar{y}_i)^2. \tag{10}$$

R^2 取值范围为 0—1, R^2 越接近于 1, 说明模型的预测效果越好, 越接近于 0, 说明模型的预测效果越差. 在 (8) 式—(10) 式中, N 表示测试数据集的数量, $f(x_i)$ 为模型预测结果, y_i 为对应的最优结果, $\bar{y}_i=\frac{1}{N}\sum_{i=1}^{N}y_i$ 为验证集最优结果的均值. 标准情况下验证集的各个回归指标计算数值展示在表 3 中.

表 3 标准情况下模型结果评估

Table 3. Evaluation of the results under standard conditions.

协议	R^2	MAE/10^{-3}	MSE/10^{-5}
TF-QKD	0.9916	3.42	8.05
MDI-QKD	0.9993	0.37	1.70

由表 3 可知, 在标准情况下, 以 CART 算法构建的回归模型在预测验证集数据时效果较为理想. 这说明对于 QKD 系统中可能用到的不同 QKD 协议, 对应决策树模型均能较好完成其最优参数的预测. 接下来, 使用预测得到的配置参数分别计算两协议的预测密钥率, 并与已知最优密钥率相比得到结果如图 7 和图 8 所示.

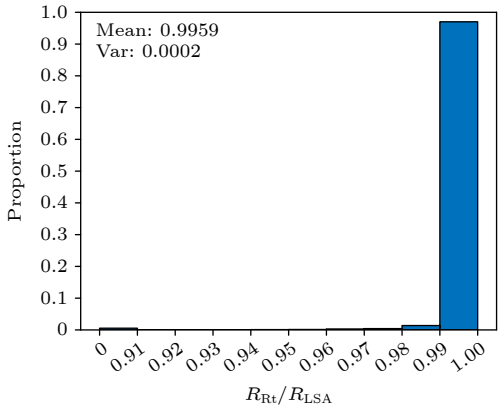

图 7 TF-QKD 模型比例柱状图

Fig. 7. Model scale histogram of TF-QKD.

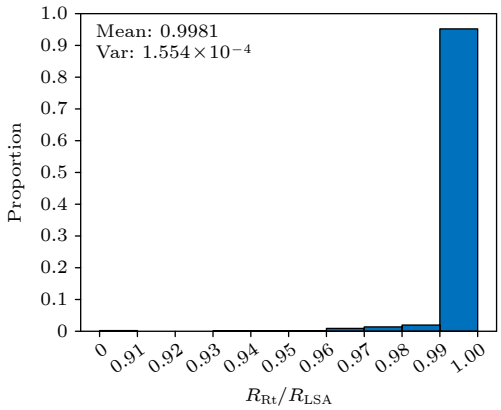

图 8 MDI-QKD 模型比例柱状图

Fig. 8. Model scale histogram of MDI-QKD.

图 7 和图 8 中 R_{Rt} 是通过决策树模型输出参数计算出的通信密钥率, R_{LSA} 是 LSA 算法计算出的最优密钥率 (需要特别说明的是: 对于 $R_{\mathrm{Rt}}>R_{\mathrm{LSA}}$ 的情况, 认为其满足最优情况的定义, 取 $R_{\mathrm{Rt}}/R_{\mathrm{LSA}}=1$. 下文中均采取相同操作不再做特殊说明). 通过图 7 和图 8 可知, 在标准情况下, 通过决策树模型预测参数计算出的密钥率与传统方法得到的最优密钥率较为接近, 密钥率比值的均值在 0.995 以上. 说明在标准情况下, 决策树模型在非对称信道 QKD 系统优化参数配置这一应用场景下性能优异.

4.2 方案的实用性

下面要验证决策树模型在常见的两种不同场景下的实用性: 场景一是由于训练集过小导致输入数据超过训练集范围, 下文简称“超范围”; 场景二是由于训练集的精度过低导致输入数据在训练集

范围内但是没有对应数据, 下文简称“超精度”. 这两种场景在实际使用中经常发生, 都要求建立的模型具有一定的预测能力. 为了验证决策树模型这两种常见情况下的实用性, 计算了这两种情况下 3 种不同的评价指标, 并且更深入地比较了决策树模型和基于决策树的集成模型的优劣.

参与对比的决策树集成模型有 RF 模型和梯度提升决策树 (gradient boosting decision tree, GBDT) 模型. RF 模型和 GBDT 模型都是以决策树为基础集成而来, 可视为多棵决策树的集合, 不同之处在于 RF 模型的决策树是由多次取出并放回的抽样数据形成, 每棵树的权重相同, 而 GBDT 是在上一棵树的残差基础上迭代生成, 每棵树权重不同. 为了比较模型和超范围参数预测时的效果, 依旧以回归模型中常见的 3 种评价指标对 RF、决策树和 GBDT 模型进行比较和分析. 以 TF-QKD 为例, 将验证集的各个回归指标计算数值展示在表 4 中.

表 4 不同使用场景模型结果评估

Table 4. Evaluation of the results of different usage scenarios.

	模型	R^2	MAE/10^{-2}	MSE/10^{-4}
超范围	决策树	**0.9529**	**1.64**	**8.75**
	RF	0.9494	1.68	9.12
	梯度提升	0.8579	2.76	40.0
超精度	决策树	**0.9659**	**1.14**	**3.52**
	RF	0.9654	1.15	3.54
	梯度提升	0.9154	1.94	8.74

注: 粗体数据为该指标最好的结果.

由表 4 可知, 在相同训练集的训练下, 决策树模型在 MSE, MAE 和 R^2 等性能指标上的表现都优于其他模型, 这说明基于决策树的模型相较于集成模型在不同的场景中都有更好的适应性, 也证明了本文选择决策树模型的正确性. 下面计算回归决策树模型和 RF 模型在 TF-QKD 协议处于超精度状态下的预测结果密钥率和最优结果密钥率比值分布柱状图, 如图 9 和图 10 所示, 能更清晰地比较两者差别.

图 9 和图 10 中 R_{Rt} 和 R_{RF} 是验证集分别通过决策树模型与 RF 模型计算出来的通信密钥率, R_{LSA} 是 LSA 算法计算出的最优密钥率. 通过图 9 和图 10 的对比可以发现, 回归决策树模型在相同验证集下的密钥率更接近最优密钥率, 这说明决策树模型在决策精度上略好于 RF 模型, 对此我们探究了深层原因并做出如下解释. 由图 11 和图 12 残差分析可知: 回归决策树模型的鲁棒性较好, 过拟合情况较少. 在这种情形下, RF 模型较普通决策树模型的优势被削弱, 而单决策树模型对数据特征的训练更加充分. 故本文中决策树模型效果略好于 RF 模型. 最后将使用机器学习模型和使用传统 LSA 算法获得参数配置优化结果所需时间记录于表 5.

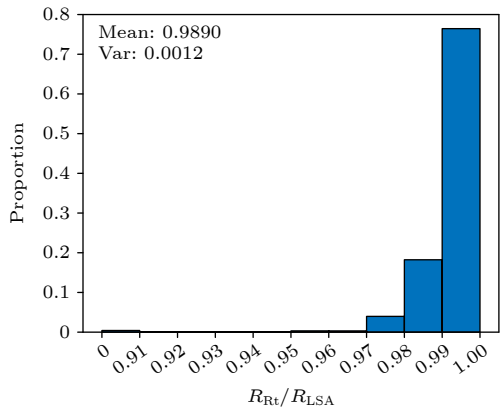

图 9 回归决策树模型比例柱状图

Fig. 9. Regression decision tree model scale histogram.

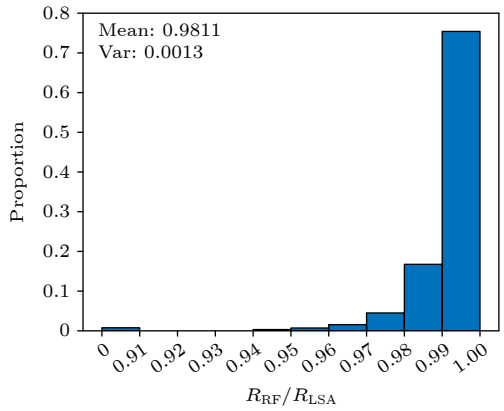

图 10 RF 模型比例柱状图

Fig. 10. Random forest model scale histogram.

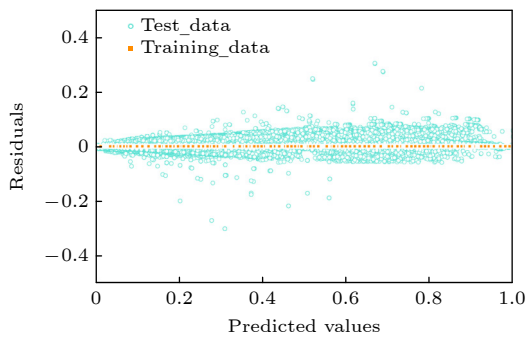

图 11 超精度情况决策树模型残差图

Fig. 11. Decision tree model residual plot for super-precision cases.

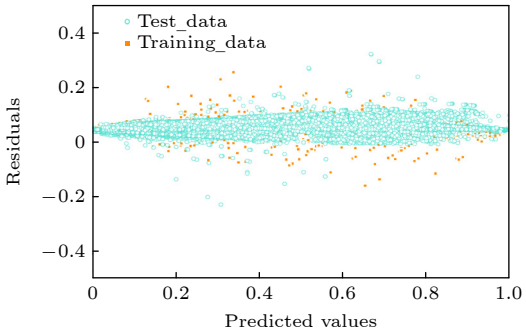

图 12 超精度情况 RF 模型残差图

Fig. 12. RF model residual plot for super-precision cases.

表 5 不同方案时间消耗对比

Table 5. Comparison of time loss between different schemes.

协议	RF/s	决策树/s	梯度提升树/s	传统/h
TF-QKD	1.426	0.713	6.748	163
MDI-QKD	1.221	0.608	5.631	116

在软硬件条件与前文相同的条件下, 分别通过不同方案计算多组数据后统计所需时间, 其中 TF-QKD 协议共计算数据 55063 组, MDI-QKD 协议共计算数据 43741 组. 结果表明在保证安全密钥率的前提下, 决策树模型极大地降低了传统方案需要的时间损耗, 这表明决策树模型能够很好的实现多用户实时进行量子通信的目的.

为了验证决策树模型的环境鲁棒性, 构建了决策树和 RF 在超精度应用场景下的可视化残差图, 如图 11 和图 12 所示. 图 11 和图 12 中橙色点是训练集的残差分布图, 绿色点是验证集的残差分布图. 可知验证集的残差大部分在 0.08 以下且与预测值本身相关性较小, 这进一步说明了本文决策树模型拥有较强的环境鲁棒性, 且通过和 RF 残差图的对比可说明决策树模型的过拟合现象不明显.

5 总结和展望

本文提出了基于回归决策树的非对称信道场景下 MDI-QKD 系统优化参数配置方案. 与使用搜索算法的传统方案相比, 本文的方案大幅度缩短了获得参数配置所需时间, 减少了时间资源和计算资源的消耗, 残差分析也证明决策树方案有较好的稳定性. 此外, 介绍了决策树方案的生成过程, 并展示了多个回归模型的效果对比, 最终发现在实际应用场景中, CART 模型相较于 KNN 和 RF 等模型的效果最佳, 且预测数据所得的密钥率与使用 LSA 方式得到的最优密钥率比值的均值在 0.995 以上. 同时, 在“超范围”和“超精度”两种极限条件下, CART 模型在维持良好鲁棒性的同时, 预测参数计算得到的密钥率与最优密钥率比值的均值仍维持在 0.988 左右, 能较好满足实际通信需要. 可见本文构建的决策树模型在保证密钥分发速度的条件下, 以较低的算力和时间成本完成 QKD 参数配置. 综上所述, 本文对非对称信道 MDI-QKD 系统的实现有重要意义.

QKD 分为两类, 即离散变量 DV-QKD 和连续变量 CV-QKD. 本文主要聚焦于 DV-QKD 的各项参数优化, 近年 CV-QKD 的发展同样迅速. CV-QKD 的高密钥速率和与标准通信组件的出色兼容性使得其在未来 QKD 系统中同样拥有广阔的应用前景 [37]. 学界近年也做出了许多将机器学习模型运用于 CV-QKD 系统参数预测的尝试, 能够利用机器学习模型较好完成系统密钥率的计算及参数估计 [22,38–40]. 上述案例证明了将机器学习用于 CV-QKD 系统参数预测的可行性. 虽然 CV-QKD 系统拥有参数数量众多等特性 [41], 但依靠决策树模型的多输入-多输出特性及较强的普适性, 只要训练参数取值范围恰当且数量足够, 本文方案将能够用于 CV-QKD 系统参数预测. 本文方案在 CV-QKD 系统中的运用是我们未来的潜在研究方向和应用场景.

参考文献

[1] Gisin N, Thew R 2007 *Nat. Photonics.* **1** 165
[2] Scarani V, Bechmann P H, Cerf N J, Dusek M, Lutkenhaus N, Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[3] Wootters W K, Zurek W H 1982 *Nature* **299** 802
[4] Busch P, Heinonen T, Lathi P 2007 *Phys. Rep.* **452** 155
[5] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S, Sanpera A 1996 *Phys. Rev. Lett.* **77** 2818
[6] Bennett C H, Brassard G 2014 *Theoret. Comput. Sci.* **560** 7
[7] Yang L X, Su Z K 2022 *China High and New Technol.* **11** 82 (in Chinese) [杨林轩, 苏志锟 2022 中国高新科技 **11** 82]
[8] Lütkenhaus N 2000 *Phys. Rev. A* **61** 052304
[9] Acin A, Gisin N, Scarani V 2004 *Phys. Rev. A* **69** 012309
[10] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V 2010 *Nat. Photonics.* **4** 686
[11] Lo H K, Curty M, Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[12] Braunstein S L, Pirandola S 2012 *Phys. Rev. Lett.* **108** 130502
[13] Lucamarini M, Yuan Z L, Dynes J F, Shields A J 2018 *Nature.* **557** 400
[14] Takeoka M, Guha S, Wilde M M 2014 *Nat. Commun.* **5** 5235
[15] Wang X B, Yu Z W, Hu X L 2018 *Phys. Rev. A* **98** 062323
[16] Ma X, Zeng P, Zhou H 2018 *Phys. Rev. X* **8** 031043

[17] Wang H, Zhao Y L 2019 *J. Commun.* **40** 168 (in Chinese) [王华, 赵永利 2019 通信学报 **40** 168]

[18] Hughes R J, Morgan G L, Peterson C G 2000 *J. Mod. Opt.* **47** 533

[19] Ren Z A, Chen Y P, Liu J Y, Ding H J, Wang Q 2020 *IEEE Commun. Lett.* **25** 940

[20] Ding H J, Liu J Y, Zhang C M, Wang Q 2020 *Quant. Inform. Proces.* **19** 1

[21] Xu F, Xu H, Lo H K 2014 *Phys. Rev. A* **89** 052333

[22] Liu W, Huang P, Peng J, Fan J, Zeng G 2018 *Phys. Rev. A* **97** 022316

[23] Wang W, Lo H K 2019 *Phys. Rev. A* **100** 062334

[24] Lu F Y, Yin Z Q, Wang C, Cui C H, Teng J, Wang S, Chen W, Huang W, Xu B J, Guo G C, Han Z F 2019 *JOSA B* **36** B92

[25] Chen Y P, Liu J Y, Zhu J L, Fang W, Wang Q 2022 *Acta Phys. Sin.* **71** 220301 (in Chinese) [陈以鹏, 刘靖阳, 朱佳莉, 方伟, 王琴 2022 物理学报 **71** 220301]

[26] Wang Q, Chen Y P 2020 *J. Nanjing University of Posts and Telecommun.* **40** 141 (in Chinese) [王琴, 陈以鹏 2020 南京邮电大学学报 **40** 141]

[27] Cao Y, Li Y H, Yang K X, et al. 2020 *Phys. Rev. Lett.* **125** 260503

[28] Zhou X Y, Zhang C H, Zhang C M, Wang Q 2019 *Phys. Rev. A* **99** 062316

[29] Wang W, Xu F, Lo H K 2019 *Phys. Rev. X* **9** 041012

[30] Quinlan J R 1986 *Mach. Learn.* **1** 81

[31] Rumelhart D E, Hinton G E, Williams R J 1986 *Nature.* **323** 533

[32] Gordon A D, Breiman L, Friedman J H, Olshen R A, Stone C J 1984 *Biometrics.* **40** 874

[33] Shen Y Y, Wu T W, Liu X D 2020 *Sci. Technol. Manage. Res.* **40** 91 (in Chinese) [申媛媛, 邬锦雯, 刘鑫东 2020 科技管理研究 **40** 91]

[34] Liu Y H, Niu Z, Wang C Y 2005 *J. Remote Sens.* **9** 405 (in Chinese) [刘勇洪, 牛铮, 王长耀 2005 遥感学报 **9** 405]

[35] Wang H, Zhang W J, Liu J, Chen L F, Li Z N 2022 *J. Civil Aviation University of China* **40** 35 (in Chinese) [王辉, 张文杰, 刘杰, 陈林烽, 李泽南 2022 中国民航大学学报 **40** 35]

[36] Liu Y R, Zhao C P, Zang J, Ning Q, Zhou X Z 2017 *Comput. Appl.* **37** 57 (in Chinese) [刘玉茹, 赵成萍, 臧军, 宁芊, 周新志 2017 计算机应用 **37** 57]

[37] S. Pirandola, Andersen U L, Banchi L, et al. 2020 *Adv. Opt. Photonics* **12** 1012

[38] Huang D, Liu S, Zhang L 2021 *Photonics* **8** 511

[39] Liu Z P, Zhou M G, Liu W B, Li C L, Gu J, Yin H L, Chen Z B 2022 *Opt. Express* **30** 15024

[40] Luo H, Wang Y J, Ye W, Zhong H, Mao Y Y, Guo Y 2022 *Phys. B* **31** 020306

[41] Zhou M G, Liu Z P, Liu W B, Li C L, Bai J L, Xue Y R, Fu Y, Yin H L, Chen Z B 2022 *Sci. Rep.* **12** 8879

Regression-decision-tree based parameter optimization of measurement-device-independent quantum key distribution*

Liu Tian-Le [1)2)] Xu Xiao [1)2)] Fu Bo-Wei [1)2)] Xu Jia-Xin [1)2)]
Liu Jing-Yang [1)2)] Zhou Xing-Yu [1)2)†] Wang Qin [1)2)]

1) (*College of Telecommunications & Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*)

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

(Received 8 February 2023; revised manuscript received 17 March 2023)

Abstract

The parameter configuration of quantum key distribution (QKD) has a great effect on the communication effect, and in the practical application of the QKD network in the future, it is necessary to quickly realize the parameter configuration optimization of the asymmetric channel measurement-device-independent QKD according to the communication state, so as to ensure the good communication effect of the mobile users, which is an inevitable requirement for real-time quantum communication. Aiming at the problem that the traditional QKD parameter optimization configuration scheme cannot guarantee real-time, in this paper we propose to apply the supervised machine learning algorithm to the QKD parameter optimization configuration, and predict the optimal parameters of TF-QKD and MDI-QKD under different conditions through the machine learning model. First, we delineate the range of system parameters and evenly spaced (linear or logarithmic) values through experimental experience, and then use the traditional local search algorithm (LSA) to obtain the optimal parameters and take them as the optimal parameters in this work. Finally, we train various machine learning models based on the above data and compare their performances. We compare the supervised regression learning models such as neural network, K-nearest neighbors, random forest, gradient tree boosting and classification and regression tree (CART), and the results show that the CART decision tree model has the best performance in the regression evaluation index, and the average value of the key rate (of the prediction parameters) and the optimal key rate ratio is about 0.995, which can meet the communication needs in the actual environment. At the same time, the CART decision tree model shows good environmental robustness in the residual analysis of asymmetric QKD protocol. In addition, compared with the traditional scheme, the new scheme based on CART decision tree greatly improves the real-time performance of computing, shortening the single prediction time of the optimal parameters of different environments to the microsecond level, which well meets the real-time communication needs of the communicator in the movable state. This work mainly focuses on the parameter optimization of discrete variable QKD (DV-QKD). In recent years, the continuous variable QKD (CV-QKD) has developed also rapidly. At the end of the paper, we briefly introduce academic attempts of applying machine learning to the parameter optimization of CV-QKD system, and discuss the applicability of the scheme in CV-QKD system.

Keywords: quantum key distribution, measurement-device-independent, classification and regression tree, parameter optimization

PACS: 03.65.–w, 03.67.Hk, 42.50.Ex, **DOI:** 10.7498/aps.72.20230160

* Project supported by the National Key R&D Program of China (Grant No. 2018YFA0306400), the National Natural Science Foundation of China (Grant Nos. 12074194, 62101285, 62201276), and the Leading-edge Technology Program of Jiangsu Natural Science Foundation, China (Grant No. BK20192001).

† Corresponding author. E-mail: xyz@njupt.edu.cn

物理学报 Acta Physica Sinica

Chinese Physical Society

Institute of Physics, CAS

基于回归决策树的测量设备无关型量子密钥分发参数优化

刘天乐 徐枭 付博玮 徐佳歆 刘靖阳 周星宇 王琴

Regression-decision-tree based parameter optimization of measurement-device-independent quantum key distribution

Liu Tian-Le Xu Xiao Fu Bo-Wei Xu Jia-Xin Liu Jing-Yang Zhou Xing-Yu Wang Qin

引用信息 Citation: Acta Physica Sinica, 72, 110304 (2023) DOI: 10.7498/aps.72.20230160

在线阅读 View online: https://doi.org/10.7498/aps.72.20230160

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