评“基于变分量子分类器的量子对抗攻击生成算法”

徐兵杰

量子机器学习 (quantum machine learning, QML) 是当前量子计算理论的研究热点之一。在真实的大规模量子系统中，不可避免地存在扰动和噪声，而微小扰动将导致量子分类器分类错误，从而使量子机器学习算法失效。基于上述原因，研究在微小扰动下的量子分类器鲁棒性，是量子机器学习研究中的基本问题之一，而如何高效生成尽可能小的扰动使量子分类器失效是关键点。

针对这一问题，该文提出了一种新的量子对抗攻击生成算法——量子混淆算法。该算法利用量子分类器中输入数据的梯度信息来生成扰动，通过将这种扰动施加到编码原始数据的量子态上，就能够使已训练好的量子分类器失效。将该方案与已有的量子自适应快速梯度符号法 (Q-FGSM) 和量子自适应基本迭代法 (Q-BIM) 进行了比较，结果显示，该算法确实可以通过生成更小的扰动使分类器失效。因此，量子混淆算法提供了一种高效的量子对抗攻击生成方法，为理解量子分类器的有效性和脆弱性提供了新的思路。

评“相位匹配量子密钥分发协议统计波动分析”

徐兵杰

双场量子密钥分发 (quantum key distribution, QKD) 协议理论上可突破 PLOB 界，目前业界传输距离已突破 800 km，是当前学术界重点关注的一种长距离 QKD 解决方案，其一方面在组网应用中可减少可信中继数量以降低系统安全风险，另一方面可显著提升长距离 QKD 安全码率。

该文将统计波动分析方法与线性规划相结合，对量子密钥分发协议中广泛使用的一类双场量子密钥分发协议——相位匹配协议 (phase matching, PM) 进行了分析。针对二诱骗态与三诱骗态 PM 协议，比较了高斯分析方法和切诺夫-夫丁界方法对于两种协议统计波动分析的表现，进而通过线性回归对两种协议的密钥生成率进行了估计。结果显示，采用切诺夫-夫丁界进行统计波动分析，可以保证 PM 协议的安全性，但是在数据量较小时，其性能低于高斯分析。此外，增加诱骗态无法显著提高考虑统计波动的 PM 协议性能。综上，实现量子密钥分发时，采用二诱骗态 PM 协议，同时结合切诺夫-夫丁界统计波动分析方法是一种更优的选择。