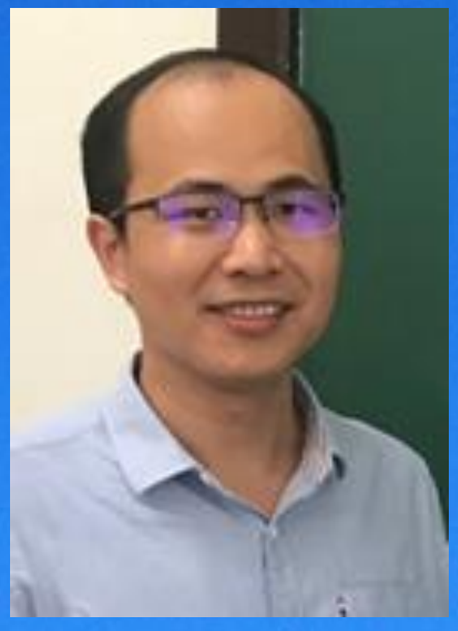
凝聚态物理-北京大学论坛

2024年第2期（No.584 since 2001）

Quantum adversarial machine learning: from theory to experiment

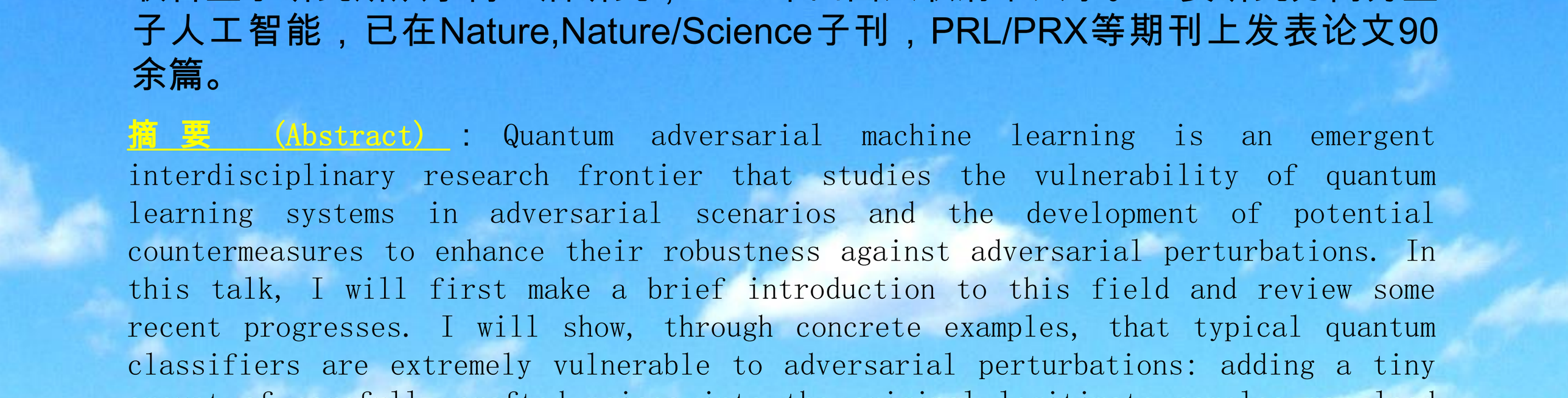


邓东灵 教授

时间：2月29日（星期四）15:00—16:30
地点：北京大学物理楼西563会议室

报告人简介（About speaker）：邓东灵，清华大学交叉信息研究院特别研究员，博士生导师，海外高层次人才青年项目、国家杰出青年科学基金获得者。2007年获南开大学物理、数学双学士学位，2015年博士毕业于美国密西根大学，博士论文获“Kent M. Terwilliger Memorial Thesis Prize”奖。2015-2018年在马里兰大学联合量子研究所从事博士后研究，2018年回国入职清华大学。主要研究方向为量子人工智能，已在Nature,Nature/Science子刊，PRL/PRX等期刊上发表论文90余篇。

摘 要 (Abstract)：Quantum adversarial machine learning is an emergent interdisciplinary research frontier that studies the vulnerability of quantum learning systems in adversarial scenarios and the development of potential countermeasures to enhance their robustness against adversarial perturbations. In this talk, I will first make a brief introduction to this field and review some recent progresses. I will show, through concrete examples, that typical quantum classifiers are extremely vulnerable to adversarial perturbations: adding a tiny amount of carefully crafted noises into the original legitimate samples may lead the classifiers to make incorrect predictions at a high confidence level. I will talk about possible defense strategies against adversarial attacks. I will also talk about a recent experimental demonstration of quantum adversarial learning with programmable superconducting qubits.



邀请人：陈基 ji.chen@pku.edu.cn