学 术 报 告

受中国矿业大学信息与控制工程学院邀请，哈尔滨工业大学（深圳）罗文坚教授在我校举行学术报告，欢迎广大师生踊跃参加！

报告题目：Evolutionary Computation in Artificial Intelligence Security

报 告 人：罗文坚，教授，哈尔滨工业大学（深圳）

报告时间：2024 年 10 月 15 日 上午 10:00

报告地点：在线　　腾讯会议号：694-827-397

主办单位：信息与控制工程学院

报告摘要：

With the wide use of artificial intelligence techniques, especially deep learning models, the security issue in artificial intelligence systems have become an important research branch. This talk will introduce recent advance in artificial intelligence security, especially evolutionary computation in artificial intelligence security. The primary content of this talk includes two aspects, i.e., multi-label adversarial examples and model version attacks. For multi-label adversarial examples, the black-box generation algorithm and the complete black-box generation algorithm will be introduced, and both algorithms are based on differential evolution. For the model version, the basic idea will be presented first, and then two model inversion test techniques, which are also based on differential evolution, will be introduced. Finally, this talk will briefly discuss the future trend of artificial intelligence security.

报告人简介：

罗文坚，哈尔滨工业大学（深圳）教授，博导，广东省珠江人才计划领军人才，深圳市鹏城孔雀计划特聘岗位，网络空间安全研究中心副主任，广东省安全智能新技术重点实验室副主任。承担了包括国家重点研发计划项目课题、国家自然科学基金面上项目、深圳市自然科学基金重点等在内的 20 多项科研项目。目前担任 Information Sciences、Swarm and Evolutionary Computation、Journal of Information Security and Applications、Applied Soft Computing、Complex & Intelligent Systems 等多个期刊的副编辑或编委，IEEE CIS Evolutionary Computation Technical Committee 委员；曾任 IEEE CIS ECTC Task Force on Artificial Immune Systems 主席，中国人工智能学会自然计算与数字智能城市专业委员会副秘书长；曾任包括 ICSI 2023 大会主席、CCF B 类会议 PPSN 2020 宣传主席、CCF C 类会议 IJCNN 2021 讲座主席等在内的 20 多个国际国内学术会议程序委员会和组织委员会的各类主席。获授权专利 10 余项，在 IEEE/ACM Transactions 和 JCR 一区期刊及 CCF A 类会议发表学术论文 60 多篇。