林国鹏

邮箱：17302010022@fudan.edu.cn　　微信：linguopeng1015277323
研究方向：安全多方计算，隐私保护机器学习，MPC漏洞检测

教育经历

复旦大学 2021年09月 – 至今
计算机科学与技术 直博生

复旦大学 2017年09月 – 2021年06月
软件工程 本科

论文代表作

1. Is MPC Secure? Leveraging Neural Network Classifiers to Detect Data Leakage Vulnerabilities in MPC Implementations （**S&P 2025，CCF A，安全四大顶会，第一作者**）
   - 利用神经网络分类器设计针对安全多方计算协议实现的数据泄漏漏洞检测工具
   - 在TF-Encrypted、Crypten、MP-SPDZ共计发现12个数据泄漏漏洞，被授予2个CVE（全球首次MPC框架数据泄漏漏洞被授予CVE）
2. Kona: An Efficient Privacy-Preservation Framework for KNN Classification by Communication Optimization. （**ICML 2025， CCF A，机器学习三大顶会， 第一作者**）
   - 基于安全多方计算协议设计并实现隐私保护下的高效KNN分类框架，使得欧几里得距离计算无需在线通信且在寻找最近邻时所需要的通信轮次大量减少
   - 效率较之前的SOTA方案（TIFS 2024）提升1.1～232.6倍，通信量优化了1.1～3121.2倍，通信轮次优化了19.1～5783.2倍
3. Ents: An Efficient Three-party Training Framework for Decision Trees by Communication Optimization. （**CCS 2024， CCF A，安全四大顶会， Distinguished Artifact Award，第一作者**）
   - 基于安全多方计算协议设计并实现隐私保护下的决策树训练框架，使得在训练时所需的通信量和通信轮次大量减少
   - 效率较之前的SOTA方案（PETS 2023）提升了3.5～6.7倍，通信量优化了5.5～9.3倍，通信轮次优化了3.9～5.3倍
4. 安全多方学习：从安全计算到安全学习（**计算机学报 2023，CCF A类中文期刊，共同一作**）
   - 系统阐述安全多方学习这一概念，并根据底层技术路径对安全多方学习的分类，阐述相关的优缺点

项目经历

安全多方学习平台Garnet （项目负责人） 2023年3月 – 至今
- 主导Garnet平台的设计、开发、发布等过程，并完成其中的树类模型相关代码
- 项目链接：https://github.com/FudanMPL/Garnet

国家重点研发计划项目、国家密码科学基金重点项目，国家自然科学基金项目，华为/蚂蚁产学研项目等
- 主导/参与项目的申请、实施、答辩等过程，完成Garnet平台在上海市检察院部署等

工作经历

微软上海（软件开发工程师实习生） 2020年06月 – 2021年02月
- 独立开发autorest-ansible，自动生成微软Azure的ansible调用API代码

XMAN冬令营/夏令营，上海市青浦区/嘉定区公安局，浦发银行等（CTF二进制攻防讲师）
- 为学员讲解二进制漏洞利用的相关知识

获奖情况

ACM CCS 2024 Distinguish Artifact Award（第一作者） 2024年
高等院校发明选拔赛金奖（队长） 2024年
上海市优秀毕业生 2021年
全国大学生信息安全竞赛创新实践能力赛一等奖（队长） 2019年
复旦大学一/二等学业奖学金、优秀学生、优秀团员等 2022年、2020年、2019年、2018年等