杨军港

出生年月：1997 年 1 月　　性　　别：男
籍　　贯：江苏常州　　电话、微信：18912325515
年　　级：博士四年级　　邮　　箱：yangjungang@sjtu.edu.cn

教育背景

2019.9 至今　博士　上海交通大学　电子信息与电气工程学院 计算机科学与工程
导师：向立瑶、王新兵　约翰·霍普克罗夫特计算机科学中心

2015.9-2019.6　本科　南京大学　数学系 信息与计算科学

发表论文

以一作发表 **CCF A 类论文 3 篇**，共计发表论文 4 篇。主要包含的方向为：**深度神经网络中的差分隐私、对抗学习中的理论鲁棒性的保证**等。

1. **Jungang Yang**; Liyao Xiang; Pengzhi Chu; Xinbing Wang; Chenghu Zhou; “Certified Distributional Robustness on Smoothed Classifiers,” in IEEE Transactions on Dependable and Secure Computing (TDSC), DOI: 10.1109/TDSC.2023.3264850, 2023.
2. **Jungang Yang**; Liyao Xiang; Ruidong Chen; Weiting Li; Baochun Li; “Differential Privacy for Tensor-Valued Queries,” in IEEE Transactions on Information Forensics & Security (TIFS), DOI: 10.1109/TIFS.2021.3089884, 2021.
3. **Jungang Yang**; Liyao Xiang; Jiahao Yu; Xinbing Wang; Bin Guo; Zhetao Li; Baochun Li; “Matrix Gaussian Mechanisms for Differentially-Private Learning,” in IEEE Transactions on Mobile Computing (TMC), DOI: 10.1109/TMC.2021.3093316, 2021.
4. Liyao Xiang; Weiting Li; **Jungang Yang**; Xinbing Wang; Baochun Li; “Differentially-Private Deep Learning with Directional Noise,” in IEEE Transactions on Mobile Computing (TMC), 2021

项目经历

2021-2022 华为-上海交通大学网络空间安全学院创新实验室合作项目

通过研究深度神经网络中数据方向分布，改进差分隐私噪声方向。基于高维数据下的模型效用方向，设计差分隐私高斯机制的噪声方向，将数据分布和噪声分布相结合，优化给定任务下的模型分类性能。在 Pytorch 平台，Jax 平台上分别完成了项目的代码实现，结合现有先进的工作，提升整体性能，获得项目**优秀个人奖**。

2021 至今 参与国家自然科学基金委员会重点项目

通过研究联邦学习中的隐私保护技术，改进差分隐私机制在联邦学习中部署的机制；通过部署压缩机制，降低差分隐私噪声扰动，提高模型分类性能，且降低了通信开销。

研究方向

研究方向：深度神经网络中的**差分隐私**、**对抗学习**、**遗忘学习**等。主要研究课题包括：差分隐私机制设计与分析、深度学习中训练数据隐私保护，对抗学习中的理论分析。

未来研究方向：基于**联邦学习**，挖掘提升隐私保护下性能的方法；在**大模型方向**，研究预训练模型隐私保护，以及**大模型的鲁棒学习**；在**迁移学习**领域，进行 zero shot 模型的训练，通过公开数据集对隐私训练进行指导。