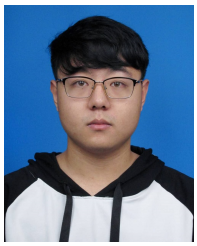

刘博超

政治面貌：中共党员
电　　话：17863928239
电子邮件：liubochao@iie.ac.cn
个人主页：刘博超

教育背景

- 中国科学院大学 · 网络空间安全 · 博士（2020 年 9 月-至今）（保送）
- 山东大学 · 电子信息工程 · 本科（2016 年 9 月-2020 年 6 月）

科研方向

- 生成式模型，差分隐私，计算机视觉，模型压缩，模型安全

论文列表

1. **Bochao Liu**, Pengju Wang, Shikun Li, Dan Zeng and Shiming Ge. Model Conversion via Differentially Private Data-Free Distillation. In IJCAI, 2023. (**CCF-A**)
2. Shiming Ge, **Bochao Liu** and Pengju Wang. Learning Privacy-Preserving Student Networks via Discriminative-Generative Distillation. IEEE TIP, 2023.(**CCF-A, SCI-Q1**, 导师一作)
3. **Bochao Liu**, Jianghu Lu, Pengju Wang and Shiming Ge. Privacy-Preserving Student Learning with Differentially Private Data-Free Distillation. In IEEE MMSP, 2022. (**最佳学生提名奖**)
4. Pengju Wang, **Bochao Liu**, Shiming Ge. Fusion of Current and Historical Knowledge for Personalized Federated Learning. In IJCNN, 2024. (**CCF-C**)
5. 王鹏举，卢江虎，**刘博超**，葛仕明. 资源受限场景中的联邦学习技术综述. 信息安全学报，2022. (**CCF-B**)
6. Haolin Liu, Chenyu Li, **Bochao Liu**, Pengju Wang, Shiming Ge*, Weiping Wang. Differentially Private Learning with Grouped Gradient Clipping. In ACM MM Asia, 2021. (**CCF-C**)
7. **Bochao Liu**, Shiming Ge, Pengju Wang and Liansheng Zhuang. Generative Modeling via Private Manifold Gradient Estimation. In IJCAI, 2024. (**CCF-A**, submitted)
8. **Bochao Liu**, Shiming Ge, and Tongliang Liu. Privacy-Preserving Model Transcription with Differentially Private Synthetic Distillation. IEEE TPAMI. (**CCF-A，SCI-Q1**, submitted)
9. **Bochao Liu**, Pengju Wang, Shiming Ge. Learning Differentially Private Diffusion Models via Stochastic Adversarial Distillation. In ECCV, 2024. (**CCF-B, CV 三大顶会之一**, submitted)

授权专利

- 王伟平; 葛仕明; **刘博超**; 李晨钰。一种多方参与数据不共享的网络模型训练方法。
- 葛仕明; 刘浩林; **刘博超**; 王伟平。一种基于少量公共数据的隐私模型训练方法及装置。

实习经历

- 百度 · AI 安全组

  负责图像隐水印算法的扩容和鲁棒性研究。设计了一种基于 DCT 的图像隐水印方案；成功破解提取了一言的水印；改进了 RivaGAN（32bit—>64bit）；设计了一种基于 DiT 的水印方案。

项目实践

- **行业大数据安全受控共享核心系统研发（北京市科学技术委员会）-核心算法研发人员**

  该项目面向数据安全领域研发共享数据资产地图、数据分级分类管理系统和数据安全受控共享系统。本人主要负责数据安全受控共享系统中数据分布极端不均匀情况下的算法研究。

- **信息缺失情况下资源动态需求的因素分析（国家重点研发计划）-核心算法研究人员**

  该项目主要研究多维度表征与多模态数据补全技术，构建动态需求分析模型。本人主要负责针对文本数据的预测和补全算法研究。

- **Deepfake 检测竞赛（DFDC 2020）**

  该比赛的主要任务是训练一个 AI 模型去检测出那些视频是经过后期修改的。主办方 Facebook 提供了 470G 的训练数据和 400 段视频的验证集。本人参与了该竞赛获得了世界排名前 14% 的成绩。

专业技能

- 熟悉计算机视觉领域的研究进展，熟悉生成式模型（GAN，DDPM，DiT 等）、模型微调（LoRA，Dreambooth 等）、差分隐私学习、模型压缩等领域；熟悉 Transformer 及其原理与应用。了解文生视频（SVD，Sora，Mora（初步复现，还需微调一些细节）等）
- 熟悉 PyTorch 深度学习框架，了解 TensorFlow；熟练使用 Python 语言；熟练使用 Linux 系统；了解 C++ 语言。

获奖情况

- 中国科学院大学优秀党员（2023）
- 山东大学优秀学生奖学金（2016-2020）
- 山东大学三好学生、优秀毕业生（2020）
- 全国大学生数学建模竞赛省级三等奖（2018）
- 全国大学生数学竞赛国家级一等奖（2018）
- 社会实践省级三等奖（2018）
- 全国大学生数学竞赛国家级一等奖（2017）

学生活动

- **山东大学电子信息与物联网党支部组织委员**
- **山东大学羽毛球协会副部长**

兴趣爱好

- 羽毛球、乒乓球、健身