HE, PENGFEI

428 Shaw Ln., East Lansing, Michigan, 48824 | (+1) 608-622-3144 | hepengf1@msu.edu |

SUMMARY

Second year Ph.D student of Computer Science and Engineering at Michigan State University.

Research interests include adversarial learning; robustness of machine learning models; trustworthy large language models and generative models; machine learning theory.

Homepage: `https://pengfeihepower.github.io/`

EDUCATION

- Ph.D., Computer Science and Engineering, Michigan State University, Advisor: Dr. Jiliang Tang, 09/2022 to 08/2025
- Ph.D., Probability and Statistics, Michigan State University, Advisor: Dr. Yuehua Cui and Dr. Haolei Weng, 09/2020 to 08/2025
- Master., Statistics, University of Wisconsin-Madison, 09/2019 to 05/2020
- Bachelor., Mathematics, Nankai University, China, 09/2015 to 05/2019

PROFICIENCY SKILLS

- Coding: Python, R
- Software: MATLAB

PUBLICATIONS

Google Scholar: `https://scholar.google.com/citations?user=nsSrd6kAAAAJ&hl=en`

Conference and Journal Publications

- **Pengfei He**, Haochen Liu, Xiangyu Zhao, Jiliang Tang. **PROPN: Personalized Probabilistic Strategic Parameter Optimization in Recommendations** In the Proceedings of 31st ACM International Conference on Information & Knowledge Management, 2022.
- **Pengfei He**, Nicolas Garcia Trillos, Chenghui Li **Large Sample Spectral Analysis of Graph-based Multi-manifold Clustering** Journal of Machine Learning Research, 2023
- Han Xu,**Pengfei He**, Jie Ren, Yuxuan Wan, Zitao Liu, Jiliang Tang. **Probabilistic Categorical Adversarial Attack & Adversarial Training** , In the Proceedings of 40th International Conference on Machine Learning, 2023
- Margret V. Bjarnadottir, Siddharth Chandra, **Pengfei He**, Greg Midgette. **Analyzing Illegal Psychostimulant Trafficking Networks Using Noisy and Sparse Data**, IISE Transactions, 2023

Preprints and Submissions

- **Pengfei He**, Han Xu, Jie Ren, Yingqian Cui, Charu C. Aggarwal, Jiliang Tang. **Sharpness-Aware Data Poisoning Attack**
- Yingqian Cui, Jie Ren, Han Xu, **Pengfei He**, Hui Liu, Lichao Sun, Jiliang Tang. **DiffusionShield: A Watermark for Copyright Protection against Generative Diffusion Models**
- **Pengfei He**, Han Xu, Yue Xing, Jie Ren, Yingqian Cui, Shenglai Zeng, Jiliang Tang, Makoto Yamada, Mohammad Sabokrou. **Confidence-driven Sampling for Backdoor Attacks**
- Yingqian Cui, Jie Ren, Yuping Lin, Han Xu, **Pengfei He**, Yue Xing, Wenqi Fan, Hui Liu, Jiliang Tang. **FT-Shield: A Watermark Against Unauthorized Fine-tuning in Text-to-Image Diffusion Models**
- Han Xu, Jie Ren, **Pengfei He**, Shenglai Zeng, Yingqian Cui, Amy Liu, Hui Liu, Jiliang Tang. **On the Generalization of Training-based ChatGPT Detection Methods**
- Shenglai Zeng, Yaxin Li, Jie Ren, Yiding Liu, Han Xu, **Pengfei He**, Yue Xing, Shuaiqiang Wang, Jiliang Tang, Dawei Yin. **Exploring Memorization in Fine-tuned Language Models**

OTHER WORKING EXPERIENCES

Researching

Research Scientist at James Madison College, Michigan State university, December 2021 - August 2022
Visiting research student at Okinawa Institute of Science and Technology (OIST), May 2023 - July 2023

TEACHING AND MENTORING EXPERIENCE

- Fall 2019 - Graduate Teaching Assistant for Introductory Applied Statistics for Engineers. University of Wisconsin-Madison.
- Fall 2020/Spring 2021 - Graduate Teaching Assistant for Statistical Methods. Michigan State University.
- Summer 2021 - Graduate Teaching Assistant for Statistics for Scientists. Michigan State University.
- Fall 2021 - Graduate Teaching Assistant for Fundamentals of Data Science Methods, Probability and Statistics II: Statistics, Bayesian Statistical Methods. Michigan State University.

AWARDS AND SERVICES

- Recipient of Second Prize, Nankai University, September 2016
- Ranked Top 5% in the Department of Statistics, Nankai University, September 2019
- Awarded the Professor James Stapleton Prize in Statistics, Michigan State University, Fall 2021

- KDD-2022 Student Registration Award
- CIKM-2022 Student Registration Award
- Serve as PC Member: AAAI-2022, AAAI-2023, KDD-2023, SDM-2023, SDM-2024,ICDM-2023, PAKDD-2023
- Serve as Journal Reviewer: Journal of the American Statistical Association (JASA), Transactions on Knowledge and Data Engineering (TKDE), Transactions on Knowledge Discovery from Data (TKDD)
- Serve as conference volunteers: KDD-2022
- Member of International Volunteer HQ: Spent a month volunteering in Romania and helping hold summer camps for local children, 2017