Yuxuan Wan

(+1) 517-944-9530 | wanyuxua@msu.edu | https://wanyu42.github.io/

Summary

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

Research Interests include privacy-preserving machine learning and adversarial robustness.

Education

2021–present	Ph.D. in Computer Science Advisor: Prof. Jiliang Tang Michigan State University	4.0/4.0
2020 spring	Exchange University of Minnesota-Twin Cities	3.86/4.0
2017–2021	B.Eng in Computer Engineering The Hong Kong University of Science and Technology	3.63/4.3

Publications

Google Scholar: https://scholar.google.com/citations?user=jTwbiScAAAAJ&hl

Preprints

- **Yuxuan Wan**, Han Xu, Xiaorui Liu, Jie Ren, Wenqi Fan, Jiliang Tang, **Defense Against Gradient Leakage Attacks via Learning to Obscure Data**, Preprint: arXiv: 2206.00769, 2022.

Conference and Journal Publications

-

Conference Tutorials

- Wentao Wang, Han Xu, **Yuxuan Wan**, Jie Ren, Jiliang Tang, **Towards Adversarial Learning: From Evasion Attacks to Poisoning Attacks**, Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (SIGKDD), Pages 4830–4831, 2022.

Academic Honors & Awards

University's Scholarship Scheme for Continuing Undergraduate Students, HKUST	*2020, 2021*
Overseas Learning Experience Scholarship, HKUST	*Spring, 2020*
Dean's List, School of Engineering, HKUST	*2018-2020*
Dean's List, College of Science and Engineering, UMN	*Spring, 2020*

Services

Program Committee Member

- AAAI Conference on Artificial Intelligence (AAAI) 2023
- Conference on Web Search and Data Mining (WSDM) 2023

Conference External Reviewer

- International Conference on Machine Learning (ICML) 2022
- SIGKDD Conference on Knowledge Discovery and Data Mining (KDD) 2022
- Conference on Information and Knowledge Management (CIKM) 2021–2022

Volunteering

- SIGKDD Conference on Knowledge Discovery and Data Mining (KDD) 2022

- Conference on Neural Information Processing Systems (NeurIPS) 2021