Wenxin Ding

Email: wenxind@uchicago.edu
Tel: (412)-961-2629
Website: wenxind.github.io

RESEARCH INTEREST

My research interest lies in machine learning security and privacy. Specifically, I focus on bridging the gap between theoretical understanding and empirical practice. Recently, I have been working on problems regarding vulnerabilities of diffusion models.

EDUCATION

University of Chicago, Chicago, IL — Sep 2021 – June 2026
Ph.D. in Computer Science
Advisors: Prof. Heather Zheng and Prof. Ben Zhao

Carnegie Mellon University, Pittsburgh, PA
M.S. in Computer Science – Research Thesis — May 2021
Advisors: Prof. Nihar Shah and Prof. Weina Wang
B.S. in Computer Science and B.S. in Mathematical Sciences — May 2020

PUBLICATION & PREPRINT

Conference

- **Ding, Wenxin**, Arjun Nitin Bhagoji, Ben Y. Zhao, and Haitao Zheng. "Towards Scalable and Robust Model Versioning." *2nd IEEE Conference on Secure and Trustworthy Machine Leaning (2024).*
- Dai, Sihui*, **Wenxin Ding***, Arjun Nitin Bhagoji, Daniel Cullina, Ben Y. Zhao, Haitao Zheng, and Prateek Mittal. "Characterizing the Optimal 0-1 Loss for Multi-class Classification with a Test-time Attacker." *Advances in Neural Information Processing Systems* (2023). ***Spotlight***
- Shan, Shawn, **Wenxin Ding**, Emily Wenger, Haitao Zheng, and Ben Y. Zhao. "Post-breach recovery: Protection against white-box adversarial examples for leaked DNN models." In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pp. 2611-2625. 2022.
- **Ding, Wenxin**, Gautam Kamath, Weina Wang, and Nihar B. Shah. "Calibration with privacy in peer review." In *2022 IEEE International Symposium on Information Theory (ISIT)*, pp. 1635-1640. IEEE, 2022.

Workshop and Preprint

- *Shan, Shawn,* **Wenxin Ding**, Josephine Passananti, Haitao Zheng, Ben Y. Zhao. "Prompt-Specific Poisoning Attacks on Text-to-Image Generative Models." *arXiv preprint arXiv:2310.13828 (2023).*

- **Ding, Wenxin**, Nihar B. Shah, and Weina Wang. "On the privacy-utility tradeoff in peer-review data analysis." *AAAI Privacy-Preserving Artificial Intelligence (PPAI) workshop* (2021) ***Spotlight***

TEACHING EXPERIENCE

Teaching Assistant

University of Chicago

- CMSC 25300/35300 Mathematical Foundations of Machine Learning

Carnegie Mellon University

- 15110 Principles of Computing (Head Teaching Assistant)
- 15213 Introduction to Computer Systems
- 15440 Distributed Systems

Mentor

Strong Women Strong Girls, Pittsburgh, PA

SERVICE

- **Volunteer**
  The ACM Conference on Computer and Communications Security (CCS), Los Angeles, USA (Nov 7—11, 2022)

AWARDS

- 2021 University of Chicago Eckhardt Scholar
- 2020 Carnegie Mellon University Senior Leadership Recognition
- 2019 Mark Stehlik SCS Alumni Undergraduate Impact Scholarship
- 2017 William Lowell Putnam Mathematical Competition (Rank: 255 / 4638)