Wenxin Ding

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

EDUCATION

University of Chicago, Chicago, IL Sep 2021 -- Present
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

- 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." *arXiv preprint arXiv:2302.10722* (2023).
- 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.
- **Ding, Wenxin**, Nihar B. Shah, and Weina Wang. "On the privacy-utility tradeoff in peer-review data analysis." *arXiv preprint arXiv:2006.16385* (2020).

TEACHING EXPERIENCE

Teaching Assistant

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

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)