Zonghao Huang

Email: zonghao.huang@duke.edu | Homepage: https://zonghaohuang007.github.io/home/
Address: LSRC Building D227, 308 Research Drive, Durham, NC, 27708

Research Interest

- My research interests are broadly in the fields of computer security and privacy. Currently, my work focuses on developing *data auditing* algorithms for authentication and machine learning systems. My goal is to protect against unauthorized data access by *proactively* detecting data-use in computing systems while ensuring trustworthy detection, with a *provably bounded* false-detection rate.

Education

Duke University, Durham, NC — *2025 (expected)*
Ph.D. *in Computer Science* (Advisor: Prof. Michael K. Reiter)

Oklahoma State University, Stillwater, OK — *2019*
M.S. *in Electrical & Computer Engineering*

Nanyang Technological University, Singapore — *2016*
M.S. *in Electronics*

Xiamen University, Xiamen, China — *2015*
B.Eng. *in Electronic & Information Engineering*

Research Experience

Research Intern
Department of Computer Science, The University of Hong Kong, Hong Kong — *Oct. 2020 - Feb. 2021*
Research: *Privacy-preserving Algorithms and Distributed Optimization*, Host: Dr. Hubert T. H. Chan

Graduate Research Assistant
School of Electrical and Computer Engineering, Oklahoma State University, Stillwater, OK — *Jan. 2017 - Jul. 2019*
Research: *Differentially Private Distributed Optimization*

Publications and Manuscripts

- **Zonghao Huang**, Neil Zhenqiang Gong, Michael K. Reiter, "A general framework for data-use auditing of ML models", In *Proceedings of the 31st ACM Conference on Computer and Communications Security*, October 2024. To appear.
- **Zonghao Huang**, Lujo Bauer, Michael K. Reiter, "The impact of exposed passwords on honeyword efficacy", In *Proceedings of the 33rd USENIX Security Symposium*, August 2024. To appear.
- **Zonghao Huang**, Neil Zhenqiang Gong, Michael K. Reiter, "Mendata: A framework to purify manipulated training data", *Under Submission*, 2024.
- Before 2020:
  - **Zonghao Huang**, Yanmin Gong, "Differentially private ADMM for convex distributed learning: Improve accuracy with multi-step approximation", *Manuscript*, 2020.
  - **Zonghao Huang**, Rui Hu, Yuanxiong Guo, Eric Chan-Tin, Yanmin Gong, "DP-ADMM: ADMM-based distributed learning with differential privacy", *IEEE Transactions on Information Forensics and Security 15:1002–1012,* January 2020.
  - **Zonghao Huang**, Miao Pan, Yanmin Gong, "Robust truth discovery against data poisoning in mobile crowdsensing", In *Proceedings of the IEEE Global Communications Conference*, December 2019.
  - **Zonghao Huang**, Yanmin Gong, "Differential location privacy for crowdsourced spectrum sensing", In *Proceedings of the 5th IEEE Conference on Communications and Network Security*, October 2017.

Awards and Honors

- **Duke Graduate Fellowship**, Duke University, USA — *2020, 2021*
- **Student Travel Grant for IEEE CNS 2017**, NSF and ARO, USA — *2017*
- **The First Prize Scholarship**, Xiamen University, China — *2015, 2013, 2012*
- **The Second Prize Scholarship**, Xiamen University, China — *2014*

Teaching Experience

COMPSCI 371 Elements of Machine Learning
Teaching Assistant, Department of Computer Science, Duke University *Fall 2022*

COMPSCI 520 Numerical Analysis
Teaching Assistant, Department of Computer Science, Duke University *Spring 2022*

ECEN 4024 Senior Design 2
Teaching Assistant, School of Electrical and Computer Engineering, Oklahoma State University, Stillwater *Fall 2019*

Academic Activities

- **Reviewer for Conference Manuscript Submissions** :
  - IEEE INFOCOM 2018, IEEE ICC 2018, IEEE CNS 2018, IEEE MASS 2024
- **External Reviewer for Conference Manuscript Submissions** :
  - ESORICS 2021
- **Journal Reviewer**:
  - IEEE Transactions on Information Forensics and Security.
  - IEEE Transactions on Automatic Control.

Programing Skills and Languages

- **Programming**: MATLAB (proficient), Python (proficient), C (good), Latex (proficient)
- **Languages**: English (proficient), Chinese (native), Cantonese (native)