# Zonghao Huang

Email: zonghao.huang@duke.edu | Homepage: https://zonghaohuang007.github.io/home/
Address: LSRC Building D229, 308 Research Drive, Durham, NC, 27708

## Education

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

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

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

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

## Research Experience

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

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

## Publications and Manuscripts

- **Zonghao Huang**, Neil Gong, Michael K. Reiter, "A General Framework for Data-Use Auditing of ML Models", In *Proceedings of the* $31^{st}$ *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* $33^{rd}$ *USENIX Security Symposium*, August 2024. To appear.
- **Zonghao Huang**, Neil 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* $5^{th}$ *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*
- **First-Class Scholarship of Academic Excellence**, Xiamen University, China — *2015, 2013, 2012*
- **Scholarship of Recreation and Sports Excellence**, Xiamen University, China — *2015*
- **Second-Class Scholarship of Academic Excellence**, 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)