

# Zonghao Huang

Email: [zonghao.huang@duke.edu](mailto:zonghao.huang@duke.edu) | Homepage: <https://zonghaohuang007.github.io/home/>

Address: LSRC Building D311, 308 Research Drive, Durham, NC, 27708

## RESEARCH INTEREST

- Adversarial Machine Learning, Learning Theory, Computer Security & Privacy, Differential Privacy, Stochastic Optimization, ADMM

## EDUCATION

### Duke University

*Ph.D. in Computer Science (Advisor: Prof. Michael K. Reiter)*

Durham, NC, USA

Aug. 2020 - Present

### Oklahoma State University

*M.S. in Electrical & Computer Engineering*

Stillwater, OK, USA

Jan. 2017 - Dec. 2019

### Nanyang Technological University

*M.S. in Electronics*

South West, Singapore

Aug. 2015 - Jul. 2016

### Xiamen University

*B.Eng. in Electronic & Information Engineering*

Xiamen, Fujian, China

Sept. 2011 - Jul. 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 Machine Learning, 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 Machine Learning

## PUBLICATIONS AND MANUSCRIPTS

### • Works @ OSU:

- Zonghao Huang, Yanmin Gong, “Differentially Private ADMM for Convex Distributed Learning: Improve Accuracy with Multi-Step Approximation”, *arXiv preprint*, 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 (TIFS)*, 2020.
- Zonghao Huang, Miao Pan, Yanmin Gong, “Robust Truth Discovery Against Data Poisoning in Mobile Crowdsensing”, *Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM)*, 2019.
- Zonghao Huang, Yanmin Gong, “Differential Location Privacy for Crowdsourced Spectrum Sensing”, *Proceedings of the 2017 IEEE Conference on Communications and Network Security (CNS)*, 2017.

## AWARDS AND HONORS

- Duke Graduate Fellowship, Duke University, USA 2020
- Student Travel Grant for IEEE CNS 2017, National Science Foundation and Army Research Office, 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

### 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.

## PROGRAMING SKILLS AND LANGUAGES

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