Zonghao Huang

Email: zonghao.huang@duke.edu | Homepage: https://zonghaohuang007.github.io/home/
Address: LSRC Building D101, 308 Research Drive, Durham, NC, 27708

Research Interest

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

Education

Duke University — *Durham, NC, USA*
Ph.D. *in Computer Science (Advisor: Prof. Michael Reiter)* — *Aug. 2020 - Present*

Oklahoma State University — *Stillwater, OK, USA*
M.S. *in Electrical & Computer Engineering* — *Jan. 2017 - Dec. 2019*

Nanyang Technological University — *South West, Singapore*
M.S. *in Electronics* — *Aug. 2015 - Jul. 2016*

Xiamen University — *Xiamen, Fujian, China*
B.Eng. *in Electronic & Information Engineering (rank: top 10%)* — *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", *submitted to the 2021 International Joint Conference on Artificial Intelligence (IJCAI), 2021.*
  - **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 CS Ph.D. Fellowship**, Department of Computer Science, Duke University, USA — *2020 - 2022*
- **Student Travel Grant for IEEE CNS 2017**, National Science Foundation and Army Research Office, USA — *2017*
- **First-Class Graduate Scholarship of Academic Excellence**, Xiamen University, China — *2015*
- **Graduate Scholarship of Recreation and Sports Excellence**, Xiamen University, China — *2015*
- **Second-Class Scholarship of Academic Excellence**, Xiamen University, China — *2014*
- **First-Class Scholarship of Academic Excellence**, Xiamen University, China — *2013, 2012*

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)