Zonghao Huang

Email: zonghao.huang@duke.edu | Homepage: https://zonghaohuang007.github.io/home/
Address: LSRC Building D124, 308 Research Drive, Durham, NC, 27708

Research Interest

- Deep Neural Network, Computer Security & Privacy, Cryptography, Differential Privacy, Learning Theory, Stochastic Optimization, ADMM

Education

Duke University *Durham, NC, USA*
Ph.D. *in Computer Science (Advisor: Prof. Michael K. 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* *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

- **Zonghao Huang**, Lujo Bauer, Michael K. Reiter, "The Impact of Exposed Passwords on Honeyword Efficacy", *Manuscript, 2023.*
- **Before Ph.D.:**
  - **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*
- **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

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.
- **External Reviewer for Conference Manuscript Submissions** :
    - ESORICS 2021.
- **Journal Reviewer**:
    - IEEE Transactions on Information Forensics and Security.

Programing Skills and Languages

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