Wenjie Qu

Department of Artificial Intelligence and Automation
Huazhong University of Science and Technology
https://quwenjie.github.io/
wenjiequ@hust.edu.cn

EDUCATION

Huazhong University of Science and Technology, Wuhan, China 2019-NOW
B.E. Automation, Honor Class

- **GPA: 3.92/4.0**

RESEARCH INTERESTS

Trustworthy Machine Learning, AI for Computer Security

EXPERIENCE

Research Intern, Network & Information Security Lab, Tsinghua University, 2021.7
Advisor: Chao Zhang
Topic: AI Binary Analysis

Research Intern, Gong Research Group, Duke University, 2021.1
Advisor: Neil Gong
Topic: Provably Robust Machine Learning

Research Intern, School of Cyber Science and Engineering, HUST, 2020.7
Advisor: Pan Zhou
Topic: Adversarial Machine Learning on Computer Vision

PUBLICATIONS

- **EncoderMI: Membership Inference against Contrastive Learning**
  Hongbin Liu*, Jinyuan Jia*, **Wenjie Qu**, Neil Gong
  To appear in *ACM Conference on Computer and Communications Security (**CCS**)* 2021,

- **MultiGuard: Provably Robust Multi-label Classification against Adversarial Examples**
  Jinyuan Jia*, **Wenjie Qu***, Neil Gong
  Under Review

- **Disguiser: An Effective and Practical Black-box Attack for Static Machine Learning Based Malware Detectors**
  Jialai Wang, Chao Zhang, **Wenjie Qu**, Yi Rong, Chaofan Zhang, Hengkai Ye, Qi Li
  Under Review.

PATENT

Certified radius guided adversarial attack, and robust training method (CN113052314A)
Pan Zhou, Qiming Wu, **Wenjie Qu**, Yulai Xie, Ruixuan Li

HONORS & AWARDS

- **Autodriving CTF, DEFCON 29, 4th place** 2021
- **National Scholarship (6/350)(the highest honor for undergraduates in China)** 2020
- **Outstanding Graduate in Term of Academic Performance (top 1%)** 2020
- Merit Student (1/30) 2018
- Bronze Medal, Asia-Pacific Informatics Olympiad 2018
- Bronze Medal, National Olympiad in Informatics Winter Camp 2018
- First Prize, National Olympiad in Informatics in Provinces 2017