

## 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  
B.E. Automation, Honor Class

2019.9-NOW

- **GPA: 3.92/4.0**

### RESEARCH INTERESTS

Trustworthy Machine Learning, AI for Computer Security

### EXPERIENCE

AI Binary Analysis June 2021-January 2022  
Research Intern, Network & Information Security Lab, Tsinghua University Beijing, China  
Under supervision of Professor Chao Zhang.

Designed a novel method for AI-based semantic similar function retrieval, which overcomes the robustness weaknesses of previous graph-based works.

Participated in development of a novel method for generating malware adversarial examples. Work submitted to AAAI 2022.

Provably Robust Machine Learning and Machine Learning Privacy January 2021-January 2022  
Research Intern, Neil Gong's Research Group, Duke University Durham, USA(remote)  
Under supervision of Professor Neil Gong.

Designed a novel method to provide robustness guarantee for contrastive learning encoder services, and a method to train provably robust encoders, work submitted to Usenix Security 2022.

Participated in development of a novel method for providing robustness guarantee for multi-label classification, work submitted to CVPR 2022.

Participated in development of a novel method for performing membership inference for contrastive learning, work accepted by CCS 2021.

Adversarial Machine Learning on Computer Vision July 2020-December 2020  
Research Intern, School of Cyber Science and Engineering, Huazhong University of S&T Wuhan, China  
Under supervision of Dr.Binghui Wang and Professor Pan Zhou  
Designed a novel method to leverage certified radius to perform attack to semantic segmentation, work submitted to S&P 2021.

### 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,

- **REaaS: Robust Encoder as a Service in Contrastive Learning**  
Wenjie Qu, Jinyuan Jia, Neil Gong  
Under Review
- **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 (CN 113052314 B)  
Pan Zhou, Qiming Wu, Wenjie Qu, Yulai Xie, Ruixuan Li

#### HONORS & AWARDS

- Autodriving CTF, DEFCON 29, 4th place 2021
- National Scholarship (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