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   2019.9-2023.6
B.E. Automation, Honor Class

- **GPA: 3.93/4.0**

RESEARCH INTERESTS

Machine Learning for Computer Security, Trustworthy Machine Learning

EXPERIENCE

Automatic Decompilation   February 2022-Octor 2022
Research Intern, HexHive Lab, École polytechnique fédérale de Lausanne(EPFL)   Lausanne, Switzerland
Under the supervision of Professor Mathias Payer.

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

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

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 the supervision of Dr.Binghui Wang and Professor Pan Zhou

PUBLICATIONS

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

- **jTrans: Jump-Aware Transformer for Binary Code Similarity Detection**
  Hao Wang*, **Wenjie Qu***, Gilad Katz, Wenyu Zhu, Zeyu Gao, Han Qiu, Jianwei Zhuge, Chao Zhang
  Submitted to ISSTA 2022

- **Certified Radius-Guided Attacks to Image Segmentation Models**
  Wenjie Qu*, Youqi Li*, Binghui Wang
  Submitted to ACM CCS 2022

- **REaaS: Robust Encoder as a Service in Contrastive Learning**
  Wenjie Qu, Jinyuan Jia, Neil Gong
  Submitted to Usenix Security 2022

- **MultiGuard: Provably Robust Multi-label Classification against Adversarial Examples**
  Jinyuan Jia*, **Wenjie Qu***, Neil Gong
  Submitted to CVPR 2022

- **MPass: Bypassing Learning-based Static Malware Detectors**
  Jialai Wang, Han Qiu, **Wenjie Qu**, Chao Zhang, Yi Rong, Qi Li
  Submitted to IJCAI 2022

ACADEMIC SERVICE

External Reviewer

- International Conference on Machine Learning (ICML), 2022

HONORS & AWARDS

- Autodriving CTF, DEFCON 29, 4th place   2021
- **National Scholarship (the highest honor for undergraduates in China)**   2020
- **Outstanding Graduate(top 1%)**   2020
- Merit Student (1/30)   2020

  Programming Competitions

- 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