Wenjie Qu
Department of Artificial Intelligence and Automation
Huazhong University of Science and Technology
https://quwenjie.github.io/
wen_jie_qu@outlook.com

EDUCATION

Huazhong University of Science and Technology, Wuhan, China 2019.9-2023.6(Expected)
B.E. in Automation, Honor Class
GPA: 3.88/4.0
Chinese National Scholarship (Highest Honor, 6/350)

RESEARCH INTEREST

Various topics in Computer Science, mainly Security:

- AI for Security, Software Engineering, System
- Machine Learning Security& Privacy
- Multi-Party Computation

Also interested in Blockchain.

PUBLICATIONS

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

[2] **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
*International Symposium on Software Testing and Analysis(**ISSTA**)* 2022

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

[4] **MPass: Bypassing Learning-based Static Malware Detectors**
Jialai Wang, **Wenjie Qu**, Yi Rong, Chao Zhang, Han Qiu, Qi Li, Zongpeng Li
Submitted to AAAI 2023

[5] **A Certified Radius-Guided Attack Framework to Image Segmentation Models**
Wenjie Qu*, Youqi Li*, Binghui Wang
Submitted to NDSS 2023

[6] **REaaS: Enabling Adversarially Robust Downstream Classifiers via Robust Encoder as a Service**
Wenjie Qu, Jinyuan Jia, Neil Gong
Submitted to NDSS 2023

[7] **Pre-trained Encoders in Self-Supervised Learning Improve Secure and Privacy-preserving Supervised Learning**
Hongbin Liu*, **Wenjie Qu***, Jinyuan Jia, Neil Gong
Submitted to NDSS 2023

RESEARCH EXPERIENCE

CoLink: A Programming Framework for Decentralized Data Science
Research Intern at UC Berkeley April 2022-
Advisor: **Prof. Dawn Song**

- Participated in the design of CoLink, a programming framework which greatly simplifies the deployment of decentralized data science solutions.

- Designed and implemented CoLink SDK python interface, based on gRPC services.
- Designed and implemented CoLink-crypten protocols which enables user to perform general privacy-preserving machine learning tasks without writing code, based on crypten MPC library & python sdk.

jTrans: Jump-Aware Transformer for Binary Code Similarity Detection[2]
Research Intern at Tsinghua University July 2021-January 2022
Advisor: **Prof. Chao Zhang**

- Proposed a novel neural network architecture for binary function similarity detection, encodes control flow information into the transformer.
- Proved through attention weights how our mechanism delivers the jump target information.
- Released the currently largest binary dataset to the community as a benchmark.
- Outperformed state-of-the-art binary similarity detection methods by 30.5%.

REaaS: Enabling Adversarially Robust Downstream Classifiers via Robust Encoder as a Service[6]
Research Intern at Duke University March 2021-February 2022
Advisor: **Prof. Neil Gong**

- Proposed a novel method for encoder cloud service which enables a client to build a certifiably robust downstream classifier and derive certified radius while reducing the number of queries.
- Proposed a novel pre-training method to enhance the robustness of the encoder based on a spectral-norm regularization term.
- Achieves much better certified robustness for the clients' downstream classifiers when the cloud server pre-trains the encoder via our spectral-norm regularized training method.

A Certified Radius-Guided Attack Framework to Image Segmentation Models[5]
Research Intern at Illinois Institute of Technology August 2020-January 2021
Advisor: **Prof. Binghui Wang**

- Designed an attack framework for image segmentation models leveraging the properties of certified radius.
- Proposed the first blackbox attack to image segmentation models via gradient estimation based on bandits.
- Outperformed state-of-the-art PGD attack by 13% relatively.

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
- 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