

Wenjie Qu

Email: wen_jie_qu@outlook.com

Website: <https://quwenjie.github.io/>

EDUCATION

Huazhong University of Science and Technology
B.E. in Automation

Wuhan, China
2019.9-2023.6(*Expected*)

PAPERS UNDER REVIEW

- [1] X. Liu, T. Shi, **W. Qu**, S. Zhuang, D. Song. “Decentralized Programming” Submitted to *USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, 2023
- [2] **W. Qu***, Y. Li*, B. Wang. “A Certified Radius-Guided Attack Framework to Image Segmentation Models” Submitted to *IEEE European Symposium on Security and Privacy (EuroSP)*, 2023

PUBLICATIONS

- [1] **W. Qu**, J. Jia, N. Gong. “REaaS: Enabling Adversarially Robust Downstream Classifiers via Robust Encoder as a Service” in *Network and Distributed System Security (NDSS)*, 2023
- [2] J. Jia*, **W. Qu***, and N. Gong. “MultiGuard: Provably Robust Multi-label Classification against Adversarial Examples” in *Advances in Neural Information Processing Systems (NeurIPS)*, 2022, *Spotlight*
- [3] H. Wang*, **W. Qu***, G. Katz, W. Zhu, Z. Gao, H. Qiu, J. Zhuge, and C. Zhang. “jTrans: Jump-Aware Transformer for Binary Code Similarity Detection” in *International Symposium on Software Testing and Analysis (ISSTA)*, 2022
- [4] H. Liu*, J. Jia*, **W. Qu**, and N. Gong. “EncoderMI: Membership Inference against Pre-trained Encoders in Contrastive Learning” in *ACM Conference on Computer and Communications Security (CCS)*, 2021

RESEARCH EXPERIENCE

CoLink: A Framework for Decentralized Programming

Research Intern at University of California, Berkeley

April 2022-Present

Advisor: **Prof. Dawn Song**

- Implemented CoLink SDK python APIs, based on gRPC services, the basis for most CoLink-based machine learning applications.
- Designed and implemented an ML-MPC framework, enabling users to perform general privacy-preserving data collaboration tasks.

jTrans: Jump-Aware Transformer for Binary Code Similarity Detection

Research Intern at Tsinghua University

July 2021-January 2022

Advisor: **Prof. Chao Zhang**

- Proposed a novel neural network architecture for binary function similarity detection, encoding control flow information into the transformer.
- Released the currently largest binary dataset to the community as a benchmark.

REaaS: Enabling Adversarially Robust Downstream Classifiers via Robust Encoder as a Service

Research Intern at Duke University

June 2021-November 2022

Advisor: **Prof. Neil Gong**

- Proposed a novel method for cloud encoder service that enables a client to build a provably robust downstream classifier while reducing the number of queries to the encoder by orders.
- Proposed a novel pre-training method to enhance the robustness of the encoder based on a spectral-norm regularization term.

MultiGuard: Provably Robust Multi-label Classification against Adversarial Examples

Research Intern at Duke University

February 2021-May 2021

Advisor: **Prof. Neil Gong**

- Proposed the first provable defense algorithm against adversarial examples on multi-label classification task.
- Implemented the practical algorithm for calculating the certified intersection size between the set of labels predicted by our MultiGuard and ground truth labels.

A Certified Radius-Guided Attack Framework to Image Segmentation Models

Research Intern at Illinois Institute of Technology

August 2020-January 2021

Advisor: **Prof. Binghui Wang**

- Designed an attack framework against image segmentation models leveraging the properties of certified radius derived by randomized smoothing.
- Proposed the first blackbox attack to image segmentation models via gradient estimation based on bandits.

ACADEMIC SERVICE

External Reviewer

- International Conference on Machine Learning (ICML), 2022

HONORS & AWARDS

- | | |
|--|------|
| • China Optics Valley Rising Star Scholarship | 2022 |
| • Science and Technical Innovation Scholarship | 2022 |
| • Huawei Scholarship | 2022 |
| • Autodriving CTF, DEFCON 29, Runner-up Winner | 2021 |
| • National Scholarship | 2020 |
| • Outstanding Undergraduate of Academic Performance | 2020 |
| • Merit Student | 2020 |
| • Bronze Medal, National Olympiad in Informatics Winter Camp | 2018 |
| • First Prize, National Olympiad in Informatics in Provinces | 2017 |

SKILLS

- Programming Languages: C, C++, Python, Rust
- Libraries/Software: Pytorch, OpenCV, Numpy, IDA Pro