Wenjie Qu

Email: wen_jie_qu@outlook.com

EDUCATION

National University of Singapore	2023.8-2027.6(Expected)
Ph.D. student in Computer Science	Advisor: Prof. Jiaheng Zhang
Huazhong University of Science and Technology	2019.9-2023.6
B.E. in Automation	

PUBLICATIONS

[1] **W. Qu***, Y. Li*, B. Wang. "A Certified Radius-Guided Attack Framework to Image Segmentation Models" in *IEEE European Symposium on Security and Privacy (**EuroSP**), 2023*

[2] J. Wang, **W. Qu**, Y. Rong, H. Qiu, Q. Li, Z. Li, C. Zhang. "MPass: Bypassing Learning-based Static Malware Detectors" in *Design Automation Conference (**DAC**), 2023*

[3] **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*

[4] 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***

[5] 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*

[6] 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*

EXPERIENCES

Efficient Distributed Inference for Large Language Models
Intern at Microsoft Research Asia, Trustworthy Systems Group — *March 2023-July 2023*
Mentor: **Zhongxin Guo**, **Yang Chen**

CoLink: A Framework for Decentralized Programming
Research Intern at University of California, Berkeley — *April 2022-Februrary 2023*
Advisor: **Prof. Dawn Song**

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

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**

MultiGuard: Provably Robust Multi-label Classification against Adversarial Examples
Research Intern at Duke University *February 2021-May 2021*
Advisor: **Prof. Neil Gong**

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**

ACADEMIC SERVICE

External Reviewer

- International Conference on Machine Learning (ICML), 2022

HONORS & AWARDS

• NUS President's Graduate Fellowship	2023
• 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