Wenjie Qu

Homepage: quwenjie.github.io Email: wen_jie_qu@outlook.com

EDUCATION

National University of Singapore 2023.8-
Ph.D. student in Computer Science Advisor: Prof. Jiaheng Zhang
Huazhong University of Science and Technology 2019.9-2023.6
B.E. in Electrical and Computer Engineering

PUBLICATIONS

Total Citations: **701**, Google Scholar Link, **10** papers in Top Security Conferences (**5** first authors), **4** papers in Top AI/ML Conferences/Journals

[1] **W. Qu***, Y. Guo*, Y. Ying, J. Zhang. "VerfCNN, Optimal Complexity zkSNARK for Convolutional Neural Networks" in *IEEE Symposium on Security and Privacy (**SP**), 2026*

[2] S. Zhao, C. Wang, Y. Li, Y. Huang, **W. Qu**, S. Lam, Y. Xie, K. Chen, J. Zhang, T. Zhang. "Towards Effective Prompt Stealing Attack against Text-to-Image Diffusion Models" in *Network and Distributed System Security (**NDSS**), 2026*

[3] K. Cheng, Y. Xia, A. Song, J. Fu, **W. Qu**, Y. Shen, J. Zhang. "Mosformer: Maliciously Secure Three-Party Inference Framework for Large Transformers" in *ACM Conference on Computer and Communications Security (**CCS**), 2025*

[4] X. Yang*, J. Han*, R Bommasani*, J Luo*, **W Qu***, W Zhou*, et al. "Reliable and Responsible Foundation Models" in *Transactions on Machine Learning Research (**TMLR**), 2025*

[5] S. Zhai, J. Li, Y. Liu, H. Chen, Z. Tian, **W. Qu**, Q. Shen, R. Jia, Y. Dong, J. Zhang. "Efficient Input-level Backdoor Defense on Text-to-Image Synthesis via Neuron Activation Variation" in *International Conference on Computer Vision (**ICCV**), 2025, **Highlight***

[6] Z. Tian, Y. Ding, **W. Qu**, X. Yu, E. Gong, J. Zhang, J. Liu, K. Ren. "Towards Collaborative Anti-Money Laundering Among Financial Institutions" in *ACM Web Conference (**WWW**), 2025*

[7] **W. Qu**, Y. Zhou, Y. Wu, T. Xiao, B. Yuan, Y. Li, J. Zhang. "Prompt Inversion Attack against Collaborative Inference of Large Language Models" in *IEEE Symposium on Security and Privacy(**SP**), 2025*

[8] C. Li, P. Zhu, Y. Li, C. Hong, **W. Qu**, J. Zhang. "HyperPianist: Pianist with Linear-Time Prover and Logarithmic Communication Cost" in *IEEE Symposium on Security and Privacy(**SP**), 2025*

[9] **W. Qu**, Y. Sun, X. Liu, T. Lu, Y. Guo, K. Chen, J. Zhang. "zkGPT: An Efficient Non-interactive Zero-knowledge Proof Framework for LLM Inference" in *USENIX Security (**SEC**), 2025*

[10] **W. Qu**, W. Zheng, T. Tao, D. Yin, Y. Jiang, Z. Tian, W. Zou, J. Jia, J. Zhang. "Provably Robust Multi-bit Watermarking for AI-generated Text " in *USENIX Security (**SEC**), 2025*

[11] Y. Guo, X. Liu, K. Huang, **W. Qu**, W. Zheng, T. Tao, D. Yin, Y. Jiang, T. Tao, J. Zhang. "DeepFold: Efficient Multilinear Polynomial Commitment from Reed-Solomon Code and Its Application to Zero-knowledge Proofs" in *USENIX Security (**SEC**), 2025*

[12] **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*

[13] **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*

[14] 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*

[15] 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***

[16] 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*

[17] 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*

ACADEMIC SERVICE

Program Committee
- CCS 2025, 2026

Workshop Organizer
- ICLR 2025 Workshop on Foundation Models in the Wild

Journal Reviewer
- IoT-J, TIFS, TDSC, TMC, JSS.

Reviewer
- ICML 2022, MM 2024, NeurIPS 2025, COLM 2025, CVPR 2026

Sub-Reviewer
- PKC 2024

INVITED TALKS

Towards LLM auditing, Peking University	2025.7
Zero-knowledge proofs and its applications, Shanghai Jiaotong University	2025.6
Towards reliable large language models, risks and solutions, Tsinghua University	2023.12
Towards reliable large language models, risks and solutions, Zhejiang University	2023.12

SELECTED AWARDS & HONORS

- DAAD AInet Fellowship 2025
- Ant Group Intech Scholarship Future (10 recipients globally) 2025
- **NUS President's Graduate Fellowship** (most prestigious scholarship for NUS PhD) 2023
- Stars of Tomorrow, Microsoft Research Asia 2023
- Outstanding Graduate, HUST 2023
- Huawei Scholarship (sole recipient in department) 2022
- National Scholarship (highest honor for undergraduate in China) 2020
- Outstanding Undergraduate of Academic Performance (top 1% in department) 2020
- First Prize, National Olympiad in Informatics in Provinces 2017