Wenhao Zhang

Evanston, IL | wenhao.zhang@northwestern.edu | wzhang.cc

Education

Northwestern University — Evanston, IL
Ph.D. Student in Computer Science. Advisor: Xiao Wang. — *Sept. 2022 – Present*
Research Interests: Secure Two-Party/Multi-Party Computation.

Southern University of Science and Technology — Shenzhen, Guangdong, China
B.Eng. in Computer Science. Advisor: Qi Wang. — *Aug. 2018 – Jun. 2022*

Experience

Research Internship - Multi-Party Computation — Shanghai, China
Shanghai Key Laboratory of Privacy-Preserving Computation (Mentor: Xiang Xie) — *Mar. 2022 – Jun. 2022*

- Implemented the Ferret COT protocol in Rust based on swanky suite.
- Surveyed on protocols of OT and VOLE in different settings.

Research Internship - Network Security — Remote
University of California, Irvine (Mentor: Zhou Li) — *Jun. 2021 – Sept. 2021*

- Proposed an attacking strategy of Manufacturer Usage Description based on DHCP crafting.
- Implemented a proof-of-concept attack script and set up a testbed to verify the feasibility of such an attack.
- Proposed some strategies to prevent this kind of attack.

Teaching Assistant — Shenzhen, Guangdong, China
Southern University of Science and Technology — *Sept. 2019 – Dec. 2021*

Cryptography Research Projects

Efficient Actively Secure DPF and RAM-based 2PC with One-Bit Leakage — Nov. 2022 – Dec. 2023

This project is to propose actively secure protocols for distributed point function (DPF) without using actively secure generic two-party computation (2PC) and dual-execution-based 2PC supporting reactive circuits, both with one-bit leakage. Its performance is significantly better than the SOTA malicious secure protocol and it is even competitive when compared to the SOTA semi-honest secure protocol in many settings.

Half-Tree: Halving the Cost of Tree Expansion in COT and DPF — Jun. 2022 – Oct. 2022

This project is to apply a suite of optimizations on the GGM tree to reduce the computation and communication complexity. It halves the number of AES calls and the communication of GGM tree generation in the SOTA COT and sVOLE protocols. It halves the communication and the round complexity of the SOTA DPF/DCF protocols.

Coded Computing and Its Applications — Sept. 2020 – Jun. 2021

This project is to apply information and coding theory to mitigate the effects of straggler and malicious nodes in the framework of distributed computing. Coding methods in different computational scenarios are designed to keep the distributed computation private and efficient.

Honors and Awards

- SUSTech Outstanding Graduate — *Jun. 2022*
- International Collegiate Programming Contest(ACM-ICPC) Asia East Final — ***Gold Medal*** — *Dec. 2019*
- International Collegiate Programming Contest(ACM-ICPC) Asia Regional — ***Gold Medal*** — *Nov. 2018*

Publications

2. **Efficient Actively Secure DPF and RAM-based 2PC with One-Bit Leakage**
   Wenhao Zhang, Xiaojie Guo, Kang Yang, Ruiyu Zhu, Yu Yu and Xiao Wang
   Under Review

1. **Half-Tree: Halving the Cost of Tree Expansion in COT and DPF**
   Xiaojie Guo, Kang Yang, Xiao Wang, Wenhao Zhang, Xiang Xie, Jiang Zhang and Zheli Liu
   Annual International Conference on the Theory and Applications of Cryptology and Information Security (Eurocrypt), 2023

Technical Skills

Language: C/C++, Python, Java, Rust, Shell.

Tools: Docker, Git, EMP-toolkits.