Zhou Zhang

37 Xueyuan Road, Haidian District, Beijing, P.R. China, 100191.
(+86) 18600665799 zhouzhang@buaa.edu.cn zhouzhangwalker.github.io github.com/zhouzhangwalker

Education

Beihang University **Sep. 2023 – Present**
Ph.D. in Cyber Science and Technology *Beijing, China*

Beihang University **Sep. 2021 - Jun. 2023**
M.S. in Cyber Science and Technology *Beijing, China*

Beihang University **Sep. 2017 - Jun. 2021**
B.S. in Cyber Science and Technology *Beijing, China*

Research Interest

- Fully Homomorphic Encryption (FHE)
- Multi-party Computation (MPC)
- Encrypted Database

Publications

- Song Bian, Zian Zhao, **Zhou Zhang**, Ran Mao, Kohei Suenaga, Yier Jin, Zhenyu Guan, and Jianwei Liu, HEIR: A Unified Representation for Cross-Scheme Compilation of Fully Homomorphic Computation, Network and Distributed System Security Symposium (NDSS), February 2024
- Song Bian[1], **Zhou Zhang**[1], Haowen Pan, Ran Mao, Zian Zhao, Yier Jin, and Zhenyu Guan, HE3DB: An Efficient and Elastic Encrypted Database Via Arithmetic-And-Logic Fully Homomorphic Encryption, ACM Conference on Computer and Communications Security (ACM CCS), November 2023
- Guan Zhenyu, Jing Junpeng, Deng Xin, Xu Mai, Jiang, Lai, **Zhang Zhou** and Li Yipeng, DeepMIH: Deep Invertible Network for Multiple Image Hiding, IEEE Transactions on Pattern Analysis and Machine Intelligence (IEEE TPAMI), January 2023

Research Experience

Research on the improvement of HE3DB **Sept. 2023 – Present**
- Tried to address the main bottleneck in HE3DB, which is a lot of homomorphic ciphertext-ciphertext comparisons.

Research on the homomorphic encrypted database HE3DB **Sept. 2022 – Aug. 2023**
- Developed a homomorphically encrypted database framework including homomorphic filtering, aggregation, and ciphertext conversion that supports types of SQL query evaluations over FHE ciphertext.
- Proposed high-precision homomorphic comparison to support accurate homomorphic filtering and fast algorithms to perform both arithmetic (e.g., SUM, AVG) and logic (e.g., MIN, MAX) aggregations on homomorphic filtered results.
- Implemented HE3DB based on SEAL and TFHEpp and benchmarked the cryptographic blocks and SQL queries. The work was published on ACM CCS 2023 and got ACM CCS Distinguished Paper Award.

Research on the basic homomorphic encryption schemes and implementations **Sept. 2021 – Aug. 2022**
- Reviewed the literature on FHE, including BFV, CKKS, and FHEW/TFHE, along with implementations like SEAL and OpenFHE, analyzed their strengths and limitations, and explored the conversion between different schemes.
- Implemented a homomorphic instruction set architecture that supports evaluations of both arithmetic and logic circuits over FHE ciphertexts. The instruction set supports the work about the homomorphic compiler HEIR (NDSS 2024).

Honors & Awards

Distinguished Paper Award | *ACM CCS 2023* **Nov. 2023**

Merit Student | *Beihang University* **Sept. 2023**

Outstanding Graduates Awards | *Beihang University* **Jun. 2021**

National Scholarship | *Ministry of Education of the People's Republic of Chin* **Dec. 2020**

First Prize | *National College Student Information Security Contest* **Aug. 2019**

Presentations

ACM Conference on Computer and Communication Security (ACM CCS) **Nov. 2023**

HE3DB: An Efficient and Elastic Encrypted Database Via Arithmetic-And-Logic Fully Homomorphic Encryption *Denmark*

- Presented our work about a fully homomorphically encrypted, efficient and elastic database HE3DB.

Technical Skills

Programming: C++, Python, SQL, LaTeX
Languages: Chinese, English