XIAN WANG

Room 3664, Academic Building, HKUST, Clear Water Bay, Hong Kong S.A.R.
852-98369821 ⋄ xwanggj@connect.ust.hk ⋄ xxiwa.github.io ⋄ Google Scholar

EDUCATION

The Hong Kong University of Science and Technology — Hong Kong S.A.R.
Master of Philosophy in Computer Science and Engineering — Jul. 2023 - Jul. 2025 (expected)
Supervisor: Dr. Dimitris Papadopoulos

Xidian University — Xi'an, China
Bachelor of Software Engineering, GPA: 3.7/4 (top 3%) — Sep. 2018 - Jun. 2022

PUBLICATION

SOTER: Guarding Black-box Inference for General Neural Networks at the Edge
USENIX ATC'22 (with result reproduced badge), links: [paper][code][video][slides]
Tianxiang Shen, Ji Qi, Jianyu Jiang, Xian Wang, Siyuan Wen, Xusheng Chen, Shixiong Zhao, Sen Wang, Li Chen, Xiapu Luo, Fengwei Zhang, Heming Cui
This work leverages the associativity property of inference operators to outsource neural network computation to untrusted GPU and restores the results within TEE at the edge. It also devises an oblivious fingerprint to detect integrity breaches. I did the code implementation and experiments, and wrote the evaluation part.

ENIDrift: A Fast and Adaptive Ensemble System for Network Intrusion Detection under Real-world Drift
ACSAC'22 (with artifact functional badge), links: [paper][code][video][slides]
Xian Wang
The work devises an incremental neural network to extract features of network packets and constructs an adaptive ensemble of ML classifiers to detect anomalies of network packets under real-world drift. It also provides a novel dataset for network intrusion detection. I led the whole work (implementation, experiment, writing, etc.)

Scalable Oblivious Data Analytics Platform in Trusted Execution Environment
Under submission
This work provides efficient and oblivious designs for several data analysis programs in hardware enclave in the cloud. The solution includes several essential algorithms like sort. We improve their scalability by optimizing memory and enabling high-level parallelism. I was responsible for its algorithms, code, and experiments.

PROFESSIONAL EXPERIENCE

The University of California, Santa Cruz — Remote
Research assistant, advisor: Dr. Ioannis Demertzis — Aug. 2023 - Feb. 2024

The University of Hong Kong — Hong Kong S.A.R.
Research assistant — Sep. 2022 - Apr. 2023

Apple — Shanghai, China
Full-time data science intern — Jan. - Jun. 2022

HONORS & AWARDS

- 2023 - 2025 HKUST postgraduate full scholarship
- 2021 National Scholarship (top 1%)
- 2020 Chinese Modern Scientist Memorial Scholarship (top 0.05%)
- 2020 National Scholarship (top 1%)
- 2019 National Scholarship (top 1%)

SKILLS

Language — Fluent in English (TOEFL 103); native Mandarin speaker
Programming & tools — C/C++, Python, Intel SGX, PyTorch, TensorFlow, Linux