Jingtao Li

480-738-3855 • jingtao1@asu.edu • linkedin.com/in/lijingtaoz • github.com/zlijingtao • bit.ly/jingtaoscholar

SUMMARY

Electrical Engineering Ph.D. student specializing in AI security & privacy, CV, federated learning, algorithm development, and software-hardware co-design, seeking full-time research position in related fields, starting August 2023.

EDUCATION

Ph.D. Electrical Engineering — Graduating July 2023
Arizona State University, Tempe, AZ — 4.0 GPA

B.S. Microelectronic Science and Engineering — June 2018
University of Electronic Science and Technology of China, Chengdu, China — 3.9 GPA

TECHNICAL SKILLS

Programming Languages: Python, Java, C/C++, Bash
Frameworks: PyTorch, Tensorflow, TVM, Scikit-Learn
Tools and OS: Docker, AWS, Hadoop, Synopsys, Gem5, Git, SQL, MATLAB, Windows, Linux

PROFESSIONAL EXPERIENCE

Sony AI, Tokyo, JP: Research Intern — May 2022 – Aug 2022
Responsible for conducting research and developing solutions in the field of private-preserving machine learning.

- Built a practical **self-supervised federated learning** system that achieves accurate and budget-friendly cross-device learning performance. Demonstrated on Raspberry Pi with 1,000 clients. Work was presented at FL-NeurIPS' 22.
- Delivered a **multi-task learning** framework for task-shifting to meet a tight memory requirement.

Arizona State University, Tempe, US: Research Assistant — Aug 2018 – Now
Responsible for evaluating the performance of a cutting-edge cache-reconfigurable multi-core processor.

- Developed and optimized workloads including CV workloads such as **Point Cloud**, ML workloads such as **Graph NN**, **ResNet**, and **XGBoost**, and graph algorithms such as **PageRank**, **SSSP**, and **BFS**. We achieve 69x-80x energy efficiency on assigned workloads compared to C++/CUDA implementations.
- Proposed a decision-tree-based cache reconfiguration search engine on accelerating CNN workloads, presented at ISCAS-22, and a point sampling heuristic to accelerate point cloud workloads, which was presented at SIPS-22.

RESEARCH PROJECTS

Privacy & Efficiency of Federated Learning Systems — Aug 2021 – Now
Paper Publication: CVPR-22, SIPS-21, JSPS

- Developed an "adversarial training + transfer learning" framework named ResSFL to improve the privacy of Split **Federated Learning** models. Successfully mitigated the data privacy threat of SFL. On a VGG-11 model, the proposed ResSFL makes model inversion attacks >10 times harder to succeed, with only a <1% drop in model accuracy.
- Designed an "energy + loss-aware" **federated learning** scheduler with 8-bit float quantization to reduce communication and save energy by 43.7%-80.5% for VGG11, ResNet20 on CIFAR-10/100 datasets.

DNN Architecture IP Protection — Nov 2020 – Now
Paper Publication: HOST-21

- Proposed NeurObfuscator, an end-to-end DNN obfuscation framework with obfuscation knobs including layer transformation, **TVM** schedule, and layer fusion permutation, against side-channel attacks targeting architecture IP.
- Optimized obfuscation knobs using Genetics Algorithm and successfully defended a **CTC-LSTM**-based model architecture thief with only 2% time overhead and non-drop accuracy.

Edge AI System Security — Mar 2019 – Oct 2020
Paper Publication: TPAMI, DATE-21, DAC-20, CVPR-20

- Invented the first targeted bit-flip attacks that causes a significant accuracy drop with a few bit-flips on DNN weights.

- Developed RADAR, WRecon, Piece-wise Clustering defensive methods against bit-flip attacks, recovering ImageNet accuracy from <1% to above 69% with a latency overhead of <0.6% in inference shown by **Gem-5**.

Reliability & Efficiency of ReRAM Accelerators Aug 2018 – Feb 2019

Paper Publication: JETCAS, SIPS-19

- Proposed MAX^2, a multi-tile ReRAM accelerator that maximizes data reuse and reduces on-chip bandwidth, improving computation efficiency by 2.5x and energy efficiency by 5.2x compared with a SOTA ReRAM-based accelerator.
- Proposed a hybrid SRAM + ReRAM architecture with novel weight representation to mitigate the severe 9.04% stuck-at-1 faults of ReRAM, showing 88.07% test accuracy (a 1.10% accuracy drop) on a CIFAR-10 dataset.

Successive Approximation Register ADC Design Apr 2016 – June 2018

Paper Publication: TCAS-I, IEEE Access

- Proposed ordering technique and demonstrated 2~3 bits more in the static linearity performances using a segmented architecture with 8~16 groups of elements sorting and optimal selection.
- Presented a statistics-optimized organization technique to achieve better element matching in a 14-bit SAR ADC with a significant improvement of around 23 dB in SFDR compared to the conventional.

PATENTS

- Systems and Methods for a Full-Stack Obfuscation Framework to Mitigate Neural Network Architecture Thief (Under Provisional Application: 63/350,765)
- Method of Arranging Capacitor Array of Successive Approximation Register Analog-to-Digital Converter (Application Granted: US10298254B1)

OTHER PROJECTS

- Job Salary Prediction (JPS-LKM) - 3rd place on the Kaggle leaderboard
- Implemented a Split Federated Learning framework on a microcontroller that has only 256KB SRAM. The demo on keyword spotting shows better accuracy than FedAvg.
- Built an expandable AR framework on Android, RANSAC pose estimation is optimized using OpenCV.
- Extended secure computing CrypTen framework with functionality support for Meanshift Clustering.
- Designed and built a Convolutional & Average Pooling engine in digital circuits, including synthesis, Layout, and post-layout evaluation with the use of Synopsys Design Compiler, Virtuoso Layout, and Primetime.

COURSES

- Secure ML computation • Embedded ML system • Statistical ML • Deep Learning
- Physics-based CV • Mobile System & Architecture • Computer Architecture • VLSI design

AWARDS

- 57th DAC Young Fellows Poster Presentation Award
- Graduate College Travel Award
- Engineering Graduate Fellowship Award
- UESTC Outstanding Undergraduate Student Award

SERVICES

- Peer Journal Reviewer of IEEE TGCN, IEEE TCSVT, IEEE JETCAS
- Conference Reviewer of CVPR (2023), ECCV (2022), CVPR (2022), ISCAS (2022), and GLSVLSI (2020)
- Member of IEEE and SRC