Jingtao Li

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

SUMMARY

Electrical Engineering Ph.D. student specializing in AI Security & Privacy, Computer Vision, Federated Learning, Algorithm Development, and R&D on Low-power Devices, seeking full-time research position 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 developing solutions to harden internal and customer systems against fraudulent intrusion. Role included assessments, risk evaluations, solutions, testing, and implementation.

- Built a practical **unsupervised federated learning** system with a demo on Raspberry Pi, presented at FL-NeurIPS' 22.
- Delivered a **multi-task learning** framework to meet a tight memory requirement.

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" **Pytorch** scheduler with 8-bit float quantization to reduce communication and save energy by 43.7%-80.5% with only a 0.5% sacrifice in accuracy for VGG11, ResNet20 on CIFAR-10/100 datasets.

DNN Architecture IP Protection against Side-Channel Attacks Nov 2020 – Now
Paper Publication: HOST-21

- Proposed NeurObfuscator, an end-to-end DNN obfuscation framework with obfuscation knobs consisting of functional-equivalent layer transformation, **TVM** schedule, and layer fusion permutation.
- Search for the optimal obfuscations using a Genetics Algorithm search engine and successfully fools a **CTC-LSTM**-based model architecture thief with only 2% time overhead and non-drop accuracy.

Hardware-oriented CV and Graph Algorithm Development Aug 2019 – Now
Paper Publication: SIPS-22

- Developed and Optimized **Point Cloud**, **Graph NN**, and **CNN** workloads on a **Gem5**-based 14nm multi-core processor. We exploit cache reconfiguration, asynchronous processing, loop tiling, DVFS, and approximation heuristics and achieve 69-80x energy efficiency on assigned workloads compared to C++/CUDA implementations.

Parameter Security of Edge AI systems 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 as active and passive 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**.

Reliable and Efficient ReRAM AI architecture 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 (SAR) ADC Design Aug 2018 – Feb 2019

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 FL.
- Implemented an expandable AR framework on Android, RANSAC pose estimation is optimized using OpenCV.
- Implemented Secure Multi-party-computation-based Meanshift Clustering based on CrypTen.
- Design of a Convolutional & Average Pooling engine. Synthesize, Automatic Place & Route (APR), and measure the Post-layout Power using Verilog, Synopsys Design Compiler, Virtuoso Layout, and Primetime.

COURSES

- Secure ML computation (A+) • Embedded ML system (A+) • Statistical ML (A) • Deep Learning (A)
- Foundation of Algorithm (A+) • Physics-based Computer Vision (A) • Mobile System & Architecture (A+)
- Computer Architecture (A+) • VLSI design (A) • Digital Systems & Circuits (A+)
- Random Signal Theory (A-) • Probability and Mathematical Statistics (90/100) • Linear Algebra (90/100)

AWARDS

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

SERVICES

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