Jingtao Li

jingtao1@asu.edu
Tempe, Arizona
(480) 738-3855
zlijingtao.github.io

Objective: Research Scientist in AI or Semiconductor Industry
Expertise: AI Security & Privacy, Hardware-oriented Algorithm Development

EDUCATION

Arizona State University, Tempe — *direct P.h.D.* **(Aug. 2018 - Now)**

Major: Electrical Engineering, **Advisor:** Prof. Chaitali Chakrabarti

Expected Graduation: 2023 Summer

GPA:**4.0/4.0**

Research Focus: Improving Security, Privacy and Efficiency of centralized and federated learning AI systems.

UESTC, Chengdu— *B.Eng.* **(Aug. 2014 - June 2018)**

Major: Microelectronic Science and Engineering

GPA: **3.9/4.0** (Outstanding Student Award, 10 recipients annually)

WORK EXPERIENCE

SONY AI, Tokyo— *Research Intern* **(May. 2022 - Aug. 2022)**
Mentors: Lingjuan Lyu, Daisuke Iso

- Built the first practical unsupervised learning system for a massive number of low-end clients. Created a multi-task learning framework and successfully delivered it to Sony's production team.

KAUST, Saudi Arabia—*Research Assistant* **(Aug. 2017 - Jan. 2018)**
Mentors: Xiaohang Li, Haiding Sun

- Designed an AlN/Ga_2O_3-based High-Electron-Mobility Transistor (HEMT) based on polarization property. Actively engaged in developing heterojunctions.

FEATURED RESEARCH PROJECTS

Privacy & Efficiency of Federated AI systems **(Duration: 1.5 years)**

Jingtao Li, et al., "ResSFL: A Resistance Transfer Framework for Defending Model Inversion Attack in Split Federated Learning". (CVPR' 22)
Link to Code: https://github.com/zlijingtao/ResSFL

- Developed a two-step "adversarial training + transfer learning" framework to resolve the privacy issue in Split Federated Learning.
- Successfully mitigated the data privacy threat of SFL. The proposed ResSFL framework makes model inversion attacks **>10** times harder to succeed, with only a **<1%** drop in model accuracy.

Xing Chen, **Jingtao Li**, et al., "Energy and Loss-aware Selective Updating for SplitFed Learning with Energy Harvesting-Powered Devices". (JSP)

- Designed an energy+loss-aware communication reduction scheme that successfully save total energy consumption by **43.7%** to **80.5%** with only a **0.5%** sacrifice in model accuracy.

SKILLS [Bold marks proficient]

Python/C++/Java/HTML

Pytorch/Tensorflow/TVM

Matlab/CUDA/Neon

Git/Docker/AWS/SQL

FEATURED COURSES

Secure ML Computation	A+
Embedded ML system	A
Statistical ML	A
Deep Learning	A
Foundation of Algorithm	A+
Computer Vision	A
Mobile System & Arch.	A+
Computer Architecture	A+
VLSI design	A
Digital Systems & Circuits	A+

PUBLICATIONS [Clickable]

CVPR' 22	**[1st author]**
SIPS' 22	**[1st author]**
JSP	[2nd author]
HOST' 21	**[1st author]**

Security of Centralized AI systems **(Duration: 3 years)**

Jingtao Li, et al., "NeurObfuscator: A Full-stack Obfuscation Tool to Mitigate Neural Architecture Stealing". (HOST' 21)

Link to Code: https://github.com/zlijingtao/Neurobfuscator

- Proposed NeurObfuscator, a full-stack DNN model processing obfuscation framework embedded in the compilation of a DNN model.
- Obfuscated model generates drastically different hardware traces and successfully fools a potential architecture thief by keeping fast execution (**2%** increase in time) and equivalent model functionality.

Jingtao Li, et al., "RADAR: Run-time Adversarial Weight Attack Detection and Accuracy Recovery". (DATE' 21)

- Proposed RADAR, a DNN weight attack detector/rescuer that can restore the accuracy from **<1%** caused by **10** bit-flips to above **69%**.

Jingtao Li, et al., "Defending Bit-flip Attack through DNN Weight Reconstruction". (DAC' 20)

- Designed a DNN weight attack mitigator based on weight reconstruction that helps the DNN model maintain **>60%** accuracy for **5** bit-flips while the baseline accuracy drops to **<1%**.

Jingtao Li, et al., "Improving Reliability of ReRAM-based DNN Implementation through Novel Weight Distribution". (SIPS' 19)

- Designed a ReRAM/SRAM hybrid system utilizing a novel weight distribution to resolve the stuck-at-fault fault in manufacturing - The resulting model accuracy only drops by **1.10%** under **9%** stuck-at-1 fault.

Hardware-oriented Algorithm Development **(Duration: 3 years)**

Link to Project: Poster/ Demo / Paper

- Implemented and Benchmarked Pointnet++, GNN, and other big-data-driven workloads on a reconfigurable multi-core processor. By exploiting cache reconfiguration, synchronize-free coding, DVFS, and approximation heuristics, the resulting GNN achieved **69-80x** better energy efficiency compared to CPU/GPU baselines.
- Proposed an efficient point cloud sampling heuristic that achieves **34-280x** speed up on the FPS kernel with only a **0.0035** drop in the mIoU metric of a part segmentation task. (**Jingtao Li**, et al., SIPS' 22)

PATENTS

- Systems And Methods For A Full-Stack Obfuscation Framework To Mitigate Neural Network Architecture Theft (Under Provisional Application: 63/350,765)
- Method Of Arranging Capacitor Array Of Successive Approximation Register Analog-To-Digital Converter (Application Granted: US10298254B1)

FEATURED SPARE-TIME PROJECTS

- Job Salary Prediction (JPS-LKM) - **3rd** place on Kaggle leaderboard
- Implemented a complete SFL framework on Arduino Nano BLE 33 that has only **256KB** memory, achieving better accuracy than FL baselines.
- Implemented a simple and expandable Augmented Reality framework on mobile devices using Andriod Studio, based on the OpenCV library.
- Implemented a Secure MPC-based Meanshift Clustering algorithm to extend the original CrypTen framework.

SIPS' 21	[2nd author]
TPAMI	[3rd author]
DATE' 21	**[1st author]**
DAC' 20	**[1st author]**
CVPR' 20	[3rd author]
SIPS' 19	**[1st author]**
TCAS-I	[2nd author]
JETCAS	[4th author]
IEEE Access	[2nd author]

AWARDS

57th DAC Young Fellows Poster Presentation Award

Engineering Graduate Fellowship Award

Graduate College Travel Award

SERVICES

Reviewer of

- IEEE TGCN
- IEEE TCSVT
- IEEE JETCAS
- ECCV (2022)
- CVPR (2022)
- ISCAS (2022)
- GLSVLSI (2020)

Member of

- IEEE
- SRC

INTERESTS

🤖Artificial Intelligence

✈️Traveling

🏀Basketballl