

Jingtao Li

Target Job: Research Scientist, Applied Scientist, MLE

Expertise: ML, DL, CV, AI Security & Privacy

jingtao1@asu.edu

Tempe, Arizona

(480) 738-3855

zlijingtao.github.io



EDUCATION

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

Major: Electrical Engineering, Advisor: Prof. [Chaitali Chakrabarti](#)

Expected Graduation: 2023 July to December

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 Federated learning system (**FL-NeurIPS' 22**). Delivered a multi-task learning framework to the production team.

KAUST, Saudi Arabia — *Research Assistant* (Aug. 2017 - Jan. 2018)

Mentors: Xiaohang Li, Haiding Sun

- Designed an $\text{AlN}/\text{Ga}_2\text{O}_3$ -based High-Electron-Mobility Transistor (HEMT) based on polarization property. Actively engaged in developing heterojunctions.

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>

- Built a Pytorch-based inversion attack toolbox, consisting of decoder models with varying architectural complexity to evaluate model privacy.
- 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.

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" 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.

SKILLS [Bold marks proficient]

Python/C++/Java/HTML

Pytorch/Tensorflow/TVM

Matlab/CUDA/SQL

Git/Docker/AWS/Hadoop

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]

FL-NeurIPS' 22 [1st author]

SIPS' 22 [1st author]

JSP [2nd 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/Neurobfusator>

- Simulated architecture thieves by generating an architecture-trace oracle and training a TF-based LSTM predictor with CTC loss (widely used in NLP, OCR).
- Proposed NeurObfuscator, a DNN obfuscation framework with obfuscation knobs consisting of layer transformation, TVM-based optimization, and kernel scheduling, across the model compilation process.
- Using a Genetics-Algorithm-based search engine, the “optimized” obfuscated model generates drastically different hardware traces and successfully fools a potential architecture thief with only 2% time overhead and non-drop accuracy.

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

- Proposed RADAR, an ultra-fast DNN model integration check engine (using addition checksum) for detection & recovery of adversarial weight attacks, that recovered the ResNet-18 ImageNet model accuracy from <1% to above 69%.
- Gem5-based implementation shows a tiny increase of <0.6% in inference time.

Jingtao Li, et al., “Defending Bit-flip Attack through DNN Weight Reconstruction”. (DAC’ 20)

- Designed a Pytorch-based novel weight reconstruction technique to limit any potential weight value change on a DNN model. It helped an 8-bit quantized ResNet-18 ImageNet model maintain >60% accuracy against attacks.

Hardware-oriented Algorithm Development (Duration: 3 years)

Link to Project: [Poster](#) / [Demo](#) / [Paper](#)

- Implemented Pointnet++, GCN, and other CV/graph workloads on a Gem5-based 14nm multi-core processor. By exploiting cache reconfiguration, asynchronous processing, loop tiling, DVFS, and approximation heuristics, the optimized GCN achieved 69-80x energy efficiency compared to C++/CUDA.
- Proposed an efficient point cloud sampling heuristic that achieves a 34-280x speedup on the FPS kernel of a PointNet++ model. (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)

SPARE-TIME PROJECTS

- Job Salary Prediction (JPS-LKM) - 3rd place on Kaggle leaderboard
- Implemented a Split Federated Learning framework on an MCU that has only 256KB memory. The demo on keyword spotting shows better accuracy than FL.
- Implemented a simple and expandable AR framework using Andriod Studio, with its key kernel RANSAC pose estimation accelerated using OpenCV.
- Implemented Secure MPC-based Meanshift Clustering based on CrypTen.
- IC 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 Primitime.

HOST’ 21	[1st author]
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

 Basketball