Jingtao Li

Objective: To embrace cutting-edge AI research & projects

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

EDUCATION

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

Expected Graduation: 2023 Summer

GPA:4.0/4.0

Research Interests: Efficient, secure, and private machine learning systems.

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

Major: Electrical Engineering

GPA: 3.88/4.0 (Outstanding Student Award, 10 recipients annually)
Past Research Experiences: Design of ADC and semiconductor devices.

WORK EXPERIENCE

SONY AI, Tokyo— *Research Intern* **(May. 2022 - Aug. 2022)**

Achievements: Build an efficient privacy-preserving deep learning system

FEATURED PROJECTS

Reliable/Secure/Private DNN Research **(Aug. 2018 - Now)**

- Model extraction attack on split federated learning (Under review)
- Protect split federated learning against inversion attacks. (CVPR' 22)
- Prevent neural architecture stealing of DNN architectures. (Host' 21)
- Reduction of communication overhead of split learning. (SIPS' 21)
- Target version of Bit-flip attack on DNN system (TPAMI)
- Efficient detection & recovery of DNN weight corruption. (DATE' 21)
- DNN training scheme to mitigate fault injection attacks (DAC' 20).
- DNN training scheme to mitigate natural stuck-at-fault (SIPS' 19)

Software Development Research **(Aug. 2019 - Now)**

- Building and Benchmarking big-data-driven applications including Pointnet++, GraphNN on a super-scalar processor.
- Propose efficient point cloud sampling heuristics. (SIPS' 22)
- Exploit cache reconfiguration, synchronize-free transformation, graph partition, and approximate computing heuristics.

OTHER PROJECTS

- Job Salary Prediction (JPS-LKM) - 3rd place on Kaggle leaderboard
- Implement SFL Framework on Arduino Nano Microcontroller
- Simple Expandable Augmented Reality Framework on Mobile Devices
- Secure Meanshift Clustering based on CrypTen

SKILLS

Python/C++/Java/HTML

Pytorch/Tensorflow/TVM

CUDA/Neon Intrinsics

Git/Docker/AWS

COURSES

Embedded ML system	A
Computer Arch.	A+
Secure ML Computation	A+
Mobile System & Arch.	A+
Foundation of Algorithm	A+

PUBLICATIONS

CVPR' 22 [1st author]

SIPS' 22 [1st author]

HOST' 21 [1st author]

SIPS' 21 [2nd author]

TPAMI [3rd author]

DATE' 21 [1st author]

DAC' 20 [1st author]

SIPS' 19 [1st author]

TCAS-I [2nd author]

INTERESTS

🤖Artificial Intelligence

✈️Traveling

🏀Basketball