SUNHO LEE

https://github.com/myshlee417 https://myshlee417.github.io/ myshlee417@gmail.com
KAIST, Daejeon, Republic of Korea (+82)10-3617-1820

RESEARCH INTERESTS

I am interested in the architecture of accelerators dedicated to machine learning.

Since machine learning requires fast and secure processing, my research objective is to design high-performance accelerators with security guarantees. To achieve this goal, my recent studies proposed architectures to support efficient hardware-based protection for accelerators. In these works, I focus on security solutions that leverage characteristics of machine learning.

EDUCATION

KAIST, Daejeon, Republic of Korea *Mar 2021 -*
Doctor of Philosophy, School of Computing
Advisor: Jaehyuk Huh

KAIST, Daejeon, Republic of Korea *Mar 2019 - Feb 2021*
Master of Science, School of Computing
Advisor: Jaehyuk Huh
Thesis: *Hardware Security Techniques for Trusted Machine Learning Accelerators*

Yonsei University, Seoul, Republic of Korea *Mar 2015 - Feb 2019*
Bachelor of Science, Computer Science

PUBLICATIONS

- Seungbeom Choi, **Sunho Lee**, Yeonjae Kim, Jongse Park, Youngjin Kwon, and Jaehyuk Huh, "Serving Heterogeneous Machine Learning Models on Multi-GPU Servers with Spatio-Temporal Sharing", *The 2022 USENIX Annual Technical Conference (**USENIX ATC**)*, July 2022
- **Sunho Lee**, Jungwoo Kim, Seonjin Na, Jongse Park, and Jaehyuk Huh, "TNPU: Supporting Trusted Execution with Tree-less Integrity Protection for Neural Processing Unit", *the 28th IEEE International Symposium on High-Performance Computer Architecture (**HPCA**)*, Feburary 2022
- Seonjin Na, **Sunho Lee**, Yeonjae Kim, Jongse Park, and Jaehyuk Huh, "Common Counters: Compressed Encryption Counters for Secure GPU Memory", *the 27th IEEE International Symposium on High-Performance Computer Architecture (**HPCA**)*, Feburary 2021

PATENTS

- **[Pending]** Jaehyuk Huh, Seungbeom Choi, **Sunho Lee**, Yeonjae Kim, Youngjin Kwon, Jongse Park, "Machine Learning Inference Time-spatial SW Scheduler Based on Multiple GPU", *Korean Patent*
- **[Pending]** Jaehyuk Huh, **Sunho Lee**, and Seonjin Na, "Hardware-based Security Architecture for Trusted Neural Processing Unit", *Korean Patent* (with Samsung Electronics)
- **[Pending]** Jaehyuk Huh, Seonjin Na, **Sunho Lee**, Yeonjae Kim, and Jongse Park, "Efficient Encryption Method and Apparatus for Hardware-based Secure GPU Memory", *Korean Patent* (with Samsung Electronics)

RESEARCH EXPERIENCES

KAIST, Daejeon, Republic of Korea *Mar 2019 -*
Ongoing Researches at CASYS (Computer Architecture and SYStem) Lab
Advisor: Jaehyuk Huh

Accelerator Hardware-based Security

- Memory protection optimization for GPU: Common counters for duplicate counters (Published at **HPCA 2021**)
- Memory protection optimization for multi-tenant GPU
- Trusted execution environment for NPU: Tensor-granularity counters (Published at **HPCA 2022**)

- Memory protection optimization for NPU: Partial memory protection
- Side-channel attack protection for NPU

Accelerator Performance

- Multi-tenancy support for a multi-GPU system: Time and spatial sharing (Accepted at **USENIX ATC 2022**)
- Multi-tenancy support for NPU: Shared resources management

Yonsei University, Seoul, Republic of Korea *Sep 2017 - June 2018*
Undergraduate Research Intern at ELC (Embedded systems Languages and Compilers) Lab
Advisor: Bernd Burgstaller

Parallelism

- Accelerating big-data streaming engine: Multi-thread and shared-memory
- Parallelization of SFA (Simultaneous Deterministic Finite Automata) construction: MPI and Huang's algorithm

RECOGNITION

KAIST, Daejeon, Republic of Korea
Excellent Teaching Assistant Award - CS311 Computer Organization *Spring 2021*

Yonsei University, Seoul, Republic of Korea
Dean's List *Spring 2015, Spring 2018*
Undergraduate Capstone Project Award (Third Place) - Project Leader *Spring 2018*
Title: *Cloud SFA: Parallel Construction of Simultaneous Deterministic Finite Automata in Distributed System*

SKILLS

Programming Languages	C, C++, Python
NPU Simulators	SCALE-Sim, MAESTRO, Gemmini
GPU Programming	CUDA, MPS
Multi-core CPU Programming	MPI, OpenMP
Machine Learning Frameworks	Pytorch, Tensorflow

TEACHING EXPERIENCES

KAIST, Daejeon, Republic of Korea
Teaching Assistant
CS230 System Programming *Fall 2021*
CS311 Computer Organization *Spring 2021, Fall 2019*
CS211 Digital System and Lab *Spring 2019*

KAIST Education Center, Daejeon, Republic of Korea
Mentor & Lecturer
Seocho AI College *Summer 2019, Summer 2021*
Python for Beginners *Summer 2021*