LUCAS HSIUNG

lucas.j.hsiung@gmail.com | 630-862-9852 | linkedin.com/in/lucas-hsiung | github.com/ljhsiun2 | Website ljhsiung.com

WORK EXPERIENCE

Security Verification Engineer
Nuvia/Qualcomm

Aug 2020 – Present | Santa Clara, CA

- Responsible for verifying multiple security blocks on SoC
- Creating testplans, methodologies, and infrastructure to evaluate desired security properties

Security Verification Engineer
SiFive

Jul 2019 – Aug 2020 | San Mateo, CA

- Creating testplans for specific security IP blocks and building models to detect security violations
- Work closely with the design team to ensure products stay up-to-date with current security defenses

Undergraduate Teaching Assistant (ECE411)
University of Illinois

Jan 2019 – May 2019 | Champaign

- Developing material to aid workflow of course such as anti-cheating program.
- Assisting students in learning CPU design material such as office hours, writing problems, etc.

RESEARCH EXPERIENCE

Research Group under Chris Fletcher

Jan 2018 – May 2019

- Assisting in designing hardware features to mitigate security vulnerabilities with low area and performance cost
- Analyzing modern processors for various side-channels e.g. cache attacks

PROJECTS

Data Oblivious ISA Extensions for Side Channel-Resistant and High Performance Computing
J Yu, L Hsiung, M E Hajj, C W Fletcher

Jan 2018 – Aug 2018 | NDSS'19

- Addresses current issues with data-oblivious codes (e.g. constant time cryptography) via minor changes to existing hardware
- Aided in implementation on BOOM and evaluation of performance cost on various benchmarks
- To appear in Micro IEEE Top Picks 2020 Special Edition as well

Cryptology ePrint Archive, Report 2018/808, 2018. http://eprint.iacr.org

Elliptic Curve Cryptography on FPGA

Nov 2017 – Ongoing

- Toy cryptoprocessor using ElGamal's Encryption Scheme
- Optimizations such as Tonelli-Shanks, Barrett's reduction, etc.

OBJECTIVE

To push boundaries of modern computation. Most interested in hardware and cryptography.

EDUCATION

B.S. in Computer Engineering
University of Illinois

Aug 2015 – May 2019 | GPA: 3.36

★ Dean's List (Sp '17, Fa '17)

PROUDEST MOMENTS

Published Paper!
After working with my professor for several months, and learning an incredible amount, my paper will appear in NDSS '19! See "Research Experience/Projects"

2nd in Design Competition
For ECE411 (processor design), my group made a minimal dual-issue processor. It was the first superscalar design the professor had seen in the course.

Co-Founder of SIGARCH
CO-Founder of ACM SIGARCH @ Illinois, a club dedicated to discussing computer architecture. I talk about hardware security.

SKILLS

C/C++ | SystemVerilog | Python | x86 | Kali | Metasploit | gem5

Hardware | Cryptography | Security | Embedded | Firmware

RELEVANT CLASSES

- Applied Cryptography - ECE498AM - A
- Processor Design - ECE411 - A
- FPGA Programming - ECE385 - B+
- Operating Systems Design - ECE391 - A-
- Computer Security - CS461 - A
- Data Structures - CS225 - A