Tyler Sheaves Curriculum Vitae

Email: tsheaves@ucdavis.edu Phone: (415)-279-2195

Research Interests

Reconfigurable, confidential, and trusted computing; Digital IC design and verification; Computer architecture; IP protection through hardware obfuscation; Hardware security.

Education

University California, Davis (September 2020-Present)

- Doctor of Philosophy in Electrical and Computer Engineering

San Francisco State University (September 2012 - May 2020)

- Bachelor of Science in electrical engineering
- Master of Science in embedded electrical and computer systems
  - Transferred to UC Davis before completion during COVID to pursue Ph.D.

Professional Appointments

Graduate Technical Intern (June 2020 – Present)

Intel Corporation

- Implemented a confidential computing framework, allowing for a secure kernel to be offloaded from Intel Xeon CPUs to Intel FPGAs.
- Developed the Remote Console educational application, a TCL/TK interface to allow the Quartus System Console debugging tool to update arbitrary TCL/TK-based GUIs.
- Assisted in dozens of trainings for Quartus simulation/debug tools, intro to Quartus, NIOS II and Qsys/System Buillder.

Graduate Research Assistant (September 2020 – February 2023)

University of California, Davis

- Assisted in research projects spanning FPGA security, HW Trojan detection and threat modeling, IP theft prevention, emerging device applications in HW security, ASIC EDA tool security, and machine learning for HW security.
- Secured grants for NSF CHEST projects (P19_21, P20_21, P20_21, P19_22)

Graduate Teaching Assistant (September 2020 – Present)

University of California, Davis

- EEC170 - Introduction to Computer Architecture Fall 2020, Fall 2022
- EEC172 - Embedded Systems Spring 2021
- EEC289Q – Seminar in Hardware Security Winter 2022
- EEC180 - Digital Systems II Winter 2022, Winter 2023, Spring 2023

Graduate Lecturer (January 2020 – May 2020)
San Francisco State University
- Instructor for a first-year embedded systems course, Introduction to Microcontrollers.

Graduate Teaching Assistant (August 2019 – May 2020)
San Francisco State University
- ENGR378 - Digital Systems Design Fall 2019, Spring 2020

Graduate Research Assistant (January 2017 – May 2020)
San Francisco State University NeCRL Lab
- Nanoelectronics and Computing Research Lab (NeCRL) research assistant.
- Conducted research in digital integrated circuit IP reverse engineering mitigation.
- DARPA sponsored project (DARPA-AFRL #FA8650-15-C-7569) addressing IP-security threats from untrusted foundries.

Research Peer Mentor (Summer 2017 & 2018)
San Francisco State University ASPIRE Summer Program
- Mentored first generation college students transitioning from community colleges to STEM fields at 4-year universities in how to perform experiments, test research hypotheses, and write technical documents.
- Provided mentees with an introduction to theory & applications in engineering and digital design.

Conference Publications (Peer Reviewed)

[1] S. Salehi, **T. Sheaves**, K. I. Gubbi, S. Arash Beheshti, D. Sai Manoj P, S. Rafatirad, A. Sasan, T. Mohsenin and H. Homayoun, "Neuromorphic-Enabled Security for IoT," in *2022 20th IEEE Interregional NEWCAS Conference (NEWCAS)*, 2022.

[2] G. Kolhe, H. M. Kamali, M. Naicker, **T. D. Sheaves**, H. Mahmoodi, P. S. Manoj, H. Homayoun, S. Rafatirad and A. Sasan, "Security and complexity analysis of lut-based obfuscation: From blueprint to reality," in *2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2019.

[3] G. Kolhe, S. Salehi, **T. D. Sheaves**, H. Homayoun, S. Rafatirad, M. P. D. Sai and A. Sasan, "Securing Hardware via Dynamic Obfuscation Utilizing Reconfigurable Interconnect and Logic Blocks," in *2021 58th ACM/IEEE Design Automation Conference (DAC)*, 2021.

[4] G. Kolhe, **T. Sheaves**, K. I. Gubbi, S. Salehi, S. Rafatirad, P. D. Sai Manoj, A. Sasan and H. Homayoun, "LOCK&ROLL: Deep-Learning Power Side-Channel Attack Mitigation Using Emerging Reconfigurable Devices and Logic Locking," in *Proceedings of the 59th ACM/IEEE Design Automation Conference*, New York, NY, USA, 2022.

[5] K. I. Gubbi, S. A. Beheshti-Shirazi, **T. Sheaves**, S. Salehi, P. D. Sai Manoj, S. Rafatirad, A. Sasan and H. Homayoun, "Survey of Machine Learning for Electronic Design Automation," in *Proceedings of the Great Lakes Symposium on VLSI 2022*, New York, NY, USA, 2022.

[6] K. I. Gubbi, B. S. Latibari, A. Srikanth, **T. Sheaves**, S. A. Beheshti-Shirazi, S. M. Pd, S. Rafatirad, A. Sasan, H. Homayoun and S. Salehi, "Hardware Trojan Detection Using Machine Learning: A Tutorial," *ACM Trans. Embed. Comput. Syst.,* January 2023.

[7] A. Attaran, **T. D. Sheaves**, P. K. Mugula and H. Mahmoodi, "Static Design of Spin Transfer Torques Magnetic Look Up Tables for ASIC Designs," in *Proceedings of the 2018 on Great Lakes Symposium on VLSI*, New York, NY, USA, 2018.

Journal Publications (Peer Reviewed)

[1] G. Kolhe, **T. D. Sheaves**, D. Sai Manoj P., H. Mahmoodi, S. Rafatirad, A. Sasan and H. Homayoun, "Breaking the Design and Security Trade-off of Look-up-Table–Based Obfuscation," *ACM Trans. Des. Autom. Electron. Syst.,* vol. 27, June 2022.

Conference Presentations

[1] "Silicon Validation of LUT-based Logic-Locked IP Cores", Design Automation Conference, Session: Keep moving up and looking sideways with verification boosters! San Francisco, CA, 2022.

Recent Course Projects

CUDA Accelerated AES CPA

Modern Parallel Computing - EEC 289Q UC Davis

- Performed AES CPA attack on the open-source AES-HD dataset.
- Using CUDA, key recovery performance improved 150x

Cyclone V FPGA Time-to-digital Converter

Design & Optimization of Embedded Computing Systems - EEC 284 UC Davis

- Implemented a power side-channel sensitive time-to-digital converter on an Intel Cyclone V FPGA. The sensor was able to fingerprint power wasting circuit switching activity and show characteristic power traces of several IPs.

Detecting Behavior-sensitive Cross-site 3rd-party Web Trackers

Topics in Network Security and Privacy – ECS 289M

- Used the OpenWPM web privacy measurement framework to crawl 1000 top-sites and identify which 3rd-party trackers log user mouse movements such as hovering.
- Instrumented JavaScript API calls and used Selenium to drive stimulus to the browser windows during the crawl.
- Classified 3rd-party trackers from cookie data to determine cross-site tracking capabilities.