Tyler Sheaves

tsheaves@ucsc.edu | (415) 279-2195

Research Interests

Temporal and spatial side-channels; confidential computing; digital IC design and verification; computer architecture; logic locking; hardware Trojan attacks and mitigations.

Education

University of California, Santa Cruz
Ph.D. in Computer Science and Engineering. — In Progress

University of California, Davis
Ph.D. in Electrical and Computer Engineering. — Transfer

San Francisco State University
B.S. in Electrical Engineering. — January 2017

Academic Appointments and Internships

Graduate Research Assistant, UC Santa Cruz — Jan 2025 – Present

- ◇ Semiconductor wear-out side-channels.

Graduate Teaching Assistant, UC Santa Cruz — Jan 2025 – Mar 2025

- ◇ *Logic Design.*

Graduate Research Assistant, UC Davis — Sep 2020 – Feb 2023

- ◇ Power side-channels, logic locking and HW Trojan attacks.
- ◇ NSF CHEST projects P19-21, P20-21, P19-22.

Graduate Teaching Assistant, UC Davis — Sep 2020 – Jun 2023

- ◇ *Introduction to Computer Architecture*, *Embedded Systems*, *Digital Systems II*, *Seminar in Hardware Security.*

Graduate Technical Intern, Intel Corporation — Jun 2020 – Jun 2023

- ◇ Implemented confidential computing IP.
- ◇ Developed remote FPGA educational tools.

Graduate Lecturer, San Francisco State University — Jan 2020 – May 2020

- ◇ *Introduction to Microcontrollers.*

Graduate Teaching Assistant, San Francisco State University — Aug 2019 – May 2020

- ◇ *Digital Systems Design*

Graduate Research Assistant, SFSU NeCRL Lab — Jan 2017 – May 2020

- ◇ Addressed IP-security threats from untrusted foundries.
- ◇ DARPA-AFRL Grant no. FA8650.

Research Peer Mentor, SFSU ASPIRES — Summer 2017 & 2018

Publications

- C. Drewes, **T. Sheaves**, O. Weng, K. Ryan, B. Hunter, C. McCarty, R. Kastner, and D. Richmond, "Turn on, tune in, listen up: Maximizing side-channel recovery in cross-platform time-to-digital converters," *ACM Transactions on Reconfigurable Technology and Systems*, 2024. DOI: 10.1145/3666092.

- C. Fang, N. Miao, H. Wang, J. Zhou, **T. Sheaves**, J. M. Emmert, A. Sasan, and H. Homayoun, "Gotcha! i know what you are doing on the fpga cloud: Fingerprinting co-located cloud fpga accelerators via measuring communication links," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, 2023, pp. 2024–2037. DOI: 10.1145/3576915.3616606.

- 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 Transactions on Embedded Computing Systems*, 2023. DOI: 10.1145/3579823.

- K. I. Gubbi, S. A. Beheshti-Shirazi, **T. Sheaves**, S. Salehi, P. D. S. Manoj, S. Rafatirad, A. Sasan, and H. Homayoun, "Survey of machine learning for electronic design automation," in *Great Lakes Symposium on VLSI*, 2022. DOI: 10.1145/3526241.3530834.

- G. Kolhe, **T. Sheaves**, K. I. Gubbi, S. Salehi, S. Rafatirad, P. D. S. Manoj, A. Sasan, and H. Homayoun, "Lock&roll: Deep-learning power side-channel attack mitigation using emerging reconfigurable devices and logic locking," in *59th ACM/IEEE Design Automation Conference*, 2022. DOI: 10.1145/3489517.3530414.

- G. Kolhe, **T. Sheaves**, D. S. M. P., H. Mahmoodi, S. Rafatirad, A. Sasan, and H. Homayoun, "Breaking the design and security trade-off of look-up-table–based obfuscation," *ACM Transactions on Design Automation of Electronic Systems*, vol. 27, 2022. DOI: 10.1145/3510421.

- S. Salehi, **T. Sheaves**, K. I. Gubbi, S. A. Beheshti, D. S. M. P., S. Rafatirad, A. Sasan, T. Mohsenin, and H. Homayoun, "Neuromorphic-enabled security for iot," in *20th IEEE Interregional NEWCAS Conference*, 2022. DOI: 10.1109/NEWCAS52662.2022.9842256.

- 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 *58th ACM/IEEE Design Automation Conference*, 2021. DOI: 10.1109/DAC18074.2021.9586242.

- 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 *IEEE/ACM International Conference on Computer-Aided Design*, 2019. DOI: 10.1109/ICCAD45719.2019.8942100.

- 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 *Great Lakes Symposium on VLSI*, 2018. DOI: 10.1145/3194554.3194651.

Chairing and Presentations

- ◇ Session Moderator, WOSET 2024
- ◇ Tutorial & Workshop Co-chair, ISFPGA, Feb 2023
- ◇ Speaker, DAC 2022 — *Silicon Validation of LUT-based Logic-Locked IP Cores*
- ◇ Speaker, Intel Federal Summit, Washington, DC, Jun 2022

Selected Course Projects

CUDA Accelerated AES CPA
Accelerated CPA attack on AES-HD using CUDA; achieved 150x performance improvement.

Time-to-Digital Converter on Cyclone V FPGA
TDC implementation for power side-channels on embedded FPGAs.

Cross-Site Tracker Detection
Web privacy audit using OpenWPM to identify trackers that log user behavior.