Armaiti Ardeshiricham

☎ +858 281 3776 • ✉ aardeshi@eng.ucsd.edu • armitttt.github.io

Education

Ph.D. Computer Engineering – Hardware Security

Dep. of Computer Science and Engineering, University of California San Diego. Fall 2014 – Fall 2019

Advisors: Prof. Ryan Kastner & Prof. Sicun Gao

M.Sc. Computer Engineering – Embedded Systems

Dep. of Computer Science and Engineering, University of California San Diego. Jun. 2017

GPA: 3.9/4

B.Sc. Electrical Engineering – Digital Systems

Dep. of Electrical Engineering, Sharif University of Technology, Tehran, Iran. Jun. 2014

GPA: 3.7/4

Skills

- **Programming Languages:** Python, C++, Verilog, SVA, Java, X86 Assembly.
- **Tools:** Vivado, Vivado HLS, Modelsim, Yosys, Quetsa Formal, Design Compiler.
- **Other Skills:** Linux, FPGA Design Flow, Latex, Theorem Proving.

Interesets

- Hardware Security – Security Verification, Side Channel Attacks, Security Architectures.
- Formal Methods – Verification, Theorem Proving, Program Synthesis and Repair.

Work Experience

- Security Architecture Intern at Apple Inc., Summer 2018.
- Graduate Research Assistant at UCSD, Fall 2014-present.

Research Projects

- **Information Flow Tracking for Hardware Designs:**
  - Writing Python tool to instrument RTL Verilog code with Information Flow Tracking logic
  - Proving security properties of instrumented RTL Verilog designs using EDA and SMT solvers
- **Program Synthesis for Hardware Security:**
  - Developing property-based program synthesis flow in Python
  - Accelerating design and verification of Verilog code using automatic code generation and SVA
  - Extending Verilog syntax to enable program sketching
- **Error Localization in Hardware Designs:**
  - Developing an automated framework to identify buggy source code statements in Verilog RTL
  - Using formal methods to reason about verification failures
- **Constant Time Architectures:**
  - Formally verifying RISC-V processors using IFT tools
  - Applying micro-architectural modifications to satisfy timing constraints

Publications

VeriSketch: Synthesizing Secure Hardware Designs with Timing-Sensitive Information Flow Properties, A. Ardeshiricham, Y. Takashima, S. Gao, and R. Kastner. (CCS'19)
Property Specific Information Flow Analysis for Hardware Security Verification, W. Hu, A. Ardeshiricham, M. Gobulukoglu, X. Wang, and R. Kastner. (ICCAD'18)
Clepsydra: Modeling Timing Flows in Hardware Designs, A. Ardeshiricham, W. Hu, and R. Kastner. (ICCAD'17)
Register Transfer Level Information Flow Tracking for Provably Secure Hardware Design, A. Ardeshiricham, W. Hu, J. Marxen, and R. Kastner. (DATE'17)
Why You Should Care About Don't Cares: Exploiting Internal Don't Care Conditions for Hardware Trojans, W. Hu, L. Zhang, A. Ardeshiricham, J. Blackstone, B. Hou, Y. Tai and R. Kastner. (ICCAD'17)
Identifying and Measuring Security Critical Path for Uncovering Circuit Vulnerabilities, W. Hu, A. Ardeshiricahm, R. kastner. (MTV'17)
Examining the Consequences of High-Level Synthesis Optimizations on the Power Side Channel, L. Zhang, W. Hu, A. Ardeshiricham, Y. Tai, J. Blackstone, D. Mu, and R. Kastner. (DATE'18)
Imprecise Security: Quality and Complexity Tradeoffs for Hardware Information Flow Tracking, W. Hu, A. Becker, A. Ardeshiri, Y. Tai, P. Ienne, D. Mu, and R. Kastner. (ICCAD'16)
Towards Property Driven Hardware Security, W. Hu, A. Althoff, A. Ardeshiricham, and R. Kastner. (MTV'16)

Teaching Assistantship

- FPGA High-Level Synthesis - UCSD
- Components and Design Techniques for Digital Systems - UCSD
- Intro to Computer Architecture - Sharif University
- Microprocessor System Lab. - Sharif University
- Embedded System Lab. - Sharif University

Recent Coursework–UCSD

- Operating Systems
  - Profiled Android Operating System using Java
  - Implemented Nachos OS - Multiprogramming, Multithreading, and Memory Management.
- FPGA High-Level Synthesis
  - Implemented and accelerated RSA/FIR/DFT/FFT modules using Vivado HLS
- Computer Architecture, Synthesis Methods in CAD/VLSI, Probabilistic Reasoning and Learning, Algorithm Design and Analysis