# Armaiti Ardeshiricham

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

## Education

**University of California San Diego**
*PhD Student in Computer Science and Engineering with Prof. Ryan Kastner* *Fall 2014 – now*
Masters degree in Computer Engineering (GPA:3.9)

**Sharif University of Technology, Tehran, Iran**
*Bachelor's degree in Electrical Engineering, Majoring in Digital Systems* *2009 – 2014*

## Research Projects

- **Information Flow Tracking for Hardware Designs:**
  - Developing a precise and flexible IFT tool at the RTL level
  - Tracking functional and timing flows in isolated channels
  - Formally proving security properties on hardware units
- **Program Synthesis for Hardware Security:**
  - Developing a property-based synthesis flow to accelerate hardware design and verification
  - Incorporating the IFT model to generate secure-by-construction hardware designs
- **Constant Time Architectures:**
  - Using precise IFT tools to analyze timing behavior of processors at the granularity of instructions
  - Providing formal guarantees that a piece of software runs in constant time

## Publications

**Counterexample-Based Design Synthesis for Hardware Security**, A. Ardeshiricham, S. Gao, R. Kastner. (Submitted to DAC'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)

## Skills

- **Programming Languages:** Python, C++, Verilog, X86 Assembly, Matlab, Haskell.
- **Software Tools:** Vivado HLS, Vivado, Modelsim, Quartus, Yosys, Quetsa Formal Tool.
- **Others:** Linux, FPGA Design Flow, Latex.

## 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

- Computer Architecture
- FPGA High Synthesis
- Synthesis Methods in CAD/VLSI
- Operating Systems
- Compiler Design
- Probabilistic Reasoning and Learning
- Algorithm Design and Analysis
- Automated Reasoning in AI (Audited)
- Program Synthesis (Audited)