Rohith Prakash

114 E31st St. #201, Austin, TX 78705
rohith.prakash@utexas.edu
+1 (972) 352-0082
https://github.com/rnprakash

Research Interests

Security & Privacy	Differential privacy; contention and covert side channels; inference attacks; machine learning; OS and systems level defenses
Computer Arch.	Memory and cache systems; hardware modifications for private queues
Current Research	Resource-agnostic side channel defense: apply differential privacy to generative models of program execution to obfuscate payloads

Education

Current Masters + PhD in Computer Engineering, **University of Texas**, Austin
Research Topics: Secure memory controllers, machine learning and privacy algorithms for time series data, optimization algorithms.
Advisor: Prof. Mohit Tiwari GPA: 3.7

May 2014 Bachelor of Science in Computer Engineering, **University of Texas**, Austin
Topic: Computer Architecture GPA: 3.7
Senior Project: "TEx86: A FAST Simulator for Processor Design Architects"
Advisor: Prof. Derek Chiou

May 2014 Bachelor of Science in Mathematics, **University of Texas**, Austin
Topic: Pure Mathematics GPA: 3.5

Research and Publications

WASP-SC Workload-Agnostic Statistical Privacy for Side Channels. Created a novel hardware design for thwarting side channels on shared architectural resources with a configurable level of privacy. Protects against against an adversary observing hardware resource contention such as third party cloud providers. The scheme works by building models of program behavior and applying statistical noise to obfuscate the perceived contention for these hardware resources.

Work Experience

Jan 2015–*Current* Graduate Research Assistant
UT Austin

Optimization of attacker models for side-channel attacks using machine learning and optimization techniques. Use transforms and predictive models along with dimensionality reduction to demonstrate potential information leakage.

Design of memory controller for obfuscation of memory traces using differential privacy. Model memory patterns of program workloads and obfuscate the resulting memory traces with the Laplacian differential privacy method.

Thwarting queue contention channels with differential privacy. Creation of a generic queue architectural structure which can be tuned to give variable privacy guarantees with speed trade-offs.

Reduction of network side channel leakage over SSL/TLS connections by modifying hardware encryption module for network I/O. Apply differential privacy in hardware to models created from common network traffic, reducing adversaries' abilities to glean private information.

May 2015–Aug 2015 | **Security Research Intern**
Altera Corp

Researched, tested, and analyzed various hardware and algorithmic implementations for physical-unclonable functions (PUFs).

Given actual SRAM cells for use in prototype PUFs, analyzed temperature, current, and other data to create algorithms for determining PUF reliability, resilience, enrollment procedures, and bit selection.

Aug 2014–Dec 2014 | **Graduate Teaching Assistant**
UT Austin

Teaching assistant for sophomore undergraduate C/C++ class (EE 312: Software Design and Implementation I).

Basic problem solving, design and implementation techniques for imperative programming; structured programming in the C/C++ language; programming idioms; introduction to software design principles, including modularity, coupling and cohesion; introduction to software engineering tools; elementary data structures; asymptotic analysis.

Jun 2014–May 2015 | **Graduate Technical Intern**
Intel Corp

Tested, verified, and debugged camera unit memory interface systems. Compiled models, ran regressions, and debugged synthesized Verilog for Intel Atom processors.

Feb 2014–Aug 2014 | **Tutor Level II**
Tutor.com

Tutored high-school and college-level students in Geometry, Algebra, Calculus I, II, III, Discrete Math, Computer Science, and Linear Algebra. Helped students complete homework, study for tests, and learn concepts through the online Tutor.com classroom application via a virtual whiteboard with text and voice features.

Feb 2012–Aug 2013 | **Undergraduate Technical Intern**
Intel Corp

Worked on gate-level simulation (GLS) for the Intel Atom processor. Compiled models, ran regressions, and debugged synthesized Verilog. Created and maintained validation automation tool (written in C, Perl and Tcl/Tk) which allowed validation engineers to automatically build and fix common build errors quickly.

Computer Skills

Proficient Languages: C/C++, x86 ISA, Julia, Python, ARM ISA, Java, and more
Operating Systems: Linux/Unix/Unix-based, Windows

Scholarships and Awards

2014–Current Graduate Research and Tuition Grant
aug 2010–2014 Engineering Undergraduate Honors
2012, 2014, 2015 Intel Individual Contributor Award
2015 UTexas Hackathon - Dell Innovation Award

Other

Languages: English, French
Citizenship: US Citizen