USC Viterbi School of Engineering
Ming Hsieh Department of Electrical Engineering

Seminar Announcement

Trustworthy Integrated Circuit Design

Jeyavijayan (JV) Rajendran
New York University

Thursday April 2, 2015
10:00 am
EEB 248

Abstract: Designers use third-party intellectual property (IP) cores and outsource various steps in their integrated circuit (IC) design and manufacturing flow. As a result, security vulnerabilities have been emerging, forcing IC designers and end users to reevaluate their trust in ICs. If an attacker gets hold of an unprotected IC, attacks such as reverse engineering the IC and piracy are possible. Similarly, if an attacker gets hold of an unprotected design, insertion of malicious circuits in the design, and IP piracy are possible. To thwart these and similar attacks, we have developed three defenses: IC camouflaging, logic encryption, and split manufacturing. IC camouflaging modifies the layout of certain gates in the IC to deceive attackers into obtaining an incorrect netlist, thereby, preventing reverse engineering by a malicious user. Logic encryption implements a built-in locking mechanism on ICs to prevent reverse engineering and IP piracy by a malicious foundry and user. Split manufacturing splits the layout and manufactures different metal layers in two separate foundries to prevent reverse engineering and piracy by a malicious foundry. We then describe how these techniques are enhanced by using existing IC testing principles, thereby leading to trustworthy ICs.

Biography: Jeyavijayan (JV) Rajendran is a PhD Candidate in the Electrical and Computer Engineering Department at New York University. His research interests include hardware security and emerging technologies.

He has won three Student Paper Awards (ACM CCS 2013, IEEE DFTS 2013, IEEE VLSI Design 2012); four ACM Student Research Competition Awards (DAC 2012, ICCAD 2013, DAC 2014, and the Grand Finals 2013); Service Recognition Award from Intel; Third place at Kaspersky American Cup, 2011; and Myron M. Rosenthal Award for Best Academic Performance in M.S. from NYU, 2011.

He organizes the annual Embedded Security Challenge, a red-team/blue-team hardware security competition. He is a student member of IEEE and ACM.

Website: wp.nyu.edu/jv

Host: Peter Beerel, pabeerel@usc.edu, EEB 350, x04481