UCF Stands For Opportunity

THE DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE, ECE DIVISION

Presents the Spring 2012 EECS Seminar Series

Yier Jin

Yale University

"Trusted Integrated Circuits: Challenges & Opportunities Ahead"

Tuesday, March 13, 2012 1:30 p.m. HEC 450

Abstract

The problem of maliciously intended modifications in hardware intellectual property (IP) and manufactured integrated circuits (ICs), commonly known as hardware Trojans, has recently garnered interest not only in academia but also in governmental agencies and industry. Partly because of design outsourcing and migration of fabrication to low-cost areas across the globe, and partly because of increased reliance on third-party intellectual property and design automation software, the integrated circuit supply chain is now considered far more vulnerable to malicious modifications than ever before. Such modifications, known as hardware Trojans, provide additional functionality that is unknown to the designer and user, but which can be exploited by the perpetrator after deployment to sabotage or incapacitate a chip, or to steal sensitive information.

This presentation outlines the challenges and elucidates the research opportunities associated with certifying trustworthiness of integrated circuits. Three solutions developed by the presenter for various instances of the problem will be discussed. These include i) the use of side-channel information along with statistical analysis methods to detect hardware Trojans in wireless cryptographic circuits, ii) the use of on-chip neural networks for post-deployment trust monitoring, and iii) a novel third-party hardware intellectual property acquisition and delivery protocol facilitating IP core trustworthiness evaluation based on proof-carrying code (PCC) concepts.

Biography

Yier Jin received the B.S. and M.S. degrees in Electrical Engineering from Zhejiang University, China, in 2005 and 2007, respectively. He is currently a 5th year doctoral candidate in the Department of Electrical Engineering at Yale University. His doctoral research pioneered several novel directions in the field of trusted integrated circuits (ICs) and hardware intellectual property (IP) cores, which have been extensively acknowledged and referenced by the newly emerging scientific community in the area of trusted hardware. These include the first hardware Trojan detection methodology relying on local side-channel information, the first post-deployment hardware trust assessment framework, and the first proof-carrying hardware IP protection scheme. Besides his research in secure, trusted, and reliable ICs, he is also interested in cyber physical security and, more particularly, in trusted cloud computing platforms.

DEPARTMENT OF ELECTRICAL ENGINEERING & COMPUTER SCIENCE