UCF DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCEINCE

Fall 2014 Seminar Series

Presented by the ECE Division

HARDWARE PRIMITIVES FOR TRUSTED AND SECURE SYSTEMS

FRIDAY NOVEMBER 21, 2014

11:00 AM – HEC 101

In this talk, Dr. Plusquellic will describe several on-chip and PCB-level security and trust primitives (STPs) that are designed to serve multiple security-related roles including encryption, IC metering (as a countermeasure to over-building) and as side-channel attack detectors, and multiple trust-related roles including authentication, hardware Trojan detection (for the detection of malicious modifications to lay-outs) and as aging monitors (to combat component 'reuse' in the supply chain). The STPs that they propose are designed to measure basic circuit parameters related to power and delay. Key to the success of using these parameters in security and trust functions is measuring them across the 3-D structure of ICs and PCBs at high resolutions.

JIM PLUSQUELLIC

University of New Mexico

Professor Plusquellic received both his Ph.D. degree in Computer Science from the University of Pittsburgh in 1997. He is currently a Professor in Electrical and Computer Engineering at the University of New Mexico. His research interests are in the area of nano-scale VLSI and include security and trust in IC hardware, silicon validation, design for manufacturability and delay test methods. Dr. Plusquellic received an "Outstanding Contribution Award" from IEEE Computer Society in 2012 for co-founding and for his contributions to the Symposium on Hardware-Oriented Security and Trust (HOST). He served as General Chair for HOST in 2010 and is currently serving as Associate Editor for Transactions on Computers. He received the "10 Years of Continuous Service Award" from the International Test Conference, a Best Paper Award from VTS, an ACM Distinguished Service Award from SIGDA and two Austin CAS Fellow Awards from IBM. He recently received a "2014 Innovation Award" from the Science and Technology Center at the University of New Mexico, is a "Featured Entrepreneur" within the School of Engineering and has 3 patents and several provisional applications filed with the U.S. Patent and Trademark Office. He has published more than 70 refereed conference and journal papers.

Hosted by: Dr. Jiann-Shiun Yuan