UCF DEPARTMENT OF COMPUTER SCIENCE

Spring 2017 Speaker Series

RECORD: TEMPORARILY RANDOMIZED ENCODING OF COMBINATIONAL LOGIC FOR RESISTANCE TO DATA LEAKAGE FROM HARDWARE TROJANS

Wednesday January 11, 2017 • 2:00 PM – HEC 450

Many design companies have gone fabless and rely on external fabrication facilities to produce chips due to increasing cost of semiconductor manufacturing. However, not all of these facilities can be considered trustworthy; some may inject hardware Trojans and jeopardize the security of the system. One common objective of hardware Trojans is to a establish side channel for data leakage. While extensive literature exists on various defensive measures, almost all of them focus on preventing the establishment of side channels, and can be compromised if attackers gain access to the physical chip and can perform reverse engineering between multiple fabrication runs. This talk discusses RECORD: Temporarily Randomized Encoding of COmbinational Logic for Resistance to Data Leakage. RECORD a novel scheme of temporarily randomized encoding for combinational logic that, with the aid of Quilt Packaging, aims to prevent attackers from interpreting the data.

Kevin A. Kwiat

U.S. Air Force Research Laboratory (AFRL)

Kevin A. Kwiat is a Principal Computer Engineer with the U.S. Air Force Research Laboratory (AFRL) in Rome, New York where he has worked for over 33 years. Currently he is assigned to the Cyber Assurance Branch. He received the BS in Computer Science and the BA in Mathematics from Utica College of Syracuse University, and the MS in Computer Engineering and the Ph.D. in Computer Engineering from Syracuse University. He holds 4 patents. In addition to his duties with the Air Force, he is an adjunct professor of Computer Science at the State University of New York Polytechnic Institute, an adjunct instructor of Computer Engineering at Syracuse University, and a Research Associate Professor with the University at Buffalo. He is an advisor for the National Research Council. He has been by recognized by the AFRL Information Directorate with awards for best paper, excellence in technology teaming, and for outstanding individual basic research. His main research interest is dependable computer design.

Hosted by: Dr. Mainak Chatterjee