UCONN
COLLEGE OF ENGINEERING
ELECTRICAL & COMPUTER ENGINEERING

ECE Fall 2024 Colloquium Series

Friday, October 11, 2024
11:15 am ITE 336
(Refreshments in ITE 301 at 11 am)

Root-cause Analysis of Power-Based Side-channel Leakage

Prof. Patrick Schaumont

Abstract:

Power-based side-channel leakage is a well-known vulnerability in secure system operations. A wide array of countermeasure techniques is available to designers of secure hardware and software. Surprisingly, no generally accepted design verification for power-based side-channel leakage exists today. This leads to expensive build-and-test design cycles in practice.

I will review recent efforts by my group and others in root-cause analysis for side-channel leakage. This is a verification technique to pinpoint the source of side-channel leakage. There are two major challenges for this subfield in secure design, and neither is fully solved today. First, there is an abundant set of different types of side-channel leakage. These exist at different levels of abstraction and at different granularities of modeling detail. Complete verification is therefore exceedingly hard. Second, some types of side-channel leakage do not yet have an efficient modeling technique. I will conclude with a list of open research challenges.

Bio:

Patrick Schaumont is a Dean's Excellence Professor and Joseph Samuel Satin Distinguished Fellow in Electrical and Computer Engineering at WPI. Prior to this, he was a staff researcher at IMEC, Belgium, and a faculty member at Virginia Tech. He has also been a visiting researcher at the National Institute of Information and Communications Technology (NICT) in Japan, as well as Laboratoire d'Informatique de Paris 6 in France. Additionally, he served as a Radboud Excellence Initiative Visiting Faculty member at Radboud University, Netherlands. His research interests focus on the design and methodologies of secure, efficient, and real-time embedded computing systems. Schaumont has co-chaired several prominent conferences in cryptographic and secure engineering, including CHES, HOST, ASHES, and FDTC. Currently, he serves as the Associate Editor-in-Chief for the IEEE Transactions on Emerging Topics in Computing. In 2007, he received the National Science Foundation CAREER Award.

https://www.wpi.edu/people/faculty/pschaumont