Challenges for the Logic Design of Secure Embedded Systems

Speaker: ***Dr. Patrick Schaumont*** **–** University of California, Los Angeles

Abstract: Networked embedded systems have become pervasive in our society. Their reliable and trustworthy operation thus is essential, and it should come as no surprise that security has been acknowledged as a new dimension in modern embedded systems design, next to traditional factors such as cost, area, and power.

The implementation of such a secure embedded system is non-trivial because security attacks can be mounted at multiple abstraction levels. We will discuss our design experience in the ThumbPod-2 project, a secure embedded fingerprint authentication system. The defenses designed in ThumbPod-2 include a sound security partitioning over the entire design trajectory, in combination with a side-channel leakage free logic design style at the lowest level.

Based on this experience, we can formulate several challenges for logic design of future secure embedded systems. These challenges are located at the system-level, at the logic-level, and the circuit-level. We cannot claim full solutions exist for all of them today, but we hope they will provide research stimuli to the logic synthesis community.

Speaker Bio: Patrick Schaumont is a postdoctoral researcher at UCLA's Embedded Security group. He received the PhD degree in Electrical Engineering from UCLA (2004), and the MS degree in Computer Science from Rijksuniversiteit Ghent, Belgium (1990). Before joining UCLA in 2001, he was a researcher at IMEC, Belgium from 1992. His research focuses on design methods and architectures for embedded systems, and he works in close cooperation with designers to demonstrate new methodologies on practical applications. He has co-authored over 60 conference and journal publications, and holds 3 US patents. He has also served as a TPC member for DATE, ICCAD, and HLDVT.