University of Rochester
Department of Electrical and Computer Engineering Colloquia Series

Secure and Efficient Design Techniques for Modern Integrated Systems

Selçuk Köse
Department of Electrical Engineering
University of South Florida

Wednesday, March 14th
12:00PM – 1:00PM
1400 Wegmans Hall

Abstract
The continuous quest to simultaneously achieve high power efficiency and high level of security has become a significantly challenging design objective in modern integrated systems. While various techniques have been proposed to increase the power efficiency at a given operating point, these techniques typically offer low power efficiency at light-load. Additionally, although software-based isolation mechanisms can rarely prevent information leakage to malicious hardware-based attacks, the amount of research to tackle malicious attacks at the hardware level has been limited. Side-channel analysis – one of the primary hardware attacks – utilizes certain physical properties of computing devices such as power, temperature, sound, light, timing, and electromagnetic emanations to obtain critical information. The emergence of Internet of Things (IoT) devices, datacenters, and cloud computing has exacerbated the stringent design requirements to achieve security against side-channel attacks without a significant degradation in power efficiency, performance, and cost. Leveraging existing hardware compoiiiidJ -23 -1.16dst.e efntawo c18 1818e I 310.1(14)3(de(I)16.3( )0.5(r373241I)10.5(18(ge(I)
side-