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 components as a countermeasure to enhance security is proposed as an effective way to minimize these potential overheads. I will present our recent research on a new on-chip power delivery architecture that provides high power efficiency under a wide range of workload conditions and explain how to utilize voltage regulator components as a countermeasure against various side-channel attacks.
First, a recently proposed on-chip power delivery architecture, converter-gating, will be discussed. In this technique, individual voltage converter stages are adaptively turned on and turned off based on the workload information to concurrently achieve high power efficiency, low voltage noise, and reduced thermal gradient. Then, a brief overview of side-channel attacks and our motivation to utilize voltage regulators as a countermeasure will be discussed. A design methodology for security-aware voltage regulation against various power analysis attacks will be explored. The security enhancement and related overheads in performance, area, and power consumption of the proposed technique will be compared with other state-of-the-art countermeasures. Finally, future research directions will be offered.

Bio
Selçuk Köse received the B.S. degree in electrical and electronics engineering from Bilkent University, Ankara, Turkey, in 2006, and the M.S. and Ph.D. degrees in electrical engineering from the University of Rochester, Rochester, NY, in 2008 and 2012, respectively. He previously worked at Intel Corporation, Eastman Kodak, and NXP Semiconductors (previously Freescale Semiconductor). He is currently an Assistant Professor with the Department of Electrical Engineering, University of South Florida, Tampa, FL. His current research interests include hardware security, on-chip power delivery and management, 3-D integration, and sustainable computing. Dr. Köse is a recipient of NSF CAREER Award, multiple Cisco Research Awards, USF College of Engineering Outstanding Junior Researcher Award, USF Outstanding Faculty Award, and USF Outstanding Research Achievement Award. He published over 50 articles in refereed journals and conferences. He holds ten US granted/pending patents. He is an associate editor of the Journal of Circuits, Systems, and Computers and the Microelectronics Journal. He serves on the technical program and organization committees of various conferences.

Pizza and soda provided