Seminar Talk

Weize Yu, Ph.D.
Associate Professor
Department of Electrical & Computer Engineering
Old Dominion University

Tuesday, September 26, 2017
3:00 p.m. KH 224

Title: Exploiting Lightweight Countermeasures against Leakage Power Analysis Attacks

Abstract:
Non-invasive side-channel attacks (SCA) are powerful attacks which can be used to obtain the secret key in a cryptographic circuit in feasible time without the need for expensive measurement equipment. Leakage power analysis (LPA) attacks are a type of SCA that exploit the correlation between the leaked power consumption information and processed/ stored data. Leakage power dissipation primarily has two components: subthreshold power leakage and gate-oxide power leakage. These two power leakage components increase significantly with the continuous scaling of the silicon technology and the reduced supply voltage levels. Conventional LPA attacks are quite sensitive to measurement noise and therefore have attracted relatively less attention as compared to differential power analysis (DPA) attacks. LPA attacks can still be quite effective if the clock frequency of the cryptographic circuit is lowered by the attacker and the analysis is reinforced with average sampling analysis. In this talk, I will introduce how to leverage lightweight countermeasures against LPA attacks.

Bio:
Weize Yu received the B.S. degree in electrical engineering from University of Electronic Science and Technology of China, Chengdu, in 2009, and the M.S. and Ph.D. degrees in electrical engineering from Chinese Academy of Sciences, Beijing, and University of South Florida, Florida, in 2012 and 2017, respectively. Currently, he is an Assistant Professor in the Department of Electrical and Computer Engineering at Old Dominion University. Weize Yu is an Associate Editor of the Elsevier Microelectronics Journal. His current research interests are mainly focused on power management IC, hardware security, and Internet of things (IOT).