UCF DEPARTMENT OF ELECTRICAL & COMPUTER ENGINEERING

Spring 2016 Seminar Series

RELIABLE AND SECURE CRYPTOGRAPHIC HARDWARE AND DEEPLY EMBEDDED SYSTEMS

THURSDAY MARCH 3, 2016

11:00 AM – HEC 113

Computing platforms are expected to be deeply embedded within physical objects, including human body, creating an Internet of Things. These embedded computing platforms enable a wide spectrum of applications, including implantable and wearable medical devices, smart homes, smart meters, physical infrastructure monitoring, and near-field communication (NFC) or radio-frequency identification (RFID)-based emerging applications. The explosion in devices and connectivity creates a much larger attack surface, hence opening up new opportunities for malicious attacks and, therefore, requiring effective implementations of cryptographic primitives. Not only do the implementations of cryptographic hardware and embedded systems face challenges in terms of efficiency, energy-awareness, and high performance in platforms such as application-specific integrated circuit (ASIC) and field-programmable gate array (FPGA), but they also need to be immune to malicious side-channel fault attacks.

In this talk, we address both these challenges in order to realize lightweight and efficient cryptographic hardware systems and also realize them to counteract the accidental and malicious faults aiming at deriving the secret keys. As case study, through exhaustive search, the nonlinear S-boxes within the Advanced Encryption Standard (AES) – the current symmetric-key standard – are evaluated on ASIC to reach the highest efficiency. In order to realize high-throughput and efficient VLSI implementations of authentication and ensure low-latency and efficient crypto-hardware for this standard, we propose augmenting the confidentiality guaranteed by the AES and implementing efficient and parallel VLSI architectures of the Galois/counter mode (GCM). In addition, we present several novel fault diagnosis schemes for the hardware implementations of lightweight cryptographic entities and post-quantum cryptographic solutions. These techniques have been benchmarked on recent Xilinx FPGAs and standard-cell ASICs and have been simulated to assess their error coverage, which is close to 100%. The proposed approaches result in more reliable and efficient architectures for cryptographic hardware, suitable for implementation on deeply embedded applications.

DR. MEHRAN KERMANI

Rochester Institute of Technology

Dr. Mehran Mozaffari Kermani received the B.Sc. degree in electrical and computer engineering from the University of Tehran, Tehran, Iran, and the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Western Ontario, London, Canada, in 2011, respectively. He joined the Advanced Micro Devices as a senior ASIC/layout designer, integrating sophisticated security/cryptographic capabilities into a single accelerated processing unit. In 2012, he joined the Electrical Engineering Department, Princeton University, New Jersey, as an NSERC post-doctoral research fellow. Currently, he is with the Department of Electrical and Microelectronic Engineering, Rochester Institute of Technology, Rochester, NY. His current research interests include emerging security/privacy measures for deeply embedded systems, cryptographic hardware systems, fault diagnosis and tolerance in cryptographic hardware, VLSI reliability, and low-power secure and efficient FPGA and ASIC designs. Currently, he is serving as an Associate Editor for the IEEE Transactions on VLSI Systems, the ACM Transactions on Embedded Computing Systems, the IEEE Transactions on Circuits and Systems I, and the Guest Editor for the IEEE Transactions on Dependable and Secure Computing for the special issue of Emerging Embedded and Cyber Physical System Security Challenges and Innovations (2016 and 2017). He was the lead Guest Editor for the IEEE/ACM Transactions on Computational Biology and Bioinformatics and the IEEE Transactions on Emerging Topics in Computing for special issues on security. He was a recipient of the prestigious Natural Sciences and Engineering Research Council of Canada Post-Doctoral Research Fellowship in 2011 and the Texas Instruments Faculty Award in 2014.