UCF Electrical and Computer Engineering

# Spring 2017 Seminar Series

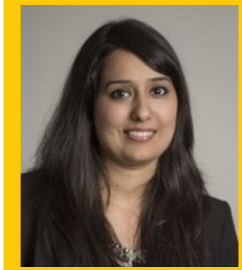
## Hardware based Authentication and Trust for IOTs

THURSDAY APRIL 6, 2017

1:30 PM – HEC 356

The increased integration and reliance on remote and embedded electronics as the basis of personal, commercial and industrial systems in internet of things (IoT) is driving the need for upgraded security and trust in these cyber physical systems. Many of the emerging applications, such as smart voting machines, smart home, advanced diver assistance systems (ADAS), autonomous vehicles, etc. incorporate resource-constrained devices, which create new vulnerabilities and increase the opportunity for malicious adversaries to steal private information, subvert systems, destroy property, and in extreme cases cause the loss of human life. With the proliferation of new information-sharing and control systems, it is crucial that a higher level of security be integrated into the hardware. It is imperative that these devices embed a hardware root of trust for improved security on which secure systems can be built. In the context of hardware systems, authentication refers to the process of confirming the identity and authenticity of chip, board and system components such as RFID tags, smart cards and remote sensors. A physical unclonable function (PUF) is an emerging hardware security primitive, capable of providing bitstrings and secret keys for authentication and encryption in these types of systems.

The colloquium presents an overview of IoT device vulnerabilities and the challenges associated with authenticating components in supply chain, as well as the benefits physical unclonable functions (PUFs) provide in dealing with these types of security risks. There is a growing commercial interest in using PUF to improve the security and trust in hardware based systems, including desktops and IoTs. PUF capabilities extend the security features of TPM by providing key management, pre-boot authentication and secure storage encryption. In particular, recent results of a hardware based authentication platform, which is based on a strong hardware embedded delay PUF (HELP) capable of generating a large number of secret keys and bitstring for encryption and authentication resource constrained applications, are presented. An important focus of the work is in evaluating the cryptographic strengths, properties of the bitstrings and keys produced by the HELP PUF. The role of HELP PUF in important emerging security functions including IC metering, temper detection and supply chain authentication will be discussed.



## Fareena Saqib

Florida Institute of Technology

Dr. Fareena Saqib earned her Ph.D. and M.S. degrees in Electrical and Computer Engineering from University of New Mexico (UNM). Her current research interests include: IoT security, hardware security and trust, supply chain risk management and security, physical unclonable functions (PUF) based authentication, high performance computing and hardware accelerators design using FPGAs for small and resource constrained embedded electronic devices. Dr. Saqib is presently working as Assistant Professor of Electrical and Computer Engineering at Florida Institute of Technology; and has varied experience in industry, consultancy services as well as teaching and research. Dr. Fareena Saqib has been awarded with two NSF current grants in the area of hardware security and trust relating to IoTs. She has published a number of journal articles and refereed conference papers. Additionally, she is co-author of a book chapter on "VLSI Test and Hardware Security Background for Hardware Obfuscation" which was recently published in 2017 by Springer.

Dr. Fareena Saqib serves as Guest Editor for Cryptography Special Issue on PUF-Based Authentication, Member on technical program committees of leading conferences and workshops. She is also the Vice Program Chair of workshop for women in hardware systems security (WISE), Organizer for summer camp for girls in collaboration with the GE, Faculty Advisor for students' chapter of IEEE at Florida Tech, reviewer for a number of specialized publications, and NSF Panelist. She is a member of IEEE.