**March 16, 4PM T&B 104**

**Hardware-based Solutions for Internet of Things (IoT) Security and Trust**

**Abstract**: The rapidly growing number of Internet of Things (IoT) devices is changing the way we work, communicate and think. It is estimated that currently there are more than 10 billion connected IoT devices and this number is expected to rise to 50 billion by the year 2020. The IoT is typically comprised of devices that are resource-constrained, power efficient and typically unmonitored. The ubiquitous deployment of such unprotected IoT devices raises critical security and trust concerns due to their accessibility and vulnerabilities to various malicious attacks. Conventional security mechanisms require costly cryptographic primitives like secure hash and encryption algorithms, whose secret keys are typically stored in non-volatile memories (NVMs). A Physically Unclonable Function (PUF) is a cost-effective hardware circuit that leverages random, unpredictable and uncontrollable variations introduced during chip fabrication to produce unique identifiers for individual hardware devices. Such chip-specific "DNA-like" information is derived from the analog characteristics that are intrinsic to the physical hardware and therefore: (1) does not need to be stored in digital form thereby eliminating costly and vulnerable NVM storage and (2) provides tamper evidence. The uncontrollable fabrication process makes it infeasible to make a clone of the PUF instance. In my presentation, I will describe our Hardware-Embedded Delay PUF called HELP that is dramatically different from all other proposed PUF architectures, and provides significant advantages including resistance to model-building attacks. I will also discuss how the HELP PUF can be used in securing IoT devices including its use in authentication protocols, key generation and other embedded security applications.

**BIO**

Dr. Wenjie Che is now working as a research engineer in a hardware security startup company "Enthentica Inc.". He received his MS degree in Computer Engineering from Hunan University in China in 2013, and Ph.D degree from the Department of Electrical and Computer Engineering at the University of New Mexico in 2016. His main research interests include hardware-based security and trust for IoT devices, embedded systems, Hardware and Software Co-Design and machine learning applied within the field of hardware security. He was awarded the 2nd place in the hardware demo competition among 26 participants at the IEEE International Symposium on Hardware Oriented Security and Trust (HOST) 2017. Dr. Che has served as a reviewer for several prestigious peer-reviewed journals and conferences including IEEE Transactions on Very Large Scale Integration Systems (TVLSI), IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), IEEE Transactions on Information Forensics and Security (TIFS), IEEE International Symposium on Hardware-Oriented Security and Trust (HOST) and Design, Automation and Test in Europe (DATE). Dr. Che has (co)-authored 15 papers and holds three provisions that are licensed by Enthentica Inc. He is a member of IEEE.