UNIVERSITY OF SOUTH FLORIDA

Major Research Area Paper Presentation

Reliable Error Detection Architectures for Secure Post-quantum Cryptosystems and Cloud Data Encryption

by

Ausmita Sarker

For the Ph.D. degree in Computer Science and Engineering

With the advent of quantum computers, the classical encryption schemes will be broken. Research on secure post-quantum cryptographic architectures is crucial and highly time-sensitive. Lattice-based cryptography is one of the most efficient as well as hard-to-break post-quantum cryptosystems. Error detection schemes of such architectures are essential to ensure correct mathematical operations, improved security, and thwart active side-channel attacks mounted through faults. This talk will discuss error detection schemes on various lattice-based architectures, which detect fault injection while maintaining high performance and low hardware overhead. As our schemes provide acceptable complexity and high efficiency, they can be utilized in compact hardware implementations of constrained applications, e.g., deeply-embedded architectures.

Friday, November 22, 2019
1:00
Mehran Mozaffari Kermani, Ph.D., Major Professor
Srinivas Katkoori, Ph.D.
Hao