UNIVERSITY OF SOUTH FLORIDA

Defense of a Doctoral Dissertation

Secure Hardware Constructions for Fault Detection of Lattice-based Post-quantum Cryptosystems

by

Ausmita Sarker

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

The advent of quantum computers and the exponential speed-up of quantum computation will render classical cryptosystems insecure, as that can solve current encryptions in minutes, resulting in a catastrophic failure of privacy preservation and data security. Through the standardizing of quantum-resistant public-key cryptography algorithms, the National Institute of Standards and Technology (NIST) is evaluating potential candidates to thwart such quantum attacks. In this talk, countermeasures against fault attacks are proposed to secure various lattice-based cryptosystems, one of the most promising post-quantum cryptosystems. Fault detection architectures for crucial building blocks of lattice-based cryptosystems, i.e., number