## UNIVERSITY OF SOUTH FLORIDA

Major Research Area Paper Presentation

Quantum computers are presumed to be able to break nearly all public-key encryption algorithms used today. The National Institute of Standards and Technology (NIST) started the process of soliciting and standardizing one or more quantum computer resistant public-key cryptographic algorithms in late 2017. Among those candidates, code-based cryptography is a promising solution for thwarting attacks based on quantum computers. Nevertheless, although code-based cryptography, e.g., McEliece and Niederreiter cryptosystems, have good error correction capabilities, research has shown their hardware architectures are vulnerable to faults due to the complexity and large footprint of the finite field arithmetic architectures used in those architectures. This talk will discuss error detection schemes