UNIVERSITY OF SOUTH FLORIDA

Major Research Area Paper Presentation

Efficient Hardware Constructions for Error Detection of Post-Quantum Cryptographic Schemes

by

Alvaro Cintas Canto

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

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 on various post-quantum cryptosystems that use finite fields, e.g., code-based and multivariate cryptography, proving the high efficiency and error coverage of such schemes, and the acceptable overhead needed to implement them in deeply-embedded architectures.

Tuesday, December 1st, 2020

11:00 AM

Online, Microsoft Teams

Please email alvarocintas@usf.edu for more information

THE PUBLIC IS INVITED

Examining Committee

Mehran Mozaffari Kermani, Ph.D., Major Professor
Sriram Chellappan, Ph.D.
Srinivas Katkoori, Ph.D.
Nasir Ghani, Ph.D.
Reza Azarderakhsh, Ph.D.

Yu Sun, Ph.D.
Graduate Program Director
Computer Science and Engineering
College of Engineering

Sudeep Sarkar, Ph.D.
Department Chair
Computer Science and Engineering
College of Engineering

Disability Accommodations:
If you require a reasonable accommodation to participate, please contact the Office of Diversity & Equal Opportunity at 813-974-4373 at least five (5) working days prior to the event.