UNIVERSITY OF SOUTH FLORIDA

Defense of a Doctoral Dissertation

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 and ending in 2022-2024. Among those candidates, code-based and multivariate-based cryptography are a promising solution for thwarting attacks based on quantum computers. Nevertheless, although code-based and multivariate-based cryptography, e.g., McEliece, Niederreiter, and Luov cryptosystems, have good error correction capabilities, research has shown that their hardware architectures are vulnerable to faults due to the complexity and large footprint of the finite field arithmetic architectures used in those architectures. In this talk, error detection schemes on various post-quantum cryptosystems that use finite fields are discussed, proving the high efficiency and error coverage of such schemes, and the acceptable overhead needed to implement them in deeply-embedded architectures.

Examining Committee

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

Tuesday, March 16, 2021
10:00 AM
Online (MS Teams)
Please email for more information
alvarocintas@usf.edu
THE PUBLIC IS INVITED

Publications

1) **A. Cintas Canto**, M. Mozaffari Kermani, and R. Azarderakhsh, "Reliable CRC-based error detection constructions for finite field multipliers with applications in cryptography," *IEEE Transactions on Very Large Scale Integrated (VLSI) Systems*, vol. 29, no. 1, pp. 232-236, Jan. 2021.
2) **A. Cintas Canto**, M. Mozaffari Kermani, and R. Azarderakhsh, "Reliable architectures for composite-field-oriented constructions of McEliece post-quantum cryptography on FPGA," *IEEE Transactions on Computer-Aided Design Integr. Circuits Syst.*, accepted, 2020.
3) **A. Cintas Canto**, M. Mozaffari Kermani, and R. Azarderakhsh, "CRC-based error detection constructions for FLT and ITA finite field inversions over GF(2^m)," *IEEE Transactions on Very Large Scale Integrated (VLSI) Systems*, accepted, 2021.

Robert Bishop, Ph.D.
Dean, College of Engineering

Dwayne Smith, Ph.D.
Dean, Office of Graduate Studies

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.