# UNIVERSITY OF SOUTH FLORIDA

## *Major Research Area Paper Presentation*

*Signature Schemes Based on Efficient Additively Homomorphic One-way Functions*

*by*

## *Rouzbeh Behnia*

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

Efficient authentication is vital for applications that need to verify a large volume of incoming transactions or commands. While symmetric key primitives (e.g., HMAC) can provide very fast authentication, they fail to offer non-repudiation which is often vital for these applications. Achieving Efficient authentication becomes even more challenging when quantum computers are taken into the account.

In this talk, we present two new efficient digital signature schemes. The main idea behind our schemes is to elevate the additive homomorphic property of the underlying one-way function to transform a well-known one-time signature construction (HORS) to a (polynomially-bounded) many time signature. In our first scheme, ARIS, we select a ECDLP-based one-way function and leverage its homomorphic property. Next, we propose a new post-quantum signature named TACHYON which uses the inherit additive homomorphic property of a post quantum secure one-way function (generalized compact knapsack) to achieve efficient signing and verification. Both schemes achieve the lowest end-to-end delay among their counterparts and enjoy from significantly efficient verification algorithms. However, ARIS and TACHYON suffer from a large public key due to the message-encoding technique that is used in the underlying one-time signature.

*Tuesday, July 21, 2020*
*2:00 PM*
*Online (Blackboard Collaborate)*
*Please email behnia@usf.edu for more information*

THE PUBLIC IS INVITED

*Examining Committee*
Attila A. Yavuz, Ph.D., Major Professor
Jay Ligatti, Ph.D.
Mehran Mozaffari Kermani, Ph.D.
Xinming (Simon) Ou, Ph.D.
Mike Rosulek, Ph.D.
Kaiqi Xiong, 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.*