UNIVERSITY OF SOUTH FLORIDA

Major Research Area Paper Presentation

Reliable Hardware Architectures for Lightweight Cryptographic Constructions in Secure Deeply Embedded Systems

by

Jasmin Kaur

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

Lightweight cryptography plays a vital role in securing resource-constrained embedded systems such as deeply embedded systems, RFID tags, sensor networks, and the Internet of nano-Things. Utilizing lightweight security in hardware has the advantage of adopting the mechanisms to battery-constrained usage models including implantable and wearable medical devices. Thus, reliable lightweight cryptographic systems are important to protect sensitive information in various resource-constrained devices. This work introduces reliability in lightweight cryptographic hardware by exploring the following: 1) Fault detection mechanisms for the block ciphers QARMA and ASCON, 2) Fault detection mechanisms for the Welch Gong stream ciphers WAGE and WG-29, 3) Benchmark hardware overheads for the proposed schemes on the FPGA hardware platform, and 4) Verify the high error coverage of the proposed schemes using simulations. Comparisons with other state of the art ciphers show that the protected hardware implementations provide acceptable overheads with high error coverage (over 99%) for resource constrained applications.

Friday, November 11th 2022
4:30 PM
Online (Microsoft Teams)
Please email for more information
jasmink1@usf.edu

THE PUBLIC IS INVITED

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

Alfredo Weitzenfeld, Ph.D.
Associate Chair for Graduate Affairs
Computer Science and Engineering
College of Engineering

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