UNIVERSITY OF SOUTH FLORIDA

Defense of a Doctoral Dissertation

Secure Lightweight Cryptographic Hardware Constructions for Deeply Embedded Systems

by

Jasmin Kaur

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

Lightweight cryptography plays a vital role in securing various resource-constrained embedded systems, including deeply-embedded systems, implantable and wearable medical devices, smart homes, RFID tags, sensor networks, and privacy-constrained usage models. However, the security of these systems can be compromised by fault analysis attacks, a type of active side-channel attack where an intelligent adversary injects bit/byte faults to retrieve the secret key. This dissertation aims to address this challenge by proposing effective methods to prevent fault analysis attacks through the implementation of different error detection strategies in the hardware applications of state-of-the-art lightweight cryptosystems. The study includes comprehensive case studies on prominent lightweight cryptographic ciphers such as QARMA, Welch-Gong ciphers WAGE and WG-29, and ASCON, the winner of the NIST standardization process for lightweight cryptography. The proposed error detection schemes are designed to be architecture-oblivious and cost-effective for the hardware constructions of these ciphers. The schemes are evaluated on a field-programmable gate array (FPGA) hardware platform to assess their error coverage and performance impact. The outcomes of this dissertation contribute to the development of more reliable lightweight cryptography, which is resilient against implementation attacks.

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

Tuesday, June 13th, 2023
2:00 PM
Online (Microsoft Teams)
Please email for more information
Jasmink1@usf.edu
THE PUBLIC IS INVITED

Publications

1) J. Kaur, M. Mozaffari Kermani, and R. Azarderakhsh, "Hardware constructions for lightweight cryptographic block cipher QARMA with error detection mechanisms," *IEEE Transactions on Emerging Topics in Computing*, vol. 10, no. 1, pp. 514-519, March 2022.
2) J. Kaur, A. Sarker, M. Mozaffari Kermani, and R. Azarderakhsh, "Hardware constructions for error detection in lightweight Welch-Gong (WG) oriented streamcipher WAGE benchmarked on FPGA," *IEEE Transactions on Emerging Topics in Computing*, vol. 10, no. 2, pp. 1208-1215, April 2022.
3) J. Kaur, M. Mozaffari Kermani, and R. Azarderakhsh, "Hardware constructions for error detection in lightweight authenticated cipher ASCON benchmarked on FPGA," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, no. 4, pp. 2276-2280, April 2022.
4) A. Cintas Canto, A. Sarker, J. Kaur, M. Mozaffari Kermani, and R. Azarderakhsh, "Error detection schemes assessed on FPGA for multipliers in lattice-based key encapsulation mechanisms in post-quantum cryptography," *IEEE Transactions on Emerging Topics in Computing*, October 2022.

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

Ruth H. Bahr, 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.