UNIVERSITY OF SOUTH FLORIDA

Defense of a Doctoral Dissertation

Secure Hardware Constructions for Fault Detection of Lattice-based Post-quantum Cryptosystems

by

Ausmita Sarker

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

The advent of quantum computers and the exponential speed-up of quantum computation will render classical cryptosystems insecure, as that can solve current encryptions in minutes, resulting in a catastrophic failure of privacy preservation and data security. Through the standardizing of quantum-resistant public-key cryptography algorithms, the National Institute of Standards and Technology (NIST) is evaluating potential candidates to thwart such quantum attacks. In this talk, countermeasures against fault attacks are proposed to secure various lattice-based cryptosystems, one of the most promising post-quantum cryptosystems. Fault detection architectures for crucial building blocks of lattice-based cryptosystems, i.e., number-theoretic transform, ring polynomial multiplication, and ring learning with error are introduced. Moreover, the secure hardware architecture of post-quantum key encapsulation mechanism SABER and the signature scheme Falcon are explored. The proposed architectures can also detect natural faults, caused by device malfunctions, which are crucial to proper functionalities of sensitive and secure deeply-embedded systems with stringent constraints.

Examining Committee

Ismail Uysal, Ph.D., Chairperson
Mehran Mozaffari Kermani, Ph.D., Major Professor
Srinivas Katkoori, Ph.D.
Hao Zheng, Ph.D.
Nasir Ghani, Ph.D.
Reza Azarderakhsh, Ph.D.

Wednesday, March 9, 2022
9:00 AM
Online (MS Teams)
Please email for more information
asarker@usf.edu
THE PUBLIC IS INVITED

Publications

1) **A. Sarker**, M. Mozaffari Kermani, and R. Azarderakhsh, "Efficient error detection architectures for post quantum signature Falcon's sampler and KEM SABER", *IEEE Transactions on Very Large Scale Integrated (VLSI) Systems*, in press, 2022.
2) **A. Sarker**, M. Mozaffari Kermani, and R. Azarderakhsh, "Fault detection architectures for inverted binary Ring-LWE construction benchmarked on FPGA," *IEEE Transactions on Circuits and Systems II*, vol. 68, no. 4, pp. 1403-1407, Apr. 2021.
3) **A. Sarker**, M. Mozaffari Kermani, and R. Azarderakhsh, "Error detection architectures for ring polynomial multiplication and modular reduction of Ring-LWE in $Z=pZ[x]/x^n+1$ benchmarked on ASIC," *IEEE Transactions on Reliability*, vol. 70, no. 1, pp. 362-370, Mar. 2021.
4) **A. Sarker**, M. Mozaffari Kermani, and R. Azarderakhsh, "Hardware constructions for error detection of number-theoretic transform utilized in secure cryptographic architectures," *IEEE Transactions on Very Large Scale Integrated (VLSI) Systems*, vol. 27, no. 3, pp. 738-741, Mar. 2019.
5) 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*, accepted, 2021.
6) M. Mozaffari Kermani, R. Azarderakhsh, **A. Sarker**, and A. Jalali, "Efficient and reliable error detection architectures of Hash-Counter-Hash tweakable enciphering schemes," *ACM Transactions on Embedded Computing Systems*, vol. 17, no. 2, pp. 54:1-54:19, May 2018.

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.