FAU COLLEGE OF ENGINEERING AND COMPUTER SCIENCE
FLORIDA ATLANTIC UNIVERSITY

Announces the Ph.D. Dissertation Defense of

Rami Elkhatib

for the degree of Doctor of Philosophy (Ph.D.)

“Efficient Implementation of Post-Quantum Cryptography”

July 1, 2022, 9:00 a.m.
Virtual Dissertation

Zoom Meeting
Meeting ID: 864 1142 7495
Passcode: aNs1Wd

DEPARTMENT:
Electrical Engineering and Computer Science

ADVISOR:
Reza Azarderakhsh, Ph.D.

PH.D. SUPERVISORY COMMITTEE:
Reza Azarderakhsh, Ph.D., Chair
Jason Hallstrom, Ph.D.
Feng-Hao Liu, Ph.D.
Mehran Mozaffari Kermani, Ph.D.

ABSTRACT OF DISSERTATION
Efficient Implementation of Post-Quantum Cryptography

Cryptography relies on hard mathematical problems that current conventional computers cannot solve in a feasible amount of time. On the other hand, quantum computers, with their quantum mechanic construction, are presumed to be able to solve some of these problems in a reasonable amount of time. More specifically, the current hard problems that public key cryptography relies upon are expected to be easily broken during the quantum era, a time when large-scale quantum computers are available. To address this problem ahead of time, researchers and institutions have proposed post-quantum cryptography (PQC), which is an area of research that focuses on quantum-resistant public key cryptography algorithms. One of the candidates in the NIST PQC standardization process is SIKE, an isogeny-based candidate. The main advantage of SIKE is that it provides the smallest key size out of all the NIST PQC candidates at the cost of performance. Therefore, the development of hardware accelerators for SIKE is very important to achieve high performance in time-constrained applications. In this thesis, we implement several accelerators for SIKE and its primitives using different design approaches, all of which are suitable for different applications. We deliver significant enhancements to SIKE's most expensive component, the modular multiplier. We design SIKE using a hardware-based approach and a software-hardware codesign approach, the latter of which utilizes a RISC-V processor. We also design SIKE with multi-level security level support for applications that require support of multiple security levels with minimal area usage. We enclose our performance and area results, which provide a reference to evaluate our work with other implementations.

BIOGRAPHICAL SKETCH
Born in Chakra, Lebanon
B.S., American University of Beirut, Lebanon, 2013

CONCERNING PERIOD OF PREPARATION
& QUALIFYING EXAMINATION

Time in Preparation: Summer 2018-Summer 2022

Qualifying Examination Passed: Spring 2019

Published Papers:

El Khatib, R., Azarderakhsh, R., & Mozaffari-Kermani, M. "Optimized Algorithms and Architectures for Montgomery Multiplication for Post-Quantum Cryptography." International Conference on Cryptology and Network Security (CANS-2019). Springer, Cham, 2019.

Elkhatib, R., Azarderakhsh, R., & Mozaffari-Kermani, M. "Highly Optimized Montgomery Multiplier for SIKE primes on FPGA." IEEE 27th Symposium on Computer Arithmetic (ARITH-2020). IEEE, 2020.

Elkhatib, R., Azarderakhsh, R., & Mozaffari-Kermani, M. "High-performance FPGA accelerator for SIKE." IEEE Transactions on Computers, vol. 71, no. 6, pp. 1237-1248, 2021

Elkhatib, R., Azarderakhsh, R., & Mozaffari-Kermani, M. "Accelerated RISC-V for SIKE." IEEE 28th Symposium on Computer Arithmetic (ARITH-2021). IEEE, 2021.

Elkhatib, R., Koziel, B., Azarderakhsh, R., & Mozaffari-Kermani, M. "Accelerated RISC-V for post-quantum SIKE." IEEE Transactions on Circuits and Systems I: Regular Papers.

Elkhatib, R., Koziel, B., Azarderakhsh, R., & Mozaffari-Kermani, M. "Cryptographic Engineering a Fast and Efficient SIKE in FPGA." Transactions on Embedded Computing Systems 2022. (Major Revision)

Koziel, B., Ackie, A. B., El Khatib, R., Azarderakhsh, R., & Mozaffari-Kermani, M. "SIKE’d up: Fast Hardware Architectures for Supersingular Isogeny Key Encapsulation." IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 67, no. 12, pp. 4842-4854, 2020.

Bisheh Niasar, M., Elkhatib, R., Azarderakhsh, R., & Mozaffari-Kermani, M. "Fast, Small, and Area-Time Efficient Architectures for Key-Exchange on Curve25519," IEEE 27th Symposium on Computer Arithmetic (ARITH-2020). IEEE, 2020.

Azarderakhsh, R., Biasse, J. F., El Khatib, R., Langenberg, B., & Pring, B. “Parallelism strategies for the tuneable golden-claw finding problem.”, International Journal of Computer Mathematics: Computer Systems Theory, vol. 6, no. 4, pp. 337-363, 2021.