FAU COLLEGE OF ENGINEERING AND COMPUTER SCIENCE
FLORIDA ATLANTIC UNIVERSITY

Announces the Ph.D. Dissertation Defense of

Amir Jalali

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

"Efficient Implementations of Post-Quantum Isogeny-Based Cryptography"

Nov. 9, 2018, 10:30 a.m.
777 Glades Road, Engineering East, Room 405
FAU Boca Raton Campus

DEPARTMENT
Computer and Electrical Engineering and Computer Science

ADVISOR
Reza Azarderakhsh, Ph.D.

PH.D. SUPERVISORY COMMITTEE
Reza Azarderakhsh, Ph.D., Chair
Jason Hallstrom, Ph.D.
Koray Karabina, Ph.D.
Mehrdad Nojoumian, Ph.D.

ABSTRACT OF DISSERTATION

Efficient Implementations of Post-Quantum Isogeny-Based Cryptography

Quantum computers are envisioned to be able to solve mathematical problems which are currently unsolvable for conventional computers, because of their exceptional computational power from quantum mechanics. Therefore, if quantum computers are ever built in large scale, they will certainly be able to solve many hard problems, including the problems which the current public key cryptography is constructed upon. To counteract this problem, post-quantum cryptography protocols are required to preserve the security in the presence of quantum adversaries. Regardless of whether we can estimate the exact time for the advent of the quantum computing era, security protocols are required to be resistant against potentially-malicious power of quantum computing.
In this thesis, the main focus is devoted on the performance improvement of one of the potential PQC candidates, isogeny-based cryptography. Several optimized implementation of cryptography applications based on this primitive on different platforms are presented. From a general viewpoint, the proposed methods, implementation techniques and libraries have a practical impact in the performance evaluation of post-quantum cryptography schemes in a wide range of applications. In particular, the provided benchmarks and optimizations on ARM-powered processors provide a reference for comparison and evaluation of isogeny-based cryptography with other post-quantum candidates during the first round of NIST's PQC standardization process.

BIOGRAPHICAL SKETCH
Born in Tehran, Iran
B.S., Shahid Beheshti University, Tehran, Iran, 2009
M.S., Amirkabir University of Technology, Tehran, Iran, 2012
Ph.D., Florida Atlantic University, Boca Raton, Florida, 2018

CONCERNING PERIOD OF PREPARATION
& QUALIFYING EXAMINATION
Time in Preparation: 2015 – 2018

Qualifying Examination Passed: Fall 2016

Published Papers:
Jalali, A., Azarderakhsh, R., Kermani, M.M. and Jao, D., 2017. Supersingular isogeny Diffie-Hellman key exchange on 64-bit ARM. IEEE Transactions on Dependable and Secure Computing.

Jalali, A., Azarderakhsh, R. and Mozaffari-Kermani, M., 2017, August. Efficient post-quantum undeniable signature on 64-bit ARM. In International Conference on Selected Areas in Cryptography (pp. 281-298). Springer, Cham.

Jalali, A., Azarderakhsh, R. and Mozaffari-Kermani, M., 2018, Dec. "NEON SIKE: Supersingular isogeny key encapsulation on ARMv7," in Proc. Int. Conf. Security, Privacy, and Applied Cryptography Engineering (SPACE), accepted.

B. Koziel, R. Azarderakhsh, A. Jalali, D. Jao, and M. Mozaffari Kermani, "NEON-SIDH: Efficient implementation of supersingular isogeny Diffie-Hellman key exchange protocol on ARM," in Proc. Conf. Cryptology and Network Security (CANS), pp. 88-103, 2016.

Jalali, A., Azarderakhsh, R., Kermani, M.M. and Jao, D., 2017. ARMv8 SIKE: Supersingular isogeny key encapsulation on 64-bit ARM. IEEE Transactions on Circuits and Systems I (submitted).