COLLEGE OF ENGINEERING AND COMPUTER SCIENCE
FLORIDA ATLANTIC UNIVERSITY

Announces the Ph.D. Dissertation Defense of

Brian Koziel

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

"Towards Deployable Quantum-Safe Cryptosystems"

July 11, 2022, 9:00 A.M.
Virtual Dissertation
Zoom Meeting
Meeting ID: 847 8422 2235
Passcode: pKN6Vw

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
Towards Deployable Quantum-Safe Cryptosystems
It is well known that in the near future, a large-scale quantum computer will be unveiled, one that could be used to break the cryptography that underlies our digital infrastructure. Quantum computers operate on quantum mechanics, enabling exponential speedups to certain computational problems, including hard problems at the cornerstone of our deployed cryptographic algorithms. With a vulnerability in this security foundation, our online identities, banking information, and precious data is now vulnerable. To address this, we must prepare for a transition to post-quantum cryptography, or cryptosystems that are protected from attacks by both classical and quantum computers. This is a dissertation proposal targeting cryptographic engineering that is necessary to deploy isogeny-based cryptosystems, one known family of problems that are thought to be difficult to break, even for quantum computers. Isogeny-based cryptography utilizes mappings between elliptic curves to achieve public-key encryption, digital signatures, and other cryptographic objectives necessary to support our digital infrastructure's security. This proposal focuses on three aspects of isogeny-based cryptography: 1) cryptographic engineering of isogeny-based cryptosystems; 2) developing and optimizing security-enabling isogeny applications; and 3) improving the security from known and emerging implementation attacks. By improving each of these aspects, we are providing confidence in the deployability of isogeny-based cryptography and helping to prepare for a post-quantum transition.

BIOGRAPHICAL SKETCH
Born in Ohio, United States

B.S., Rochester Institute of Technology, Rochester, New York, 2016
M.S., Rochester Institute of Technology, Rochester, New York, 2016
Ph.D., Florida Atlantic University, Boca Raton, Florida, 2022

CONCERNING PERIOD OF PREPARATION
& QUALIFYING EXAMINATION

Time in Preparation: Summer 2017 – Summer 2022

Qualifying Examination Passed: 2020

Published Papers:

Brian Koziel, Reza Azarderakhsh, and David Jao. Side-Channel Attacks on Quantum-Resistant Supersingular Isogeny Diffie-Hellman. In Carlisle Adams and Jan Camenisch, editors, *Selected Areas in Cryptography - SAC 2017 - 24th International Conference, Ottawa, ON, Canada, August 16-18, 2017, Revised Selected Papers*, volume 10719 of *Lecture Notes in Computer Science*, pages 64–81. Springer, 2017.

D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. De Feo, B. Hess, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, J. Renes, V. Soukharev, and D. Urbanik. Supersingular Isogeny Key Encapsulation. Submission to NIST Post-Quantum Cryptography Standardization Competition, 2017.

Brian Koziel, Reza Azarderakhsh, and Mehran Mozaffari Kermani. A High-Performance and Scalable Hardware Architecture for Isogeny-Based Cryptography. *IEEE Trans. Computers*, 67(11):1594–1609, 2018.

Reza Azarderakhsh, Elena Bakos Lang, David Jao, and Brian Koziel. EdSIDH: Supersingular Isogeny Diffie-Hellman Key Exchange on Edwards Curves. In Anupam Chattopadhyay, Chester Rebeiro, and Yuval Yarom, editors, *Security, Privacy, and Applied Cryptography Engineering - 8th International Conference, SPACE 2018, Kanpur, India, December 15-19, 2018, Proceedings*, volume 11348 of *Lecture Notes in Computer Science*, pages 125–141. Springer, 2018.

Brian Koziel, Reza Azarderakhsh, and David Jao. An Exposure Model for Supersingular Isogeny Diffie-Hellman Key Exchange. In Nigel P. Smart, editor, *Topics in Cryptology - CT-RSA 2018 - The Cryptographers' Track at the RSA Conference 2018, San Francisco, CA, USA, April 16-20, 2018, Proceedings*, volume 10808 of *Lecture Notes in Computer Science*, pages 452–469. Springer, 2018.

Aaron Hutchinson, Jason T. LeGrow, Brian Koziel, and Reza Azarderakhsh. Further Optimizations of CSIDH: A Systematic Approach to Efficient Strategies, Permutations, and Bound Vectors. In Mauro Conti, Jianying Zhou, Emiliano Casalicchio, and Angelo Spognardi, editors, *Applied Cryptography and Network Security - 18th International Conference, ACNS 2020, Rome, Italy, October 19-22, 2020, Proceedings, Part I*, volume 12146 of *Lecture Notes in Computer Science*, pages 481–501. Springer, 2020.

Reza Azarderakhsh, David Jao, Brian Koziel, Jason T. LeGrow, Vladimir Soukharev, and Oleg Taraskin. How Not to Create an Isogeny-Based PAKE. In Mauro Conti, Jianying Zhou, Emiliano Casalicchio, and Angelo Spognardi, editors, *Applied Cryptography and Network Security - 18th International Conference, ACNS 2020, Rome, Italy, October 19-22, 2020, Proceedings, Part I*, volume 12146 of *Lecture Notes in Computer Science*, pages 169–186. Springer, 2020.

Brian Koziel, A.-Bon E. Ackie, Rami El Khatib, Reza Azarderakhsh, and Mehran Mozaffari Kermani. SIKE'd Up: Fast Hardware Architectures for Supersingular Isogeny Key Encapsulation. *IEEE Trans. Circuits Syst.*, 67-I(12):4842–4854, 2020.

Brian Koziel, Mehran Mozaffari Kermani, and Reza Azarderakhsh. *Emerging Topics in Hardware Security*, chapter Post-Quantum Cryptographic Hardware and Embedded Systems, pages 229–255. Springer International Publishing, Cham, 2021.

Reza Azarderakhsh, Lubjana Beshaj, Emrah Karagoz, and Brian Koziel. Supersingular Isogeny Exposure Model: Revisited. (in Submission)

Jason LeGrow, Brian Koziel, and Reza Azarderakhsh. Multiprime Strategis in Serial eSIDH. (In Submission)