

Brian KOZIEL

Plano, Texas
1-469-893-0515

kozielbrian.com

kozielbrian@gmail.com

Revised Dec. 15, 2018

- Applied Cryptography, Blockchain, PQC, Security
- Strong research drive to solve complex problems
- Diverse background in cryptography, programming, and mathematics

EDUCATION

2011-2016 Master's in COMPUTER ENGINEERING - **RIT**, Rochester, NY
Thesis: "Low-Resource and Fast Elliptic Curve Implementations over Binary Edwards Curves" | Advisor: Prof. Reza AZARDERAKHSH
GPA: 4.0 - *summa cum laude*

2011-2016 Bachelor's in COMPUTER ENGINEERING - **RIT**, Rochester, NY
GPA: 4.0 - *summa cum laude*

PROFESSIONAL EXPERIENCE

MAR 2018-
Current Consultant at PQSECURE TECHNOLOGIES, Boca Raton, FL
Cryptographic Engineer
Commercializing quantum-resilient hardware architectures for lightweight devices.

AUG 2016-
Current Full-Time at TEXAS INSTRUMENTS, Dallas, TX
Cryptographic Design Engineer in Embedded Processing
Designing, evaluating, and testing cryptographic components for use in IoT devices, especially the public-key accelerator and true random number generator.

AUG 2015-
MAY 2016 Research at RIT, Rochester, NY
Cryptography Research Assistant in Applied Cryptography and Information Security Lab
Investigated various aspects of isogeny-based cryptography and supervised peers. Published research on efficient implementations of SIDH [J2] [C5] [C6], isogeny-based key compression [C4], and isogeny-based computations [C7].

JUNE 2015-
AUG 2015 Co-op at MIT LINCOLN LABORATORY, Lexington, MA
Hardware Security Intern in Secure Resilient Systems and Technology
Performed design and security analysis of a secure computing platform. Designed and implemented a secure cache model based on an open source synthesizable SoC.

JUNE 2014-
AUG 2014 Co-op at MIT LINCOLN LABORATORY, Lexington, MA
Hardware Security Intern in Cyber Systems and Technology
Involved in the design of an optical physical unclonable function. Designed and implemented a digital image sensor interface to generate a cryptographic key.

JUNE 2012-
AUG 2012 Co-op at AMERICAN GREETINGS, Cleveland, OH
Web Development Intern in Internal Print on Demand
Created Java programs for Tomcat servers to facilitate the creation and delivery of greeting cards. Developed the Packing Slip and Bundle Separator creation code.

PUBLICATIONS

Journal Articles

- [J1] **B. Koziel**, R. Azarderakhsh, and M. M. Kermani. A High-Performance and Scalable Hardware Architecture for Isogeny-Based Cryptography. *IEEE Transactions on Computers: Special Section on Cryptographic Engineering in a Post-Quantum World*, Nov 2018.
- [J2] **B. Koziel**, R. Azarderakhsh, M. M. Kermani, and D. Jao. Post-Quantum Cryptography on FPGA Based on Isogenies on Elliptic Curves. *IEEE Transactions on Circuits and Systems I: Regular Papers*, Jan 2017.

Conference Proceedings

- [C1] **B. Koziel**, R. Azarderakhsh, and D. Jao. An Exposure Model for Supersingular Isogeny Diffie-Hellman Key Exchange. In *CT-RSA: The Cryptographers' Track at the RSA Conference*, 2018.
- [C2] R. Azarderakhsh, D. Jao, **B. Koziel**, and E. B. Lang. EdSIDH: Supersingular Isogeny Diffie-Hellman on Edwards Curves. In *SPACE: 8th International Conference on Security, Privacy, and Applied Cryptography Engineering*, 2018.
- [C3] **B. Koziel**, R. Azarderakhsh, and D. Jao. Side-Channel Attacks on Quantum-Resistant Supersingular Isogeny Diffie-Hellman. In *SAC: 24th International Conference on Selected Areas in Cryptography*, 2017.
- [C4] R. Azarderakhsh, D. Jao, K. Kalach, **B. Koziel**, and C. Leonardi. Key Compression for Isogeny-Based Cryptosystems. In *AsiaPKC: 3rd ACM International Workshop on ASIA Public-Key Cryptography*, 2016.
- [C5] **B. Koziel**, R. Azarderakhsh, and M. M. Kermani. Fast Hardware Architectures for Supersingular Isogeny Diffie-Hellman Key Exchange on FPGA. In *INDOCRYPT: 17th International Conference on Cryptology in India*, 2016.
- [C6] **B. Koziel**, A. Jalali, R. Azarderakhsh, D. Jao, and M. M. Kermani. NEON-SIDH: Efficient Implementation of Supersingular Isogeny Diffie-Hellman Key Exchange Protocol on ARM. In *CANS: 15th International Conference on Cryptology and Network Security*, 2016.
- [C7] **B. Koziel**, R. Azarderakhsh, D. Jao, and M. M. Kermani. On Fast Calculation of Addition Chains for Isogeny-Based Cryptography. In *Inscrypt: 12th International Conference on Information Security and Cryptology*, 2016.
- [C8] **B. Koziel**, R. Azarderakhsh, and M. M. Kermani. Low-Resource and Fast Binary Edwards Curves Cryptography. In *INDOCRYPT: 16th International Conference on Cryptology in India*, 2015.

Standardization Competitions

- [M1] 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.

Posters

- [P1] R. Azarderakhsh, E. B. Lang, D. Jao, and **B. Koziel**. EdSIDH: Supersingular Isogeny Diffie-Hellman on Edwards Curves. In *MathCrypt*, 2018.
- [P2] **B. Koziel**, R. Azarderakhsh, and D. Jao. On Secure Implementations of Quantum-Resistant Supersingular Isogeny Diffie-Hellman. In *HOST: IEEE International Symposium on Hardware Oriented Security and Trust*, 2017.

AWARDS AND SCHOLARSHIPS

- 2016 **RIT Outstanding Undergraduate Award**
2016 **RIT Honor's Program Graduate**
2014-2016 **RIT BS-MS Dual-Degree Scholarship**
2013 **Tau Beta Pi Honor's Society**
2011-2016 **RIT Presidential Scholarship**
2011 **High School Class Valedictorian**

TECHNICAL SKILLS

Programming: C, Matlab, Python, Windows, Unix, Git, \LaTeX
Crypto: Isogeny-Based Crypto, ECC, PQC, Crypto Engineering
Hardware: VHDL, Verilog, FPGA, ASIC, GPU

COURSEWORK AT RIT 2013-2016

- **Advanced Cryptography**
- **Cryptographic Computations**
- **Computer Vision**
- **Advanced Computer Architecture**
- **High Performance Architectures**
- **Data and Communication Networks**
- **Digital IC Design**
- **Analytical Topics in Computer Engineering**

REVIEWER

2018 ISSCC (4), PQCrypto (3)
2017 ISSCC, TCAS, PQCrypto (2), SPACE
2016 CHES, Journal of Cryptographic Engineering
2015 LightSec

INTERESTS

Running, Rock Climbing, Cultural Immersion

Marathon time: 2:49

Languages: English (native speaker), Japanese (intermediate), French (intermediate), Chinese (intermediate)