Brian Koziel

Plano, Texas
1-469-893-0515
kozielbrian.com
kozielbrian@gmail.com
linkedin.com/in/brian-koziel

- 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: 4.0/4.0 - *summa cum laude*

2011-2016 Bachelor's in Computer Engineering - **RIT**, Rochester, NY
GPA: 4.0/4.0 - *summa cum laude*

Professional Experience

Mar 2018-*Current* | Consultant at PQSecure Technologies, Boca Raton, FL
Cryptographic Engineer
Designing post-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] [C4] [C5], isogeny-based key compression [C3], and isogeny-based computational aspects [C6].

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*, 2018 (to appear).

[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*, 64(1):86–99, Jan 2017.

Conference Proceedings

[C1] **B. Koziel**, R. Azarderakhsh, and D. Jao. An Exposure Model for Supersingular Isogeny Diffie-Hellman Key Exchange. In *Topics in Cryptology -* ***CT-RSA 2018*** *- The Cryptographers' Track at the RSA Conference 2018, San Francisco, CA, USA, April 16-20, 2018, Proceedings*, pages 452–469, 2018.

[C2] **B. Koziel**, R. Azarderakhsh, and D. Jao. Side-Channel Attacks on Quantum-Resistant Supersingular Isogeny Diffie-Hellman. In *Selected Areas in Cryptography: 24th International Conference,* ***SAC 2017****, Ottawa, ON, Canada, August 16-18, 2017, Revised Selected Papers*, pages 64–81, 2017.

[C3] R. Azarderakhsh, D. Jao, K. Kalach, **B. Koziel**, and C. Leonardi. Key Compression for Isogeny-Based Cryptosystems. In *Proceedings of the 3rd ACM International Workshop on ASIA Public-Key Cryptography,* ***AsiaPKC****@AsiaCCS, Xi'an, China, May 30 - June 03, 2016*, pages 1–10, 2016.

[C4] **B. Koziel**, R. Azarderakhsh, and M. M. Kermani. Fast Hardware Architectures for Supersingular Isogeny Diffie-Hellman Key Exchange on FPGA. In *Progress in Cryptology –* ***INDOCRYPT 2016****, 17th International Conference on Cryptology in India, Kolkata, India, December 11-14, 2016, Proceedings*, pages 191–206, 2016.

[C5] **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 *Cryptology and Network Security - 15th International Conference,* ***CANS 2016****, Milan, Italy, November 14-16, 2016, Proceedings*, pages 88–103, 2016.

[C6] **B. Koziel**, R. Azarderakhsh, D. Jao, and M. M. Kermani. On Fast Calculation of Addition Chains for Isogeny-Based Cryptography. In *Information Security and Cryptology - 12th International Conference,* ***Inscrypt 2016****, Beijing, China, November 4-6, 2016, Revised Selected Papers*, pages 323–342, 2016.

[C7] **B. Koziel**, R. Azarderakhsh, and M. M. Kermani. Low-Resource and Fast Binary Edwards Curves Cryptography. In *Progress in Cryptology -* ***INDOCRYPT 2015*** *- 16th International Conference on Cryptology in India, Bangalore, India, December 6-9, 2015, Proceedings*, pages 347–369, 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] **B. Koziel**, R. Azarderakhsh, and D. Jao. On Secure Implementations of Quantum-Resistant Supersingular Isogeny Diffie-Hellman. In *2017 IEEE International Symposium on Hardware Oriented Security and Trust, **HOST 2017**, McLean, VA, USA, May 1-5, 2017*, page 160, 2017.

Awards and Scholarships

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

Languages

English:	Native Speaker
Japanese:	Basic Knowledge
French:	Basic Knowledge

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

- **Advanced Cryptography** CSCI-762
- **Cryptographic Computations** CMPE-789
- **Computer Vision** CMPE-685
- **Advanced Computer Architecture** CMPE-750
- **High Performance Architectures** CMPE-755
- **Data and Communication Networks** CMPE-670
- **Digital IC Design** CMPE-630
- **Analytical Topics in Computer Engineering** CMPE-610

Paper Reviews

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

Interests and Activities

Security, Cryptography, Research, Algorithms
Running, Rock-Climbing, Cultural Immersion