Shannon Veitch

ssveitch@uwaterloo.ca

Education

University of Waterloo MMath, Computer Science *2020 – current*
Cryptography, Security, and Privacy Lab. Supervised by Professor Doug Stinson.

University of Waterloo BMath, Combinatorics and Optimization *2016 – 2020*

Research Experience

Dept. of Combinatorics and Optimization, University of Waterloo *May – Aug. 2020*
Undergraduate Research Assistant, Supervised by Professor Douglas Stebila

- Cryptanalysis of lattice-based key exchange protocols.
- Developed key-reuse attacks, optimized implementations, and performed analysis of attacks.

Dept. of Combinatorics and Optimization, University of Waterloo *Sept. – Dec. 2019*
Undergraduate Research Assistant, Supervised by Professor David Jao

- Optimized implementations of isogeny-based cryptosystems in ARM assembly language.
- Achieved 10x speed improvement of SIKE (Supersingular Isogeny Key Encapsulation) on ARM Cortex-M3 microcontroller, 7x speed improvement on ARM Cortex-M0+.

David R. Cheriton School of Computer Science, University of Waterloo *Sept. – Dec. 2018,*
Cryptography, Security and Privacy (CrySP) Lab *May – Aug. 2019*
Undergraduate Research Assistant, Supervised by Professor Douglas Stinson

- Investigated variations on the problem of sequencing triple systems and properties of orthogonal arrays with repeated rows.
- Developed and analyzed algorithms for constructing combinatorial designs.
- Proved new existence results of designs via recursive and direct constructions.

Publications

1. C. J. Colbourn, D. R. Stinson and S. Veitch. Constructions of optimal orthogonal arrays with repeated rows. *Discrete Mathematics* **342** (2019), 2455-2466.

2. D. Kreher, D. R. Stinson and S. Veitch. Block-avoiding point sequencings of directed triple systems. *Discrete Mathematics* **343** (2020), 111773.

3. D. Kreher, D. R. Stinson and S. Veitch. Block-avoiding point sequencings of Mendelsohn triple systems. *Discrete Mathematics* **343** (2020), 111799.

4. D. R. Stinson and S. Veitch. Block-avoiding point sequencings of arbitrary length in Steiner triple systems. *Australasian Journal of Combinatorics* **77** (2020), 87-99.

Technical Reports

5. D. Kreher, D. R. Stinson and S. Veitch. Good sequencings for small directed triple systems. 305 pages. July 2019.

6. D. Kreher, D. R. Stinson and S. Veitch. Good sequencings for small Mendelsohn triple systems. 121 pages. September 2019.

Industry Experience

ISARA Corporation *Jan. – Apr. 2019*

Security Developer

- Implemented quantum-safe cryptographic algorithms in C and SageMath.
- Optimized implementations of multivariate and lattice-based cryptosystems.

Cisco Systems *May – Aug. 2018*

Software Developer

- Performed tests on the Cisco enterprise networking operating system using Python.
- Developed features in an internal test framework using Python, Bash, and JavaScript.

Volunteering

CSGirls at UWaterloo *2019*

Workshop Assistant

- Assisted in running a cryptography and security session for high school girls.
- Answered questions about network security and guided students through a network simulation game.

StarCon *2018 – 2019*

Speakers Team Member

- Collaborated with a team to run a two-day, single-track, software engineering conference.
- Researched and documented potential frameworks for the call for proposals.
- Developed a review process that minimizes bias via anonymization and bidding of submissions.

University of Waterloo Faculty of Mathematics *2017 – 2020*

Math Faculty Ambassador

- Participated in student panel as a representative for Combinatorics and Optimization.
- Answered questions from prospective students about mathematics at Waterloo.

UW Capture the Flag (CTF) Club *2017*

Workshop Presenter

- Designed and presented a workshop on computer networks, covering the 4 Layer Internet Model, DNS, IP/TCP protocols, and link layer responsibilities.

Teaching Assistantships

CS135 Designing Functional Programs University of Waterloo *Fall 2020*

MATH135 Algebra for Honours Mathematics University of Waterloo *Winter 2018*

MATH135 Algebra for Honours Mathematics University of Waterloo *Fall 2017*

Awards

David R. Cheriton Graduate Scholarship University of Waterloo *2020*

President's Graduate Scholarship University of Waterloo *2020*

Ontario Graduate Scholarship (OGS) – *declined* *2020*

Alexander Graham Bell Canada Graduate Scholarship (CGS-M) NSERC *2020*

CRA Outstanding Undergraduate Researcher Award (Honorable Mention) *2020*

Undergraduate Student Research Award NSERC *2020*

President's Research Award University of Waterloo *2020*

Experience Award NSERC *2019*

President's Research Award University of Waterloo *2019*

President's Scholarship of Distinction University of Waterloo *2017*