Shannon Veitch

shannon.veitch@inf.ethz.ch

Education

ETH Zürich Doctoral Student *2022 – present*
Applied Cryptography Group. Advisor: Kenny Paterson

University of Waterloo MMath, Computer Science *2020 – 2022*
Cryptography, Security, and Privacy (CrySP) Lab. Advisor: Douglas Stinson
Thesis: *Contextualizing Alternative Models of Secret Sharing*

University of Waterloo BMath, Honours Combinatorics and Optimization *2016 – 2020*
Graduated With Distinction — Dean's Honours List

Publications

1. D. Keeler, C. Komlo, E. Lepert, S. Veitch, and X. He. DPrio: Efficient Differential Privacy with High Utility for Prio. *Proceedings on Privacy Enhancing Technologies* 2023 (3): 375–390.

2. T. Humphries, R. A. Mahdavi, S. Veitch, and F. Kerschbaum. Selective MPC: Distributed Computation of Differentially Private Key-Value Statistics. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22).* Association for Computing Machinery, New York, NY, USA, 1459–1472.

3. N. Bindel, D. Stebila, and S. Veitch. Improved attacks against key reuse in learning with errors key exchange. In Patrick Longa, Carla Ràfols, editors, *Proc. 7th International Conference on Cryptology and Information Security in Latin America (LATINCRYPT) 2021, LNCS.* Springer, October 2021.

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.

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

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

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

Preprints

8. S. Veitch and D. R. Stinson. Unconditionally Secure Non-malleable Secret Sharing and Circular External Difference Families.

Technical Reports

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

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

Academic Service

Organizing Committee
IEEE ISTAS 2021 (Fundraising & Sponsorship), StarCon 2019 (Speakers Team)

External Reviewer
ACISP 2021, IEEE S&P 2023

Supervision

Iana Peix, Semester Project, 2023. *Repairable Threshold Schemes with Malicious Security.*
Co-advisor: Kenny Paterson.

Lena Csomor, Master Thesis, 2023. *Bridging the Gap between Privacy Incidents and PETs.*
Co-advisors: Kenny Paterson, Anwar Hithnawi, Alexander Viand.

Teaching Assistantships

Diskrete Mathematik ETH Zürich	*Autumn 2023*
Informatik II ETH Zürich	*Spring 2023*
SYDE361 Engineering Design University of Waterloo	*Spring 2022*
SYDE362 Capstone Project University of Waterloo	*Winter 2022*
SYDE161 Introduction to Design University of Waterloo	*Fall 2021*
CS458/658 Computer Security and Privacy University of Waterloo	*Spring 2021*
CS458/658 Computer Security and Privacy University of Waterloo	*Winter 2021*
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 & Grants

ProtocolLabs Research Grant for RFP-014: Private retrieval of data Joint with Miti Mazmudar and Rasoul Akhavan Mahdavi	*2023*
Ontario Graduate Scholarship (OGS)	*2021 – 2022*
David R. Cheriton Graduate Scholarship University of Waterloo	*2020 – 2022*
President's Graduate Scholarship University of Waterloo	*2020 – 2022*
Cybersecurity and Privacy Excellence Graduate Scholarship CPI	*2020*
Ontario Graduate Scholarship (OGS) [declined]	*2020*
NSERC Alexander Graham Bell Canada Graduate Scholarship (CGS-M)	*2020*
CRA Outstanding Undergraduate Researcher Award (Honorable Mention)	*2020*
NSERC Undergraduate Student Research Award	*2020*
President's Research Award University of Waterloo	*2020*
NSERC Experience Award	*2019*
President's Research Award University of Waterloo	*2019*
President's Scholarship of Distinction University of Waterloo	*2017*

Selected Talks & Workshops

Bridging the Gap between Privacy Incidents and PETs *Best HotPETs Talk Award* *2023*
With Lena Csomor, Alexander Viand, Anwar Hithnawi, and Bailey Kacsmar.

Mending Engineering: A Workshop to Start Radically Repairing Engineering's Relationship with the Rest of the World *2022*
With Matt Borland, Kate Mercer, Jenny Howcroft, Alexi Orchard, and Matt Robichaud. Canadian Engineering Education Association Annual Conference 2022, York University.

Cybersecurity and Privacy Institute Speaker Series: Women in Tech *2020*
Panel with Jennifer Whitson, Bonnie Butlin, and Cat Coode.

Computer Networks Workshop *2017*
UW Capture the Flag (CTF) Club.