Shannon Veitch

shannon.veitch@inf.ethz.ch

Education

ETH Zurich 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. Francolla, M. Filić, and S. Veitch. Privacy implications of AMQ-based PQ TLS authentication. In *Companion of the 20th International Conference on emerging Networking EXperiments and Technologies (CoNEXT 2024).* Association for Computing Machinery, New York, NY, USA, 65–72.

2. F. Günther, D. Stebila, and S. Veitch. Obfuscated Key Exchange. In *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24).* Association for Computing Machinery, New York, NY, USA, 2024.

3. S. Veitch and D. R. Stinson. Unconditionally Secure Non-malleable Secret Sharing and Circular External Difference Families. *Designs, Codes and Cryptography.* **92**, 941–956 (2024).

4. 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.

5. 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.

6. 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.

7. 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.

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

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

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

Preprints

11. M. Mazmudar, S. Veitch, and R. A. Mahdavi. Peer2PIR: Private Queries for IPFS. 2024.

Technical Reports

12. F. Günther, D. Stebila, and S. Veitch. Kemeleon Encodings. Internet-Draft, November 2024.

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

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

Academic Service

Organizing Committee
WIP (Workshop in PIR) 2024 (Organization/Programme Committee)
IEEE ISTAS 2021 (Fundraising & Sponsorship)
StarCon 2019 (Speakers Team)

External Reviewer
ACISP 2021, IEEE S&P 2023, Eurocrypt 2024

Supervision

Luca Maier, Master Thesis, 2025. *Formal Analysis of the SecureDrop Protocol.*
Co-advisors: David Basin, Felix Linker.

Eduarda Assunção, Semester Project, 2025. *Analyzing Real-World Variants of IKEv2.*
Co-advisor: Kenny Paterson.

Antonino Orofino, Master Thesis, 2024. *An Investigation of VPN Fingerprinting.*
Co-advisors: Kenny Paterson, Lenka Mareková.

Dimitri Francolla, Semester Project, 2024. *Privacy implications of AMQ-based PQ TLS authentication.*
Co-advisors: Kenny Paterson, Mia Filić.

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

ETH Zurich

- Applied Cryptography (Spring 2024, Spring 2025)
- Discrete Mathematics (Autumn 2023, Autumn 2024)
- Computer Science II (Spring 2023)

University of Waterloo

- SYDE361 Engineering Design (Spring 2022)
- SYDE362 Capstone Project (Winter 2022)
- SYDE161 Introduction to Design (Fall 2021)
- CS458/658 Computer Security and Privacy (Winter 2021, Spring 2021)
- CS135 Designing Functional Programs (Fall 2020)
- MATH135 Algebra for Honours Mathematics (Fall 2017, Winter 2018)

Awards & Grants

Protocol Labs Research Grant for RFP-014: Private retrieval of data *2023*
Joint with Miti Mazmudar and Rasoul Akhavan Mahdavi

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 UWaterloo 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

Obfuscated Key Exchange *Real World Crypto 2024*
Based on joint work with Felix Günther and Douglas Stebila. *SKECH 2024*
CCS 2024

Bridging the Gap between Privacy Incidents and PETs *HotPETs 2023*
Best HotPETs Talk Award
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 *CEEA 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.