

Bailey Kacsmar

200 University Ave W
Waterloo, Ontario
N2L 3G1

bkacsmar@uwaterloo.ca
(306) 740-8070
cs.uwaterloo.ca/~bkacsmar/

Academic Background

Post-Secondary Education

- **PhD, University of Waterloo** Waterloo, Ontario
in Computer Science 2018 - Present
– Supervisor: Florian Kerschbaum
- **MMath, University of Waterloo** Waterloo, Ontario
in Computer Science 2016 - 2018
– Supervisor: Doug Stinson
– Thesis: Designing Efficient Algorithms for Combinatorial Repairable Threshold Schemes
- **BSc (Honours), Brandon University** Brandon, Manitoba
Majors in Computer Science and Philosophy, Minor in Mathematics 2011 - 2016
– Graduated with “Greatest Distinction”
– “Silver Medal in Philosophy” for highest GPA among philosophy majors

Co-Curricular Professional Development

- **Certificate in University Teaching** Waterloo, Ontario
Through the University of Waterloo’s Centre for Teaching Excellence 2021
- **Certificate in Student Leadership** Waterloo, Ontario
Through the University of Waterloo’s Student Success Office 2018
- **Certificate in Fundamentals of University Teaching** Waterloo, Ontario
Through the University of Waterloo’s Centre for Teaching Excellence 2017

Publications and Research Talks

Peer-Reviewed Journal Publications

- **Bailey Kacsmar**, Chelsea H. Komlo, Florian Kerschbaum, Ian Goldberg. (2020). Mind the Gap: Ceremonies for Applied Secret Sharing. *Proceedings on Privacy Enhancing Technologies*, 2020(2), pages 397-415.
- **Bailey Kacsmar** and Douglas R. Stinson. A Network Reliability Approach to the Analysis of Combinatorial Repairable Threshold Schemes. *Advances in Mathematics of Communications*, 13-4 (2019), pages 601-612.
- Chenkuan Li, Changpin Li, **Bailey Kacsmar**, Roque Lacroix and Kyle Tilbury. The Abel integral equations in distribution, *Advances in Analysis*, 2 (2017), pages 88-104.

Peer-Reviewed Conference Publications

- Rasoul Akhavan Mahdavi, Thomas Humphries, **Bailey Kacsmar**, Simeon Krastnikov, Nils Lukas, John Premkumar, Masoumeh Shafeinejad, Simon Oya, Florian Kerschbaum, Erik-Oliver Blass. Practical Over-Threshold Multi-Party Private Set Intersection. *Annual Computer Security Applications Conference (ACSAC 2020)*. Accepted.

- **Bailey Kacsmar**, Basit Khurram, Nils Lukas, Alexander Norton, Masoumeh Shafieinejad, Zhiwei Shang, Yasser Baseri, Maryam Sepehri, Simon Oya, and Florian Kerschbaum. Differentially Private Two-Party Set Operations. The 5th IEEE European Symposium on Security and Privacy 2020. Accepted.
- **Bailey Kacsmar**, Sarah Plosker, Ryan Henry. Computing Low-Weight Discrete Logarithms, The 24th Annual Conference on Selected Areas in Cryptography (SAC 2017), Volume 10719 of LNCS, pages 106-126. Ottawa, ON, Canada.

Conference Presentations without Proceedings

- “State-Level Secrets: When Theory Meets Practice for Journalists Working with Encrypted Documents”, Real World Crypto 2019, San Jose, California, United States. (January 2019). Co-presenter: Chelsea Komlo

Poster Presentations and Extended Abstracts

- **Bailey Kacsmar**, Sarah Plosker, Ryan Henry *Computing Low-Weight Discrete Logarithms*, Waterloo Cybersecurity and Defence Forum 2017, Waterloo, Ontario
- **Bailey Kacsmar**, Sarah Plosker, Ryan Henry *Computing Low-Weight Discrete Logarithms*, Second Annual Canadian Celebration of Women in Computing (2017), Montreal, Quebec
- Ryan Henry, **Bailey Kacsmar**, and Sarah Plosker: Computing Low-Weight Discrete Logarithms. Extended abstract at the 1st International Workshop on Mathematical Methods for Cryptography (MMC 2017), Svolvær-Lofoten, Norway (September 2017).

Theses

- **Bailey Kacsmar**: *Designing Efficient Algorithms for Combinatorial Repairable Threshold Schemes*. UWSpace: MMath thesis, University of Waterloo, Waterloo, ON, Canada (October 2018).

Technical Reports

- **Bailey Kacsmar**, Sarah Plosker, Ryan Henry. Computing Low-Weight Discrete Logarithms, IACR Cryptology ePrint Archive: Report 2017/720 (July 2017).

Invited Talks

- *Some Advancements in Cryptography*, Brandon University Senior Colloquium, Brandon University, April 11, 2016
- *Computing Low-Weight Discrete Logarithms*, Department of Mathematics & Computer Science Seminar Series, Brandon University, Mar. 3, 2016

Other Research Experience

- Summer school student, invited to participate in the 2018 Program for Women and Mathematics: Mathematics of Modern Cryptography, Institute for Advanced Study, Princeton, New Jersey, May 19-26, 2018.
- Summer school student, invited to participate in the 2014 Summer School for Women in Mathematics, University of Waterloo, Waterloo, Ontario, August 10-23, 2014.

Honours & Awards

Alexander Graham Bell Canada Graduate Scholarship (CGS-D₃) (\$105,000), NSERC 2019-2022
President's Graduate Scholarship (\$30,000), University of Waterloo 2019-2022
David R. Cheriton Graduate Scholarship(\$20,000), University of Waterloo 2018-2019
Provost Doctoral Entrance Award for Women(\$5,000), University of Waterloo 2018
University of Waterloo Entrance Scholarship(\$4,000), University of Waterloo 2016
Karl Popper Scholarship in Philosophy(\$1,985), Brandon University 2016
Queen Elizabeth II Scholarship(\$10,800) , University of Calgary 2016
Inducted into the Brandon University Honour Society, Brandon University 2015
Placed on the Dean's Honour List, Brandon University 2015
President's Leadership Scholarship(Full Tuition: \$3,152.94), Brandon University 2015
Harold Vidal Memorial Scholarships in the Humanities(\$1,500), Brandon University 2014,2015
R. Murray Simmons Scholarship in Humanities(\$575), Brandon University 2015
Placed on the Honours List, Brandon University, Brandon University 2011, 2012, 2013, 2014
Brandon College Class of '50 Millennium Scholarship (\$600), Brandon University 2013
Dr. W.N Hargreaves-Mawdsley Third Year Scholarshi (\$500), Brandon University 2013
John Odin Scholarship, Brandon University (\$770) 2013
Adam Sus Bursary in Computer Science (\$2,450), Brandon University 2012
Inducted into the Presidents Honour Society, Brandon University 2011, 2013
Brandon University Board of Governors Entrance Scholarship (\$1,400), Brandon University . . . 2011

Academic Service

- Co-Chair (Artifact Committee): Privacy Enhancing Technologies Symposium (PoPETs) 2022
- Artifact Committee Member: Privacy Enhancing Technologies Symposium (PoPETs) 2021
- External Reviewer: Privacy Enhancing Technologies Symposium (PoPETs) 2021

Teaching Experience

- **Teaching Assistant** Waterloo, Ontario
University of Waterloo 2016 - present
 - CS490 Information Systems Management (Winter '17, Winter '21)
Mark assignments, projects and exams, proctor exams
 - CS458/658 Computer Security and Privacy (Spring '17, Fall '17, Winter '18, Spring '18, Fall '18, Winter '20)
Create and mark assignments, hold office hours, proctor exams, and mark exams
 - CS135 Designing Functional Programs (Fall '16)
Proctoring, and marking both assignments and exams
- **Guest Lecturer** Waterloo, Ontario
University of Waterloo
 - CS458/658 Computer Security and Privacy (Winter '21)
Lecture Topic: Ethics
 - CS458/658 Computer Security and Privacy (Winter '21)
Lecture Topic: Address Resolution Protocol (ARP) Cache Posinoing Attacks

- CS490 Information Systems Management (Winter '17)
Lecture Topic: Introduction to Business Process Improvement Methodologies

- **Teaching Assistant** Brandon, Manitoba
Brandon University *January 2013 - May 2016*
 - 62.206 Discrete Structures and Programming (Winter '15, Fall '15, Winter '16)
Instruct students in the lab portion of the course as well as evaluate their lab work
 - 70:163 Critical Thinking (Winter '16)
Present tutorial sessions for students in the philosophy course
 - 62:182 Linear Algebra (Winter '13, Fall '13, Winter '14, Fall '14, Winter '15, Fall '15, Winter '16)
Assist students during the lab portion of the course as well as marking assignments and exams
 - 70:162 Introduction to Logic (Fall '14, Fall '15)
Marking assignments and exams

Community Service

- **Coding Coach at Technovation Workshops** Waterloo, Ontario
Providing coding guidance and help to teams *2019, 2021*
- **Girls Mean Business** Waterloo, Ontario
Co-facilitator Miti Mazmudar, online workshop on Network Security *November 23, 2020*
- **Technovation Girls Waterloo** Waterloo, Ontario
Volunteer and coding coach throughout the season and at seven events *January to May 2020*
- **CEMC Workshop in Computer Science for Young Women** Waterloo, Ontario
Co-presenter with Miti Mazmudar for a session on Network Privacy and Security *May 14, 2019*
- **Volunteer at Technovation Live Pitch Event** Waterloo, Ontario
Help with set-up and take down, registration *May 11, 2019*
- **Mentor at Ladies Who L(a)unch** Waterloo, Ontario
Speed networking luncheon presented by Women in Math (WiM) Committee *March 8, 2019*
- **Volunteer at Technovation Workshop** Waterloo, Ontario
Assist participants with setup and their MIT App Inventor projects *February 2, 2019*
- **Volunteer at GIRLsmarts4tech** Waterloo, Ontario
Assist participants following the tutorial in MIT App Inventor *June 10, 2018*
- **Volunteer at Technovation Workshop** Waterloo, Ontario
Assist participants with setup and their MIT App Inventor projects *February 11, 2018*
- **Mentor for StarCon Software Engineering Conference** Waterloo, Ontario
Provide feedback and advice to StarCon presenters preparing their talks *December 2017*
- **Mentor, WICS Speed Mentoring Event** Waterloo, Ontario
A mentoring event for undergraduate women in computer science *November 21, 2017*
- **Mentor, WICS Dinner with the Profs** Waterloo, Ontario
An opportunity for undergraduates to speak with professors and graduate students in a casual setting *March 28, 2017*
- **Guest Presenter, Cryptography, Security, and Privacy** Waterloo, Ontario
For the Junior Achievement in the Waterloo Region Advanced Camp *August 23, 2017*
- **Student Leader Coordinator** Brandon, Manitoba
Training student leaders for the student leader program *May 2014 - August 2016*