Bailey Kacsmar

Assistant Professor, Faculty of Science, Department of Computing Science
University of Alberta, Edmonton, Alberta, Canada
Amii Fellow, Alberta machine intelligence institute
Google Scholar ID: QZLnUAzKwpcC
kacsmar@ualberta.ca

Research Interests: Privacy in Machine Learning, Human Centered Privacy Technologies

Academic Background

Post-Secondary Education

- **PhD, University of Waterloo** — Waterloo, Ontario
  in Computer Science — *2023*
  - Supervisor: Florian Kerschbaum
  - Thesis: Perceptions and Practicalities for Private Machine Learning
- **MMath, University of Waterloo** — Waterloo, Ontario
  in Computer Science — *2018*
  - Supervisor: Douglas R. 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 — *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 Conference Publications

- Rasoul Akhavan Mahdavi, Faezeh Ebrahimianghazani, Thomas Humphries, **Bailey Kacsmar**, Emily Lepert, Xinda Li, Nils Lukas, John A. Premkumar, Simon Oya, Florian Kerschbaum. PEPSI: Practically Efficient Private Set Intersection in the Unbalanced Setting. The 33rd USENIX Security Symposium (USENIX Security 2024).
- Abdulrahman Diaa, Lucas Fenaux, Thomas Humphries, Marian Dietz, Faezeh Ebrahimianghazani, **Bailey Kacsmar**, Xinda Li, Nils Lukas, Rasoul Akhavan Mahdavi, Simon Oya, Ehsan Amjadian and Florian Kerschbaum. Fast and Private Inference of Deep Neural Networks by Co-designing Activation Functions. The 33rd USENIX Security Symposium (USENIX Security 2024).

- **Bailey Kacsmar**, Vasisht Duddu, Kyle Tilbury, Blase Ur, and Florian Kerschbaum. Comprehension from Chaos: Towards Informed Consent for Private Computation. Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (ACM CCS 2023), pages 210-224.

- **Bailey Kacsmar**. Improving Interactive Instruction: Faculty Engagement Requires Starting Small and Telling All. Koli Calling Proceedings of the 22nd International Conference on Computing Education Research. ACM. November 2022.

- **Bailey Kacsmar**, Kyle Tilbury, Miti Mazmudar, Florian Kerschbaum. Caring about Sharing: User Perceptions of Multiparty Data Sharing. The 31st USENIX Security Symposium (USENIX Security 2022), pages 899-916.

- Rasoul Akhavan Mahdavi, Thomas Humphries, **Bailey Kacsmar**, Simeon Krastnikov, Nils Lukas, John Premkumar, Masoumeh Shafieinejad, Simon Oya, Florian Kerschbaum, Erik-Oliver Blass. Practical Over-Threshold Multi-Party Private Set Intersection. Annual Computer Security Applications Conference (ACSAC 2020), pages 772-783.

- **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. (Euro S&P), pages 390-404.

- **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.

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.

Workshop Papers, Posters, and Extended Abstracts

- Kyle Tilbury, **Bailey Kacsmar**, Jesse Hoey. Towards Safety in Multi-agent Reinforcement Learning through Security and Privacy by Design. RLC 2024 Workshop CoCoMARL, Amherst, Massachusetts.

- **Bailey Kacsmar**, Kyle Tilbury, Miti Mazmudar, Florian Kerschbaum. Caring about Sharing: User Perceptions of Multiparty Data Sharing. SOUPS 2022, Boston, Massachusetts.

- **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).

Invited Talks

- "Usability and Cryptography Tutorial", SAC Summer School 2024, Montreal, Canada.
- "Human-Centered Privacy in Machine Learning", 2024 Seminar, University of Guelph, Guelph, Canada.
- "Privacy Pinch Points for Applied ML", Amii Upper Bound 2024, Edmonton, Canada.
- "Privacy and AI in Society", 2023 Amii DevCon Keynote, Edmonton, Alberta, Canada.
- "Contextual Integrity and Multiparty Data Sharing", 2023 BIRS Workshop on Contextual Integrity for Differential Privacy. Banff International Research Station UBC Okanagan Campus, Canada.
- "Human-Centered Privacy in Machine Learning", 2023 ZISC Seminar Series, ETH Zurich, Zurich, Switzerland.
- "Beyond Data Privacy for Machine Learning", 2023 Upper Bound Academic Symposium, AMII, Edmonton, Canada.

Presentations and Other Research Experience

- Visiting Researcher at EnCORE Institute (Institute for Emerging CORE Methods in Data Science) at UC San Diego, January 6-18, 2025.
- "Bridging the Gap between Privacy Incidents and PETs", 2023 Hot PETs, Lausanne, Switzerland. Collaboration with: Shannon Veitch, Lena Csomor, Alexander Viand, Anwar Hithnawi. *Best Hot PETs Talk Award.*
- "Improving Interactive Instruction", Math Teaching Colloquium at 2023 MAA Seaway Section, Waterloo, Canada.
- "State-Level Secrets: When Theory Meets Practice for Journalists Working with Encrypted Documents", Real World Crypto 2019, San Jose, United States. (January 2019). Collaboration with: Chelsea Komlo
- The 2018 Program for Women and Mathematics: Mathematics of Modern Cryptography, Institute for Advanced Study, Princeton, United States, May 19-26, 2018.

Awards, Grants, and Honours

Grants

NSERC Discovery Grant ($125,000), NSERC 2024-2029
NSERC Early Career Researcher (ECR) ($12,500), NSERC 2024

Awards and Honours

Math Faculty Teaching Development Fund ($2100), University of Waterloo 2022
Cybersecurity and Privacy Excellence Graduate Scholarship ($10,000), Waterloo CPI 2022
Alexander Graham Bell Canada Graduate Scholarship (CGS-D_3) ($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 Scholarship ($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

Chair

- HotPETs 2025, 2026
- Canadian AI Graduate Student Symposium 2024
- (Artifact Committee) Privacy Enhancing Technologies Symposium (PoPETs) 2022, 2023

Workshop Organization

- "Defining Holistic Private Data Science for Practice", Co-Organizer for Workshop at EnCORE Institute (Institute for Emerging CORE Methods in Data Science), UCSD, January 8-10, 2025.

Program Committee

- IEEE Symposium on Security and Privacy 2025
- Privacy Enhancing Technologies Symposium (PoPETs) 2023, 2024, 2025
- AAAI Conference on Artificial Intelligence (AAAI) 2024, 2025
- ACM Workshop on Artificial Intelligence and Security (AISec 2024)
- Symposium on Usable Privacy and Security (SOUPS) 2024
- ACM Conference on Computer and Communications Security (CCS) 2023, 2024
- Workshop on Technology and Consumer Protection (ConPro) 2024
- Workshop on Security and Privacy in Augmented, Virtual, and Extended Realities (SePAR) 2024
- Innovation and Technology in Computer Science Education (ACM ITiCSE) 2023, 2024

Invited/External Reviewer:

- Computer Human Interaction (ACM SIGCHI) 2023, *CHI 2023 Special Recognition for Outstanding Reviews*
- Innovation and Technology in Computer Science Education (ACM ITiCSE) 2022
- Privacy Enhancing Technologies Symposium (PoPETs) 2021, 2022

- Journal of Privacy and Confidentiality (JPC) 2022

Artifact Committee:

- Privacy Enhancing Technologies Symposium (PoPETs) 2021

Teaching Experience

Instructor Edmonton, Alberta
University of Alberta *2023-present*

- Graduate Course: Machine Learning and Practical Privacy (Fall '23, Fall '24)
- Undergraduate Course: Cryptography for Digital Privacy (Fall '24)
- Undergraduate Course: Machine Learning (Winter '24)

Sessional Instructor Waterloo, Ontario
University of Waterloo *2023*

- New Course on Privacy, Cryptography, Networks and Data Security (Winter '23)

Teaching Assistant Waterloo, Ontario
University of Waterloo *2016 - 2021*

- Information Systems Management (Winter '17, Winter '21)
- Computer Security and Privacy (Spring '17, Fall '17, Winter '18, Spring '18, Fall '18, Winter '20)
- Designing Functional Programs (Fall '16)

Guest Lecturer Waterloo, Ontario
University of Waterloo *2017, 2021*

- Computer Security and Privacy (Winter '21)
  Lecture Topic: Ethics
- Computer Security and Privacy (Winter '21)
  Lecture Topic: Address Resolution Protocol (ARP) Cache Posinoing Attacks
- Information Systems Management (Winter '17)
  Lecture Topic: Introduction to Business Process Improvement Methodologies

Teaching Assistant Brandon, Manitoba
Brandon University *2013 - 2016*

- Discrete Structures and Programming (Winter '15, Fall '15, Winter '16)
- Critical Thinking (Winter '16)
- Linear Algebra (Winter '13, Fall '13, Winter '14, Fall '14, Winter '15, Fall '15, Winter '16)
- Introduction to Logic (Fall '14, Fall '15)

Student Supervision

Masters of Science Edmonton, Alberta
University of Alberta

- Oufan (Steven) Hai (2024 - Ongoing)
- Rabeya Bosri (2023 - Ongoing)

- Afari Darfoor (2023 - Ongoing

Undergraduate Researchers Edmonton, Alberta
University of Alberta

- Jialiang Yan (2024)

Selected Awards and Outcomes
for Undergraduate Students

Jialiang Yan (2024)

- *Full summer salary from the competitive University of Alberta undergraduate research initiative2024 (URI), which only funded approximately 20% of applicants*

Community Service and Outreach

Youth Outreach
Focus on technology and entrepreneurial skills

- **Panelist for TeamUP Science's CS Workshop** Edmonton, Alberta
  Answering questions from high schoolers pertaining to my work and field *2024*
- **Technovation Girls Waterloo** Waterloo, Ontario
  Volunteer and coding coach throughout the season *2018, 2019, 2020, 2022*
- **Girls Mean Business** Waterloo, Ontario
  Co-facilitator with Miti Mazmudar, online workshop on Network Security *2020*
- **CEMC Workshop in Computer Science for Young Women** Waterloo, Ontario
  Co-facilitator with Miti Mazmudar, session on Network Privacy and Security *2019*
- **Volunteer at GIRLsmarts4tech** Waterloo, Ontario
  Assist participants following the tutorial in MIT App Inventor *2018*
- **Guest Presenter, Cryptography, Security, and Privacy** Waterloo, Ontario
  For the Junior Achievement in the Waterloo Region Advanced Camp *2017*

Undergraduate Outreach
Industry and Academia

- **Demystifying Grad School Workshop Faculty Panel** Edmonton, Alberta
  Panelist for discussion with undergraduates about grad school *2023, 2024*
- **WiCS Careers in Tech Panel** Waterloo, Ontario
  Panelist for discussion with undergraduates about different tech careers *2022*
- **Mentor at Ladies Who L(a)unch** Waterloo, Ontario
  Speed networking luncheon presented by Women in Math (WiM) Committee *2019*
- **Mentor for StarCon Software Engineering Conference** Waterloo, Ontario
  Provide feedback and advice to first time presenters preparing their talks *2017*
- **Mentor, Women in Computer Science (WICS) Speed Mentoring** Waterloo, Ontario
  A mentoring event for undergraduate women in computer science *2017*
- **Mentor, Women in Computer Science (WICS) Dinner with the Profs** Waterloo, Ontario
  An opportunity for undergraduates to speak with professors and graduate students in a casual setting *2017*

Media

- Interview, Unit.Ai Interview Series. `https://www.unite.ai/bailey-kacsmar-phd-candidate-at-university-of-waterloo-interview-series/`