# 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:** Usable Privacy and Artificial Intelligence, Human Centered Privacy

## 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

*Authors names marked with an * indicates work done as HQP under my direct supervision.*

Peer-Reviewed Conference Publications

- Miriam Bakija*, **Bailey Kacsmar**, Irene Cheng. An Analysis of Post-Fire Active Reforestation using Sentinel-2. The International Geoscience and Remote Sensing Symposium (IGARSS 2026).
- Masoumeh Shafieinejad, Xi He, **Bailey Kacsmar**. Adopt a PET! An Exploration of PETs, Policy, and Practicalities for Industry in Canada. Symposium on Usable Security and Privacy (USEC 2026).

- 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**. Privacy, Policy, and Compliance in Yet Another 'Age'. IEEE Data Engineering Bulletin (2025) Vol. 49 No. 4.

- **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

- Afari Darfoor*, Patrick Pilarski, **Bailey Kacsmar**. Exposed by Motion: An Investigation into the Privacy Risks of Highly-Sensorized Robotic Prostheses. The 11th IEEE RAS/EMBS International Conference on Biomedical Robotics and Biomechatronics (BioRob 2026), Edmonton, Canada.
- Afari Darfoor*, Laura C. Petrich, Patrick Pilarski, **Bailey Kacsmar**. Privacy Risks of AI-Enhanced Bionic Limbs. Responsible AI 2025, Calgary, Canada. *–Won Best Poster Presentation Award–*
- Jialiang Yan*, **Bailey Kacsmar**. When Privacy Notices Matter: Investigating the Impact of Timing on the Salience of Smartphone App Privacy Notices. Privacy Enhancing Technologies Symposium Poster Session 2024, Bristol, England.
- 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. *–Won Best Poster Presentation Award–*
- **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

- "*Detangling Design Variables for Human-Centred Privacy*", CISPA Helmholtz Center for Information Security, Saarbrücken, Germany. July 2025.
- "*The Secret Life of Data*", Upper Bound Conference 2025, Edmonton, Canada, May 2025.
- "*Human-Centred Privacy in a Digital Society*", Science Talks Webinars, University of Alberta, Edmonton, Canada. April 2025.
- "*PETs Intro: Multiparty Computation and Homomorphic Encryption*", Dagstuhl Seminar 25112 PETs and AI: Privacy Washing and the Need for a PETs Evaluation Framework, March 2025, Schloss Dagstuhl, Wadern, Germany.
- "*Usability and Cryptography Tutorial*", Select Areas of Cryptography (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*", Upper Bound Conference 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*", Upper Bound Conference 2023, Edmonton, Canada.

Panelist

- "*User Perspective of PETs*", 2025 Dagstuhl Seminar 25112 PETs and AI: Privacy Washing and the Need for a PETs Evaluation Framework, Schloss Dagstuhl, Wadern, Germany.

Other Research Presentations

- "*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

## Research Visits

- Schloss Dagstuhl Seminar 25261 *Future of Human-Centered Privacy*, June 2025
- Schloss Dagstuhl Seminar 25112 *PETs and AI: Privacy Washing and the Need for a PETs Evaluation Framework*, March 2025
- Visiting Researcher at EnCORE Institute (Institute for Emerging CORE Methods in Data Science) at UC San Diego, January 6-18, 2025. Includes co-organizing the "Defining Holistic Private Data Science for Practice" workshop, at EnCORE Institute (Institute for Emerging CORE Methods in Data Science), UCSD, January 8-10, 2025.
- The 2018 Program for Women and Mathematics: Mathematics of Modern Cryptography, Institute for Advanced Study, Princeton, United States, May 19-26, 2018.

## Expert Consultation and Policy Advising

*Organization of relevance indicated in* **bold** *with corresponding consultation or advising information provided below in italics.*

**Canada School of Public Policy**

- *"Fireside Chat: Navigating AI and Data Sovereignty, Stewardship and Trust", panel at the tenth GC Data Conference 2026.*

- **College of Dental Surgeons of Alberta (CDSA)**
  *"It's Not About Data Privacy", presentation and panel at CDSA's AI in Dentistry Symposium 2025.*

**Future of Privacy Forum**

- *For the Research Coordination Network for Privacy-Preserving Data Sharing and Analytics Focused on Artificial Intelligence, contribute as part of a multidisciplinary expert group of scholars and practitioners (RCN Expert Group) who use and develop PETs and understand the risks of data sharing and analytics for individuals, marginalized and vulnerable groups, civil rights, and civil liberties, 2025.*

**Technology and Innovation Ministry of the Government of Alberta**

- *Consultation and feedback with the Privacy, Policy and Governance Division in regards to an early version of their privacy portal and collaboration on transparency and data privacy. 2024 and 2025.*

**Canadian Standards Association**

- *Providing expertise in regards to AI safety and privacy research in addition to challenges and concerns associated with training AI to the Committee on Artificial Intelligence, 2025*

## Awards, Grants, and Research Funding

### Grants

NSERC Alliance - Alberta Innovates Advance Program ($40,000) . . . . . 2026-2028
Research Allocation Panel (RAP) ($36,884) . . . . . 2026
Amii Trust & Safety Funding, Co-PI Patrick Pilarski, ($73,725) . . . . . 2026
NSERC Discovery Grant ($160,000), NSERC . . . . . 2024-2029
Research Allocation Panel (RAP) ($48,000) . . . . . 2025
NSERC Early Career Researcher (ECR) ($12,500), NSERC . . . . . 2024

### Awards and Honours

Outstanding Mentorship in Undergraduate Research Award, University of Alberta . . . . . 2025
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

- General Co-Chair - The 26th Privacy Enhancing Technologies Symposium (PETS 2026)
- Co-Chair - The 18th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2025)
- Graduate Student Symposium Chair - Canadian AI 2024
- Artifact Co-Chair - Privacy Enhancing Technologies Symposium (PoPETs 2022 and 2023)

Advisory Boards

- PETS (Privacy Enhancing Technologies Symposium) Advisory Board

Grant Reviewer

- Catalyst Projects on Sociotechnical Considerations in AI Safety, by the Canadian AI Safety Institute (CAISI) Research Program at CIFAR

Program Committee

- IEEE Symposium on Security and Privacy 2025, 2026
- Symposium on Usable Privacy and Security (SOUPS) 2024, 2026
- AAAI Conference on Artificial Intelligence (AAAI) 2024, 2025
- ACM Conference on Computer and Communications Security (CCS) 2023, 2024, 2025
- Privacy Enhancing Technologies Symposium (PoPETs) 2023, 2024, 2025, 2027
  - *Recognized as a distinguished editor/top reviewer in 2024 and 2025*
- ACM Workshop on Artificial Intelligence and Security (AISec 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, 2025, 2026
  - *–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, Winter '26)
- Undergraduate Course: Cryptography for Digital Privacy (Fall '24, Fall '25)
- Undergraduate Course: Formal Systems and Logic in Computing Science (Fall '25)
- Undergraduate Course: Machine Learning (Winter '24)

**Guest Lecturer** Edmonton, Alberta
*University of Alberta* *2024-present*

- AI Everywhere (Winter '25, Fall '25)
  Lecture Topic: Artificial Intelligence and Privacy

- Computing Science Honours Seminar Course (Fall '24)
  Lecture Topic: Privacy Enhanced Data Science

**Guest Lecturer** Waterloo, Ontario
*University of Waterloo* *2017, 2021, 2024*

- Privacy, Cryptography, Network and Data Security (Spring '24)
  Lecture Topic: Network Security and Privacy

- Computer Security and Privacy (Winter '21)
  Lecture Topic: Ethics

- Computer Security and Privacy (Winter '21)
  Lecture Topic: Address Resolution Protocol (ARP) Cache Poisoning Attacks

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

**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, Computer Security and Privacy, Designing Functional Programs

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

- Discrete Structures and Programming, Critical Thinking, Linear Algebra, Introduction to Logic

## Supervision and Training of Highly Qualified Personnel

**PhD** Edmonton, Alberta
*University of Alberta*

- Afari Darfoor (2025 - Ongoing), co-advised with Patrick Pilarski, *Privacy and Bionic Limbs*
- Rabeya Bosri, (2026 - Ongoing), *Privacy in Practice*

**Masters of Science** Edmonton, Alberta
*University of Alberta*

- Gwen Delos Santos (2026 - Ongoing), co-advised with Michael Bowling
- Sara Jerin Prithila (2026 - Ongoing)
- Miriam Bakija (2025 - Ongoing)
- Samuel Feldman (2025 - Ongoing), *Applied Cryptography*
- Afrida Hossain (2025 - Ongoing), *Privacy, Software Design, and Artificial Intelligence*
- Rabeya Bosri (MSc. 2026), *Contextualizing Trade-offs: The Interplay of Privacy,Fairness, and Robustness in High-Stakes Automatic Decision Systems*
- Afari Darfoor (MSc. 2025), *Identifying Privacy Threat Vectors in AI-Enhanced Bionic Devices*

**Undergraduate Research Assistants** Edmonton, Alberta
*University of Alberta*

- Sasha Dudiy (2025, 2026), *Privacy Problems in Theory versus Media, Blackout Resistant Comm.*
- Gwen Delos Santos (2025), *Privacy and Reinforcement Learning*
- Qiantong Guo (2025), *Privacy Problems in Theory versus Media*
- Naone Kim (2025), *Privacy Problems in Theory versus Media*
- Khoi Le (2025), *Privacy Problems in Theory versus Media*
- Lina Saha (2025), *Privacy Problems in Theory versus Media*
- Castor Shem (2025), *Privacy Problems in Theory versus Media*
- Jialiang Yan (2024), *Mobile Privacy Notices Effectiveness*

**Selected Student Awards and Outcomes**
*achieved by students under my supervision*

- **Sasha Dudiy (2026)**
  *NSERC Undergraduate Student Research Award*
- **Gwen Delos Santos (2026)**
  *Honourable mention for the 2026 CRA Outstanding Undergraduate Researcher Award*
- **Samuel Feldman (2025)**
  *Alberta Graduate Excellence Scholarship (AGES) recognizes outstanding academic achievement of students pursuing graduate studies in Alberta with a value of $12,000*
- **Jialiang Yan (2025)**
  *Honourable mention for the 2025 CRA Outstanding Undergraduate Researcher Award*
- **Rabeya Bosri (2024)**
  *Alberta Graduate Excellence Scholarship (AGES) recognizes outstanding academic achievement of students pursuing graduate studies in Alberta with a value of $12,000*
- **Jialiang Yan (2024)**
  *Full summer salary from the competitive University of Alberta undergraduate research initiative (URI), which only funded approximately 20% of applicants*

## Community Service and Outreach

**Youth Outreach**
*Focus on technology and entrepreneurial skills*

- **Edmonton Public School Board Student AI Conference** Edmonton, Alberta
  *Keynote: "AI Could, but Should I"* *2026*
- **Telus World of Science AI Summit** Edmonton, Alberta
  *Presentation: "The (Not So Secret) Days of Data"* *2026*
- **Edmonton Public School Board Student AI Conference** Edmonton, Alberta
  *Presentation: "AI Found a Secret, and Used it Badly"* *2025*
- **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*

- **Privacy in the Modern Digital World Panel** — Edonton, Alberta
  *Speaking on privacy at the local chapter of women in cybersecurity (WiCys)* — *2025*
- **Demystifying Grad School Workshop, Faculty Panel** — Edmonton, Alberta
  *Panelist for discussion with undergraduates about grad school* — *2023, 2024, 2025*
- **Diversity in Engineering/HackED Hackathon 2025** — Edmonton, Alberta
  *Judge* — *2025*
- **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**

- "Alberta agencies work to educate public amid rise of online child sexual exploitation", CBC News. 2025. https://www.cbc.ca/news/canada/edmonton/alberta-education-online-child-sexual-exploitation-1.7438866
- "Bailey Kacsmar, PhD Candidate at University of Waterloo Interview Series", Unit.Ai Interview Series. 2023. https://www.unite.ai/bailey-kacsmar-phd-candidate-at-university-of-waterloo-interview-series/