Thomas Humphries

200 University Ave W
Waterloo, Ontario
N2L 3G1

thomas.humphries@uwaterloo.ca
cs.uwaterloo.ca/~t3humphr/

Research Interests
Deployable systems for AI and data science with meaningful privacy guarantees.
Utilizing: Evolutionary Algorithms, Differential Privacy, Secure Computation, and Privacy Auditing.

Education

Post-Secondary Education

- **Doctor of Philosophy in Computer Science** — University of Waterloo, Canada
  Supervisor: Florian Kerschbaum — *Expected 2026*
- **Master of Mathematics in Computer Science** — University of Waterloo, Canada
  MMath Thesis Program - Supervisor: Florian Kerschbaum — *2021*
  - Thesis: Differentially Private Simple Genetic Algorithms
- **Bachelor of Science (Hons)** — Brandon University, Canada
  Mathematics Major, Computer Science Major — *2019*

Co-Curricular Professional Development

- **Certificate in University Teaching** — University of Waterloo, Canada
  Through the University of Waterloo's Centre for Teaching Excellence — *Expected 2026*
- **Fundamentals of University Teaching Certification** — University of Waterloo, Canada
  Through the University of Waterloo's Centre for Teaching Excellence — *2023*

Publications and Research Talks

Conference Papers

*denotes equal contribution

- Abdulrahman Diaa, **Thomas Humphries**, Florian Kerschbaum (2025). "FastLloyd: Federated, Accurate, Secure, and Tunable k-Means Clustering with Differential Privacy". *34th USENIX Security Symposium (USENIX Security 25)*, pp. 2733–2752. [link to paper].
- Abdulrahman Diaa*, Lucas Fenaux*, Thomas Humphries*, Marian Dietz, Faezeh Ebrahimianghazani, Bailey Kacsmar, Xinda Li, Nils Lukas, Rasoul Akhavan Mahdavi, Simon Oya, Ehsan Amjadian, Florian Kerschbaum (2024). "Fast and Private Inference of Deep Neural Networks by Co-designing Activation Functions". *33rd USENIX Security Symposium (USENIX Security 24)*, pp. 2191–2208. [link to paper].
- Rasoul Akhavan Mahdavi, Nils Lukas, Faezeh Ebrahimianghazani, **Thomas Humphries**, Bailey Kacsmar, John Premkumar, Xinda Li, Simon Oya, Ehsan Amjadian, Florian Kerschbaum (2024). "PEPSI: Practically Efficient Private Set Intersection in the Unbalanced Setting". *33rd USENIX Security Symposium (USENIX Security 24)*, pp. 6453–6470. [link to paper].

DRAFT

- Lucas Fenaux, **Thomas Humphries**, Florian Kerschbaum (2023). "Gaggle: Genetic Algorithms on the GPU using PyTorch". *Proceedings of the Companion Conference on Genetic and Evolutionary Computation (GECCO '23 Companion)*, pp. 2358–2361. [link to paper].

- **Thomas Humphries**, Florian Kerschbaum (2023). "Differentially Private Simple Genetic Algorithms". *Proceedings on Privacy Enhancing Technologies (PoPETs)*, pp. 540–558. [link to paper].

- **Thomas Humphries**, Simon Oya, Lindsey Tulloch, Matthew Rafuse, Ian Goldberg, Urs Hengartner, Florian Kerschbaum (2023). "Investigating Membership Inference Attacks under Data Dependencies". *IEEE Computer Security Foundations Symposium (CSF)*, pp. 473–488. [link to paper].

- Ashraf M. Abdelbar, **Thomas Humphries**, Jesús Guillermo Falcón-Cardona, Carlos A. Coello Coello (2022). "An Extension of the IMOACOR Algorithm Based on Layer-Set Selection". *Swarm Intelligence: 13th International Conference (ANTS)*, pp. 266–274. [link to paper].

- Thomas Humphries*, Rasoul Akhavan Mahdavi*, Shannon Veitch*, Florian Kerschbaum (2022). "Selective MPC: Distributed Computation of Differentially Private Key-Value Statistics". *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pp. 1459–1472. [link to paper].

- Miti Mazmudar, **Thomas Humphries**, Jiaxiang Liu, Matthew Rafuse, Xi He (2022). "Cache Me If You Can: Accuracy-Aware Inference Engine for Differentially Private Data Exploration". *Proceedings of the VLDB Endowment*, pp. 574–586. [link to paper].

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

Journal Articles

- Chenkuan Li, Changpin Li, **Thomas Humphries**, Hunter Plowman (2019). "Remarks on the Generalized Fractional Laplacian Operator". *Mathematics*. [link to paper].

- Chenkuan Li, **Thomas Humphries**, Hunter Plowman (2018). "Solutions to Abel's Integral Equations in Distributions". *Axioms*. [link to paper].

Under Review

- Matthew Y. R. Yang, **Thomas Humphries**, and Florian Kerschbaum, Improved Accuracy vs. Privacy Trade-off in Perturbed Nearest Neighbour Searches. Under Review.

Invited Talks

- Cache Me If You Can: Accuracy-Aware Inference Engine for DP Data Exploration (January 2024). *Snowflake*.

- Investigating Membership Inference Attacks under Data Dependencies (November 2023). *Math Research Days - Research Spotlight*, University of Waterloo.

- Differentially Private Learning Does Not Bound Membership Inference (April 2021). *SPRING lab at EPFL*.

DRAFT

Poster Presentations

- Abdulrahman Diaa, **Thomas Humphries**, Florian Kerschbaum (October 2025). FastLloyd: Federated, Accurate, Secure, and Tunable k-Means Clustering with Differential Privacy. UWaterloo CPI Annual Conference (best poster award).
- **Thomas Humphries**, Santiago Zanella-Béguelin, and Lukas Wutschitz (October 2024). Generating Private Synthetic Text Data without Fine-Tuning. UWaterloo CPI Annual Conference and Microsoft Internship Poster Event.
- **Thomas Humphries** (November 2023). Cache Me If You Can: Accuracy-Aware Inference Engine for DP Data Exploration. UWaterloo CPI Annual Conference and Math Innovation Research Days.
- **Thomas Humphries** (October 2021). Is Differential Privacy the Right Defence against Membership Inference Attacks? UWaterloo CPI Annual Conference: Poster Session, Online.
- Miti Mazmudar, **Thomas Humphries**, Matthew Rafuse, Xi He (November 2020). Cache Me If You Can: Accuracy-Aware Inference Engine for DP Data Exploration. TPDP Workshop 2020, Online.
- **Thomas Humphries** and Hunter Plowman (June 2018). Fractional Calculus. Prairie Discrete Math Workshop, Brandon, MB.

Honours & Awards

Microsoft Research Redmond Azure Credit Award ($4,000)	2025-2026
Queen Elizabeth II Scholarship in Science & Technology ($15,000)	2025-2026
President's Graduate Scholarship ($43,333), University of Waterloo	2020-2021, 2022-2026
Canada Graduate Scholarship - Doctoral (CGS D) award ($35,000), NSERC	2024-2025
Postgraduate Scholarship - Doctoral (PGS D) award ($43,000), NSERC	2022-2024
David R. Cheriton Graduate Scholarship ($40,000), University of Waterloo	2019-2021, 2022-2024
QNX Graduate Scholarship ($6,667), University of Waterloo	2023-2024
Alexander Graham Bell Canada Graduate Scholarship (CGS M) ($17,500), NSERC	2020-2021
Mathematics Domestic Masters Scholarship ($8,000), University of Waterloo	2019, 2021
Inducted into the Brandon University Honour Society, Brandon University	2019
Certificate of Honourable Mention for the Silver Medal in Computer Science, Brandon University	2019
Placed on the Dean's Honour List, Brandon University	2015-2019
Inducted into the President's Honour Society, Brandon University	2015-2019
Peter D. and Una B. Cameron Memorial Scholarship ($2,135), Brandon University	2019
Roland Kitchen Scholarship in Mathematics ($9,815), Brandon University	2017-2019
Undergraduate Student Research Award ($4,500), NSERC	2018
General Proficiency Scholarship in First Year Science ($300), Brandon University	2016
Lois B. Hunter Memorial Scholarship ($1,200), Brandon University	2016
Brandon University Board of Governors Entrance Scholarship ($2,000), Brandon University	2015
Governor General of Canada Academic Medal (Bronze)	2015

Academic Service

Program Committee

- ACM Conference on Computer and Communications Security (CCS) 2026

DRAFT

- ACM Workshop on Artificial Intelligence and Security (AISec) 2025
- Theory and Practice of Differential Privacy (TPDP) Workshop 2025

Reviewer

- International Conference on Learning Representations (ICLR) 2023
- Conference on Neural Information Processing Systems (NeurIPS) 2023
- Privacy Enhancing Technologies Symposium (PoPETs) (External Reviewer) 2021, 2022, 2023

Artifact Committee

- ACM Conference on Computer and Communications Security (CCS) 2023

Teaching Experience

Sessional Instructor Waterloo, Ontario
University of Waterloo *2023*

Inaugural co-instructor for a new fourth-year course at the University of Waterloo. Designed course materials, delivered lectures, created assignments and exams with hands-on programming components, managed course logistics, led TA meetings, and conducted office hours.

- CS489/689: Privacy, Cryptography, Network, and Data Security (Winter ’23)

Undergraduate Research Assistant Supervision Waterloo, Ontario
University of Waterloo *2021 - present*

Led the research project direction, delivered background mini lectures, mentored students on research practices, and provided on-demand problem-solving support.

- Evan Qi (URA)
- Steven Lee (URA)
- Jin Yang Liu (URA)
- Dan Li (URA and URF)
- Haoyan Ni (URA)
- Matthew Yang (URF)
- Jiaxiang Liu (URA with Xi He)
- Tim Li (URF with Xi He)

Teaching Assistant Waterloo, Ontario
University of Waterloo *2020 - 2024*

Designed and delivered course assignments, conducted office hours, facilitated online questions, and evaluated student work.

- CS459/659: Privacy, Cryptography, Network, and Data Security (Winter ’21)
- CS458/658: Computer Security and Privacy (Fall ’20, Winter ’21)

Lab Assistant and Marker Brandon, Manitoba
Brandon University *2016 - 2019*

Supervised labs and tests, answered student questions, and graded assignments and exams.

- Computer Science II (2017)
- Calculus I (2017, 2018)
- Intro to Statistics (2016, 2017, 2018)
- Intro to Statistical Inference (2016, 2017, 2019)
- Applied Statistics (2019)

DRAFT

Math Walk-In Group Tutoring Brandon, Manitoba
Brandon University *2016 - 2019*

Provided walk-in assistance through the Academic Skills Centre for students in first and second-year mathematics courses. Answered questions and explained concepts in a group setting, helping students with homework, exam preparation, and course material comprehension.

Peer Tutor Brandon, Manitoba
Brandon University *2018*

Delivered supplemental instruction through group tutorial sessions for undergraduate students.

- Calculus I (2018)
- Computer Science I (2018)

Professional Experience

Graduate Research Assistant 2019-Present
Cryptography, Security, and Privacy (CrySP) Lab, University of Waterloo *Supervisor: Dr. Florian Kerschbaum*

- Conducted research towards my dissertation.
- Led group research projects in collaboration with the Royal Bank of Canada and Snowflake.
- Managed lab social media accounts, posting videos of talks and highlighting conference presentations.
- Coordinated lab seating assignments and handled general maintenance inquiries.

Research Intern 2025
Microsoft Research, Redmond WA *Supervisor: Dr. Zinan Lin*

- Worked on diagnosing low recall in private evolution for synthetic data generation.
- Identified algorithmic bottlenecks and proposed solutions.
- Collaboration ongoing to publish results.

Research Intern 2024
Azure Research, Microsoft Research, Cambridge UK *Supervisor: Dr. Santiago Zanella-Béguelin*

- Worked on improving differentially private synthetic text data generation.
- Identified reproducibility and diversity issues in private evolution algorithm.
- Designed initial prototypes to improve diversity issues.

Research Assistant I 2019
Department of Mathematics and Computer Science, Brandon University *Supervisor: Dr. Shahla Nasserasr*

- Conducted theoretical and computational analysis in matrix algebra using Sage.
- Summer position after graduation.

Leadership and Community Involvement

Volunteer Board Member 2020-2024
KW Musical Productions *Waterloo, ON*

- Served as director at large, attending regular board meetings and supporting organizational operations.

DRAFT

- Led multiple technology infrastructure projects to modernize services and reduce organizational costs.

Founder and Operator 2013-2019
Fusion Audio Visual *Elkhorn, MB*

- Founded and operated company providing sound and lighting services for local events.
- Managed all business operations including team leadership for multiple simultaneous events.
- Provided consulting, installation of technical equipment, and end user education for venue renovations.

Volunteer Board Member 2015-2019
Virden Auditorium Theatre Board *Virden, MB*

- Attended regular board meetings and managed technical department operations.
- Completed facility renovations and streamlined theatre operations.

Student Leader 2019
Student Leader Program *Brandon University*

- Completed 20 volunteer hours supporting campus events and providing math tutoring.

Volunteer 2018
Brandon High School Computer Competition and Fair *Brandon, MB*

- Assisted with competition logistics and provided project feedback to student participants.

DRAFT