



Mahdi Haghifam


✉ haghifam.mahdi@gmail.com  mhaghifam.github.io/mahdihaghifam/

Education

University of Toronto and Vector Institute 

Sept 2017 – May 2023

Ph.D in Electrical and Computer Engineering Department.

- **Advisor:** Prof. **Daniel Roy**
- **Dissertation:** Information-Theoretic Measures of Generalization in Machine Learning ([link](#)) 

Sharif University of Technology

Sept. 2010 – Aug. 2016

B.Sc and M.Sc in Electrical Engineering Department.

Employment

Research Assistant Professor, Toyota Technological Institute at Chicago (TTIC), Chicago. [Information about the role.](#)  *Sept. 25–Present*

Distinguished Postdoctoral Fellow, Khoury College of Computer Science, Northeastern University, Boston. [Information about the role.](#)  *Sept. 23–Aug. 25*

Advisor: Prof. **Jonathan Ullman** and Prof. **Adam Smith**.

Research Intern, Google DeepMind, California, U.S. *Sept. 22–Dec. 22*

Research Intern, ServiceNow Research, Toronto, Canada *Nov. 20–Mar. 21*

Graduate Student Researcher, Vector Institute for AI, Toronto, Canada *Mar. 20–Aug. 23*

Research Assistant, University of Toronto & Vector Institute, Toronto, Canada *Sept. 17–Aug. 23*

Honors & Awards

Simons Institute (UC Berkeley) Research Fellowship Award *2025*

Best Paper Award at ICML 2024 (top 10 of 10,000 submissions) *2024*

Khoury College of Computer Sciences Distinguished Postdoctoral Fellowships *2023*

Czeslaw and Irene Klawe Scholarship from University of Toronto *2023*

Henderson and Bassett Research Fellowship from University of Toronto *2023*

Viola Carless Smith Research Fellowship from University of Toronto *2023*

Top 8% of reviewers at NeurIPS *2021, 2023*

MITACS Accelerate Fellowship *2019, 2021*

Publications

The Sample Complexity of Membership Inference and Privacy Auditing

M. Haghifam, A. Smith, J. Ullman ($\alpha\beta$)

[arXiv:2508.19458](#)  (Preprint, 2025).

On the Traceability in ℓ_p Stochastic Convex Optimization

S. Voito vych*, **M. Haghifam***, I. Attias, G. K. Dziugaite, R. Livni, D. M. Roy

NeurIPS 2025 ([Spotlight](#), < 3% of submissions). [arXiv:2502.17384](#) .

Private Geometric Median

M. Haghifam, T. Steinke, J. Ullman ($\alpha\beta$)

NeurIPS 2024. [arXiv:2406.07407](#) .

Information Complexity of Stochastic Convex Optimization: Applications to Generalization and Memorization

I. Attias, G. K. Dziugaite, **M. Haghifam**, R. Livni, D. M. Roy ($\alpha\beta$)

ICML 2024. [Best Paper Award \(Top 10 of 10,000 submissions\)](#). [arXiv:2402.09327](#) .

Faster Differentially Private Convex Optimization via Second-Order Methods

A. Ganesh, **M. Haghifam**, T. Steinke, A. Thakurta ($\alpha\beta$)

NeurIPS 2023. [arXiv:2305.13209](#) [🔗](#).

Why Is Public Pretraining Necessary for Private Model Training?

A. Ganesh, **M. Haghifam**, M. Nasr, S. Oh, T. Steinke, O. Thakkar, A. Thakurta, L. Wang ($\alpha\beta$)

ICML 2023. [arXiv:2302.09483](#) [🔗](#).

Limitations of Information-Theoretic Generalization Bounds for Gradient Descent Methods in Stochastic Convex Optimization

M. Haghifam*, B. Rodríguez-Gálvez*, R. Thobaben, M. Skoglund, D. M. Roy, G. K. Dziugaite

ALT 2023. [arXiv:2212.13556](#) [🔗](#).

Privacy-Preserving and Approximately Truthful Local Electricity Markets: A Differentially Private VCG Mechanism

M. Hoseinpour, M. Hoseinpour, **M. Haghifam**, M. R. Haghifam

IEEE Transactions on Smart Grid, 2023. [IEEE Xplore \(10201886\)](#) [🔗](#).

Understanding Generalization via Leave-One-Out Conditional Mutual Information

M. Haghifam, S. Moran, D. M. Roy, G. K. Dziugaite

ISIT 2022. [arXiv:2206.14800](#) [🔗](#).

Towards a Unified Information–Theoretic Framework for Generalization

M. Haghifam, G. K. Dziugaite, S. Moran, D. M. Roy

NeurIPS 2021 ([Spotlight](#), < 3% of submissions). [arXiv:2111.05275](#) [🔗](#).

Information-Theoretic Generalization Bounds for Stochastic Gradient Descent

G. Neu, G. K. Dziugaite*, **M. Haghifam***, D. M. Roy*

COLT 2021. [arXiv:2102.00931](#) [🔗](#).

On Streaming Codes With Unequal Error Protection

M. Haghifam*, M. N. Krishnan*, A. Khisti, X. Zhu, W.-T. Tan, J. Apostolopoulos

IEEE Journal on Selected Areas in Information Theory, 2021. [PDF](#) [🔗](#).

Sequential Classification with Empirically Observed Statistics

M. Haghifam, V. Y. F. Tan, A. Khisti

IEEE Transactions on Information Theory, 2021. [PDF](#) [🔗](#).

Sharpened Generalization Bounds based on Conditional Mutual Information and an Application to Noisy, Iterative Algorithms

M. Haghifam, J. Negrea, A. Khisti, D. M. Roy, G. K. Dziugaite

NeurIPS 2020. [arXiv:2004.12983](#) [🔗](#).

Information-Theoretic Generalization Bounds for SGLD via Data-Dependent Estimates

J. Negrea*, **M. Haghifam***, G. K. Dziugaite, A. Khisti, D. M. Roy

NeurIPS 2019. [arXiv:1911.02151](#) [🔗](#).

Joint Sum Rate And Error Probability Optimization: Finite Blocklength Analysis

M. Haghifam, M. Robat Mili, B. Makki, M. Nasiri-Kenari, T. Svensson

IEEE Wireless Communications Letters, 2017. [PDF](#) [🔗](#).

Industry Research Experience

Research Intern.

Google DeepMind. Mentor: **Thomas Steinke**

Mountain View, CA
Sept. 2022 – Dec. 2022

- Conducted research on improving the runtime of differentially private optimization.
- Resulted in publications in NeurIPS2023 ([link](#)) [🔗](#).

Research Intern.

ServiceNow Research [🔗](#) Mentor: **Gintare Karolina Dziugaite**

Toronto, ON
Nov. 2020 – March 2021

- Studied the connections between different generalization approaches in ML.
- Resulted in publication in NeurIPS 2021 (spotlight) ([link](#) [↗](#)).

Research Intern.

ServiceNow Research [↗](#) Mentor: **Gintare Karolina Dziugaite**

Toronto, ON

Feb. 2019 – May. 2019

- Proposed a new analytical technique that measures algorithmic stability on random subsets of data, creating a tighter and more empirically accurate connection between the training process and real-world performance.
- Resulted in publication in NeurIPS 2019 ([link](#) [↗](#)).

Selected Talks

Apple – Apple ML Privacy Team	<i>Aug. 2025</i>
UCSD – Information Theory and Applications Workshop	<i>Feb. 2025</i>
Northwestern and TTIC – Junior Theorists Workshop	<i>Dec. 2024</i>
University of Oslo – Integreat Center	<i>Sept. 2024</i>
Google – Statistical Learning Theory	<i>July 2024</i>
Google DeepMind – Optimization Group	<i>May 2024</i>
TOC4Fairness Seminar – Online Seminar	<i>May 2024</i>
Northeastern – Theory Lunch	<i>Mar. 2024</i>
MIT – Tomaso Poggio’s Research Group	<i>Nov. 2023</i>
Boston-Area Data Privacy Seminar	<i>Oct. 2023</i>
McMaster University – Department of Computing and Software	<i>June 2023</i>
University of Minnesota – Network and Information Sciences Seminar Series	<i>Mar. 2023</i>
Harvard University – Flavio Calmon’s Research Group	<i>Mar. 2023</i>
Google – Privacy in Machine Learning Seminar	<i>Dec. 2022</i>
Google – Information Theory Seminar	<i>Sept. 2022</i>
Canadian Workshop on Information Theory – Ottawa	<i>June 2022</i>
Microsoft Research – Montreal	<i>Jan. 2022</i>
IIMAS, Mexico – Information Theory, Machine Learning and Statistics Seminar	<i>Apr. 2021</i>

Service

Area Chair

- Conference on Algorithmic Learning Theory (ALT) 2026.
- Conference on Secure and Trustworthy Machine Learning (SaTML) 2024, 2026.
- Theory and Practice of Differential Privacy Workshop 2024, 2025.
- Eastern European Machine Learning Summer School 2022.

Conference Reviewer: Conference on Neural Information Processing Systems (**NeurIPS**), International Conference on Machine Learning (**ICML**), International Conference on Learning Representations (**ICLR**), Conference on Learning Theory (**COLT**), International Symposium on Information Theory (**ISIT**).

Journal Referee: IEEE Transactions on Signal Processing. Journal of Machine Learning Research, Transactions on Machine Learning Research.

Programming Skills


Languages: C,C++, Python (Scipy, Numpy), TensorFlow, JAX, PyTorch

Leadership & Extra-Curricular Activities

Organizer — Charles River Privacy Day, Boston, MA	<i>2024</i>
Co-organizer — Boston Area Differential Privacy Seminar	<i>2023–2024</i>
◦ Coordinated speakers and scheduling; co-led outreach and logistics across Boston-area universities.	

Mentor — Graduate Application Assistance Program (GAAP), University of Toronto

2020–2024

- Volunteer mentoring on research statements, CVs, and graduate school applications. ([program link](#)) 

Executive Member — Bahar Charity Group, University of Toronto

Aug. 2020 – Aug. 2023

- Helped organize fundraising and student-support initiatives. ([baharcharity.com](#)) 