

# Mahdi Haghifam

## Curriculum Vitae

✉ [m.haghifam@northeastern.edu](mailto:m.haghifam@northeastern.edu)

📄 [mhaghifam.github.io/mahdihaghifam/](https://mhaghifam.github.io/mahdihaghifam/)

### Employment

- Sept. 25–Present **Research Assistant Professor at Toyota Technological Institute at Chicago (TTIC).**
- Sept. 23–Aug. 25 **Distinguished Research Fellow, Khoury College of Computer Science, Northeastern.**
- Working on Trustworthy ML and Foundation of ML.
- Hosts: Prof. Jonathan Ullman and Prof. Adam Smith.

### Education

- 2017–2023 **Ph.D, University of Toronto and Vector Institute**, Toronto, Canada.
- Electrical and Computer Engineering Department.
- Dissertation Topic: “Information-Theoretic Measures of Generalization in Machine Learning”
- Advisor: Prof. Daniel M. Roy
- 2014–2016 **M.Sc, Sharif University of Technology**, Tehran, Iran.
- 2010–2014 **B.Sc, Sharif University of Technology**, Tehran, Iran.

### Honors and Awards

- 2025 Simons Institute (UC Berkeley) Research Fellowship Award
- 2024 **Best Paper Award at ICML 2024** (top 10 of 10,000 submissions)
- 2023 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
- 2021,2023 Top 8% of reviewers at NeurIPS

### Past Employment

- Sept. 17–Aug. 23 **Research Assistant, University of Toronto and Vector Institute, Canada.**
- Aug. 22–Dec. 22 **Research Intern, Google Brain, California, U.S.**
- Mentors: Dr. Thomas Steinke and Dr. Abhradeep Guha Thakurta
- Nov. 20–Mar. 21 **Research Intern, Element AI-Service Now, Toronto, Canada.**
- Mentor: Dr. Gintare Karolina Dziugaite
- Mar. 20–May 20 **Visiting Researcher, Institute for Advanced Studies, Princeton, U.S.**
- Mar. 20–Present **Graduate Researcher, Vector Institute for AI, Toronto, Canada.**
- Feb. 19–May 19 **Research Intern, Element AI, Toronto, Canada.**
- Mentor: Dr. Gintare Karolina Dziugaite

## Publications

\*: equal-contribution.  $\alpha\beta$ : alphabetic authorship [760 citations, h-index 14, i-10 index 17 ]

- Conference
- **M. Haghifam**, A. Smith, J. Ullman ( $\alpha\beta$ ) “On the Sample Complexity of Membership Inference”, In Submission
  - S. Voitovich\*, **M. Haghifam**\*, I. Attias, G. K. Dziugaite, R. Livni, D. M. Roy “On the Traceability in  $\ell_p$  Stochastic Convex Optimization ”, In Submission (Available on Arxiv)
  - **M. Haghifam**, T. Steinke, J. Ullman ( $\alpha\beta$ ) “Private Geometric Median”, **NeurIPS** 2024.
  - I. Attias, G. K. Dziugaite, **M. Haghifam**, R. Livni, D. M. Roy ( $\alpha\beta$ ) “Information Complexity of Stochastic Convex Optimization: Applications to Generalization and Memorization”, **ICML** 2024. (**Best Paper Award (Top 10 of 10,000 submissions)**).
  - A. Ganesh, **M. Haghifam**, T. Steinke, A. Thakurta ( $\alpha\beta$ ) “Faster Differentially Private Convex Optimization via Second-Order Methods”, **NeurIPS** 2023.
  - A. Ganesh, **M. Haghifam**, M. Nasr, S. Oh, T. Steinke, O. Thakkar, A. Thakurta, L. Wang ( $\alpha\beta$ ) “ Why Is Public Pretraining Necessary for Private Model Training?”, **ICML** 2023.
  - **M. Haghifam**\*, B. Rodríguez-Gálvez\*, R. Thobaben, M. Skoglund, D. M. Roy, G. K. Dziugaite “Limitations of Information-Theoretic Generalization Bounds for Gradient Descent Methods in Stochastic Convex Optimization”, **ALT** 2023.
  - **M. Haghifam**, G. K. Dziugaite, S. Moran, D. M. Roy “Understanding Generalization via Leave-One-Out Conditional Mutual Information”, **ISIT** 2022.
  - **M. Haghifam**, S. Moran, D. M. Roy, G. K. Dziugaite “Towards a Unified Information–Theoretic Framework for Generalization”, **NeurIPS** 2021 (**Spotlight, <3% of submissions**).
  - G. Neu, G. K. Dziugaite, **M. Haghifam**, D. M. Roy “Information-Theoretic Generalization Bounds for Stochastic Gradient Descent”, **COLT** 2021.
  - **M. Haghifam**, J. Negrea, A. Khisti, D. M. Roy , G. K. Dziugaite “Sharpened Generalization Bounds based on Conditional Mutual Information and an Application to Noisy, Iterative Algorithms”, **NeurIPS** 2020.
  - J. Negrea\*, **M. Haghifam**\*, G. K. Dziugaite, A. Khisti, D. M. Roy “Information-Theoretic Generalization Bounds for SGLD via Data-Dependent Estimates”, **NeurIPS** 2019.

- Journal**
- M. Hoseinpour, M. Hoseinpour, **M. Haghifam**, M. Haghifam, "Privacy-Preserving and Approximately Truthful Local Electricity Markets: A Differentially Private VCG Mechanism", IEEE Transactions on Smart Grid.
  - **M. Haghifam**<sup>\*</sup>, M. N. Krishnan<sup>\*</sup>, A. Khisti, X. Zhu, W. Dan and J. Apostolopoulos, "On Streaming Codes With Unequal Error Protection", IEEE Journal on Selected Areas in Information Theory.
  - **M. Haghifam**, V. Y. F. Tan, and A. Khisti, "Sequential Classification with Empirically Observed Statistics", IEEE Transactions on Information Theory.
  - **M. Haghifam**, M. Robat Mili, B. Makki, M. Nasiri-Kenari, T. Svensson, "Joint Sum Rate And Error Probability Optimization: Finite Blocklength Analysis", IEEE Wireless Communications.

---

## Computer Skills

Programming C,C++, Python (Scipy, Numpy), TensorFlow, JAX, PyTorch  
Link to the Github repo

---

## Selected Talks

Apple – Apple ML Privacy Team Research Talk (August 25)  
UCSD – Information Theory and Applications Workshop (February 25)  
Chicago – Junior Theorists Workshop (December 24)  
University of Oslo – Integreat Center (September 24)  
Google – Statistical Learning Theory (July 24)  
Google DeepMind – Optimization Group (May 24)  
TOC4Fairness Seminar – Online Seminar (May 24)  
Northeastern – Theory Lunch (March 24)  
MIT – Tomaso Poggio's Research Group (November 23)  
Boston-Area Data Privacy Seminar (October 23)  
McMaster University – Department of Computing and Software (June 23)  
University of Minnesota – Network and Information Sciences Seminar Series (March 23)  
Harvard University – Flavio Calmon's Research Group (March 23)  
Google – Privacy in Machine Learning Seminar (December 22)  
Google – Information Theory Seminar (September 22)  
Canadian Workshop on Information Theory – Ottawa (June 22)  
Microsoft Research – Montreal (January 22)  
IIMAS, Mexico – Information Theory, Machine Learning and Statistics Seminar (April 21)

---

## Service

- 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**), Conference on Secure and Trustworthy Machine Learning (**SaTML**), International Symposium on Information Theory (**ISIT**)
- Journal Referee IEEE Transactions on Signal Processing, IEEE Transactions on Information Theory, Journal of Machine Learning Research, Transactions on Machine Learning Research.
- Area Chair
- Conference on Secure and Trustworthy Machine Learning (SaTML) 2024,2026.
  - Theory and Practice of Differential Privacy Workshop 2024,2025.
  - Information-Theoretic Methods for Rigorous, Responsible, and Reliable Machine Learning workshop in ICML 2021.
  - Eastern European Machine Learning Summer School 2022.
- Organizer
- Boston Area Differential Privacy Seminar 2023-2024.
  - Charles River Privacy Day 2024.

## Leadership and Extra-Curricular Activities

- Aug. 20–Aug. 23 Executive member of Bahar Charity group at University of Toronto. <https://www.baharcharity.com/>
- 2020-2024 Mentor at Graduate Application Assistance Program at University of Toronto. <https://sites.google.com/view/torontogaap>