

# Mahdi Haghifam

## Curriculum Vitae

✉ [haghifam.mahdi@gmail.com](mailto:haghifam.mahdi@gmail.com)

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

### Research Area

I am broadly interested in theoretical and algorithmic aspects of Machine Learning and Differential Privacy.

### Current Employment

Sept. 23–Present **Distinguished Research Fellow, Khoury College of Computer Science, Northeastern.**

Working on Differential Privacy and Foundation of ML.

Advisors: Prof. Jonathan Ullman, Prof. Hongyang Zhang, and Prof. Adam Smith

### Education

2017–2023 **Ph.D, University of Toronto**, Toronto, Ontario, Canada, August 2023.

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.

Electrical Engineering.

2010–2014 **B.Sc, Sharif University of Technology**, Tehran, Iran.

Electrical Engineering, Major in Communication Systems.

### Past Employment

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

Advisor: Prof. Daniel Roy

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.**

Feb. 19–May 19 **Research Intern, Element AI, Toronto, Canada.**

Mentor: Dr. Gintare Karolina Dziugaite

### Publications

\*: equal-contribution.  $\alpha\beta$ : alphabetic authorship

## Conference

1. A. Ganesh, **M. Haghifam**, T. Steinke, A. Thakurta, ( $\alpha\beta$ ) “Faster Differentially Private Convex Optimization via Second-Order Methods”, NeurIPS 2023
2. 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.
3. **M. Haghifam**<sup>\*</sup>, B. Rodríguez-Gálvez<sup>\*</sup>, 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.
4. **M. Haghifam**, G. K. Dziugaite, S. Moran, D. M. Roy, “Understanding Generalization via Leave-One-Out Conditional Mutual Information”, ISIT 2022.
5. **M. Haghifam**, S. Moran, D. M. Roy, G. K. Dziugaite, “Towards a Unified Information–Theoretic Framework for Generalization”, NeurIPS 2021 (Spotlight, <3% of submissions).
6. G. Neu, G. K. Dziugaite, **M. Haghifam**, D. M. Roy, “Information-Theoretic Generalization Bounds for Stochastic Gradient Descent”, COLT 2021.
7. **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.
8. J. Negrea<sup>\*</sup>, **M. Haghifam**<sup>\*</sup>, G. K. Dziugaite, A. Khisti, D. M. Roy, “Information-Theoretic Generalization Bounds for SGLD via Data-Dependent Estimates”, NeurIPS 2019.

## Journal

1. 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.
2. **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.
3. **M. Haghifam**, V. Y. F. Tan, and A. Khisti, “Sequential Classification with Empirically Observed Statistics”, IEEE Transactions on Information Theory.
4. **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.

---

## Honors and Awards

- 2023 Khoury College of Computer Sciences Distinguished Postdoctoral Fellowships
- 2023 Czeslaw and Irene Klawe Scholarship from ECE Department of University of Toronto
- 2023 Henderson and Bassett Research Fellowship from ECE Department of University of Toronto
- 2023 Viola Carless Smith Research Fellowship from ECE Department of University of Toronto
- 2021 Top 8% of reviewers at NeurIPS 2021
- 2021 Doctoral Completion Award from University of Toronto (15,000 CAD)
- 2021 Ewing Rae graduate scholarship from ECE Department of University of Toronto

- 2020–2023 Research grant from the Vector Institute for Artificial Intelligence (36,000 CAD)
- 2019,2021 MITACS Accelerate Fellowship (42,000 CAD)
- 2020 Visiting Graduate Student, Institute for Advanced Study, Princeton, New Jersey
- 2014 Ranked **5th** out of **25,000** in nationwide entrance exams for Master's degree in EE

## Invited Talks

- 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 ISIT(2019–2023), NeurIPS (2021–2023), ICLR (2022–2023), ICML (2023), COLT (2022), Conference on Secure and Trustworthy Machine Learning (2024).
- Journal Referee IEEE Transactions on Signal Processing. IEEE Transactions on Information Theory. Journal of Machine Learning Research. Transactions on Machine Learning Research.
- Area Chair Information-Theoretic Methods for Rigorous, Responsible, and Reliable Machine Learning workshop in ICML 2021. Eastern European Machine Learning Summer School 2022. Conference on Secure and Trustworthy Machine Learning (SaTML) 2024.
- Organizer Boston-Area DP Seminar.

## Leadership and Extra-Curricular Activities

- Aug. 20–Aug. 23 Executive member of Bahar Charity group at University of Toronto. <https://www.baharcharity.com/>
- 2020-2023 Mentor at Graduate Application Assistance Program at University of Toronto. <https://sites.google.com/view/torontogaap>

## Computer Skills

- Programming C,C++, Python (Scipy, Numpy), TensorFlow, JAX, PyTorch
- Mathematics MATLAB (SIMULINK , CVX), MATHEMATICA, MATHCAD, R