Jonathan Ullman

Curriculum Vitae
March 2025

Address: 623 ISEC, 805 Columbus Ave, Boston, MA
Phone: (609) 865-4466
Email: jullman@ccs.neu.edu
Web: https://jonathan-ullman.github.io/

Research Area

Privacy for machine learning and statistics, and its deep connections to other concepts in trustworthy machine learning such as statistical validity, robustness, cryptography, and fairness.

Education

Doctor of Philosophy in Computer Science **08/2009 – 06/2013**
Harvard University School of Engineering and Applied Science
Thesis Advisor: Salil P. Vadhan

Bachelor of Science and Engineering in Computer Science **08/2004 – 05/2008**
Princeton University
Graduated *magna cum laude*

Employment History

Associate Professor **06/2021 – Current**
Khoury College of Computer and Information Sciences
Northeastern University

Assistant Professor **08/2015 – 06/2021**
Khoury College of Computer and Information Sciences
Northeastern University

Junior Fellow **07/2014 – 07/2015**
Simons Society of Fellows
Host: Rocco Servedio, Columbia University

Postdoctoral Fellow **06/2013 – 06/2014**
Center for Research on Computation and Society
Harvard University

Research Intern **08/2011 – 12/2011**
Microsoft Research SVC
Host: Cynthia Dwork

Honors and Awards

NSF CAREER Award **02/2018**
Project Title: *A Stable Foundation for Trustworth Data Analysis*

Ruth and Joel Spira Outstanding Teacher Award **09/2019**
Awarded annually to a faculty member in the College of Computer Sciences

Apple Research Award **02/2021**
Project Title: *Auditing Differentially Private Machine Learning*

Google Faculty Research Award **02/2018**
Project Title: *Distributed Differential Privacy Beyond Local Protocols*

Publications

Executive Summary

Google Scholar Data (03/2025): 6,202 citations, h-index 42

Manuscripts

[1] Maryam Aliakbarpour, Konstantina Bairaktari, Adam Smith, Marika Swanberg, and Jonathan Ullman. Privacy in metalearning and multitask learning: Modeling and separations. *arXiv preprint arXiv:2412.12374*, 2024.

[2] Audra McMillan, Adam Smith, and Jon Ullman. Instance-optimal differentially private estimation. *arXiv preprint arXiv:2210.15819*, 2022.

Conference and Other Primary Publications (Reverse Chronological Order)

Like most computer scientists, my work is primarily published in competitive conferences, which are typically as selective as top journals. This list includes all primary publications of my work, either conference or journal.

[3] Gautam Kamath, Argyris Mouzakis, Matthew Regehr, Vikrant Singhal, Thomas Steinke, and Jonathan Ullman. A bias-accuracy-privacy trilemma for statistical estimation. *Journal of the American Statistical Association*, pages 1–23, 2025.

[4] Sushant Agarwal, Gautam Kamath, Mahbod Majid, Argyris Mouzakis, Rose Silver, and Jonathan Ullman. Private mean estimation with person-level differential privacy. In *ACM-SIAM Symposium on Discrete Algorithms*, SODA '25, pages 2819–2880. SIAM, 2025.

[5] Mahdi Haghifam, Thomas Steinke, and Jonathan Ullman. Private geometric median. In *Annual Conference on Neural Information Processing Systems*, NeurIPS '24, pages 46254–46293, 2024.

[6] Maryam Aliakbarpour, Konstantina Bairaktari, Gavin Brown, Adam Smith, and Jonathan Ullman. Metalearning with very few samples per task. In *Conference on Learning Theory*, COLT '24. PMLR, 2024.

[7] Naty Peter, Eliad Tsfadia, and Jonathan Ullman. Smooth lower bounds for differentially private algorithms via padding-and-permuting fingerprinting codes. In *Conference on Learning Theory*, COLT '24. PMLR, 2024.

[8] Andrew Lowy, Jonathan Ullman, and Stephen Wright. How to make the gradients small privately: Improved rates for differentially private non-convex optimization. In *International Conference on Machine Learning*, ICML '24. PMLR, 2024.

[9] Jiawen Liu, Weihao Qu, Marco Gaboardi, Deepak Garg, and Jonathan Ullman. Program analysis for adaptive data analysis. In *ACM Conference on Programming Language Design and Implementation*, PLDI '24, 2024. (authors by contribution).

[10] John Abascal, Stanley Wu, Alina Oprea, and Jonathan Ullman. TMI! finetuned models leak private information from their pretraining data. In *Privacy Enhancing Technologies Symposium*, PETS '24, 2024. (authors by contribution).

[11] Harsh Chaudhari, Giorgio Severi, Alina Oprea, and Jonathan Ullman. Chameleon: Increasing label-only membership leakage with adaptive poisoning. In *International Conference on Learning Representations*, ICLR '24, 2024. (authors by contribution).

[12] Maryam Aliakbarpour, Rose Silver, Thomas Stenke, and Jonathan Ullman. Differentially private medians and interior points for non-pathological data. In *ACM Innovcations in Theoretical Computer Science*, ITCS '24, 2024.

[13] Konstantina Bairaktari, Paul Tsela Langton, Huy Nguyen, Niklas Smedemark-Margulies, and Jonathan Ullman. Fair and useful cohort selection. *Transactions on Machine Learning Research*, 2023.

[14] Liudas Panavas, Tarik Crnovrsanin, Jane Lydia Adams, Jonathan Ullman, Ali Sargavad, Melanie Tory, and Cody Dunne. Investigating the visual utility of differentially private scatterplots. *IEEE Transactions on Visualization and Computer Graphics*, pages 1–16, 2023. (authors by contribution).

[15] Konstantina Bairaktari, Guy Blanc, Li-Yang Tan, Jonathan Ullman, and Lydia Zakynthinou. Multitask learning via shared features: Algorithms and hardness. In *Conference on Learning Theory*, COLT '23. PMLR, 2022.

[16] Hilal Asi, Jonathan Ullman, and Lydia Zakynthinou. From robustness to privacy and back. In *International Conference on Machine Learning*, ICML '23. PMLR, 2023.

[17] Matthew Jagielski, Stanley Wu, Alina Oprea, Jonathan Ullman, and Roxana Geambasu. How to combine membership-inference attacks on multiple updated models. In *Privacy Enhancing Technologies Symposium*, PETS '23, 2023.

[18] Harsh Chaudhari, John Abascal, Alina Oprea, Matthew Jagielski, Florian Tramèr, and Jonathan Ullman. SNAP: efficient extraction of private properties with poisoning. In *IEEE Symposium on Security and Privacy*, IEEE S&P '23, pages 1935–1952. IEEE Computer Society, 2023. (authors by contribution).

[19] Gautam Kamath, Argyris Mouzakis, Vikrant Singhal, Thomas Steinke, and Jonathan Ullman. A private and computationally efficient estimator for unbounded gaussians. In *Annual Conference on Learning Theory*, COLT '22, pages 544–572, London, UK, 2022. PMLR.

[20] Gavin Brown, Marco Gaboardi, Adam Smith, Jonathan Ullman, and Lydia Zakynthinou. Covariance-aware private mean estimation without private covariance estimation. In *Annual Conference on Neural and Information Processing Systems*, NeurIPS '21 Spotlight Presentation, 2021.

[21] Terrance Liu, Thomas Steinke, Jonathan Ullman, Giuseppe Vietri, and Zhiwei Steven Wu. Private query release assisted by public data. In *International Conference on Machine Learning*, ICML '21. PMLR, 2020.

[22] Albert Cheu and Jonathan Ullman. The limits of pan privacy and shuffle privacy for learning and estimation. In *ACM Symposium on Theory of Computing*, STOC '21, pages 1081–1094. ACM, 2020.

[23] Albert Cheu, Adam Smith, and Jonathan Ullman. Manipulation attacks in local differential privacy. In *IEEE Security & Privacy*, IEEE S&P '21, San Francisco, CA, USA, 2021. IEEE.

[24] Matthew Jagielski, Jonathan Ullman, and Alina Oprea. Auditing differentially private machine learning: How private is private SGD? In *Annual Conference on Neural and Information Processing Systems*, NeurIPS '20, 2020. (authors by contribution).

[25] Sourav Biswas, Yihe Dong, Gautam Kamath, and Jonathan Ullman. CoinPress: Practical private mean and covariance estimation. In *Annual Conference on Neural and Information Processing Systems*, NeurIPS '20, 2020.

[26] Clément L. Canonne, Gautam Kamath, Audra McMillan, Jonathan Ullman, and Lydia Zakynthinou. Private identity testing for high dimensional distributions. In *Annual Conference on Neural and Information Processing Systems*, NeurIPS '20 Spotlight Presentation, 2020.

[27] Gautam Kamath, Vikrant Singhal, and Jonathan Ullman. Private mean estimation of heavy-tailed distributions. In *Annual Conference on Learning Theory*, COLT '20, pages 2204–2235, Vienna, Austria, 2020. PMLR.

[28] Raef Bassily, Albert Cheu, Shay Moran, Aleksandar Nikolov, Jonathan Ullman, and Zhiwei Steven Wu. Private query release assisted by public data. In *International Conference on Machine Learning*, ICML '20, pages 6066–6074, Vienna, Austria, 2020. PMLR.

[29] Alexander Edmonds, Aleksandar Nikolov, and Jonathan Ullman. The power of factorization mechanisms in local and central differential privacy. In *ACM Symposium on Theory of Computing*, STOC '20, pages 425–438, Chicago, IL, USA, 2020. ACM.

[30] Huy Lê Nguyễn, Jonathan Ullman, and Lydia Zakynthinou. Efficient private algorithms for learning halfspaces. In *International Conference on Algorithmic Learning Theory*, ALT '20, pages 704–724, San Diego, CA, USA, 2020. PMLR.

[31] Gautam Kamath, Or Sheffet, Vikrant Singhal, and Jonathan Ullman. Differentially private algorithms for learning mixtures of well separated gaussians. In *Annual Conference on Neural and Information Processing Systems*, NeurIPS '19, pages 168–180, Vancouver, Canada, 2019.

[32] Adam Sealfon and Jonathan Ullman. Efficiently Estimating Erdős-Rényi Graphs with Node Differential Privacy. In *Annual Conference on Neural and Information Processing Systems*, NeurIPS '19, pages 3765–3775, Vancouver, BC, Canada, 2019.

[33] Jeffrey Champion, Abhi Shelat, and Jonathan Ullman. Securely sampling biased coins with applications to differential privacy. In *ACM Conference on Computer and Communications Security*, CCS'19, pages 603–614, London, UK, 2019. ACM.

[34] Matthew Jagielski, Michael Kearns, Jieming Mao, Alina Oprea, Aaron Roth, Saeed Sharifi-Malvajerdi, and Jonathan Ullman. Differentially private fair classification. In *International Conference on Machine Learning*, ICML'19, pages 3000–3008, Long Beach, CA, USA, 2019. PMLR.

[35] Gautam Kamath, Jerry Li, Vikrant Singhal, and Jonathan Ullman. Privately learning high dimensional distributions. In *Annual Conference on Learning Theory*, COLT '19, pages 1853–1902, Phoenix, AZ, USA, 2019. PMLR.

[36] Clément Canonne, Gautam Kamath, Audra McMillan, Adam Smith, and Jonathan Ullman. The structure of optimal private tests for simple hypotheses. In *ACM Symposium on the Theory of Computing*, STOC '19, pages 310–321, Phoenix, AZ, USA, 2019. ACM.

[37] Albert Cheu, Adam Smith, Jonathan Ullman, David Zeber, and Maxim Zhilyaev. Distributed differential privacy via shuffling. In *Annual Conference on the Theory and Applications of Cryptographic Techniques*, EUROCRYPT '19, pages 375–403, Darmstadt, Germany, 2019. Springer.

[38] Cynthia Dwork and Jonathan Ullman. The Fienberg problem: How to allow human interactive data analysis in the age of differential privacy. *Journal of Privacy and Confidentiality*, 8(1):1–10, 2018.

[39] Foto N. Afrati, Shantanu Sharma, Jonathan R. Ullman, and Jeffrey D. Ullman. Computing marginals using MapReduce. *Journal of Computer and System Sciences*, 94:98–117, 2018.

[40] Matthew Joseph, Aaron Roth, Jonathan Ullman, and Bo Waggoner. Local differential privacy for evolving data. In *Annual Conference on Neural and Information Processing Systems*, NeurIPS '18 Spotlight Presentation, pages 2381–2390, Montreal, Canada, 2018.

[41] Kobbi Nissim, Adam Smith, Thomas Steinke, Uri Stemmer, and Jonathan Ullman. The limits of post-selection generalization. In *Annual Conference on Neural and Information Processing Systems*, NeurIPS '18, pages 6402–6411, Montreal, Canada, 2018.

[42] Albert Cheu, Ravi Sundaram, and Jonathan Ullman. Skyline identification in multi-armed bandits. In *IEEE International Symposium on Information Theory*, ISIT '18, pages 1006–1010, Vail, CO, USA, 2018. IEEE.

[43] Lucas Kowalczyk, Tal Malkin, Jonathan Ullman, and Daniel Wichs. Hardness of non-interactive differential privacy from one-way functions. In *Annual International Cryptology Conference*, CRYPTO '18, pages 437–466, Santa Barbara, CA, USA, 2018. Springer.

[44] Mallesh M. Pai, Aaron Roth, and Jonathan Ullman. An antifolk theorem for large repeated games. *ACM Transactions on Economics and Computation (TEAC)*, 5(2):10:1–10:20, 2017.

[45] Thomas Steinke and Jonathan Ullman. Between pure and approximate differential privacy. *Journal of Privacy and Confidentiality*, 7(2):1–20, 2017.

[46] Thomas Steinke and Jonathan Ullman. Tight lower bounds for differentially private selection. In *IEEE Symposium on Foundations of Computer Science*, FOCS '17, pages 552–563, Berkeley, CA, USA, 2017. IEEE.

[47] Piotr Indyk, Sepideh Mahabadi, Ronitt Rubinfeld, Jonathan Ullman, Ali Vakilian, and Anak Yodpinyanee. Fractional set cover in the streaming model. In *International Workshop on Approximation Algorithms for Combinatorial Optimization Problems*, APPROX '17, pages 12:1–12:20, Berkeley, CA, USA, 2017.

[48] Mitali Bafna and Jonathan Ullman. The price of selection in differetial privacy. In *Annual Conference on Learning Theory*, COLT '17, pages 151–168, Amsterdam, The Netherlands, 2017. PMLR.

[49] Aaron Roth, Aleksandrs Slivkins, Jonathan Ullman, and Zhiwei Steven Wu. Multidimensional dynamic pricing for welfare maximization. In *ACM Conference on Economics and Computation*, EC '17, pages 519–536, Cambridge, MA, USA, 2017. ACM.

[50] Mark Bun, Thomas Steinke, and Jonathan Ullman. Make up your mind: The price of online queries in differential privacy. In *Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '17, pages 1306–1325, Philadelphia, PA, USA, 2017. SIAM.

[51] Ryan Rogers, Aaron Roth, Jonathan Ullman, and Salil Vadhan. Privacy odometers and filters: Pay-as-you-go composition. In *Annual Conference on Neural Information Processing Systems*, NeurIPS '16, pages 1921–1929, Barcelona, Spain, 2016.

[52] Lucas Kowalczyk, Tal Malkin, Jonathan Ullman, and Mark Zhandry. Strong hardness of privacy from weak traitor tracing. In *International Conference on Theory of Cryptography*, TCC '16b, pages 659–689, Beijing, China, 2016. Springer.

[53] Edo Liberty, Michael Mitzenmacher, Justin Thaler, and Jonathan Ullman. Space lower bounds for itemset frequency sketches. In *ACM Symposium on Principles of Database Systems*, PODS '16, pages 441–454, San Francisco, CA, USA, 2016. ACM.

[54] Raef Bassily, Kobbi Nissim, Adam Smith, Thomas Steinke, Uri Stemmer, and Jonathan Ullman. Algorithmic stability for adaptive data analysis. In *ACM Symposium on the Theory of ComputingACM Symposium on the Theory of Computing*, STOC '16, pages 1046–1059, Cambridge, MA, USA, 2016. ACM.

[55] Aaron Roth, Jonathan Ullman, and Zhiwei Steven Wu. Watch and learn: Optimizing from revealed preferences feedback. In *ACM Symposium on the Theory of Computing*, STOC '16, pages 949–962, Cambridge, MA, USA, 2016. ACM.

[56] Cynthia Dwork, Adam Smith, Thomas Steinke, Jonathan Ullman, and Salil Vadhan. Robust traceability from trace amounts. In *IEEE Symposium on Foundations of Computer Science*, FOCS '15, pages 650–669, Berkeley, CA, USA, 2015. IEEE.

[57] Thomas Steinke and Jonathan Ullman. Interactive fingerprinting codes and the hardness of preventing false discovery. In *Annual Conference on Learning Theory*, COLT '15, pages 1588–1628, Paris, France, 2015. PMLR.

[58] Jonathan Ullman. Private multiplicative weights beyond linear queries. In *ACM Symposium on Principles of Database Systems*, PODS '15, pages 303–312, Melbourne, Australia, 2015. ACM.

[59] Pavel Hubácek, Moni Naor, and Jonathan Ullman. When can limited randomness be used in repeated games? In *IACR International Symposium on Algorithmic Game Theory*, SAGT '15, pages 259–271, Saarbrücken, Germany, 2015. Springer.

[60] Ryan M. Rogers, Aaron Roth, Jonathan Ullman, and Zhiwei Steven Wu. Inducing approximately optimal flow using truthful mediators. In *ACM Conference on Economics and Computation*, EC '15, pages 471–488, Portland, OR, USA, 2015. ACM.

[61] Moritz Hardt and Jonathan Ullman. Preventing false discovery in interactive data analysis is hard. In *IEEE Annual Symposium on Foundations of Computer Science*, FOCS '14, pages 454–463, Philadelphia, PA, USA, 2014. IEEE.

[62] Justin Hsu, Aaron Roth, Tim Roughgarden, and Jonathan Ullman. Privately solving linear programs. In *International Colloquium on Automata, Languages, and Programming, Track A*, ICALP(A) '14, pages 612–624, Copenhagen, Denmark, 2014. Springer.

[63] Karthekeyan Chandrasekaran, Justin Thaler, Jonathan Ullman, and Andrew Wan. Faster private release of marginals on small databases. In *ACM Conference on Innovations in Theoretical Computer Science*, ITCS '14, pages 287–402, Princeton, NJ, USA, 2014. ACM.

[64] Michael Kearns, Mallesh M. Pai, Aaron Roth, and Jonathan Ullman. Mechanism design in large games: incentives and privacy. In *ACM Conference on Innovations in Theoretical Computer Science*, ITCS '14, pages 403–410, Princeton, NJ, USA, 2014. ACM.

[65] Mark Bun, Jonathan Ullman, and Salil Vadhan. Fingerprinting codes and the price of approximate differential privacy. In *Annual ACM Symposium on the Theory of Computing*, STOC '14, pages 1–10, New York, NY, USA, 2014. ACM.

[66] Justin Hsu, Aaron Roth, and Jonathan Ullman. Differential privacy for the analyst via private equilibrium computation. In *ACM Symposium on the Theory of Computing*, STOC '13, pages 341–350, Palo Alto, CA, USA, 2013. ACM.

[67] Jonathan Ullman. Answering $n^{2+o(1)}$ counting queries with differential privacy is hard. In *ACM Symposium on the Theory of Computing*, STOC '13, pages 361–370, Palo Alto, CA, USA, 2013. ACM.

[68] Justin Thaler, Jonathan Ullman, and Salil P. Vadhan. Faster algorithms for privately releasing marginals. In *International Colloquium on Automata, Languages, and Programming, Track A*, ICALP(A) '12, pages 810–821, Warwick, UK, 2012. Springer.

[69] Anupam Gupta, Aaron Roth, and Jonathan Ullman. Iterative constructions and private data release. In *IACR International Conference on Theory of Cryptography*, TCC '12, pages 339–356, Taormina, Italy, 2012. Springer.

[70] Anupam Gupta, Moritz Hardt, Aaron Roth, and Jonathan Ullman. Privately releasing conjunctions and the statistical query barrier. In *ACM Symposium on Theory of Computing*, STOC '11, pages 803–812, San Jose, CA, USA, 2011. ACM.

[71] Jonathan Ullman and Salil P. Vadhan. PCPs and the hardness of generating private synthetic data. In *IACR International Conference on Theory of Cryptography*, TCC '11, pages 400–416, Providence, RI, USA, 2011. Springer.

[72] Shiva Prasad Kasiviswanathan, Mark Rudelson, Adam Smith, and Jonathan Ullman. The price of privately releasing contingency tables and the spectra of random matrices with correlated rows. In *ACM Symposium on Theory of Computing*, STOC '10, pages 775–784, Cambridge, MA, USA, 2010. ACM.

[73] Scott Duke Kominers, Mike Ruberry, and Jonathan Ullman. Course allocation by proxy auction. In *International Workshop on Internet and Network Economics*, WINE '10, pages 551–558, Stanford, CA, USA, 2010. Springer.

Secondary Publications (Reverse Chronological Order)

Some of my work appears in journals as a secondary form of publication, after initially appearing in a computer science conference. This list includes all such publications.

[74] Raef Bassily, Kobbi Nissim, Adam Smith, Thomas Steinke, Uri Stemmer, and Jonathan Ullman. Algorithmic stability for adaptive data analysis. *SIAM Journal on Computing*, 50(3):377–405, 2021.

[75] Adam Sealfon and Jonathan Ullman. Efficiently estimating Erdős-Rényi graphs with node differential privacy. *Journal of Privacy and Confidentiality*, 11(1), 2021.

[76] Albert Cheu, Adam Smith, and Jonathan Ullman. Manipulation attacks in local differential privacy. *Journal of Privacy and Confidentiality*, 11(1), 2021.

[77] Jonathan Ullman and Salil Vadhan. PCPs and the hardness of generating synthetic data. *Journal of Cryptology*, pages 1–35, 2020.

[78] Aaron Roth, Aleksandrs Slivkins, Jonathan Ullman, and Zhiwei Steven Wu. Multidimensional dynamic pricing for welfare maximization. *ACM Transactions on Economics and Computation*, 8(1):6:1–6:35, 2020.

[79] Mark Bun, Thomas Steinke, and Jonathan Ullman. Make up your mind: The price of online queries in differential privacy. *Journal of Privacy and Confidentiality*, 9(1):1–35, 2019.

[80] Mark Bun, Jonathan Ullman, and Salil Vadhan. Fingerprinting codes and the price of approximate differential privacy. *SIAM Journal on Computing*, 47(5):1888–1938, 2018.

[81] Pavel Hubáček, Moni Naor, and Jonathan Ullman. When can limited randomness be used in repeated games? *Theory of Computing Systems*, 59(4):722–746, 2016.

[82] Jonathan Ullman. Answering $n^{2+o(1)}$ counting queries with differential privacy is hard. *SIAM Journal on Computing*, 45(2):473–496, 2016.

[83] Anupam Gupta, Moritz Hardt, Aaron Roth, and Jonathan Ullman. Privately releasing conjunctions and the statistical query barrier. *SIAM Journal on Computing*, 42(4):1494–1520, 2013.

Other Writings (Reverse Chronological Order)

[84] Clément Canonne, Gautam Kamath, Thomas Steinke, Jonathan Ullman, and Zhiwei Steven Wu. DifferentialPrivacy.org. `https://differentialprivacy.org/`, 2020.

[85] Gautam Kamath and Jonathan Ullman. A primer on private statistics. *arXiv preprint arXiv:2005.00010*, 2020.

[86] Jonathan Ullman. Technical perspective: Building a safety net for data reuse. *Communications of the ACM*, 60(4):85–85, 2017.

[87] Cynthia Dwork, Adam Smith, Thomas Steinke, and Jonathan Ullman. Exposed! a survey of attacks on private data. *Annual Review of Statistics and Its Application*, 4:61–84, 2017.

[88] Aaron Roth, Jonathan Ullman, and Zhiwei Steven Wu. Watch and learn: optimizing from revealed preferences feedback. *ACM SIGecom Exchanges*, 14(1):101–104, 2015.

[89] Jonathan Ullman. Query release via online learning. *Encyclopedia of Algorithms*, pages 1–5, 2015.

Funding

Executive Summary

Total shares of research funding approximately $2.3m.
NSF CAREER Award (2018); Google Faculty Research Award (2018); Apple Research Award (2021).

Grants and Awards

NSF award #2247484 **10/2023 – 09/2026**

Project Title: *Auditing Private Statistical and Machine Learning Algorithms: Theory and Practice*
Role: co-PI; joint with Alina Oprea (Northeastern)
Amount: $600k total, $300k for PI Ullman

NSF award #2232692 **04/2023 – 03/2027**

Project Title: *Private Model Personalization*
Role: Lead PI; joint with Adam Smith (BU), Zhiwei Steven Wu (CMU)
Amount: $1.2m total, $450k for PI Ullman

NSF award #2120603 **10/2021 – 10/2022**

Project Title: *Foundations for the Next Generation of Private Learning Systems*

Role: PI; joint with Alina Oprea (Northeastern), Adam Smith (Boston University), Roxana Geambasu (Columbia), Zhiwei Steven Wu (CMU)
Amount: $500k total, $100k for PI Ullman

Gift from Apple, Inc. **04/2021**
Project Title: *Auditing Differentially Private Machine Learning*
Role: PI; joint with Alina Oprea (Northeastern)
Amount: $100k, $50k for PI Ullman

NSF award #1916020 **10/2019 – 10/2021**
Project Title: *Understanding and Mitigating the Privacy and Societal Risks of Advanced Advertising Targeting and Tracking*
Role: co-PI; joint with Alan Mislove (Northeastern) and Alexandra Korolova (USC)
Amount: $1.2m total, $400k for co-PI Ullman

NSF award #1816028 **08/2018 – 08/2021**
Project Title: *New Approaches to Decentralized Differential Privacy*
Role: PI; joint with abhi shelat (Northeastern)
Amount: $500k total; $250k for PI Ullman

Google Faculty Research Award **02/2018**
Project Title: *Distributed Differential Privacy Beyond Local Protocols*
Amount: $65k

NSF CAREER award #1750640 **08/2018 – 08/2023**
Project Title: *CAREER: A Stable Foundation for Trustworthy Data Analysis*
Amount: $500k

NSF award #1718088 **08/2017 – 08/2020**
Project Title: *Programming Tools for Adaptive Data Analysis*
Role: PI; joint with Marco Gaboardi (SUNY Buffalo)
Amount: $448k total; $224k for PI Ullman

Mentoring

Postdoc Mentoring

Mahdi Haghifam **09/2023 – Current**
Research: foundations of machine learning and privacy
Khoury Distinguished Postdoctoral Fellow

Maryam Aliakbarpour **08/2021 – 08/2023**
Research: statistical estimation and testing, differential privacy
Joint with Boston University
Next Position: Assistant Professor, Rice University

Audra McMillan **06/2018 – 06/2020**
Research: differentially private statistical inference
Cybersecurity & Privacy Institute Fellow; joint with Boston University
Next Position: Research Scientist, Apple, Inc.

PhD Mentoring

John Abascal **09/2021 – Current**
Co-advised with Alina Oprea

Rose Silver **09/2021 – Current**
CMU PhD Student, co-advised with Elaine Shi

Konstantina Bairaktari **09/2020 – Current**
Co-advised with Huy Le Nguyen

Lydia Zakynthinou **09/2017 – 08/2023**
Thesis Title: *Algorithms and Frameworks for Preventing Privacy Leakage and Overfitting in Machine Learning*
Facebook Fellowship winner and Khoury Graduate Researcher Award winner
Co-advised with Huy Le Nguyen
Next Position: Postdoctoral Researcher, UC Berkeley

Albert Cheu **09/2016 – 04/2021**
Thesis Title: *Differential Privacy in the Shuffle Model*
Khoury Graduate Researcher Award winner
Next Position: Postdoctoral Researcher, Georgetown University
Last Known Position: Research Scientist, Google Inc.

Vikrant Singhal **09/2016 – 07/2021**
Thesis Title: Differentially Private Statistical Estimation
Next Position: Postdoctoral Researcher, University of Waterloo
Last Known Position: Research Fellow, OpenDP

Undergraduate Mentoring

Eric Chapdelaine **06/2023 – 04/2024**
Northeastern undergraduate honors thesis student

Stanley Wu **01/2021 – 08/2023**
Northeastern undergraduate research assistant
Co-advised with Alina Oprea
Paper: *How to Combine Membership-Inference Attacks on Multiple Updated Models* in *PETS 2023*
Next position: Ph.D. in Computer Science, University of Chicago

Tatiana Ediger **01/2021 – 06/2021**
Northeastern undergraduate research assistant
Project: Differentially private linear regression
Next position: Data Engineer at EightSleep

Jeffrey Champion **06/2017 – 12/2019**
Northeastern undergraduate co-op student
Paper *Securely Sampling Biased Coins with Applications to Differential Privacy* in *CCS 2019*.
Next position: Ph.D. in Computer Science, University of Texas at Austin

Mitali Bafna **06/2016 – 12/2016**

IIT Madras undergraduate
Paper *The Price of Differentially Private Selection* in *COLT 2017*.
Next position: Ph.D. in Computer Science, Harvard University

Thesis Committees

Liudas Panavas (in progress; advisor: Cody Dunne)
Lisa Oakley (in progress; advisor: Alina Oprea)
Shuyler Rosefield (graduated Fall 2024; advisor: abhi shelat)
Matthew Jones (graduated Fall 2024; advisor: Huy Le Nguyen)
Eysa Lee (graduated Summer 2023; advisor: abhi shelat)
Jack Doerner (graduated Fall 2022; advisor: abhi shelat)
Yashvanth Kondi (graduated Summer 2022; advisor: abhi shelat)
Matthew Jagielski (graduated Summer 2021; advisors: Cristina Nita-Rotaru and Alina Oprea)
Ariel Hamlin (graduated Spring 2021; advisor: Daniel Wichs)
Giorgios Zirdelis (graduated Spring 2021; advisor: Daniel Wichs)
Cheng Li (graduated Fall 2019; advisor: Jay Aslam)
Adam Sealfon (graduated Summer 2019 from MIT; advisor: Shafi Goldwasser)
Chin Ho Lee (graduated Summer 2019; advisor: Emanuele Viola)
Benjamin Kreuter (graduated Spring 2018; advisor: abhi shelat)
Maryam Aziz (graduated Fall 2018; advisor: Jay Aslam)
Zahra Jafargholi (graduated Spring 2016; advisor: Daniel Wichs)

Teaching

Northeastern University CS 3000: Algorithms & Data

Undergraduate course on algorithm design and analysis.
Formerly listed as CS 4800: Algorithms & Data

Term	Students	Course/Instructor Rating
Spring 2018	48	4.8/5.0
Fall 2018 (Sec 01)	72	4.7/5.0
Fall 2018 (Sec 04)	38	4.5/5.0
Spring 2020	70	4.8/5.0
Fall 2020	321 (4 combined sections)	4.4/4.6
Fall 2023	126	4.3/4.2
Fall 2024	117	4.1/4.0

Northeastern University CS 7880: Differential Privacy in Machine Learning and Statistics

Ph.D. level topics course on differential privacy
Previously called Rigorous Approaches to Data Privacy

Term	Students	Course/Instructor Rating
Spring 2021	15	4.7/5.0
Spring 2017	9	5.0/5.0

Northeastern University CS 7800: Advanced Algorithms

Ph.D. level core course on algorithm design and analysis.

Term	Students	Course/Instructor Rating
Fall 2015	17	4.5/5.0
Fall 2016	28	4.9/5.0
Fall 2017	27	4.5/5.0
Fall 2022	28	4.7/4.8

Talks Given (Reverse Chronological Order)

Invited Talks

Boston University CDS Colloquium	**03/2024**
University of Toronto CS **Distinguished Lecture Series**	**02/2024**
University of Wisconsin CS Seminar	**01/2024**
University of Michigan CSE Seminar	**11/2024**
UT Austin CS Colloquium	**11/2024**
TTIC Colloquium	**07/2023**
Workshop on Privacy Preserving AI	**02/2023**
UT Austin Computer Science Colloquium	**03/2022**
University of Pennsylvania CIS Colloquium	**02/2022**
TTIC Colloquium	**10/2021**
Charles River Crypto Day	**07/2021**
Apple Privacy-Preserving Machine Learning Workshop	**08/2020**
IMA Workshop on Recent Themes in Resource Tradeoffs	**06/2019**
University of Pennsylvania Warren Center Seminar	**11/2018**
Banff Mathematical Foundations of Differential Privacy Workshop	**05/2018**
Simons Statistics, Optimization, and Uncertainty Workshop	**12/2017**
Simons Differential Privacy Semester Planning Workshop	**05/2017**
IAS Symposium on Four Facets of Differential Privacy	**11/2016**
PCMI Summer Session, the Mathematics of Data	**07/2016**
IHP Nexus of Information and Computation Theories	**03/2016**
NIPS Workshop on Adaptive Data Analysis	**12/2015**
Oberwolfach meeting on complexity. **Invited Plenary Talk**	**11/2015**
Theory and Practice of Differential Privacy Workshop. **Invited Keynote Talk**	**04/2015**
Charles River Privacy Day, Boston University	**05/2014**
Northeastern University CS Colloquium	**03/2014**
University of Toronto CS Colloquium	**02/2014**
Northwestern CS Colloquium	**02/2013**
USC CS Colloquium	**02/2013**
Simons Big Data and Differential Privacy Workshop	**03/2013**
Simons Workshop on the Science of Differential Privacy	**02/2013**
China Theory Week	**10/2011**

Seminar Talks

UMass Amherst Security Seminar	**09/2024**
NTT Labs Seminar	**07/2022**
University of Washington Computer Science Seminar	**11/2021**
Google Differential Privacy Seminar	**06/2021**

Boston University Theory of Computing Seminar	**10/2019**
MIT Cryptographic and Information Security Seminar	**04/2017**
UMass Amherst Database Seminar	**10/2016**
MIT Theory of Computing Seminar	**10/2016**
University of Warwick Theory of Computing Seminar	**04/2015**
NYU Polytech Theory of Computing Seminar	**10/2014**
Penn State Theory of Computing Seminar	**09/2014**
MSR SVC Seminar	**11/2013**
Princeton Theory of Computing Seminar	**11/2013**
NYU Theory of Computing Seminar	**10/2013**
Columbia University Theory of Computing Seminar	**10/2013**
Boston Univeristy Theory of Computing Seminar	**02/2011**
MSR New England Seminar	**11/2010**
Penn State Theory of Computing Seminar	**04/2010**

Professional Activities

External Activities

Theory and Practice of Differential Privacy Workshop
Steering Committee Co-Chair
Guest Editor, Special issue of *Journal of Privacy and Confidentiality* for work from TPDP 2017

DifferentialPrivacy.org Website
Co-creator and Contributor

Boston Differential Privacy Summer School
Co-organizer

7th Bar Ilan University Winter School on Cryptography
Co-instructor for course *Differential Privacy: From Theory to Practice*

Conference and Workshop Program Committee Chair
Track Chair, Conf. on Computer and Communication Security (CCS), Privacy Track 2021
Program Committee Chair, Workshop on Theory and Practice of Differential Privacy 2017

Conference Program Committee and Reviewer
Program Committee, Symposium on Theory of Computing (STOC) 2015
Program Committee, Theory of Cryptography Conference (TCC) 2015
Program Committee, Innovations in Theoretical Computer Science (ITCS) 2015
Program Committee, Economics and Computation (EC) 2016
Program Committee, Theory of Cryptography Conference (TCC) 2016b
Reviewer, Neural and Information Processing Systems (NeurIPS) 2016
Reviewer, Neural and Information Processing Systems (NeurIPS) 2017
Program Committee, Conference on Artifical Intelligence and Statistics (AISTATS) 2017
Program Committee, Symposium on Discrete Algorithms (SODA) 2018
Reviewer, International Conference on Machine Learning (ICML) 2018
Program Committee, Symposium on Foundations of Computer Science (FOCS) 2018

Program Committee, Information Theoretic Cryptography (ITC) 2020
Reviewer, International Conference on Machine Learning (ICML) 2020
Program Committee, Conference on Computer and Communications Security (CCS) 2020
Reviewer, Conference on Learning Theory (COLT) 2020
Program Committee, Symposium on Security and Privacy (Oakland) 2021
Senior Meta-Reviewer, Conference on Artificial Intelligence (AAAI) 2022
Area Chair, Conference on Fairness, Accountability, and Transparency (FAccT) 2022
Area Chair, Conference on Learning Theory (COLT) 2023
Program Committee, Symposium on Discrete Algorithms (SODA) 2024
Program Committee, Foundations of Responsible Computing (FORC) 2024
Area Chair, Conference on Learning Theory (COLT) 2024
Program committee, Symposium on Theorty of Computing (STOC) 2025
Senior Program Committee, Conference on Learning Theory (COLT) 2025
Senior Area Chair, International Conference on Machine Learning (ICML) 2025

Journal Editor

Action Editor, Transactions on Machine Learning Research (TMLR)

Advisory

Member, Census Scientific Advisory Committee (CSAC)

Internal Activities

Area Chair for Theory Research — 09/2022 - Current

Ex-officio member of the TT Hiring Committee

Khoury College of Computer Science Committees

Representative, TT Hiring Committee — **2022/2023 AY**
Chair, Teaching Awards Committee — **2021/2022 AY**
Representative, Ph.D. Admissions Committee — **2020/2021 AY**
Representative, Ph.D. Curriculum Committee — **2020/2021 AY**
Representative, Teaching Awards Committee — **2020/2021 AY**
Co-organizer, Ph.D. Open House — **03/2020**
Representative, Ph.D. Admissions Committee — **2019/2020 AY**
Representative, Ph.D. Curriculum Committee — **2018/2019 AY**
Representative, TT Hiring Committee — **2017/2018 AY**
Representative, TT Hiring Committee — **2016/2017 AY**
Co-organizer, Ph.D. Open House — **03/2016**
Representative, Ph.D. Admissions Committee — **2015/2016 AY**