Krishna Pillutla

Contact

Website: `https://krishnap25.github.io`
Email: `krishnap@dsai.iitm.ac.in`

Position

Assistant Professor, Dept. of Data Science & Artificial Intelligence, IIT Madras *2024 - Date*

Education

University of Washington *2016-2022*
Ph.D. in Computer Science & Engineering
Thesis: From Enormous Structured Models to On-device Federated Learning:
Robustness, Heterogeneity and Optimization
Advisors: Zaid Harchaoui and Sham Kakade

Carnegie Mellon University *2014-15*
M.S. in Computer Science (QPA: 3.95/4.00)
Thesis: Data Driven Resource Allocation for Distributed Learning
Advisor: Maria-Florina Balcan

Indian Institute of Technology, Bombay *2010-14*
B.Tech (Hons) in Computer Science & Engineering (QPA: 9.54/10.0)
Thesis: Distributed Machine Learning: Iterative Convex Optimization Methods
Advisor: J. Saketha Nath

Awards

Schmidt Sciences AI2050 Early Career Fellowship *2025*
1 of 21 awardees worldwide

ASA Student Paper Award Honorable Mention *2023*
Statistical Learning and Data Science Section of the American Statistical Association (ASA)

ASA Student Paper Award Honorable Mention *2023*
Risk Analysis Section of the American Statistical Association (ASA)

Outstanding Paper at NeurIPS *2021*
Top 6 of 9000 submissions

J.P. Morgan PhD Fellowship *2019-20*
1 of 14 awardees worldwide

Anne Dinning - Michael Wolf Endowed Regental Fellowship *2016-17*
First-year PhD Fellowship awarded on merit

CBSE Merit Scholarship by the Central Board of Secondary Education in India *2010-14*
Awarded by the Govt. of India for the duration of undergraduate studies

Previous Positions

Visiting Researcher, Google Research *Sept 2022 - Feb 2024*

Research Intern, Facebook AI Research *Summers of 2019, 2021*

Publications

Monographs:

- **Pillutla**, **K**., Upadhyay, J., Choquette-Choo, C. A., Dvijotham, K., Ganesh, A., Henzinger, M., Katz, J., McKenna, R., McMahan, H.B., Rush, K., Steinke, T. & Thakurta, A. (2025).
  Correlated Noise Mechanisms for Differentially Private Learning.

Working papers and manuscripts:[1]

- McMahan, H. B., & **Pillutla, K.** (2025).
  An Inversion Theorem for Buffered Linear Toeplitz (BLT) Matrices and Applications to Streaming Differential Privacy.

Peer-reviewed journal and conference papers:

- Vishnu, V., **Pillutla, K.**, & Thakurta, A.G. (2025).
  InvisibleInk: Low-Cost and High-Utility Text Generation with Differential Privacy.
  Neural Information Processing Systems (NeurIPS).
- Charles, Z., Ganesh, A., McKenna, R., McMahan, H. B., Mitchell, N., **Pillutla, K.**, & Rush, K. (2025).
  Fine-Tuning Large Language Models with User-Level Differential Privacy.
  IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)
- Kandpal, N., **Pillutla, K.**, Oprea, A., Kairouz, P., Choquette-Choo, C., & Xu, Z (2024).
  User Inference Attacks on Large Language Models.
  Empirical Methods in NLP (EMNLP) **Oral Presentation**.
- Dvijotham, K.$^{\alpha}$, McMahan, B.$^{\alpha}$, **Pillutla, K.**$^{\alpha}$, Steinke, T.$^{\alpha}$, & Thakurta, A.G.$^{\alpha}$ (2024)
  Efficient and Near-Optimal Noise Generation for Streaming Differential Privacy.
  IEEE Symposium on Foundations of Computer Science (FOCS).
- Mehta, R., Roulet, V., **Pillutla, K.***, & Harchaoui, Z. (2023)
  Distributionally Robust Optimization with Bias and Variance Reduction.
  International Conference on Learning Representations (ICLR) **Spotlight**.
- Choquette-Choo, C.$^{*\alpha}$, Dvijotham, K.$^{*\alpha}$, **Pillutla, K.**$^{*\alpha}$, Ganesh, A., Steinke, T., & Thakurta, A.G. (2024)
  Correlated Noise Provably Beats Independent Noise for Differentially Private Learning.
  International Conference on Learning Representations (ICLR).
- **Pillutla, K.**, Andrew, G., Kairouz, P., McMahan, H. B., Oprea, A., & Oh, S. (2023)
  Unleashing the Power of Randomization in Auditing Differentially Private ML.
  Neural Information Processing Systems (NeurIPS).
- Charles, Z.*, Mitchell, N.*, **Pillutla, K.***, Reneer, M., & Garrett, Z. (2023)
  Towards Federated Foundation Models: Scalable Dataset Pipelines for Group-Structured Learning.
  Neural Information Processing Systems (NeurIPS), Datasets and Benchmarks Track.
- **Pillutla, K.***, Liu, L.*, Thickstun, J., Welleck, S., Swayamdipta, S., Zellers, R., Oh, S., Choi, Y., Harchaoui, Z. (2023)
  MAUVE Scores for Generative Models: Theory and Practice.
  Journal of Machine Learning Research (JMLR) **Best Papers Track**.
- **Pillutla, K.***, Laguel, Y.*, Malick, J., & Harchaoui, Z. (2023)
  Federated Learning with Superquantile Aggregation for Heterogeneous Data.
  Machine Learning.
- Mehta, R., Roulet, V., **Pillutla, K.**, Liu, L. & Harchaoui, Z. (2023)
  Stochastic Algorithms for Ordered Empirical Risk Minimization.
  Artificial Intelligence and Statistics Conference (AISTATS).
  ASA Student Paper Award Honorable Mention (Risk Analysis Section).
- Fisher, J., Liu, L., **Pillutla, K.**, Choi, Y., Harchaoui, Z. (2023)
  Statistical and Computational Guarantees for Influence Diagnostics.
  Artificial Intelligence and Statistics Conference (AISTATS).
  ASA Student Paper Award Honorable Mention (Statistical Learning and Data Science Section).

[1] equal contribution denoted by * and alphabetical order by α

- **Pillutla, K.**, Malik, K., Mohamed, A., Rabbat, M., Sanjabi, M., & Xiao, L. (2022).
  Federated Learning with Partial Model Personalization.
  International Conference on Machine Learning (ICML).
- **Pillutla, K.**, Kakade, S. M., & Harchaoui, Z. (2022).
  Robust Aggregation for Federated Learning.
  IEEE Transactions on Signal Processing.
  Also presented at *International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2023).*
  IEEE SPS Top 25 Downloaded Paper in 9/22 - 9/23.
- **Pillutla, K.**, Swayamdipta, S., Zellers, R., Thickstun, J., Welleck, S., Choi, Y. & Harchaoui, Z. (2021).
  MAUVE: Measuring the Gap Between Machine Text and Human Text using Divergence Frontiers.
  Neural Information Processing Systems (NeurIPS).
  NeurIPS Outstanding Paper Award (Top 6 of 9000).
- Liu, L., **Pillutla, K.**, Welleck, S., Oh, S., Choi, Y. & Harchaoui, Z. (2021).
  Divergence Frontiers for Generative Models: Sample Complexity, Quantization Effects, and Frontier Integrals.
  Neural Information Processing Systems (NeurIPS).
- Kusupati, A., Wallingford, M., Ramanujan, V., Somani, R., Park, J. S., **Pillutla, K.**, Jain, P., Kakade, S., & Farhadi, A. (2021).
  LLC: Accurate, Multi-purpose Learnt Low-dimensional Binary Codes.
  Neural Information Processing Systems (NeurIPS).
- Laguel, Y., **Pillutla, K.**, Malick, J., & Harchaoui, Z. (2021).
  Superquantiles in Action: Subdifferential Calculus in Practice and Applications in ML.
  Set Valued and Variational Analysis.
- Laguel, Y.*, **Pillutla, K.***, Malick, J., & Harchaoui, Z. (2021).
  A Superquantile Approach to Federated Learning with Heterogeneous Devices.
  IEEE Conference on Information Sciences and Systems (CISS).
- **Pillutla, K.**, Roulet, V., Kakade, S. M., Harchaoui, Z. (2018).
  A Smoother Way to Train Structured Prediction Models.
  Neural Information Processing Systems (NeurIPS).
- Jain, P., Kakade, S. M., Kidambi, R., Netrapalli, P., **Pillutla, V. K.**, & Sidford, A. (2017).
  A Markov Chain Theory Approach to Characterizing the Minimax Optimality of Stochastic Gradient Descent (for Least Squares).
  Foundations of Software Technology and Theoretical Computer Science (FSTTCS).
- Ruffalo, M., Stojanov, P., **Pillutla, V. K.**, Varma, R., & Bar-Joseph, Z. (2017).
  Reconstructing cancer drug response networks using multitask learning.
  BMC Systems Biology.
- Dick, T.$^{\alpha}$, Li, M.$^{\alpha}$, **Pillutla, V. K.**$^{\alpha}$, White, C.$^{\alpha}$, Balcan, M-F., & Smola, A. (2017).
  Data Driven Resource Allocation for Distributed Learning.
  Artificial Intelligence and Statistics Conference (AISTATS).
- **Pillutla, V. K.***, Fang, Z.*, Devineni, P., Faloutsos, C., Koutra, D., & Tang, J. (2016).
  On Skewed Multi-dimensional Distributions: the FusionRP Model, Algorithms, and Discoveries.
  SIAM International Conference on Data Mining.

Selected Workshop papers:

- Dvijotham, K.$^{\alpha}$, McMahan, B.$^{\alpha}$, **Pillutla, K.**$^{\alpha}$, Steinke, T.$^{\alpha}$, & Thakurta, A.G.$^{\alpha}$ (2024)
  Efficient and Near-Optimal Noise Generation for Streaming Differential Privacy.
  Theory and Practice of Differential Privacy (TPDP). **Oral Presentation**.
- **Pillutla, K.**, Roulet, V., Kakade, S. M., & Harchaoui, Z. (2023)
  Modified Gauss-Newton Algorithms under Noise.
  IEEE Statistical Signal Processing Workshop.

- **Pillutla, K.***, Laguel, Y.*, Malick, J., & Harchaoui, Z. (2022)
  Tackling Distribution Shifts in Federated Learning with Superquantile Aggregation.
  NeurIPS 2022 Workshop on Distribution Shifts. **Spotlight Presentation**.
- **Pillutla, K.**, Kakade, S. M., & Harchaoui, Z. (2020).
  Robust Aggregation for Federated Learning.
  International Workshop on Federated Learning for User Privacy and Data Confidentiality (FL-ICML). **Long Oral Presentation**.

Software Released

Invisible Ink: LLM-Based Text Generation with Differential Privacy
- Installation: `pip install inkink`. GitHub

Dataset Grouper: Group-Partitioning Large Datasets for Federated Foundation Models
- Installation: `pip install dataset-grouper`. GitHub, Usage Examples.

Mauve: Measuring the Gap Between Neural Text and Human Text
- Installation: `pip install mauve-text`. **5000 monthly downloads**. GitHub, Documentation. Implementation in the HuggingFace Evaluate package.

Geom-Median: Fast and Differentiable Geometric Median in PyTorch and NumPy
- Installation: `pip install geom-median`. **265 monthly downloads**. GitHub.

SQwash: Distributionally robust learning in PyTorch with a 1 additional line of code
- Installation: `pip install sqwash`. **65 monthly downloads**. GitHub, Documentation.

Workshop/ Conference Organization

Deployable AI Workshop @ AAAI (website) *2025, 2026*
Co-Organizer

IFDS Workshop on Distributional Robustness in Data Science (website) *2022*
Local Organizer

Minisymposium on Federated Learning at ICCOPT *2022*
Main Organizer

Invited Talks

Towards Provably Privacy-Preserving AI in the Age of Foundation Models
CSML Workshop @ IISc (Nov. 2025); Early Career Highlights at CODS Conference (Dec. 2025)

Near-Optimal Private Learning with Correlated Noise Mechanisms
STCS Seminar at TIFR (Jul. 2025)

InvisibleInk: High-Utility and Low-Cost Text Generation with Differential Privacy
Microsoft Research (Jun. 2025)

Learning with User-Level Differential Privacy at Scale
Amazon India (Mar. 2025), IISc (Feb. 2025), Microsoft Research India (Feb. 2025), Université Grenoble Alpes (Feb. 2024), IIT Hyderabad (Apr. 2024)

Near-Optimal Differentially Private Learning with Correlated Noise Mechanisms
BIRS Workshop on ML and Statistics (CMI, Jan. 2025)

Was My Data Used to Train a LLM?
1st International Workshop on Responsible AI for Healthcare (Oct. 2024); Data Security Council of India Webinar (Oct. 2024).

Robust Aggregation for Federated Learning
IEEE Signal Processing Society Webinar (2024).

Federated Learning with Partial Model Personalization (2022).
Federated Learning One World Seminar.

Federated Learning with Superquantile Aggregation for Heterogeneous Data (2021-22).
IFDS Ethics and Algorithms, International Conference on Continuous Optimization.

From Enormous Structured Models to On-device Federated Learning: Robustness, Heterogeneity, and Optimization (2022).
Microsoft Research, Meta AI Research, Google Research.

MAUVE: Measuring the Gap Between Neural Text and Human Text (2022).
Stanford NLP Seminar, Microsoft Research Asia, IFML NSF Site Visit.

Mentoring

Current:

- Arun Ramaswamy (M.S. by research) *2025-date*
- Dhruv Shah (Post-baccalaureate fellow) *2025-date*
- Vraj Thakkar (Post-baccalaureate fellow) *2025-date*
- Kaushik Doddamani (M.S. by research) *2024-date*
- P. Sushanth Reddy (Dual Bachelors & Masters) *2024-date*
- Vishnu Vinod (Post-baccalaureate fellow) *2024-date*
- Pranav Ramanujam (Bachelors) *2025-date*
- Karthick Krishna M. (Dual Bachelors & Masters) *2025-date*

Previous:

- Ishita Khatri (Dual Bachelors and Masters) *2024-2025*
- Jillian Fisher (Graduate student at UW) *2021-2023*
- Ronak Mehta (Graduate student at UW) *2021-2024*
- Nikhil Kandpal (Intern at Google) *2023*

Teaching

Privacy in AI, Instructor *2024, 2026*

Machine Learning - I, Co-Instructor *2025*

Selected Topics in AI Privacy, Instructor *2025*

Statistical Learning with Differentiable Programming, Teaching Assistant (UW) *2021, 2022*

Machine Learning for Big Data, Teaching Assistant (UW) *Spring 2018*

Reinforcement Learning and Bandits, Teaching Assistant (UW) *2019*

Algorithms and Foundation of Computing, Volunteer Tutor (UW) *2016-17*

Programming 101, Chemistry 101, Numerical Analysis, Teaching Assistant (IITB) *2012-14*

Academic Honors

- Perfect 100 percentile (top 8 out of 174,000) in Common Admission Test (CAT) *2013*
- Gold medal at the Indian National Chemistry Olympiad (INChO). Part of initial shortlist for the International Chemistry Olympiad (Top 35 from 28,000) *2010*
- Secured All India Rank 22 in IITJEE, an exam taken by half million students *2010*
- Awarded the Certificates of Merit by the CBSE [2] for being in the top 0.1% in India in Mathematics and Chemistry in Grade 12 examinations, AISSCE *2010*

Service

- **Reviewer** for JMLR, Math. Prog., NeurIPS, AISTATS, JOTA, AISTATS, ICLR
- **Student Area Chair** for Machine Learning, UW CSE Graduate Admissions (2020-21) and application reader (2018 -20)
- **Organizer** for New Graduate Student Orientation at UW (2017) and Panelist (2018-20)

[2] CBSE is the Central Board of Secondary Education in India