Karan Chadha

Website: knchadha.github.io
Email: knchadha@stanford.edu
Phone: 650-272-8032
Google Scholar: Link

Research Interests

I am interested in answering questions in **Trustworthy AI, Differential Privacy, Uncertainty Quantification,** and **Federated Learning**, for which I use theoretical tools from statistics and optimization, complemented with rigorous experimentation. More concretely, in the near future, I am interested in the following directions:

- Studying the empirical privacy leakage for modern ML models (Foundation Models/LLMs) in realistic attack scenarios.
- Moving beyond differential privacy to find application-relevant definitions to evaluate models on privacy, robustness, fairness and copyright.
- Building better (trustworthy) algorithms for practically relevant ML and data analytics tasks like recommendations, ranking, frequency estimation, etc.

Education

Stanford University 2019–Present

Ph.D. in Electrical Engineering, GPA: 4.00/4.00
Advised by Prof. John Duchi

Indian Institute of Technology Bombay 2014–2019

Dual Degree (B.Tech. + M.Tech.) in Electrical Engineering, GPA: 9.68/10
Advised by Prof. Ankur Kulkarni, Prof. Jayakrishnan Nair and Prof. Vivek Borkar.

Internships

Student Researcher, Google Deepmind Summer 2023

Worked with *Matthew Jagielski* and *Nicolas Papernot* on auditing private prediction.

Machine Learning Intern, Apple Summer 2022

Worked with *Omid Javidbakht*, *Audra McMillan*, *Vitaly Feldman* and *Kunal Talwar* on learning histograms in the unknown dictionary setting with aggregate differential privacy.

Summer Research Assistant, University of Southern California Summer 2017

Worked with *Prof. Rahul Jain* on stochastic optimization and mechanism design for power grids.

Summer Research Assistant, SYSU-CMU Joint Research Institute Summer 2016

Worked with *Prof. Paul Weng* on Deep Reinforcement Learning for Atari agents.

Preprints

- **Resampling methods for private statistical inference**
  K. Chadha, J. C. Duchi and R. Kuditipudi
  Preprint available on request
- **Differentially Private Heavy Hitter Detection using Federated Analytics** [PDF]
  K. Chadha, J. Chen, J. C. Duchi, V. Feldman, H. Hashemi, O. Javidbakht, A. McMillan, and K. Talwar
  Workshops: Federated Learning and Analytics in Practice, TPDP, arxiv:2307.11749

Publications

- **Federated Asymptotics: A model for evaluating federated learning algorithms** [PDF]
  K. Chadha*, G. Cheng*, and J. C. Duchi,
  AISTATS 23
- **Private optimization in the interpolation regime: faster rates and hardness results** [PDF]
  K. Chadha*, H. Asi*, G. Cheng*, and J. C. Duchi
  ICML 22 ***(Spotlight)***
- **Accelerated, optimal, and parallel: Some results on model-based stochastic optimization** [PDF]
  K. Chadha*, G. Cheng*, and J. C. Duchi
  ICML 22
- **Minibatch stochastic approximate proximal pointmethods** [PDF]
  K. Chadha*, H. Asi*, G. Cheng*, and J. C. Duchi
  Neurips 2020 ***(Spotlight)***
- **Efficiency fairness tradeoff in battery sharing** [PDF]
  K. Chadha, A. A. Kulkarni and J. Nair
  Operations Research Letters, 2021
- **Aggregate play and welfare in strategic interactions on networks** [PDF]
  K. Chadha and A. A. Kulkarni
  Journal of Mathematical Economics, 2020
- **On independent cliques and linear complementarity problems** [PDF]
  K. Chadha and A. A. Kulkarni
  IJPAM, 2022
- **A reinforcement learning algorithm for restless bandits** [PDF]
  V.S. Borkar and K. Chadha
  Indian Control Conference, 2018

* denotes equal contribution

Ongoing Projects

Auditing private prediction

Developed novel techniques to audit the Renyi DP satisfied by a mechanism. Used the framework to elicit empirical privacy guarantees for a variety of private prediction algorithms like PATE, CaPC, PromptPATE and Private kNN across varying levels of adversary access and observation models.

Better White-Box Membership Inference Attacks

Working on developing better membership inference attacks with white-box access to mechanism outputs.

Scholarships and Awards

NVIDIA-TSMC Graduate Fellowship, Stanford University	2019
Sharad Maloo Gold Medal (for outstanding academic and extra-curricular achievements)	2019

- Bhavesh Gandhi Memorial Prize (for standing 1st in the Masters Programme) 2019
- Honda YES Award 2016
- Institute Academic Prize 2017, 2018

Skills & Courses

- **Courses:** Asymptotic Statistics, Information Theory and Statistics, Convex Optimization
- **Programming Languages & Frameworks:** Python, Numpy, JAX, Pytorch, Tensorflow

Academic Service

- Reviewer for NeurIPS, ICLR, AISTATS, ICML, SaTML, TMLR
- Organizer, ML Lunch, Stanford, Fall 2020
- Organizer, Workshop on Games and Networks, IIT Bombay, 2019