

Nirupam Gupta

Homepage: nirupam115.github.io. **Email:** nigu@di.ku.dk. **ORCID:** 0000-0003-4252-9319

Education

Doctor of Philosophy (Ph.D.)	2019
<i>Mechanical Engineering, University of Maryland, College Park, USA</i>	
Bachelors in Technology (B.Tech)	2013
<i>Electrical Engineering, Indian Institute of Technology, Delhi, India</i>	

Employment

Tenure-track Assistant Professor	2024 -
<i>Department of Computer Science, University of Copenhagen, Denmark</i>	
Postdoctoral Researcher	2021 - 2024
<i>School of Computer Science, EPFL, Switzerland</i>	
Postdoctoral Researcher	2019 - 2021
<i>Department of Computer Science, Georgetown University, USA</i>	

PhD Co-supervision

Mingzhi Wang. (co-supervisor: Prof. Yevgeny Seldin)	2025 -
<i>Department of Computer Science, University of Copenhagen, Denmark</i>	
Thomas Boudou. (co-supervisors: Dr. Aurélien Bellet & Dr. Batiste Le Bars)	2024 -
<i>INRIA-Inserm, University of Montpellier, France</i>	
Dr. John Stephan. (co-supervisors: Prof. Rachid Guerraoui & Dr. Rafael Pinot)	2021 - 2025
<i>School of Computer Science, EPFL, Switzerland</i>	
Dr. Shuo Liu. (co-supervisor: Prof. Nitin H. Vaidya)	2019 - 2024
<i>Department of Computer Science, Georgetown University, USA</i>	

Awarded Funding

Interaction between privacy and robustness in distributed learning	2025 - 26
Funds worth 14,000 € by the French CNRS (National Center for Scientific Research) for the above <i>international emerging action</i> .	
TruBrain: Trustworthy Distributed Brain-inspired Systems	2023 - 24
Awarded 522,452 CHF (550,000 €) by the Swiss NSF (National Science Foundation) through CHIST-ERA ERA-NET 2022 call for the above collaborative project involving 4 European institutes: Queen's University (coordinator), Sorbonne University, EPFL and Tubitak Bilgem.	

Research & Teaching Activities

My area of research is **distributed machine learning**, with focus on robustness and privacy. An updated list of my publications can be found on my [Google scholar profile](#). I teach the following courses at University of Copenhagen, since 2024. (i) **Machine Learning B (MLB)**: Introduction to the fundamentals of machine learning theory and algorithms. (ii)

Advanced Topics in Machine Learning (ATML): Introduction to differential privacy and distributed learning algorithms.

Bibliographic Overview

Co-authored a **textbook - Robust Machine Learning: Distributed Methods for Safe AI**, 1st edition published by Springer Nature in 2024. Published 36 peer-reviewed papers: 8 journals, 25 conferences and 3 workshops. **11 papers in A* rated conferences** (as per CORE Conference Rankings), namely NeurIPS, ICML, ICLR and PODC. As per Google Scholar, my **h-index is 20**.

Research Awards

Best Paper, International Conference on Distributed Computing and Networking (ICDCN)	2023
Best Paper Runner-up, International Symposium on Reliable Distributed Systems (SRDS)	2022

Selected Professional Activities

Affiliated to the Pioneer Center for AI, the Denmark Learning Theory and Applications (DeLTA) group, and the European Lab for Learning & Intelligent Systems (ELLIS), since 2024.

Program co-chair

International Conference on Networked Systems (NETYS), Rabat, Morocco	May, 2024
---	-----------

Program committees

AAAI International Conference on Artificial Intelligence	2026
ACM Conference on Computer and Communications Security (CCS)	2026
IEEE Secure and Trustworthy Machine Learning (SaTML)	2025 - 26
Symposium on Reliable Distributed Systems (SRDS)	2023

Co-organized workshops

Workshop on Machine Learning Theory at D3A Conference, Denmark	Aug, 2025
Workshop on Principles of Distributed Learning (PODL) at PODC, France	June, 2023
2nd PODL workshop, at DISC, L'Aquila, Italy	Oct., 2023
1st PODL workshop, at PODC, Salerno, Italy	July, 2022

Selected Invited Seminars

Machine Learning in Untrusted Environments. At Northeastern University, Rutgers University and University of Maryland - College Park, USA.	July - Aug., 2025
Machine Learning in Untrusted Distributed Environment. At the 33rd European Conference on Operational Research (EURO), Copenhagen, Denmark.	July, 2024
Machine Learning in Untrusted Environment. At INRIA Montpellier (France), INRIA Sophia-Antipolis (Nice, France) and University of Copenhagen (Denmark).	Dec., 2023
Tutorial on Byzantine Machine Learning. At the International Symposium on Distributed Computing (DISC'23), Italy.	Oct., 2023
Distributed Learning with Adversarial Nodes. At the GDR RSD Summer School on Distributed Learning, INRIA & CNRS Lyon, France.	Sept., 2023
Realizing Federated Learning in Untrusted Environment. At the 3rd IEEE Workshop on AI Hardware: Test, Reliability and Security (AI-TREATS), Italy.	May, 2023

Publications

Books and Chapters

Book: Robust Machine-Learning, Distributed Methods for Safe AI
Rachid Guerraoui, **Nirupam Gupta**, Rafael Pinot. *Springer Nature*, 2024

Chapter: Robustness & Privacy in Federated Learning

Rachid Guerraoui and **Nirupam Gupta**. *Springer*, 2024

Large Language Models and Cybersecurity: Trends in risk, exposure and mitigation.

Journal Publications

1. Byzantine Machine Learning: A Primer
Rachid Guerraoui, **Nirupam Gupta**, Rafael Pinot. *ACM Computing Surveys*, 2023.
2. Byzantine Fault-Tolerance in Federated Local SGD under 2f-Redundancy
Nirupam Gupta, Thinh T. Doan, and Nitin H. Vaidya. *IEEE Transactions on Control of Network Systems*, 2023.
3. On Pre-Conditioning of Decentralized Gradient-Descent when Solving a System of Linear Equations
Kushal Chakrabarti, **Nirupam Gupta**, and Nikhil Chopra. **IEEE Transactions on Control of Network Systems**, 2022.
4. Iterative Pre-Conditioning for Expediting the Distributed Gradient-Descent Method: The Case of Linear Least-Squares Problem
Kushal Chakrabarti, **Nirupam Gupta**, and Nikhil Chopra. **Automatica**, 2022.
5. Robustness of Iteratively Pre-Conditioned Gradient-Descent Method: The Case of Distributed Linear Regression Problem
Kushal Chakrabarti, **Nirupam Gupta**, and Nikhil Chopra. **IEEE Control Systems Letters**, 2021.
6. Preserving Statistical Privacy in Distributed Optimization
Nirupam Gupta, Shripad Gade, Nikhil Chopra, and Nitin H. Vaidya. **IEEE Control Systems Letters**, 2021.
7. False Data Injection Attacks in Bilateral Teleoperation Systems
Yimeng Dong, **Nirupam Gupta**, and Nikhil Chopra. *IEEE Transactions on Control Systems Technology*, 2018.
8. Content Modification Attacks on Consensus Seeking Multi-Agent System with Double-Integrator Dynamics
Yimeng Dong, **Nirupam Gupta**, and Nikhil Chopra. *AIP Chaos - Journal of Nonlinear Science*, 2016.

Conference Proceedings

Acronyms of **conferences rated A*/A** by CORE Conference Ranking are **in bold**.

Authors are listed in alphabetical order for my papers with Prof. Guerraoui, as per the norm in theoretical computer science community.

1. Adaptive Gradient Clipping for Robust Federated Learning
Youssef Allouah, Rachid Guerraoui, **Nirupam Gupta**, Ahmed Jellouli, Geovani Rizk, and John Stephan. *International Conference on Learning Representations (ICLR)*, 2025 [Spotlight, acceptance rate of 5%].

2. Revisiting Ensembling in One-Shot Federated Learning
Youssef Allouah, Akash Dhasade, Rachid Guerraoui, **Nirupam Gupta**, Anne-Marie Kermarrec, Rafael Pinot, Rafael Pires, Rishi Sharma. *In the 38th Conference on Neural Information Processing Systems (NeurIPS)*, 2024.
3. Fine-Tuning Personalization in Federated Learning to Mitigate Adversarial Clients
Youssef Allouah, Abdellah El Mrini, Rachid Guerraoui, **Nirupam Gupta** and Rafael Pinot. *In the 38th Conference on Neural Information Processing Systems (NeurIPS)*, 2024.
4. Tackling Byzantine Clients in Federated Learning
Youssef Allouah, Sadegh Farhadkhani, Rachid Guerraoui, **Nirupam Gupta**, Rafael Pinot, Geovani Rizk, and Sasha Voitovych. *Proceedings of the 41st International Conference on Machine Learning (ICML)*, 2024.
5. Robust Distributed Learning: Tight Error Bounds and Breakdown Point under Data Heterogeneity
Youssef Allouah, Rachid Guerraoui, **Nirupam Gupta**, Rafael Pinot, and Geovani Rizk. *In the 37th Conference on Neural Information Processing Systems (NeurIPS)*, 2023 [Spotlight, acceptance rate of 5%].
6. On the Privacy-Robustness-Utility Trilemma in Distributed Learning
Youssef Allouah, Rachid Guerraoui, **Nirupam Gupta**, Rafael Pinot, and John Stephan. *Proceedings of the 40th International Conference on Machine Learning (ICML)*, 2023.
7. Robust Collaborative Learning with Linear Gradient Overhead
Sadegh Farhadkhani, Rachid Guerraoui, **Nirupam Gupta**, Lê-Nguyễn Hoang, Rafael Pinot, and John Stephan. *Proceedings of the 40th International Conference on Machine Learning (ICML)*, 2023.
8. Fixing by Mixing: A Recipe for Optimal Byzantine ML under Heterogeneity
Youssef Allouah, Sadegh Farhadkhani, Rachid Guerraoui, **Nirupam Gupta**, Rafael Pinot, and John Stephan. *Proceedings of the 26th International Conference on Artificial Intelligence and Statistics (AISTATS)*, 2023.
9. Impact of Redundancy on Resilience in Distributed Optimization and Learning
Shuo Liu, **Nirupam Gupta**, and Nitin H. Vaidya. *Proceedings of the 24th International Conference on Distributed Computing and Networking (ICDCN)* [Best Paper], 2023.
10. Democratizing Machine Learning: Resilient Distributed Learning with Heterogeneous Participants
Karim Boubouh, Amine Boussetta, **Nirupam Gupta**, Alexandre Maurer, and Rafael Pinot. *Proceedings of the 41st International Symposium on Reliable Distributed Systems (SRDS)*, 2022.
11. Byzantine Machine Learning Made Easy by Resilient Averaging of Momentums
Sadegh Farhadkhani, Rachid Guerraoui, **Nirupam Gupta**, Rafael Pinot, and John Stephan. *Proceedings of the 39th International Conference on Machine Learning (ICML)*, 2022.
12. Accelerating Distributed SGD for Linear Regression using Iterative Pre-Conditioning
Kushal Chakrabarti, **Nirupam Gupta**, and Nikhil Chopra. *Proceedings of the 3rd Conference on Learning for Dynamics and Control (L4DC)*, 2021.
13. Byzantine Fault-Tolerance in Decentralized Optimization under 2f-Redundancy
Nirupam Gupta, Thinh T. Doan, and Nitin H. Vaidya. *The 2021 American Control Conference (ACC)*.
14. Differential Privacy and Byzantine Resilience in SGD: Do They Add Up?
Rachid Guerraoui, **Nirupam Gupta**, Rafaël Pinot, Sébastien Rouault, and John Stephan. *The ACM Symposium on Principles of Distributed Computing (PODC)*, 2021.

15. Approximate Byzantine Fault-Tolerance in Distributed Optimization
Shuo Liu, **Nirupam Gupta**, and Nitin H. Vaidya. *The ACM Symposium on Principles of Distributed Computing (PODC)*, 2021.
16. Preserving Statistical Privacy in Distributed Optimization
Nirupam Gupta, Shripad Gade, Nikhil Chopra, and Nitin H. Vaidya. *The 59th IEEE Conference on Decision and Control (CDC)*, 2020.
17. Fault-Tolerance in Distributed Optimization: The Case of Redundancy
Nirupam Gupta, and Nitin H. Vaidya. *The ACM Symposium on Principles of Distributed Computing (PODC)*, 2020.
18. Iterative Pre-Conditioning to Expedite the Gradient-Descent Method
Kushal Chakraborty, **Nirupam Gupta**, and Nikhil Chopra. *The 2020 American Control Conference (ACC)*.
19. On Distributed Solution of Ill-Conditioned System of Linear Equations under Communication Delays
Kushal Chakraborty, **Nirupam Gupta**, and Nikhil Chopra. *The Dec'19 Indian Control Conference (ICC)*.
20. Byzantine Fault-Tolerant Parallelized Stochastic Gradient Descent for Linear Regression
Nirupam Gupta, and Nitin Vaidya. *The 2019 Allerton Conference at UIUC*.
21. Statistical Privacy in Distributed Average Consensus: Bounded Real Inputs
Nirupam Gupta, Jonathan Katz, and Nikhil Chopra. *The 2019 American Control Conference (ACC)*.
22. Model-Based Encryption: Privacy of States in Networked Control Systems
Nirupam Gupta, and Nikhil Chopra. *The 2018 Allerton Conference at UIUC*.
23. Privacy in Distributed Average Consensus
Nirupam Gupta, Jonathan Katz, and Nikhil Chopra. *The World Congress of IFAC*, 2017.
24. Robustness of distributive double-integrator consensus to loss of graph connectivity
Nirupam Gupta, Yimeng Dong, and Nikhil Chopra. *The 2017 American Control Conference (ACC)*.
25. Confidentiality in Distributed Average Information Consensus
Nirupam Gupta, and Nikhil Chopra. *The 55th IEEE Conference on Decision and Control (CDC)* 2016.
26. On Content Modification Attacks in Bilateral Teleoperation Systems
Yimeng Dong, **Nirupam Gupta**, and Nikhil Chopra. *The 2016 American Control Conference (ACC)*.
27. Stability analysis of a two-channel feedback networked control system
Nirupam Gupta, and Nikhil Chopra. *The 2016 Indian Control Conference (ICC)*.