Nirupam Gupta

Nationality: Indian. Residence: Copenhagen, Denmark
(+45) 53 82 87 86, nigu@di.ku.dk

Education

Ph.D. Mechanical Engineering, University of Maryland, College Park, USA 2013 - 2018

Dissertation: Privacy in Distributed Multi-Agent Collaboration: Consensus and Optimization. **Advisor:** Prof. Nikhil Chopra

B.Tech. Electrical Engineering, Indian Institute of Technology, Delhi, India 2009 - 2013

Employment

Tenure-track Assistant Professor, Computer Science 2024 - present
University of Copenhagen, Denmark

Postdoctoral Researcher, Computer Science 2021 - 2024
EPFL, Switzerland [sponsored by Prof. Rachid Guerraoui]

Postdoctoral Researcher and **Teaching Faculty**, Computer Science 2019 - 2021
Georgetown University, USA [sponsored by Prof. Nitin H. Vaidya]

Research Assistant, Mechanical Engineering 2013 - 2018
University of Maryland, College Park, USA [sponsored by Prof. Nikhil Chopra]

PhD Co-Supervision

Sadegh Farhadkhani. PhD Candidate, Computer Science, EPFL, Switzerland. 2021 - present

John Stephan. PhD Candidate, Computer Science, EPFL, Switzerland. 2021 - present

Youssef Allouah. PhD Candidate, Computer Science, EPFL, Switzerland. 2021 - 2023

Shuo Liu. PhD, Computer Science, Georgetown University, USA. 2019 - 2024

Kushal Chakraborty. PhD, Electrical and Computer Engineering, University of Maryland, College Park, USA. 2018 - 2021

Funding

CHIST-ERA 2023

Co-PI at EPFL of *TruBrain* project, selected in the CHIST-ERA ERA-NET 2022 call on *Security and Privacy in Decentralised and Distributed Systems (SPiDDS).* Collaboration between 4 European institutes: Queen's University Belfast (coordinator), Sorbonne University, EPFL and Tubitak Bilgem. **Funds from Swiss NSF, worth** $522,452$ **CHF (approx.** $550,000$ **€).**

Awards

Best Paper, International Conference on Distributed Computing and Networking (ICDCN) 2023

Best Paper Runner-up, International Symposium on Reliable Distributed Systems (SRDS) 2022

Scholastic Honors

Merit Scholarship at the Indian Institute of Technology Delhi	2009 - 2010
India Central Board of Secondary Education Scholarship	2009 - 2013
All India Rank (AIR) 190 (/380,000) in IIT JEE (Joint Entrance Examination)	2009
AIR 130 (/960,000) in AIEEE (All India Engineering Entrance Examination)	2009

Outreach and Academic Service

Program co-chairing

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

Program committees

IEEE Secure and Trustworthy Machine Learning (SaTML)	2025
Dependable and Secure Machine Learning (DSML) workshop, at DSN	2021 & 2022
Symposium on Reliable Distributed Systems (SRDS)	2023

Co-organized workshops

3rd workshop on the Principles of Distributed Learning (PODL), at PODC, Nantes, France	June, 2023
2nd PODL workshop, at DISC, L'Aquila, Italy	Oct., 2023
1st PODL workshop, at PODC, Salerno, Italy	July, 2022

Invited talks

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, INRIA Sophia-Antipolis and University of Copenhagen	Dec., 2024
Tutorial on Byzantine Machine Learning. At the International Symposium on Distributed Computing (DISC'23)	Oct., 2023
Distributed Learning with Adversarial Nodes. At the GDR RSD Summer School on Distributed Learning	Sept., 2023
Realizing Federated Learning in Untrusted Environment. At the 3rd IEEE Workshop on AI Hardware: Test, Reliability and Security (AI-TREATS)	May, 2023

Reviewing for journals

Theoretical Computer Science (TCS)	Since 2023
Journal of Machine Learning Research (JMLR)	Since 2023
IEEE Transactions on Automatic Control (TAC)	Since 2016
Automatica and IEEE Transactions on Control of Networked Systems (TCNS)	Since 2017

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 top-tier conferences (rated A*/A by CORE Conference Ranking) are in bold.

1. 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.* [Accepted]
2. 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.* [Accepted]

3. 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.*

4. 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%].

5. 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.*

6. Robust Collaborative Learning with Linear Gradient Overhead
   Sadegh Farhadkhani, Rachid Guerraoui, Nirupam Gupta, Lê-Nguyên Hoang, Rafael Pinot, and John Stephan. *Proceedings of the 40th International Conference on Machine Learning* **(ICML)**, *2023.*

7. 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.*

8. 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), 2023.*

9. 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.*

10. 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.*

11. 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.*

12. Byzantine Fault-Tolerance in Decentralized Optimization under 2f-Redundancy
    Nirupam Gupta, Thinh T. Doan, and Nitin H. Vaidya. *The 2021 American Control Conference (ACC).*

13. 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.*

14. 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.*

15. 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.*

16. 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.*

17. Iterative Pre-Conditioning to Expedite the Gradient-Descent Method
Kushal Chakraborty, Nirupam Gupta, and Nikhil Chopra. *The 2020 American Control Conference (ACC).*

18. 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).*

19. Statistical Privacy in Distributed Average Consensus: Bounded Real Inputs
Nirupam Gupta, Jonathan Katz, and Nikhil Chopra. *The 2019 American Control Conference (ACC).*

20. Privacy in Distributed Average Consensus
Nirupam Gupta, Jonathan Katz, and Nikhil Chopra. *The World Congress of IFAC, 2017.*

21. Robustness of distributive double-integrator consensus to loss of graph connectivity
Nirupam Gupta, Yimeng Dong, and Nikhil Chopra. *The 2017 American Control Conference (ACC).*

22. Confidentiality in Distributed Average Information Consensus
Nirupam Gupta, and Nikhil Chopra. *The 55th IEEE Conference on Decision and Control (CDC) 2016.*

23. On Content Modification Attacks in Bilateral Teleoperation Systems
Yimeng Dong, Nirupam Gupta, and Nikhil Chopra. *The 2016 American Control Conference (ACC).*

24. Stability analysis of a two-channel feedback networked control system
Nirupam Gupta, and Nikhil Chopra. *The 2016 Indian Control Conference (ICC).*

Short Papers and Peer-Reviewed Workshops

1. Brief Announcement: A Case for Byzantine Machine Learning
Sadegh Farhadkhani, Rachid Guerraoui, Nirupam Gupta and Rafael Pinot. *The ACM Symposium on Principles of Distributed Computing* **(PODC)***, 2024.*

2. Redundancy in Cost Functions for Byzantine Fault-Tolerant Federated Learning
Shuo Liu, Nirupam Gupta, and Nitin H. Vaidya. *Workshop on Systems Challenges in Reliable and Secure Federated Learning (co-located with the 28th* **ACM SOSP***, 2021).*

3. Byzantine Fault-Tolerant Distributed Machine Learning with Norm-Based Comparative Gradient Elimination
Nirupam Gupta, Shuo Liu, and Nitin H. Vaidya. *The 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), 2021.*