

# Nirupam Gupta

DCL IC EPFL, Lausanne, Switzerland  
(+41) 77 209 70 50, nirupam.gupta@epfl.ch

## 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

## Research Experience

**Interest areas:** optimization, machine learning and control systems.

- Computer Science, EPFL, Switzerland.** Postdoc in the [Distributed Computing Laboratory \(DCL\)](#), supervised by Prof. Rachid Guerraoui. 2021 - present
- Computer Science, Georgetown University, USA.** Postdoc in the [Distributed Computing \(DISC\)](#) group, supervised by Prof. Nitin H. Vaidya. 2019 - 2021
- Mechanical Engg., University of Maryland College Park, USA.** Research asst. in the control systems group, supervised by Prof. Nikhil Chopra. 2013 - 2018

## Teaching Experience

- Teaching Faculty,** Computer Science, Georgetown University. 2020 - 2021  
Seminar course on distributed machine learning, including an introduction to the challenges of security (robustness) and privacy.

## PhD Co-Supervision Experience

- Sadegh Farhadkhani.** PhD Candidate, Computer Science, EPFL, Switzerland. 2021 - present
- Youssef Allouah.** PhD Candidate, Computer Science, EPFL, Switzerland. 2021 - present
- John Stephan.** PhD Candidate, Computer Science, EPFL, Switzerland. 2021 - present
- Shuo Liu.** PhD Candidate, Computer Science, Georgetown University, USA. 2019 - 2021
- Kushal Chakraborty.** PhD, Electrical and Computer Engineering, University of Maryland College Park, USA. 2018 - 2021

## Awards and Honors

### 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

## 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 ( <i>out of 380,000</i> ) in IIT JEE (Joint Entrance Examination)	2009
AIR 130 ( <i>out of 960,000</i> ) in AIEEE (All India Engineering Entrance Examination)	2009

## Fundings

<b>CHIST-ERA</b>	2023
------------------	------

Project *TruBrain* was selected in the CHIST-ERA ERA-NET call on *Security and Privacy in Decentralised and Distributed Systems (SPiDDS)*. **PIs:** Ihsen Alouani & Jesus Martinez Del Rincon (*Queen's University Belfast*); Haralampos G. Stratigopoulos (*Sorbonne University*); Rachid Guerraoui & Nirupam Gupta (*EPFL*); Hasan Erdem Yantir & Kaya Demir (*Tubitak Bilgem*). EPFL will receive funds from Swiss NSF, net worth 522,452 CHF, 2024 - 2027.

## Outreach and Academic Service

### Invited talks:

<b>Tutorial on Byzantine Machine Learning.</b> At the International Symposium on Distributed Computing (DISC'23)	Oct., 2023
<b>Realizing Federated Learning in Untrusted Environment.</b> At the 3rd IEEE Workshop on AI Hardware: Test, Reliability and Security (AI-TREATS)	May, 2023
<b>Distributed Learning with Adversarial Nodes.</b> At the GDR RSD Summer School on Distributed Learning	Sept., 2023
<b>Fault-Tolerant Distributed Gradient-Descent.</b> Data Skeptic podcast	Feb., 2021

### Co-organized workshops:

2nd workshop on the Principles of Distributed Learning (PODL) at DISC	Oct., 2023
1st PODL workshop at PODC	July, 2022

### Program committee member:

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

### Reviewer for journals:

IEEE Transactions on Automatic Control (TAC)	2016 - present
IEEE Transactions on Control of Networked Systems (TCNS)	2017 - present
IEEE Transactions on Signal Processing (TSIP)	2018 - present
IEEE Control Systems Letters (L-CSS)	2018 - present
IFAC (International Federation of Automatic Control) <i>Automatica</i>	2017 - present

## Book & Invited Chapter

**Book:** Robust Machine-Learning, Distributed Methods for Safe AI  
Rachid Guerraoui, Nirupam Gupta, Rafael Pinot.  
(In preliminary agreement with) Springer Nature Publishing Company.

**Invited Chapter:** Robustness & Privacy in Federated Learning  
Rachid Guerraoui and Nirupam Gupta.

Large Language Models and Cybersecurity: Trends in risk, exposure and mitigation. Scientific editors:  
Andrei Kucharavy, Octave Plancherel Valentin Mulder, Alain Mermoud and Vincent Lenders.  
Springer publishing company.

## 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

For papers with Prof. Rachid Guerraoui, the authors are listed in alphabetical order. For those papers, \* on my name indicates that I am a leading author.

1. On the Robustness of Distributed Machine Learning with Heterogeneous Data  
Youssef Allouah, Rachid Guerraoui, Nirupam Gupta, Rafael Pinot, and Geovani Rizk. **(Spotlight)**  
*In the 37th Conference on Neural Information Processing Systems (NeurIPS)*, 2023.

2. 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.
3. Robust Collaborative Learning with Linear Gradient Overhead  
Sadeh Farhadkhani, Rachid Guerraoui, Nirupam Gupta<sup>\*</sup>, Lê-Nguyen Hoang, Rafael Pinot, and John Stephan.<sup>1</sup> *Proceedings of the 40th International Conference on Machine Learning (ICML)*, 2023.
4. Fixing by Mixing: A Recipe for Optimal Byzantine ML under Heterogeneity  
Youssef Allouah, Sadeh Farhadkhani, Rachid Guerraoui, Nirupam Gupta, Rafael Pinot, and John Stephan. *Proceedings of the 26th International Conference on Artificial Intelligence and Statistics (AISTATS)*, 2023.
5. 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.
6. 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.
7. Byzantine Machine Learning Made Easy by Resilient Averaging of Momentums  
Sadeh Farhadkhani, Rachid Guerraoui, Nirupam Gupta<sup>\*</sup>, Rafael Pinot, and John Stephan. *Proceedings of the 39th International Conference on Machine Learning (ICML)*, 2022.
8. 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)*.
9. 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.
10. 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.
11. Byzantine Fault-Tolerance in Decentralized Optimization under 2f-Redundancy  
Nirupam Gupta, Thinh T. Doan, and Nitin H. Vaidya. *The 2021 American Control Conference (ACC)*.
12. Differential Privacy and Byzantine Resilience in SGD: Do They Add Up?  
Rachid Guerraoui, Nirupam Gupta<sup>\*</sup>, Rafaël Pinot, Sébastien Rouault, and John Stephan. *The ACM Symposium on Principles of Distributed Computing (PODC)*, 2021.
13. 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.
14. 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.
15. 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.

16. Iterative Pre-Conditioning to Expedite the Gradient-Descent Method  
Kushal Chakraborty, Nirupam Gupta, and Nikhil Chopra. *The 2020 American Control Conference (ACC)*.
17. 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)*.
18. Statistical Privacy in Distributed Average Consensus: Bounded Real Inputs  
Nirupam Gupta, Jonathan Katz, and Nikhil Chopra. *The 2019 American Control Conference (ACC)*.
19. Privacy in Distributed Average Consensus  
Nirupam Gupta, Jonathan Katz, and Nikhil Chopra. *The World Congress of IFAC, 2017*.
20. Robustness of distributive double-integrator consensus to loss of graph connectivity  
Nirupam Gupta, Yimeng Dong, and Nikhil Chopra. *The 2017 American Control Conference (ACC)*.
21. Confidentiality in Distributed Average Information Consensus  
Nirupam Gupta, and Nikhil Chopra. *The 55th IEEE Conference on Decision and Control (CDC) 2016*.
22. On Content Modification Attacks in Bilateral Teleoperation Systems  
Yimeng Dong, Nirupam Gupta, and Nikhil Chopra. *The 2016 American Control Conference (ACC)*.
23. Stability analysis of a two-channel feedback networked control system  
Nirupam Gupta, and Nikhil Chopra. *The 2016 Indian Control Conference (ICC)*.

## References

**Nikhil Chopra.** Professor, Mechanical Engineering, University of Maryland College Park, Maryland, USA. *Email:* [nchopra@umd.edu](mailto:nchopra@umd.edu)

**Nitin H. Vaidya.** Professor, Computer Science (McDevitt Chair), Georgetown University, Washington DC, USA. *Email:* [nitin.vaidya@georgetown.edu](mailto:nitin.vaidya@georgetown.edu)

**Rachid Guerraoui.** Full Professor, Computer Science, EPFL, Lausanne, Switzerland. *Email:* [rachid.guerraoui@epfl.ch](mailto:rachid.guerraoui@epfl.ch)