# 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

**Research area:** robustness and privacy in distributed optimization and machine learning.

| | |
|---|---|
| **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 |

## 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 |

## Journal Publications

1. **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.*

2. **On Pre-Conditioning of Decentralized Gradient-Descent when Solving a System of Linear Equations.**
Kushal Chakrabarti, <u>Nirupam Gupta</u>, and Nikhil Chopra. *IEEE Transactions on Control of Network Systems 2022.*

3. **Iterative Pre-Conditioning for Expediting the Distributed Gradient-Descent Method: The Case of Linear Least-Squares Problem**
Kushal Chakrabarti, <u>Nirupam Gupta</u>, and Nikhil Chopra. *Automatica 2022.*

4. **Robustness of Iteratively Pre-Conditioned Gradient-Descent Method: The Case of Distributed Linear Regression Problem**
Kushal Chakrabarti, <u>Nirupam Gupta</u>, and Nikhil Chopra. *IEEE Control Systems Letters 2021.*

5. **Preserving Statistical Privacy in Distributed Optimization**
<u>Nirupam Gupta</u>, Shripad Gade, Nikhil Chopra, and Nitin H. Vaidya. *IEEE Control Systems Letters 2021.*

6. **On Content Modification Attacks in Bilateral Teleoperation Systems**
Yimeng Dong, <u>Nirupam Gupta</u>, and Nikhil Chopra. *IEEE Transactions on Control Systems and Technology 2018 .*

7. **Content Modification Attacks on Consensus Seeking Multi-Agent System with Double-Integrator Dynamics**
Yimeng Dong, <u>Nirupam Gupta</u>, and Nikhil Chopra. *AIP Chaos - Journal of Nonlinear Science 2016.*

## Conference Proceedings (Complete DBLP List)

1. **On the Privacy-Robustness-Utility Trilemma in Distributed Learning**
Youssef Allouah, Rachid Guerraoui, <u>Nirupam Gupta</u>, Rafael Pinot, and John Stephan.[1] *Proceedings of the 40th International Conference on Machine Learning (ICML), 2023.*

2. **Robust Collaborative Learning with Linear Gradient Overhead**
Sadegh Farhadkhani, Rachid Guerraoui, <u>Nirupam Gupta</u>, Lê-Nguyên Hoang, Rafael Pinot, and John Stephan.[1] *Proceedings of the 40th International Conference on Machine Learning (ICML), 2023.*

3. **Fixing by Mixing: A Recipe for Optimal Byzantine ML under Heterogeneity**
Youssef Allouah, Sadegh Farhadkhani, Rachid Guerraoui, <u>Nirupam Gupta</u>, Rafael Pinot, and John Stephan.[1] Proceedings of the 26th *International Conference on Artificial Intelligence and Statistics (AISTATS), 2023.*

4. **Impact of Redundancy on Resilience in Distributed Optimization and Learning**
Shuo Liu, <u>Nirupam Gupta</u>, and Nitin H. Vaidya. *Proceedings of the 24th International Conference on Distributed Computing and Networking (ICDCN), 2023.*

5. **Democratizing Machine Learning: Resilient Distributed Learning with Heterogeneous Participants**
Karim Boubouh, Amine Boussetta, <u>Nirupam Gupta</u>, Alexandre Maurer, and Rafael Pinot. *Proceedings of the 41st International Symposium on Reliable Distributed Systems (SRDS), 2022.*

6. **Byzantine Machine Learning Made Easy by Resilient Averaging of Momentums**
Sadegh Farhadkhani, Rachid Guerraoui, <u>Nirupam Gupta</u>, Rafael Pinot, and John Stephan.[1] *Proceedings of the 39th International Conference on Machine Learning (ICML), 2022.*

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

---

[1]Authors in alphabetical order.

8. **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.*

9. **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 2021 (L4DC'21).*

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

11. **Differential Privacy and Byzantine Resilience in SGD: Do They Add Up?**
Rachid Guerraoui, Nirupam Gupta, Rafaël Pinot, Sébastien Rouault, and John Stephan.[1] *The ACM Symposium on Principles of Distributed Computing (PODC), 2021.*

12. **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.*

13. **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.*

14. **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.*

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

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

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

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

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

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

# Outreach and Academic Service

**Co-organizer:**

Workshop on the Principles of Distributed Learning (PODL) at PODC                    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) Automatica | 2017 - present |

## 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 *(out of 380,000)* in IIT JEE (Joint Entrance Examination) | 2009 |
| AIR 130 *(out of 960,000)* in AIEEE (All India Engineering Entrance Examination) | 2009 |

## References

**Nikhil Chopra.** Professor, Mechanical Engineering, University of Maryland College Park, Maryland, USA. *Email:* nchopra@umd.com

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

**Rachid Guerraoui**. Full Professor, Computer Science, EPFL, Lausanne, Switzerland. *Email:* rachid.guerraoui@epfl.ch