

Sayan Biswas

Research interests

Decentralized Machine Learning and Federated Learning focusing on Privacy, Fairness, and Personalization; Secure and Trustworthy Distributed Systems; Differential Privacy; Location Privacy.

Positions

2023 - present **Postdoctoral Researcher** at EPFL (Scalable Computing Systems Lab) – Lausanne, Switzerland.
Supervisor: Prof. Anne-Marie Kermarrec.

Education

2020 - 2023 **PhD in Computer Science** from INRIA, École Polytechnique, and Institut Polytechnique de Paris – Palaiseau, France.
IP Paris Award for the Best PhD Thesis in Computer Science.
Supervisor: Prof. Catuscia Palamidessi.

2016 - 2020 **Master of Mathematics (M.Math.)** with **First-Class Honours** from University of Bath – Bath, England.

Publications

Peer-Reviewed Conferences

- 2025 Jade Garcia Bourrée, Augustin Godinot, Martijn de Vos, Milos Vujasinovic, *Sayan Biswas*, Gilles Tredan, Erwan Le Merrer, Anne-Marie Kermarrec: “**Robust ML Auditing using Prior Knowledge**”. Proceedings of International Conference on Machine Learning (ICML) 2025. **Accepted as spotlight (top 2.6% papers).**
- 2025 *Sayan Biswas*, Davide Frey, Romaric Gaudel, Anne-Marie Kermarrec, Dimitri Lerévérend, Rafael Pires, Rishi Sharma, François Taïani: “**Low-Cost Privacy-Aware Decentralized Learning**”. Proceedings on Privacy Enhancing Technologies Symposium (PoPETs) 2025, Issue 3.
- 2025 *Sayan Biswas*, Anne-Marie Kermarrec, Alexis Marouani, Rafael Pires, Rishi Sharma, Martijn de Vos: “**Boosting Asynchronous Decentralized Learning with Model Fragmentation**”. Proceedings of the ACM Web Conference (WWW) 2025. **Selected for oral presentation (top 7% papers).**
- 2024 *Sayan Biswas*, Anne-Marie Kermarrec, Rishi Sharma, Thibaud Trinca, Martijn de Vos: “**Fair Decentralized Learning**”. Proceedings of IEEE Conference on Secure and Trustworthy Machine Learning (SaTML) 2025.
- 2024 *Sayan Biswas*, Mathieu Even, Anne-Marie Kermarrec, Laurent Massoulié, Rafael Pires, Rishi Sharma, Martijn de Vos: “**Noiseless Privacy-Preserving Decentralized Learning**”. Proceedings on Privacy Enhancing Technologies Symposium (PoPETs) 2025, Issue 1.
- 2023 *Sayan Biswas*, Kangsoo Jung, Catuscia Palamidessi: “**Tight Differential Privacy Guarantees for the Shuffle Model with k -Randomized Response**”. Proceedings of the International Symposium on Foundations and Practice of Security (FPS) 2023.
- 2023 *Sayan Biswas*, Catuscia Palamidessi: “**PRIVIC: A privacy-preserving method for incremental collection of location data**”. Proceedings of the Privacy Enhancing Technologies Symposium (PoPETs) 2024, Issue 1.
- 2023 Filippo Galli, *Sayan Biswas*, Kangsoo Jung, Tommaso Cucinotta, Catuscia Palamidessi: “**Group privacy for Personalized Federated Learning**”. Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP) 2023.
- 2022 *Sayan Biswas*, Graham Cormode, Carsten Maple: “**Impact of Sampling on Locally Differentially Private Data Collection**”. Proceedings of Competitive Advantage in the Digital Economy – Resilience, Sustainability, Responsibility, and Identity (CADE) 2022. **Winner of the Best Paper Award.**
- 2022 *Sayan Biswas*, Kangsoo Jung, Catuscia Palamidessi: “**Tight Differential Privacy Blanket for Shuffle Model**”. Proceedings of Competitive Advantage in the Digital Economy – Resilience, Sustainability, Responsibility, and Identity (CADE) 2022.
- 2021 *Sayan Biswas*, Kangsoo Jung, Catuscia Palamidessi: “**An Incentive Mechanism for Trading Personal Data in Data Markets**”. Proceedings of the International Colloquium on Theoretical Aspects of Computing (ICTAC) 2021.

Journals

- 2024 Ugur Ilker Atmaca, *Sayan Biswas*, Carsten Maple, Catuscia Palamidessi: “**A Privacy-Preserving Querying Mechanism with High Utility for Electric Vehicles**”. IEEE Open Journal of Vehicular Technology, Volume 5, pp 262-277.
- 2023 Filippo Galli, Kangsoo Jung, *Sayan Biswas*, Catuscia Palamidessi, Tommaso Cucinotta: “**Advancing Personalized Federated Learning: Group Privacy, Fairness, and Beyond**”. Springer Nature Computer Science, Volume 4, Issue 6, Article 831 (2023).

Book Sections

- 2021 Kangsoo Jung, *Sayan Biswas*, Catuscia Palamidessi: “**Establishing the Price of Privacy in Federated Data Trading**”. Protocols, Strands, and Logic, pp 232-250, LNCS 13066, Springer.

Non-Archival Workshops

- 2024 Sayan Biswas, Mark Dras, Pedro Faustini, Natasha Fernandes, Annabelle McIver, Catuscia Palamidessi, Parastoo Sadeghi: **"Bayes' capacity as a measure for reconstruction attacks in federated learning"**. Workshop on Security, Privacy, and Information Theory (Protect-IT) in conjunction with IEEE Computer Security Foundations Symposium (CSF) 2024. July 8, 2024; Enschede, The Netherlands.
- 2023 Sayan Biswas, Catuscia Palamidessi: **"PRIVIC: A privacy-preserving method for incremental collection of location data"**. Theory and Practice of Differential Privacy Workshop (TPDP) 2023. September 27-28, 2023; Boston, USA.
- 2023 Filippo Galli, Sayan Biswas, Kangsoo Jung, Tommaso Cucinotta, Catuscia Palamidessi: **"On the adaptive sensitivity of differentially private machine learning"**. The 4th Workshop on Privacy-Preserving Artificial Intelligence (PPAI) in conjunction with AAAI 2023. February 13, 2023; Washington DC, USA.
- 2022 Filippo Galli, Sayan Biswas, Kangsoo Jung, Tommaso Cucinotta, Catuscia Palamidessi: **"Group privacy for personalized federated learning"**. International Workshop on Federated Learning: Recent Advances and New Challenges (FL-NeurIPS) in conjunction with NeurIPS 2022. December 2, 2022; New Orleans, USA. One of the **Selected for oral presentation (top 10% papers)**.

Awards and Achievements

- 2024 Institut Polytechnique de Paris Award for Best PhD Thesis
- 2022 **Winner of the Best Paper Award at the Competitive Advantage in the Digital Economy – Resilience, Sustainability, Responsibility, and Identity (CADE) 2022** held in Venice, Italy
- 2018 **Qualified for the International Collegiate Programming Contest (ICPC) European Finals 2018** (*first solver of Problem 5 in the UK and Ireland qualification round*) held at TU Eindhoven, The Netherlands, representing University of Bath
- 2016 **Received an Honourable Mention in the final round of Indian National Philosophy Olympiad 2016** (*top 10 from India*)
- 2016 **Qualified the Zonal Informatics Olympiad, 2016** (*top 6 in West Bengal, India*), organised by the Indian Association for Research in Computing Science
- 2015 **Received an Honourable Mention at the International Linguistics Olympiad (IOL) Training Camp 2015** (*top 15 in India*) held at Microsoft Research Lab in Bangalore, India (the invitational round to be selected in the Indian team for IOL 2015)
- 2013 & 2014 **Qualified the Regional Mathematical Olympiad 2013 & 2014** (*top 28 in West Bengal, India*), organised by the National Board of Higher Mathematics and Homi Bhabha Centre for Science and Education

Miscellaneous Research Appointments

- Sep'23 - Oct'23 **Visiting Scholar**, Macquarie University, Sydney, Australia, Supervisors: Prof. Annabelle McIver and Dr. Natasha Fernandes.
- Jan'22 - Mar'22 **Visiting Scholar**, The University of Warwick, Coventry, England, Supervisors: Prof. Carsten Maple and Prof. Graham Cormode.
- Jun'20 - Aug'20 **Research Intern**, The University of Warwick, Coventry, England, Supervisors: Prof. Graham Cormode and Prof. Carsten Maple.
- Jun'19 - Sep'19 **Research Intern**, INRIA, Palaiseau, France, Supervisor: Prof. Catuscia Palamidessi.
- Jun'18 - Aug'18 **Research Intern**, Institute for Mathematical Innovation (IMI) and University of Bath, Bath, England, Supervisor: Prof. Christopher Jennison.

Teaching

- Aug'22 - Sep'22 **INRIA-DFKI European Summer School on AI (IDESSAI 2022)**, Saarbrücken, Germany, *Differential Privacy & Federated Learning: theory and implementation* (voted as the *most liked course* of IDESSAI 2022).
- Feb'21 - Jun'23 **École Polytechnique, Palaiseau, France**, CSE 102: Advanced Programming with Python.
- Oct'18 - May'20 **University of Bath, Bath, England**, XX10190: Programming & Discrete Mathematics with MATLAB (2018-19), MA10209: Algebra 1A (2019-20), and MA10212: Prob. & Stat. 1B (2019-20) .
- Jul'17 - Aug'17 **Humen Foreign Language School (HFLS), Humen, China**, Taught Mathematics and English at the HFLS International Summer Camp.

Academic Services

- 2024 Member of the Programme Committee – *IEEE Conference on Secure and Trustworthy Machine Learning (SaTML) 2025*
- 2023 - present Peer Reviewer – *IEEE Journal on Selected Areas in Information Theory*
- 2021 - present Peer Reviewer – *IEEE Transactions on Dependable and Secure Computing*
- 2022 Member of the Programme Committee – *AAAI Workshop Privacy Preserving Artificial Intelligence (PPAI) 2023*

Other Work Experience

- Nov'18 - May'20 Lead student-editor of Dept. of Mathematics newsletter of University of Bath
- Jul'19 Invigilator and examiner for the International Mathematical Olympiad (IMO) 2019 at Bath, UK
- Feb'17 - Nov'19 Project coordinator and head for Mathscon (UK's largest student-led maths conference)
- Jan'17 - Mar'20 Volunteer for United Kingdom Mathematics Trust and Mentor for British Mathematical Olympiad