Last Updated: December 8, 2025

Saswata Mukherjee

Homepage saswata@u.nus.edu profile

EDUCATION

PhD in Computer Science Aug 2024 - Present
School of Computing, National University of Singapore.
- **Advisor:** Dr. Divesh Aggarwal and Dr. Maciej Obremski

Masters in Computer Science Aug 2022 - Apr 2024
Chennai Mathematical Institute, Chennai, India.
- **Thesis:** Divisibility Testing, Factorization and Reduction to Polynomial Identity Testing in Algebraic Complexity Theory. [pdf]
- **Advisor:** Dr. Amit Kumar Sinhababu

Bachelors in Mathematics and Computer Science Aug 2019 - Apr 2022
Chennai Mathematical Institute, Chennai, India.

RESEARCH INTERESTS

Complexity Theory (specifically Boolean and Algebraic Complexity), Pseudorandomness, Information Theoretic Cryptography, Algebraic Methods in Theoretical Computer Science.

PUBLICATIONS

Under Submission

1. **Complete characterization of randomness extraction from DAG-correlated sources**, jointly with Divesh Aggarwal, Zihan Li, Maciej Obremski, João Ribeiro.
   Submitted.

Conference Publications

2. **Efficient randomized strong 2-source non-malleable extractor for any linear min-entropy**, jointly with Divesh Aggarwal, Pranjal Dutta, Satyajeet Nagargoje, Maciej Obremski. [pdf]
   In the proceedings of the 45th Annual International Cryptology Conference (CRYPTO 2025).

1. **Exponential Lower Bounds via Exponential Sums**, jointly with Somnath Bhattacharjee, Markus Bläser, Pranjal Dutta. [pdf]
   In the proceedings of the 51st EATCS International Colloquium on Automata, Languages and Programming (ICALP 2024).

RESEARCH PROJECTS/ INTERNSHIPS

Blackbox identity testing for variants of ROABPs. June - July, 2023.
IIT Kanpur, Kanpur, India.
- **Guide:** Dr. Nitin Saxena.

- Worked on blackbox polynomial identity testing of log-variate semi-diagonal circuits and some special type of ROABPs.

Exponential separation of complexity classes Aug 2022 - Sept 2023.
(Remotely)
- **Guide:** Dr. Markus Bläser.
- Worked on separation of algebraic complexity classes with the help of parameterization.

Determinantal complexity of generic polynomials. June - July, 2022
Saarland University, Saarbrücken, Germany.
- **Guide:** Dr. Markus Bläser.
- Engaged in finding several bounds (both upper and lower bounds) on exact and approximate (border) complexity, specially on uniform determinantal complexity of generic polynomials.

Reading project on complexity of approximation. Mar - Apr, 2023.
Chennai Mathematical Institute, Chennai, India.
- **Guide**: Dr. Partha Mukhopadhyay
- Studied determinantal complexity of some explicit polynomials and about the power of taking approximation in complexity classes.

Reading project on polynomial identity testing of ROABPs. May - June, 2021
(Remotely)
- **Guide:** Dr. Nitin Saxena [Report]
- Explored several approaches for solving blackbox polynomial identity testing, specially for ROABPs and diagonal circuits.

TALKS AND PRESENTATIONS

- Course presentation for **Complexity Theory II** Fall 2022
  $\mathsf{BPSpace}(s) \subseteq \mathsf{DSpace}(s^{3/2})$, by **Michael Saks & Shiyu Zhou** [Report]

- Course presentation for **Structure versus Hardness in Cryptography** Fall 2021.
  Efficient Lattice (H)IBE in Standard Model, by **Shweta Agrawal , Dan Boneh & Xavier Boyen** [Report]

ACADEMIC ACHIEVEMENTS

- Selected for Shriram & Infosys Scholarship for masters program in CMI. 2022
- Research fellow in Max Planck Institute for Software Systems. 2022
- Selected for Shriram Scholarship for undergraduate program in CMI. 2019

WORKSHOPS ATTENDED

- ICTS Workshop on HDX and Codes 28th Apr - 7th May, 2025
  ICTS, Bangalore.
- 8th Workshop on Algebraic Complexity Theory 31st Mar - 4th April, 2025
  Ruhr-Universität, Bochum.
- Quantum Computing Semester Jan - Apr, 2024
  Chennai Mathematical Institute.

- 7th Workshop on Algebraic Complexity Theory (WACT) Mar - Apr, 2023
  University of Warwick.
- gct2022 : School and Conference on Geometric Complexity Theory Fall 2021
  (online)

TEACHING ASSISTANTSHIP

In NUS

- **Discrete Structures (CS1231S)** Aug - Nov, 2025

In CMI

- **Computational Complexity 1** Jan - Apr, 2024
  Instructor: Dr. V. Arvind.
- **Discrete Mathematics** Jan - Apr, 2023
  Instructor: Dr. Amit Kumar Sinhababu & Dr. V. Arvind.
- **Computational Complexity 1** Jan - Apr, 2022
  Instructor: Dr. Prajakta Nimbhorkar.

OTHER PROFESSIONAL ACTIVITIES

- **Sub-reviewed for Conferences**:
  SODA 2026, TCC 2025, ASIACRYPT 2025, ITC 2025, EUROCRYPT 2025, SODA 2024.

REFERENCES

Dr. Divesh Aggarwal
Associate Professor
National University of Singapore,
Singapore.
mail: divesh@comp.nus.edu.sg

Dr. Pranjal Dutta
Assistant Professor
Nanyang Technological University,
Singapore.
mail: pranjal.dutta@ntu.edu.sg

Dr. Markus Bläser
Professor
Saarland University,
Saarbrücken, Germany.
mail: mblaeser@cs.uni-saarland.de

Dr. Amit Kumar Sinhababu
Assistant Professor
Chennai Mathematical Institute,
Chennai, India.
mail: amitks@cmi.ac.in

Dr. Partha Mukhopadhyay
Professor
Chennai Mathematical Institute,
Chennai, India.
mail: partham@cmi.ac.in

Dr. K.V. Subrahmanyam
Professor and Dean of Studies
Chennai Mathematical Institute
Chennai, India
mail: kv@cmi.ac.in