Manmatha Roy

Kolkata, India

✉ reach.manmatha@gmail.com
🔗 manmatha-roy.github.io

Graduate Courses

- Randomized Algorithms
- Sublinear Algorithms
- Cryptography
- Information Theory
- Optimization Techniques
- Computational Complexity
- Advanced Cryptography

Education

Ongoing **PhD in Computer Science**
Indian Statistical Institute
Kolkata, India

2020 **Master in Computer Science**
Indian Statistical Institute
Kolkata, India

2012 **Bachelor of Engineering in Computer Science**
Jadavpur University
Kolkata, indian

I am a researcher in the Crypto group at Indian Statistical Institute, Kolkata. My research interest lies broadly in Theoretical Computer Science and Cryptography. More specifically I am working on designing efficient algorithms for learning and testing functions over the Hamming Cube. Recently I have been looking into some problems in related to designing cryptographic primitives in the presence of stronger real-world adversaries e.g. leakage, subversion, trojan etc.

Experience

Dec 2022 - Now **Indian Statistical Institute, Kolkata**

Working as an **Associate Scientist**

Work details: Part of the core team, which manages IT infrastructures of ISI-Kolkata, specifically responsible for Cyber-Security Management and Incident Response

Sept 2022 - Dec 2022 **University of Warsaw**

Worked as a **Visiting Research Scientist** in Crypto group led by Prof. Stefan Dziembowski.

Work details: Worked on designing cryptographic primitives, secure in presence of real life adversaries e.g. leakage, tampering. and Two Party Secure Function Evaluation.

July 2020 - Dec 2020 **R C Bose Center for Cryptology and Security, Indian Statiscal Institute, Kolkata**

Worked as a **Senior Research Engineer** on a project , funded by National Technological Research Organization, Prime Ministers Office, Govt of India.

Work details: Classified.

Sep 2012 - Aug 2018 **Center for Distributed Computing, Jadavpur University, Kolkata**

Worked as a **Senior Research Engineer** in multiple projects funded by Funded by Advanced Systems Laboratory / System Planning and Integration Center, Defense Research and Development Organization, Govt of India.

Work details: Design and development of various software systems for Mission Critical Systems.

Manmatha Roy

Kolkata, India

✉ reach.manmatha@gmail.com
🔗 manmatha-roy.github.io

Publications

Ghosh, Kayal, Paraashar, and Roy, **Testing isomorphism of fourier sparse Boolean functions** *Submiited*

Dutta, Ghosh, Kayal, Paraashar, and Roy, **Testing isomorphism of Boolean functions over certain families of Abelian Groups** *Submitted*

Maitra, Chattopadhyay, Mandol, Tang, and Roy, **Efficient hardware implementation of Maiorana McFarland type cryptographically significant Boolean functions** *Submitted*

Ghosh, Kayal, Paraashar, and Roy, **Linear isomorphism testing of Boolean functions with small approximate spectral norm** *CoRR abs/2308.02662* **(2023)**

Maitra, Mandol, and Roy, **Modifying Bent Functions to obtain the Balanced ones with High Nonlinearity** *Indocrypt* **(2022)**

Maitra, Mandol, Tang, and Roy, **Experimental Results on Higher-Order Differential Spectra of 6 and 8-bit Invertible S-Boxes** *International Conference on Security, Privacy and Applied Cryptographic Engineering* **(2020)**

Teaching

Teaching Assistant Programming and Data Structures Lab, Indian Statistical Institute, Kolkata, Fall 2021

Co-Instructor Cryptology I, in M.Tech(CS & CrS) Programme, Indian Statiscal Institute, Kolkata, Spring 2021

Instructor Computing System Security-I, in M.Tech(CrS) Programme, Indian Statiscal Institute, Kolkata, Spring 2023

Instructor Cryptography and Security Implementation, in M.Tech(CrS) Programme, Indian Statistical Institute, Kolkata, Fall 2023

Instructor Computing System Security-I, in M.Tech(CrS) Programme, Indian Statiscal Institute, Kolkata, Spring 2024

Last updated: August, 2025.

Manmatha Roy

Kolkata, India

✉ reach.manmatha@gmail.com

🔗 manmatha-roy.github.io

References

- **Bimal Kumar Roy**

  Professor, Applied Statistics Unit, Indian Statistical Institute, Kolkata

  Email: bimal@isical.ac.in

- **Subhamoy Maitra**

  Professor, Applied Statistics Unit, Indian Statistical Institute, Kolkata

  Email: subho@isical.ac.in

- **Mridul Nandi**

  Professor, Applied Statistics Unit, Indian Statistical Institute, Kolkata

  Email: mridul.nandi@gmail.com

Last updated: August, 2025.