

Pabitra Mandal

pabitrामandal00@gmail.com |  mpabitra |  pabitrामandal

Purulia, West Bengal - 723126, India

RESEARCH INTEREST

My primary research interest is to enhance the privacy and efficiency in distributed systems using Multi-Party Computation. I am also keen on exploring areas such as Threshold Cryptography, Zero-Knowledge Proofs, Fully-Homomorphic Encryption, and Lattice-Based Cryptography.

EDUCATION

Indian Institute of Science

PhD. Computer Science and Engineering | Adv. Arpita Patra

Bengaluru, IN

Starting Aug. 2024

Indian Statistical Institute

M. Tech. Cryptology and Security | Percentage – 76.15

Kolkata, IN

Aug. 2022 – July 2024

Presidency University

M. Sc. Mathematics | CGPA – 7.75

Kolkata, IN

Nov. 2020 – Aug. 2024

Jagannath Kishore College

B. Sc. Mathematics | CGPA – 8.77

Purulia, IN

July 2017 – Oct. 2020

EXPERIENCE

WESEE, Ministry of Defence, Govt. of India

Research Intern

New Delhi, IN

Jan. 2024 – June 2024

- **Masters Dissertation:** Key Rotation using Updatable Encryption.
- Worked on some confidential projects.

SKILLS

- **Programming Languages:** C/C++, Python, SageMath, Rust.
- **Web Development:** HTML, CSS, Java Script.
- **Tools:** L^AT_EX.
- **Operating System:** Linux, Windows.

ACHIEVEMENTS

Joint CSIR-UGC NET (JRF) in Mathematics

June 2022

GATE in Mathematics

2022

CONFERENCE/WORKSHOP ATTENDED

TPMPC 2025

IISc Bengaluru

Asiacrypt 2024

TCG CREST, Kolkata

Indocrypt 2023

BITS Pilani, Goa