Pabitra Mandal

pabitram@iisc.ac.in | [in] mpabitra | [O] pabitramandal

Bengaluru, Karnataka - 560012, 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   Bengaluru, IN
PhD. Computer Science and Engineering | Adv. Arpita Patra   *Starting Aug. 2024*

Indian Statistical Institute   Kolkata, IN
M. Tech. Cryptology and Security | Percentage – 76.15   *Aug. 2022 – July 2024*

Presidency University   Kolkata, IN
M. Sc. Mathematics | CGPA – 7.75   *Nov. 2020 – Aug. 2024*

Jagannath Kishore College   Purulia, IN
B. Sc. Mathematics | CGPA – 8.77   *July 2017 – Oct. 2020*

EXPERIENCE

WESEE, Ministry of Defence, Govt. of India   New Delhi, IN
Research Intern   *Jan. 2024 – June 2024*

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

SKILLS

- **Programming Languages:** C/C++, Python, Rust.

- **Web Development:** HTML, CSS, Java Script.

- **Tools:** LaTeX.

- **Operating System:** Linux, Windows.

ACHIEVEMENTS

Joint CSIR-UGC NET (JRF) in Mathematics   June 2022

GATE in Mathematics   2022

CONFERENCE/WORKSHOP ATTENDED

TQC 2025   IISc Bengaluru

TPMPC 2025   IISc Bengaluru

Asiacrypt 2024   TCG CREST, Kolkata

Indocrypt 2023   BITS Pilani, Goa