# Arup Mazumder

Kolkata, West Bengal, India
mazumderj33@gmail.com — +91 7044184276 — arupmazumder.github.io — LinkedIn — GitHub

## Education

**M.Sc. in Mathematics**, University of North Bengal 2017–2019
Department of Mathematics
Scholarship: *Swami Vivekananda Merit-cum-Means, West Bengal State fellowship*
**B.Sc. (Hons) in Mathematics**, Rahara Ramakrishna Vivekananda Centenary College 2013–2017

## Research Experience

**Project Associate**, IISER Bhopal 2023–Present
Department of EECS, under Dr. Shashank Singh (funded by DRDO)

- Designed a lattice-based digital signature scheme (Module-LWE/SIS) inspired by Dilithium with faster signing and competitive key sizes.
- Performed cryptanalysis of Dilithium (BLISS, HAETAE, G+G) and Falcon (and its variants MITAKA, Zalcon, and Solmae); studied parameter choices and hardness assumptions using BKZ and core-SVP estimates.
- Implemented signature schemes in Python and benchmarked performance.

**Summer Internship**, QNu Labs, Bangalore Summer 2025

- Benchmarked Fully Homomorphic Encryption (FHE) libraries for training machine learning models.
- Hands-on work with OpenFHE and TenSEAL. [Certificate]

## Publications

- *Round-Optimal Lattice-based Identity-based Blind Signature*, manuscript in preparation.
- *Survey on Primal and Dual Attacks on LWE*, manuscript in preparation.

## Teaching Experience

**Guest Lecturer**, Mathematics, Greater Kolkata College of Engineering & Management 2019–2020
**Lecturer**, Mathematics, Swami Vivekananda Centre for Modern Studies 2021–2022
**Teaching Assistant**, IISER Bhopal 2024

- Courses: *Introduction to Modern Cryptography*, *Advanced Algorithms*.

## Workshops & Training

- NIWC 2024 Workshop on Lattice-based Cryptography, MNNIT Allahabad.
- Workshop on Post-Quantum Cryptography, IIT Indore, 2025.
- Attended advanced lectures in Algebraic Number Theory, Quantum Computing, and Modern Cryptography at IISER Bhopal.

## Technical Skills

- **Programming:** Python, C, SageMath, Linux
- **Cryptography:** Lattice-based crypto, Homomorphic Encryption (OpenFHE, TenSEAL)
- **Mathematical Expertise:** Algebraic Number Theory, Lattice Problems, Cryptanalysis, Complexity Theory

## Research Interests

Post-quantum cryptography, lattice-based cryptographic constructions, digital signatures, blind signatures, zero-knowledge proofs, homomorphic encryption, and lattice cryptanalysis.

## References

1. Dr. Shashank Singh, Assistant Professor, Dept. of EECS, IISER Bhopal, India
   shashank@iiserb.ac.in
2. Dr. Amit Kumar Chauhan, Senior Research Associate, QNu Labs, Bangalore, India
   amit.c@qnulabs.com

3. Dr. Dilip Chandra Pramanik, Assistant Professor of Mathematics, NBU, India
dcpramanik.nbu2012@gmail.com
4. Dr. Abhishek Mukherjee, Associate Professor of Mathematics, Kalna College, India
abhiquaternion@gmail.com