

# ABHIROOP SARKAR

✉ Mail  LinkedIn  GitHub  Scholar  Website

## Education

---

Institute of Engineering & Management, Kolkata

Oct. 2022 – July 2026

BTech in Computer Science & Engineering (Artificial Intelligence & Machine Learning)

–MAKAUT

- GPA: 9.36

NPTEL-Swayam

Jan 2023 – Nov 2024

Domain Scholar in Foundations of Computing (Computer Science) [Certificate](#)

- **Courses:** [Discrete Mathematics](#), [Design and Analysis of Algorithms](#) (Top 2%), [Introduction to Graph Algorithms](#), [Foundations of Cryptography](#) (Top 5%), [Approximation Algorithm](#)

## Research Interests

---

Cryptography, Secure Computing

## Experience

---

Presidency University, Kolkata — [Research Apprenticeship](#) — Prof. Dr. Avishek Adhikary May 2024 – July 2024

- Re-implemented multiple **Visual Cryptography** and **Secret Image Sharing (SIS)** schemes in Python, originally developed in SageMath.
- Implemented  $(k, n)$  and  $(t, k, n)$  Shamir's Secret Sharing schemes for images using finite fields (order 256) with Galois, NumPy, and PIL, achieving **lossless share reconstruction**.
- A custom **Regional Secret Image Sharing** model and integrating **region selection** and **image inpainting** with a two-secret sharing scheme. (Under progress)

## Research Publications

---

- 📄 *STAT-X: Short-term atmospheric temperature forecasting using machine learning models with explainable-AI*. Sarkar, A., Guha Roy, D., & Datta, P. (2025). Theoretical and Applied Climatology, Springer. — Impact Factor: 2.7 [doi](#)
- 📄 *AgroGenie: A smart approach to agriculture using machine learning*. Sarkar, A., Ganguly, K., Ghosh, S., Ghosh, D., Saha, S., Datta, P., & Guha Roy, D. (2024). In Lecture Notes in Networks and Systems. Springer. [doi](#)

## Projects

---

📁 **A Python framework for Secret Image Sharing** | *galois, PIL, secrets* | [GitHub](#) Ongoing

- A python library containing functions for  $(k,n)$ -threshold Visual Cryptography, and lossless  $(k,n)$ ,  $(t,k,n)$  **essential threshold** and **regional-Shamir's Secret Sharing** on Images.
- Ensured mathematically **exact reconstruction** using finite-field arithmetic, enabling cryptographically correct image sharing.
- Under Prof. Dr. Avishek Adhikary, Dept. of Mathematics, Presidency University.

📁 **RSA-Based Private Set Intersection (PSI)** | *secrets, RSA, hashlib* | [GitHub](#) February 2026

- Implemented a blind RSA-based **Private Set Intersection (PSI)** protocol in python enabling two parties to compute set intersection without revealing non-common elements with **linear on-line computation complexity**.
- Designed modular cryptographic components including hashing, full-domain hashing, RSA blinding, modular exponentiation and inverses over  $Z_n^*$  following a protocol described in [2009].
- Structured the project as a reusable Python package with separate client, server, and protocol code to ensure clarity and extensibility.

📁 **Short-Term Temperature Prediction using Machine Learning with eXplainable-AI** | [GitHub](#) Ongoing

- Implemented and evaluated supervised ML models for short-term min/max temperature forecasting from multivariate weather data for Kolkata.

- Performed Feature Engineering, and employed six algorithms, where **Gradient Boosting Regressor** and **Multi-Layer Perceptron** achieving the best performances.
- Applied model interpretability (**LIME, SHAP**) to identify key climatic factors, hance improving trust and scientific usability.
- Published in **Journal of Theoretical and Applied Climatology** Springer. — [doi](#)
- Extended to **probabilistic forecasting** using **NGBoost**, jointly predicting mean and standard deviation (uncertainty), with **Bayesian hyperparameter optimization** and **cross-city robustness** evaluation.

## Skills

---

**Programming & Tools:** Python, C, NumPy, Pandas, Git, LaTeX

**Research Skills:** Experimental Design, Scientific Writing

## Achievements

---

- AIR **2389** out of 211,020 candidates in GATE 2026-Computer Science. [Scorecard](#)
- NPTEL **Discipline Star** ( Appeared in atleast 8 exams in 4 semesters, passed in 75% of courses appeared, atleast one exam in each of the 4 semesters. ) in July-December 2024 Session. [Certificate](#)
- Recognized as a **Domain Scholar** in Foundations of Computing (Computer Science) by NPTEL, 2023-2024. - [Certificate](#)

## Training and Certifications

---

- ACM India Summer School in Foundations of Cryptography hosted by Trustlab, IIT Bombay: 2-weeks of intensive in-person lectures on cryptography with 60 participants. — [Link](#)
- Design and Analysis of Algorithms (Top 2%), NPTEL offered by IIT Madras– [Link](#)
- Foundations of Cryptography (Top 5%), NPTEL offered by IIIT Bangalore– [Link](#)
- Quantum Algorithms and Cryptography, NPTEL offered by IIT Madras – [Link](#)
- Computational Complexity (Topper), NPTEL offered by IIT Hyderabad – [Link](#)