Mrittika Nandi

DRDO Project JRF
IISER Bhopal

Email Id: nandimrittika@gmail.com
mrittikanandi@iiserb.ac.in
Webpage : mrittikanandi.com
LinkedIn : mrittikanandi14
Github : MrittikaNandi
Phone: +91-8335985957

Education

Indian Association for the Cultivation of Science, Jadavpur, Kolkata, India
Master of Science, School of Mathematical and Computational Sciences with Mathematics as major *Sept' 21 - July' 23*
CGPA: 7.85/10

Basanti Devi College, University of Calcutta, Kolkata, India
Bachelor of Science, Mathematics *Jul' 18 - Aug' 21*
CGPA: 8.822/10

South Point High School (CBSE), Kolkata, India
Higher Secondary *Apr' 16 - May' 18*
Percentage: 86.2

South Point High School (WBBSE), Kolkata, India
Secondary *Apr' 03 - Mar' 16*
Percentage: 90.57

Research Interests

Lattice-based cryptography: Exploring post-quantum secure primitives based on hard lattice problems, with applications to digital signatures, blind signatures, identity-based and searchable encryption, secure multi-party computation, secret sharing, privacy-preserving protocols, and blockchain systems.

Zero-knowledge proofs: In both pre-quantum and post-quantum setting, zero-knowledge proofs have immense applications especially in fields where anonymity are of primary importance. I am fascinated to use ZK proofs (NIZK/zk-SNARKS) to reduce the overhead of lattice-based approaches to make them lightweight and practical.

Lattice Reduction: The current state-of-the-art lattice basis reduction algorithms and their applications in the cryptanalysis of lattice-based protocols fascinate me. I am interested to work on making the enumeration and sieving algorithms for short vector generation more efficient and also use them as the SVP oracle in the BKZ algorithm.

Projects

DPI over encrypted traffic
SparQ Summer Internship, *QNu Labs* *May'25 - Aug'25*

- Investigated how middleboxes can accomplish deep-packet-inspection (DPI) on encrypted HTTPS traffic.
- Studied the 2015 paper "BlindBox: DPI over encrypted traffic".
- Gained a deep understanding of practical techniques for performing secure DPI.

New designs of post-quantum cryptographic candidates
Project JRF (DRDO), *Supervisor: Dr. Shashank Singh* *March'24-Present*

- Thoroughly cryptanalyzed Dilithium which includes understanding the parameter choices based on lattice reduction attacks and Core-SVP estimation techniques.
- Designed a new lattice-based digital signature scheme with the same hardness assumptions as Dilithium but with faster signing (less rejection/repetition).
- Simulated the behaviour of a BKZ reduced basis using the ZGSA assumption to obtain the optimal parameters for my scheme
- Implemented the scheme in python and benchmarked its performance for the NIST suggested security levels.

Wiener-Ito Integrals
MS Project, *Supervisor: Prof. Alok Goswami* *Sept'22-May'23*

- Studied Brownian Motion, Markov Processes, Wiener and Ito Integrals
- Applied the Ito formula to probabilistically solve the Dirichlet Problem, Heat Equation and some other parabolic PDEs

Flight Delay Prediction using Logistic Model
Summer Project, *Supervisor : Prof. Kiranmoy Das* *July'22-Sept'22*

- Gained expertise in running various machine-learning algorithms like k-means algorithm on a dataset from Kaggle along with hands-on experience in programming with R..
- Learned to use linear and logistic regression models for better predictive performance.

Relevant Courses

Undergraduate Courses

- Abstract Algebra (Group Theory, Ring Theory)
- Linear Algebra
- Classical Algebra (Number Theory)
- Probability and Statistics
- Discrete Mathematics (Combinatorics, Graph Theory)
- Data Structure and Algorithm
- Programming (C and Python)
- Topology, Real Analysis, Mathematical Modelling

Postgraduate Courses

- Algebra (Field Theory, Galois Theory)
- Object-Oriented Programming with C++
- Measure Theory and Probability
- Statistics with R
- MS Project (Brownian Motion, Stochastic Processes, Stochastic Integrals)

Additional Courses

- Modern Cryptography, Advanced Algorithms, Algebraic Number Theory
- Module Theory, Lattices and hard problems on lattices, Lattice Basis Reduction (LLL,BKZ), Lattice-based protocols, Zero-knowledge proofs (Research Work at IISER Bhopal)

Publications

Ayan Dutta, **Mrittika Nandi**, Smita Sarkar, Swetlina Hota, Suklav Ghosh (2023). "A MODEL-BASED APPROACH FOR FLIGHT DELAY PREDICTION". Indian Journal Of Applied Research, 13(5), 36–40. [DOI]

Other Scholastic Achievements

Q&A Expert in Advanced Mathematics at Chegg India

Secured highest marks in Mathematics and held the top rank across all science disciplines during my undergraduate studies (B.Sc.)

Qualified UGC NET June 2025 in the PhD only category

Experience

Attended the "Next-Gen Cybersecurity Workshop: Preparing for the Post-Quantum Era (Online Mode)" by IIT Indore in July, 2025.

Attended NIWC 2024 workshop on Lattice-based Cryptography held at MNNIT, Allahabad

Attended a talk on Godel's Incompleteness theorem by Dr. Shashi Mohan Srivastava at IACS, Kolkata.

Attended a talk on Recent Advances in Cryptology by Dr. Bimal Roy at IACS, Kolkata

Attended Winter School in Mathematics from 26/12/20 to 02/01/21 at St. Berchmans College

Did a Online short term course on Machine learning for Data Science using Python from 14/12/20 to 23/12/20 at NIT Warangal

Attended a Webinar on Cryptography and Web Security on 26/08/20 at Lady Brabourne College

Attended 'Infinity 2020' on 27/02/20 at Narendrapur Ramkrishna Mission College

languages

Bengali, English,Hindi

Skills

Python, Sage, C, C++, R

References

Dr. Shashank Singh
Assistant Professor, EECS, IISER BHopal
E-mail: shashank@iiserb.ac.in, sha2nk.singh@gmail.com

Prof. Kiranmoy Das
Professor, Applied Statistics and Data Science, Beijing Institute of Mathematical Sciences and Applications, Beijing, China
E-mail: kiranmoy.das@gmail.com

Prof. Alok Goswami (Retired Professor, ISI Kolkata)
Visiting Professor, School of Mathematical and Computational Sciences, IACS Kolkata
E-mail: alok.gosw@gmail.com

Dr. Amit Kumar Chauhan
Senior Research Associate, QNu Labs Pvt. Ltd., Bangalore, India
E-mail: amit.c@qnulabs.com