Ankit Kumar Misra

Fourth Year Undergraduate, CSE, IIT Bombay
ankitkmisra@cse.iitb.ac.in
www.cse.iitb.ac.in/~ankitkmisra
+91 98674 76895
ankitkmisra

Research Interests

Theoretical and Applied Cryptography, Algorithms, Theoretical Computer Science.

Education

2019 – 2023 (Expected) **Indian Institute of Technology Bombay** Major GPA = 9.64/10.0
Bachelor of Technology, Computer Science and Engineering.
Pursuing Honors in CSE.

Publications and Drafts

1. **Secure Non-Interactive Reducibility is Decidable.** (eprint.iacr.org/2022/1457.pdf)
   Accepted at the Theory of Cryptography Conference (**TCC**) 2022.
   With Kaartik Bhushan, Varun Narayanan, and Manoj Prabhakaran.
2. **Clearing a Growing 2D Region by Sequentially Eliminating Unit Discs.**
   In preparation. With Aaron Becker, Sándor Fekete, Christian Rieck, and Arne Schmidt.

Research Experience

2021-22 **Decidability of Secure Non-Interactive Reduction** *Trust Lab, IIT Bombay*
Guide: Prof. Manoj Prabhakaran | Research Project
– Proved decidability for the problem of determining the **existence** of a **statistical** SNIR between two arbitrary **correlation** matrices, using both **cryptographic** and **Boolean functional** analysis.
– Derived a new **junta theorem** for the **Fourier** transforms of functions over **generalized domains**.
– Investigated relations between **spectral properties** of source and target **multi-party** correlations.

2022 **Efficient Secure MPC for Sorting and its Applications** *Microsoft Research India*
Guide: Dr. Nishanth Chandran | Research Internship
– Surveyed current **literature** on secure multi-party computation methods of **private set intersection** (PSI), **sorting**, and **database joins**, over data distributed among several parties as **secret shares**.
– Applied **function secret sharing** (FSS) to develop a new efficient algorithm for secure sorting.
– Currently exploring applications of our work in **graph algorithms** and **aggregate measurement**.

2022 **CellTree: A Paradigm for Distributed Data Repositories** *Trust Lab, IIT Bombay*
Guide: Prof. Manoj Prabhakaran | Ongoing B.Tech. Thesis
– Designing **robust protocols** for a generalized, continually evolving **tree**-based data structure with **programmable** cells, capable of storing data with **liveness**, **correctness**, and **consistency** guarantees.
– Ideating efficient crew **leader election** & **inter-crew** communication schemes with **fault tolerance**.
– Planning to introduce **cryptographic** elements to preserve **privacy** between **crews** operating cells.

2021-22 **Algorithms for Clearage of Constantly Expanding 2D Regions** *TU Braunschweig, Germany*
Guide: Prof. Sándor Fekete | Research Internship
– Formulated unit disk placement **strategies** to constrain expanding 2D regions in $\mathbf{L_2}$ and $\mathbf{L_\infty}$ spaces.
– Programmed Python **simulators** and generated **performance plots** for comparing algorithms.
– Proved **upper bounds** on initial contamination size and currently working on **optimality proofs**.

2022 **Complexity Analysis of the KL-UCB Algorithm** *IIT Bombay*
Guide: Prof. Shivaram Kalyanakrishnan | Research Project
– Derived **time complexity** for computing KL-UCB values in an arbitrary iteration of a **multi-armed bandit**, assuming a **logarithmic** increase in **bit accuracy** requirements with each iteration.
– Proved **asymptotic optimality** of the algorithm even with only logarithmic increase in bit accuracy.

Key Projects

2021 **Cryptanalysis of Block Ciphers** *Guide: Prof. Manoj Prabhakaran*
Course Project | Cryptography and Network Security
– Studied and prepared a report on **differential** and **linear** cryptanalytic techniques for **block ciphers**.
– Performed a case study on the **FEAL-4** block cipher, by analyzing its structure, followed by successfully implementing and executing an **efficient** differential cryptanalytic **attack** for **complete key recovery**.

2022 **Efficient Key Recovery Attack on SIDH Key Exchange** *Guide: Prof. Bernard Menezes*
Course Project | Advanced Network Security and Cryptography
– Explored **isogeny**-based cryptography and implemented a recently discovered **key recovery** attack on Supersingular Isogeny Diffie-Hellman **key exchange**, previously conjectured to be **quantum secure**.

2020 **Decompiler: Register Transfer Language to Pseudo-C** *Guide: Prof. Amitabha Sanyal*
Course Project | Software Systems Lab
– Developed a **decompiler** to convert architecture dependent **RTL** into machine independent **pseudo-C** code, for enhanced **readability** across architectures, and deployed it on a **GUI** using Angular and Django.
– Applied **Lex** and **Bison** to **scan** and **parse** RTL, to identify key **elements** and **constructs** in the code.

2021 **Branch Prediction with TAGE and L-TAGE** *Guide: Prof. Biswabandan Panda*
Course Project | Computer Architecture
– Programmed 8+1 and 16+1 component **TAgged GEometric history length** branch predictors, with and without a 1024-entry **loop predictor**, in the **ChampSim** simulator, and tuned parameters for accuracy.
– Evaluated and compared **MPKI** with bimodal & hashed perceptron predictors, using 5 program traces.

2021 **Gaussian Mixture Models for Inverse Problems** *Guide: Prof. Ajit Rajwade*
Course Project | Advanced Image Processing
– Implemented **compressed sensing** over grayscale images using **GMMs**, having parameters initialized with a **directional PCA** basis and estimated iteratively using **MAP-EM** generalized for **non-zero means**.
– Utilized the trained GMMs for accurate image **inpainting** and **super-resolution** with low **RMSE**.

2020 **X-Ray Anomaly Detection using CNNs** *Institute Technical Council, IIT Bombay*
Institute Technical Summer Project | Ranked among Top 3 of 60+ Projects
– Employed **transfer learning** with **fine-tuning** on the CheXpert dataset to train five well-known **CNN** architectures to **detect** and **classify** each of five common thoracic diseases using chest X-rays.
– Developed a five-model **weighted ensemble** for prediction, with **AUC** score close to current **SOTA**.

Other Projects

2020 **Quantum Computing and Cryptography,** *Workshop on Quantum Computing with Qiskit*
Implemented the **BB84** Quantum Cryptography Protocol for secure communication through qubits, and **Deutsch-Josza** and **Grover's** algorithms to perform **classically expensive** computations efficiently.

2021 **Optimal Strategies for Anti-Tic-Tac-Toe,** *Course Project - Foundations of Intelligent and Learning Agents*
Modelled fixed-strategy adversaries as **Markov decision problems** to allow for strategy optimization through **policy iteration**, and applied this alternately on two random players until **convergence**.

2021 **Robust Mastermind Player,** *Course Project - Logic for Computer Science*
Applied **SAT solving** techniques and the **Z3 Theorem Prover** to formulate and implement a player for the game **Mastermind**, that can perform accurately against **unreliable** adversaries that sometimes lie.

2020 **Quadtrees for Image Storage and Transformations,** *Course Project - Data Structures and Algorithms*
Developed a C++ library to represent large and sparse **monochromatic images** with a **Quadtree** data structure, for efficient **storage** and **transformations** such as union, intersection, resizing, and cropping.

2021 **16-bit Multi-cycle RISC Processor,** *Course Project - Digital Logic Design*
Designed an 8-register, 16-bit multi-cycle processor with an **ISA** consisting of 15 instructions, implemented it in **VHDL**, and demonstrated the **datapath** along with the complete **controller-FSM** design.

2020 **Gestures for 3D Space,** *Seasons of Code - Web and Coding Club, IIT Bombay*
Applied **one-shot learning** to train a **Siamese** neural network for multi-label classification of 15 distinct hand gestures, by **pre-training** on an ASL dataset followed by **fine-tuning** on a self-created dataset.

Academic Achievements

- 2020 Received **Institute Academic Prize** for securing **Institute Rank 8** among **1000+** students at IIT Bombay.
- 2020 Awarded **Advanced Performer** (AP) grade (**top 2%**) in Quantum Physics, Calculus, & Physical Chemistry.
- 2022 Scored **118/120** on **TOEFL iBT**, and **169/170** (Quantitative) + **160/170** (Verbal) on **GRE General Test**.
- 2019 Secured **All India Rank 13** in **JEE Main** and **32** in **JEE Advanced**, among **1.2 million** candidates.
- 2019 Selected among **top 35** students in Indian National Physics Olympiad (**INPhO**), conducted by **HBCSE**.
- 2019 Attended the Orientation-cum-Selection Camp (**OCSC**) for International Physics Olympiad, and received the **Best Solution to a Challenging Problem** award from the **Indian Physics Association**.
- 2019 Among **top 300** selected for Indian National Olympiads in Chemistry (**INChO**) and Astronomy (**INAO**).
- 2019 Scored **470/450** (20 bonus) on **BITSAT** (Birla Institute of Technology and Science Admission Test).
- 2019 Received **KVPY** Fellowship from **Indian Institute of Science** (IISc) for securing **All India Rank 43**.

Teaching

Teaching Assistant

- 2022 **Design and Analysis of Algorithms** (CS 218M) *Course Instructor: Prof. Paritosh Pandya*
  Responsible for preparing **solutions** for **exam** and **tutorial** problems, along with **proctoring** exams and **grading** answer scripts, for **78 undergraduate students** from various years and departments.
- 2021 **Data Structures and Algorithms** (CS 213) *Course Instructor: Prof. Milind Sohoni*
  Developed and managed **course material** and **assignments**, conducted regular **tutorial** sessions, **proctored** examinations, and evaluated **answer scripts**, for a batch of **170+ CSE sophomores**.
- 2020 **Computer Programming and Utilization** (CS 101) *Course Instructor: Prof. Kameswari Chebrolu*
  Conducted weekly **QnA sessions** and **coding labs** for **13 freshers**, and **evaluated** project submissions.

Mentor - *Summer of Science (SoS)* *Maths and Physics Club, IIT Bombay*

- 2021-22 Guided **5** students in **Cryptography** (Summer 2022) and **4** students in **Deep Learning** (Summer 2021).

Technical Skills

- Programming: C/C++, Python, Java, MATLAB, Bash, SQL, VHDL, Assembly.
- Software & Tools: LaTeX, Git, Lex, Yacc, Keras, TensorFlow, PyTorch, ChampSim, NS-3, Qiskit, Quartus.
- Web Development: HTML, CSS, Bootstrap, JavaScript, JQuery, Flask, Angular, Django, NodeJS.

Relevant Coursework

Cryptography and Network Security	Logic for Computer Science	Error Correcting Codes*
Adv. Tools for Modern Cryptography	Databases and Info. Systems	Automata Theory
Game Theory and Mechanism Design*	Data Structures and Algorithms	Computer Networks
Implementation of Prog. Languages	Advanced Image Processing	Computer Architecture
Intelligent and Learning Agents	AI and Machine Learning	Operating Systems

*To be completed by November 2022.

Extracurriculars

- 2020 Completed **80 hours** of community service at **Green Campus**, under the National Service Scheme (**NSS**).
- 2019 Worked as a **Publicity Organizer** at **Techfest**, Asia's Largest Science and Technology Festival.
- 2016 Represented school at **Indian Model United Nations** (INMUN), hosted by Ryan International Group.
- 2020 Engineered a **Bluetooth**-controlled bot as part of the XLR8 competition, conducted by **ERC**, IIT Bombay.
- 2020 Declared IIT Bombay **center topper** in **Mimamsa**, a national **science quiz** conducted by IISER Pune.