Bhumika Mittal

mittalbhumika7@gmail.com | mittalbhumika7 | bhumikamittal7 | bhumikamittal.in

Research Interest

My research interests include **cryptography** and **computational complexity**, with a focus on lattice-based cryptography. In particular, I am working on the fine-grained complexity of lattice problems and pre-image samplable trapdoor functions. I am also interested in quantum cryptography and quantum computing.

Education

Ashoka University — Sonipat, India

Diploma in Advanced Studies and Research, Computer Science — *2024 – Present*

Thesis: Threshold Pre-Image Samplable Trapdoor Functions

Bachelor of Science (Honours), Computer Science; CGPA: 3.90/4.00 — *2021 – 2024*

Minors in Mathematics, and Entrepreneurial Leadership & Strategy

Relevant Coursework

Lattice-based Cryptography, SAT Solvers, Computer Security and Privacy, Elliptic Curves and Cryptography, Quantum Computing, Investigation of Dilithium, Blockchain and Cryptocurrencies, Theory of Computation

Research Experience

IIT Delhi — New Delhi, India

Research Assistant — *Sept 2024 – Present*

- Designing a scalable reduction from the Closest Vector Problem to Weighted Max-SAT for even norms
- Implementing the reduction using the RC2 MaxSAT solver to evaluate its scalability and efficiency

Max Planck Institute for Software Systems — Saarbrücken, Germany

Visiting Research Fellow — *May 2024 – Aug 2024*

- Proposed the PACT metric for evaluating phase-concurrent execution efficiency
- Benchmarked various data structures for diverse graph workloads like analytics, traversals, and pattern matching
- Designed a system to efficiently handle a wide range of heterogeneous graph workloads, achieving improved throughput and performance

Centre for Artificial Intelligence and Robotics, DRDO — New Delhi, India

Research Intern — *Nov 2023 – May 2024*

- Designed an indigenous lattice-based post-quantum public key encryption and signature scheme
- Implemented constant-time code in C and deployed it in internal software
- Conducted a study on NIST PQC finalists, contributing to the security framework against algebraic attacks

IIT Gandhinagar — Gandhinagar, India

Research Assistant — *May 2023 – Sept 2023*

- Built a tool to model data flow in computation graphs for memory hierarchy evaluation
- Analyzed the transformer architecture (BERT) to identify hardware-level operations for efficient inference
- Proposed an architecture to reduce power consumption; used Timeloop-Accelergy for energy and latency estimates

Publications

Vortex: Efficient Adaptive Graph Store — *in progress*

Seemant Achari, **Bhumika Mittal**, Ashvin Goel, Laurent Bindschaedler

Energy-Efficient Accelerator Design for Language Models for Edge Computing — Philosophical Transactions A

Tom Glint, **Bhumika Mittal**, Santripta Sharma, Abdul Ronak, Abhinav Goud, Neerja Kasture, Zaqi Momin, Aravind Krishna, Joycee Mekie

On the Existence of Balanced Generalized de Bruijn Sequences — Discrete Mathematics Journal

Matthew Baker, **Bhumika Mittal**, Haran Mouli, Eric Tang — *Link to paper*

Honors and Awards

2024 **Summa Cum Laude**, Ashoka University
2024 **Silver Medalist**, Department of Computer Science, Ashoka University
2024 **Builder's Award for Service Excellence**, Department of Computer Science, Ashoka University
2022 **Undergraduate Research Excellence Award**, Department of Mathematics, Ashoka University
2021-24 **Dean's List** (every semester), Ashoka University

Other Experiences

Ashoka University Sonipat, India
7 × Teaching Assistant *Aug 2022 – May 2024*

- Teaching Assistant for multiple courses like Data Structures, Discrete Mathematics (student feedback: 4.88/5)
- Facilitated the Science Communication module at the Lodha Genius Program for 200+ high school students

Lehigh University Bethlehem, US
Exchange Student *May 2022 – Jun 2022*

- Consulted for Global Good Fund, establishing metrics to evaluate ESG impact, measure non-monetary outcomes
- Strategized optimal investment approaches to enhance ESG goals and ensure measurable financial outcomes

Plaksha University Mohali, India
Instructor *April 2023 - June 2023*

- Taught a Microcontrollers course to 200+ high school students through IoT projects using ESP32 chipset
- Designed a game development module, building 5 mathematical and hardware games for hands-on learning

WebVeda Remote
Tech and Product Manager *Feb 2021 – April 2022*

- Ideated and developed the platform, scaling to 300k learners and generating $1M revenue within 10 months
- Managed tech infrastructure, including payment gateways, email integration, and other critical components

Other Activities

Mathematics for post-quantum cryptanalysis Eötvös Loránd University
Student Participant – Selected with a Full Grant *August 2024*

Undergrad Architecture Mentoring Workshop (uArch) ISCA 2024, Argentina
Selected with a Full Grant *July 2024*

Summer Research Institute on Systems, Security, and Privacy EPFL
Participant *July 2024*

Workshop on Lattice-based Post-quantum Cryptography Ashoka University
Speaker, Co-organiser *April 2024*

Academic Affairs Board Ashoka University
Computer Science Student Representative *May 2023 – May 2024*

IEEE Ashoka Student Branch Ashoka University
Director of Technology *Aug 2023 – May 2024*

Computer Science Society Ashoka University
Student Advisor, President *Aug 2022 – May 2024*

Technical Skills

Languages: Python, C/C++, Solidity, Assembly, SML, HTML
Technologies: Qiskit, Hyperledger Fabric, Git, LaTeX, Docker, SageMath
Other: Arduino Uno, ESP32, Raspberry Pi Pico