

Bhumika Mittal

✉ mittalbhumi7@gmail.com | 📧 mittalbhumi7 | 🌐 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

Diploma in Advanced Studies and Research, Computer Science

Thesis: Threshold Pre-Image Samplable Trapdoor Functions

Sonipat, India

2024 – Present

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

Research Assistant

New Delhi, India

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

Visiting Research Fellow

Saarbrücken, Germany

May 2024 – Aug 2024

- Proposed the PACT metric for evaluating phase-concurrent execution efficiency
- Benchmarking 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

Research Intern

New Delhi, India

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

Research Assistant

Gandhinagar, India

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 AND EXPOSITIONS

Vortex: Efficient Adaptive Graph Store

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

in progress

SEAL-ME: Secure, Energy-Efficient Accelerator Design for Language Models

Tom Glint, **Bhumika Mittal**, Santripta Sharma, Abdul Ronak, Aravind Krishna, Joycee Mekie

in review

On the Existence of Balanced Generalized de Bruijn Sequences

Bhumika Mittal, Haran Mouli, Eric Tang, Matthew Baker [link]

Discrete Mathematics Journal

April 2023

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

7 × Teaching Assistant

Sonipat, India

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

Exchange Student

Bethlehem, US

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

Instructor

Mohali, India

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

Tech and Product Manager

Remote

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 system components.

OTHER ACTIVITIES

Mathematics for post-quantum cryptanalysis

Selected Student Attendee

Eötvös Loránd University

August 2024

Summer Research Institute on Systems, Security, and Privacy

Participant

EPFL

July 2024

Undergrad Architecture Mentoring Workshop (uArch)

Full Grant Recipient

ISCA 2024, Argentina

June 2024

Workshop on Lattice-based Post-quantum Cryptography

Speaker, Co-organiser

Ashoka University

April 2024

Academic Affairs Board

Computer Science Student Representative

Ashoka University

May 2023 – May 2024

IEEE Ashoka Student Branch

Director of Technology

Ashoka University

Aug 2023 – May 2024

Computer Science Society

Student Advisor, President

Ashoka University

Aug 2022 – May 2024

TECHNICAL SKILLS

Programming & Development: C/C++, Python, Solidity, Assembly, Git, Qiskit, Hyperledger Fabric

Hardware & Tools: Timeloop/Accelergy, ESP32, Raspberry Pi Pico, L^AT_EX, Docker, SageMath