

Bhumika Mittal

 mittalbhumika7@gmail.com |  bhumikamittal7 |  bhumikamittal.in

RESEARCH STATEMENT

My research interests lie in **theoretical computer science**. In particular, I have worked on the design and analysis of lattice-based signature schemes, including my undergraduate thesis on ring trapdoor functions, which focuses on developing a general framework for secure ring signatures. I am interested in studying the foundations of quantum computing, complexity theory, and cryptography, along with formal logic, and exploring their interconnections.

EDUCATION

Ashoka University

Sonipat, India

Postgraduate Diploma in Advanced Studies and Research; CGPA: 3.93/4.00

2024 – 2025

Thesis: Ring Trapdoor Functions: A Lattice-Based Framework for Secure Ring Signatures

Bachelor of Science (Honours), Computer Science; CGPA: 3.90/4.00

2021 – 2024

Minors in Mathematics, and Entrepreneurial Leadership & Strategy

RELEVANT COURSEWORK

Information and Coding Theory, Computer Security and Privacy, Lattice-based Cryptography, Foundations of Dilithium, Blockchain and Cryptocurrencies, Quantum Computing, Symbolic Logic, Theory of Computation, Games on Graphs

RESEARCH AND WORK EXPERIENCE

Amuse Labs

Bengaluru, India

Software Engineer

July 2025 – Present

- Designing a verification endpoint that validates puzzle invariants, ensures correctness, and supports quality checks
- Improving the automated testing tool Gandalf to expand code coverage and validate system correctness
- Developed the Word Flower playlog and hint features for PuzzleMe, a digital platform for smart games, prioritizing type safety, documentation, and maintainability

IIT Delhi

New Delhi, India

Research Assistant

Sept 2024 – Jan 2025

- Designed an alternative reduction from the Closest Vector Problem to Weighted Max-SAT for even norms
- Implemented the reduction using the RC2 MaxSAT solver to evaluate its scalability and efficiency in practice

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 and analyzed lattice-based schemes for quantum-safe migration of internal communications systems
- Implemented a constant-time cryptographic module now in active use for confidential communications
- Authored a comprehensive technical report evaluating the security properties, performance, and implementation feasibility of proposed post-quantum cryptographic primitives

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 to identify hardware-level operations for efficient inference
- Proposed an architecture to reduce power consumption; used Timeloop-Accelergy for energy and latency estimates

PUBLICATIONS

AxLaM: Energy-Efficient Accelerator Design for Language Models for Edge Computing

Tom Flint, Bhumika Mittal, Santriptha Sharma, Abdul Ronak, Abhinav Goud, Neerja Kasture, Zaqi Momin, Aravind Krishna, Joycee Mekie

Philosophical Transactions A

[Link to paper](#)

On the Existence of Balanced Generalized de Bruijn Sequences

Matthew Baker, Bhumika Mittal, Haran Mouli, Eric Tang

Discrete Mathematics Journal

[Link to paper](#)

HONORS AND AWARDS

2025 Academic Excellence Award, Department of Computer Science, Ashoka University

2025 Teaching Assistantship Excellence Award, Department of Computer Science, Ashoka University

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

OTHER EXPERIENCES

Ashoka University

8 × Teaching Assistant

Sonipat, India

Aug 2022 – May 2025

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

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

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

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 components

OTHER ACTIVITIES

Workshop on Lattice-based Post-quantum Cryptography

Speaker, Student Organiser

Ashoka University

April 2024

Winter and Summer Schools in Cryptography and Security

Selected Participant

Multiple Locations

2023 – 2025

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, Interim President

Ashoka University

Aug 2022 – May 2024

TECHNICAL SKILLS

Languages: TypeScript, Java, Python, C/C++, SQL, HTML, SCSS, Solidity, Assembly, SML

Technologies: Qiskit, Hyperledger Fabric, Git, L^AT_EX, Docker, SageMath, Markdown

Other: Arduino Uno, ESP32, Raspberry Pi Pico