# Bhumika **Mittal**

mittalbhumika7@gmail.com | bhumikamittal.in

## Research Statement

My research interests lie in **theoretical computer science**. My work thus far has focused on theoretical cryptography, particularly lattice-based cryptography. 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

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

## Research and Work Experience

**Amuse Labs** — Bengaluru, India

*Software Engineer* — *July 2025 – Present*

- Improving the automated testing tool Gandalf to expand codebase coverage and validate system correctness
- Developing new features for PuzzleMe, a digital platform for smart games, in TypeScript and Java

**IIT Delhi** — New Delhi, India

*Research Assistant* — *Sept 2024 – Jan 2025*

- Proposed 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 post-quantum cryptographic schemes, focusing on theoretical security properties and hardness assumptions
- Studied the security foundations of NIST PQC finalists, analyzing their underlying algebraic structures and resistance to quantum attacks
- Implemented constant-time cryptographic primitives with provable security guarantees

**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** — Philosophical Transactions A
Tom Glint, **Bhumika Mittal**, Santripta Sharma, Abdul Ronak, Abhinav Goud, Neerja Kasture, Zaqi Momin, Aravind Krishna, Joycee Mekie — *Link to paper*

**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

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** — Sonipat, India
*8 × Teaching Assistant* — *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

**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

**Workshop on Lattice-based Post-quantum Cryptography** — Ashoka University
*Speaker, Student Organiser* — *April 2024*

**Winter and Summer Schools in Cryptography and Security** — Multiple Locations
*Selected Participant* — *2023 – 2025*

**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, Interim President* — *Aug 2022 – May 2024*

## Technical Skills

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