Bhumika **Mittal**

mittalbhumika7@gmail.com | bhumikamittal7 | bhumikamittal.in

Research Statement

My research interests lie in **theoretical computer science** and how it can help create safe and guaranteed systems. In this process, I have had the opportunity to work on cryptography, formal verification, and systems. I have worked on the design and analysis of lattice-based signature schemes, implemented SAT solvers for the CVP problem, and designed verification endpoints for production codebases.

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

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

Max Planck Institute for Software Systems — Saarbrücken, Germany

Visiting Research Fellow — *May 2024 – Aug 2024*

- Benchmarked various data structures for diverse graph workloads like analytics, traversals, and pattern matching
- Designed PACT: a metric to measure how far a system deviates from an ideal phase-concurrent execution
- Implemented a dynamic graph store with selective snapshot versioning that decouples readers from writers, achieving 72% reduction in read latency and 31% increase in throughput compared to lock-based approaches

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 and hardware optimization
- Designed an accelerator architecture, achieving 9x energy and 58% area reduction compared to existing systems
- Analyzed transformer architectures to identify hardware-level optimizations, enabling efficient deployment of language models on edge devices

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

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

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

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*

Program in Mathematics for Young Scientists Boston, US
Mehta Fellow *Jul 2020 – Aug 2021*

Relevant Coursework

Trustworthy AI, 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

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