Shashwatha Mitra G B

Email : smitragb@gmail.com
Github: https://github.com/Shashwatha-Mitra
Mobile : +91 9902038220

Education

University of Wisconsin - Madison — Madison, USA
Masters' in Computer Science; GPA: ***3.88/4.00*** — *Sep 2023 - May 2025*
Completed Courses: Cryptographic Proof Systems, Parallel Architecture, Distributed Systems
Thesis: Succinct Classical verification for BatchQMA in under 8 rounds

National Institute of Technology Karnataka — Mangalore, India
Bachelors in Computer Science and Engineering; GPA: ***9.66/10.00*** — *Jul 2017 - May 2021*
Thesis: Hierarchical Load Balancing using Bayesian estimation for resource utilization.

Work Experience

Member of Technical Staff — Bangalore, India
Oracle, India (IDC) — *Jul 2021 - Aug 2023*

Portfolio: Oracle In-Memory Expressions (IME) technology stack
Description: Data stored In-Memory using columnar formats that cache expressions for fast access.

- Sped up analytic queries involving DATE columns by ***6x*** and a ***minimal space overhead***.
- Maintained and Extended IME support to internal teams resulting in a ***2x*** query execution speedup.
- Worked on Oracle's public **23ai** database release with multiple bug fixes and enhancements

Research Experience

Quantum and Lattice-Based Crytography, Research Associate — Madison, USA
Dept of Computer Science, UW Madison — *Jan 2024 - Dec 2024*

Guide: Rishab Goyal, UW Madison, WI

- Developed an interactive protocol that could enable a future with quantum-classical cloud infrastructure.
- Studied and implemented enhancements for Lattice-based Zero Knowledge Proof of Knowledge systems.
- Experience with primitives such FHE, polynomial commitment schemes, signatures, and Merkle trees.

Graduate Teaching Assistant — Madison, USA
Dept of Mathematics, UW Madison — *Sep 2023 - May 2025*

- TA for the course: Calculus II (MA 222) from Sep 2023 to Dec 2024.
- TA for the course: Calculus III (MA 234) from Jan 2025 to May 2025.

Research Intern — Bangalore, India
Remote Internship — *June 2020 - Aug 2020*

Supervisor: Dr. S. Swayamjyothi, Indian Institute of Technology (IIT), Bhubaneshwar

- Surveyed numerical schemes to solve the ***Navier-Stokes equations*** under various flow conditions
- The study focused on Finite difference, Finite Volume, Spectral, and Monte-carlo simulation methods.

Research Intern — Bangalore, India
Dept. of Supercomputer Education and Research Center, IISc — *May 2019 - Jul 2019*

Supervisor: Prof R. Govindarajan, Indian Institute of Science (IISc)

- **Prefetchers**: Memory architecture that fetch cache lines ahead of their access.
- **Results**: Used microbenchmarks with specific access patterns to determine working of Intel's prefetchers. Successfully corroborated the working of a couple of the L1 and L2 prefetchers for the Haswell architecture.

Skills and Interests

Languages: **Adept**: C, **Intermediate**: C++, Python, **Begineer**: Rust, JavaScript, Java
Tools: gRPC, sqlite3, CUDA, vim, Confluence, gdb, OpenSSL, MySQL
Security and Cryptography: Crystals-Dilitihium, Crystals-Kyber, TLS/SSL, FIPS
Soft Skills: Mentorship, Critical/Analytical thinking, Team-player, Communication, Project Management

Publications

- **Succinct Arguments for BatchQMA and Friends under 8 rounds** San Diego, USA
  Accepted for publication at CRYPTO 2025 Aug 2025
  Authors: Rishab Goyal, Aditya Jain, *Shashwatha Mitra G B*
- **HTmRPL++ : A Trust-Aware RPL routing protocol** Bangalore, India
  12th International Conference on COMSNETS Jan 2020
  Authors: Nishanth S, *Shashwatha Mitra G B*, John P.M, Chandrasekaran K

Projects

Batching Lattice-based Zero Knowledge proofs for Integer Relations Mar 2025
Independent Project, **Stack**: C

- Extended the Integer Relations proof system with a corresponding security proof.
- Achieved **5x** smaller proof sizes and **2x** faster verification.
- Used FIPS202 implementation of SHAKE/SHA128 for simulating random oracles.

Efficient Hashing and Secure Proofs for Data Integrity Dec 2024
Independent Project, **Stack**: C

- Candidate construction for succinct local hash functions by using SHA256/SHAKE and Merkle trees.
- Enables secure local openings, allowing integrity verification with minimal overhead.

CR and Hermes Replication for a durable Key-Value Store Oct 2024
Course: Distributed Systems, **Stack**: C++, gRPC, SQLite3

- Fault-tolerant KV store with CR and Hermes Replication (https://hermes-protocol.com/)
- Ensured linearizability and performance across distributed GET/PUT operations.

Cache Coherence in Multi-Chiplet GPUs May 2024
Course: Advanced Computer Architecture II (Parallelism), **Stack**: gem5, C++

- Extended a table-based coherence protocol to reduce flushes/invalidations at kernel boundaries.
- By tracking GPU content at data-structure level, achieved an increase in L2 cache reuse by **20%**

Numerical Solver for Young's Double Slit Experiment Dec 2023
Course: Computational Mathematics I, **Stack**: Python

- Implemented Crank-Nicholson, ADI, and Fourier Spectral methods for numerical simulation.
- Scaled ADI to a 1000×1000 grid and validated results by observing fringe patterns.

Fair Queue and Token Bucket NF Jun 2020
Course: Advanced Computer Networks, **Stack**: C

- Implemented the Token Bucket and Fair Queue NF functionality using *openNetVM*
- Tested the performance of the Token Bucket NF. Verified stable throughput using *PktGen*.
- The Token Bucket NF was merged upstream after verifying functionality.

Cache Simulator Apr 2019
Course: Advanced Computer Architecture, **Stack**: C++

- A multi-level cache simulator to simulate replacement policies: lru, nru, srrip, etc.
- Analysed impact of block size and associativity on cache-hits using matrix-multiplication benchmark.

Extra Curricular

- Project head of Computer Society, **IEEE NITK** Student Chapter. Supervised multiple projects.
- Represented my local soccer team at C-division level in Bangalore (2022/23 season)

Academic Achievements

- Ranked **4th** in a class of 108 students in my undergrad.
- Ranked **3163** in JEE Mains (2017) out of 1.2 million candidates (**99.97** percentile).
- Ranked **29** at the Karnataka State Common Entrance Tests (KCETs) out of 150,000 students.