Anubhav Bhatla

✉ bhatlaanubhav2001@gmail.com • 🌐 anubhavbhatla.github.io
in anubhav-bhatla • 🎓 Anubhav Bhatla

Research Interests

I am broadly interested in Computer Architecture, Reliability, and Hardware Security. This includes advanced topics such as accelerator reliability, secure caches, and branch predictor design.

Education

Massachusetts Institute of Technology *(Sep 2025 - Present)*
Doctor of Philosophy in Electrical Engineering and Computer Science

Indian Institute of Technology Bombay *(Nov 2020 - Aug 2025)*
Integrated Bachelor and Master of Technology (Dual Degree) in Electrical Engineering *GPA: 9.39/10*
Minor Degree in Computer Science and Engineering

Publications

- A. Bhatla[†], Navneet[†], M. Qureshi, B. Panda. **"The Avatar Cache: Enabling On-Demand Security with Morphable Cache Architecture."** *Under review at an A security conference*
- A. Bhatla[†], H. Bhavsar[†], S. Saha, B. Panda. **"So, You Think You Know All About Secure Randomized Caches?"** *Presented at the USENIX Security Symposium **(USENIX Security'25)*** (Paper, Talk, Artifact)
  Distinguished Artifact Award Winner
- A. Bhatla[†], Navneet[†], B. Panda. **"The Maya Cache: A Storage-efficient and Secure Fully-associative Last-level Cache."** *Presented at the International Symposium on Computer Architecture **(ISCA'24)*** (Paper, Talk, Artifact)

[†] *denotes equal contribution*

Research Experience

Reliability of Accelerators against Silent Data Corruptions *(Sep 2025 - Present)*
Prof. Mengjia Yan, MIT (Collaborators: AMD | Prof. Joel Emer, MIT)

- Studied the effects of SDCs on **CNN accelerators** by analyzing faulty model weights and accuracy
- Analyzing various fault models for **systolic array**-based **LLM attention** accelerators and studying the **performance-hardware tradeoffs** of various mitigation techniques
- Developing an **in-house simulator** to model the effects of hardware faults in LLM attention

Practical and Secure Randomized Last-level Cache Design (Thesis) *(Jan 2023 - Aug 2025)*
Prof. Biswabandan Panda, IIT Bombay

1. **Maya Cache Design**
   - Thoroughly studied the Mirage cache design, which provides security against conflict-based attacks at a high power, storage and area overhead, and observed that > **80%** of the entries brought into the last-level cache are dead
   - Designed a security model for Maya, based on **Markov chains**, and simulated it for 1 trillion cache accesses, along with a mathematical proof to show that no set-associative evictions occur in over 10^{32} cache accesses (**10^{16} years**)
   - Modelled the Maya cache in the **ChampSim** simulator and **PCACTI** 7nm FinFET to show savings in storage (2%), power (5%), energy (13%), and area (28%), compared to a traditional non-secure set-associative cache
   - Used the **CacheFX** simulator to show that Maya performs similarly to a fully-associative cache against **occupancy-based attacks**, by estimating the number of encryptions required to break AES and modular exponentiation
2. **Avatar Cache Design** *(Collaborator: Prof. Moinuddin Qureshi, Georgia Tech)*
   - Analyzed the practicality and **design complexity** of various state-of-the-art secure LLC designs such as Mirage and Maya, to design a simpler and more practical LLC design with very little overheads
   - Observed that **increasing the cache associativity** along with **invalidation** of a fraction of cache lines helps provide security against conflict-based attacks without using any tag store-data store decoupling or storage of pointers
   - Provided **"security-on-demand"** by providing the user with the option of security in the BIOS. If the user opts for no security, Oasis operates as a traditional non-secure set-associative cache, operating at **zero overheads**
   - Implemented the Avatar design on the **ChampSim** multi-core simulator and **PCACTI** 7nm FinFET to show a < 0.2% performance overhead, a 2% power overhead, 0.9% storage overhead when operating in the secure mode

3. **Demystifying Randomized Caches** *(Collaborators: Intel India | Prof. Sayandeep Saha, IIT Bombay)*
   - Performed a thorough security analysis of various state-of-the-art secure cache designs such as Mirage and Maya, to understand the **minimal set** of **necessary and sufficient additions** required to make the LLC secure
   - **Systematized** the various secure cache design features such as the use of skews, extra invalid tag ways, tag store-data store decoupling, high associativity, replacement policy, and remapping, and analyzed their security impact **individually** and **in conjunction** with one another
   - Advocated for **high associativity** designs as they provide robust security with minimal design complexity and overheads
   - Provided **new insights** into the effect of these knobs against **occupancy-based attacks**, showing how only partitioning-based solutions can mitigate low- and full-occupancy-based attacks

Branch Predictor Partitioning for Performance *(Apr 2024 - Present)*
Prof. Dean Tullsen, University of California, San Diego

- Studied the **Half&Half** branch predictor partitioning technique and how partitioning the branch predictor between threads can help improve performance for certain application pairs running in **SMT** mode
- Used the **perf** tool to identify application pairs from the **SPEC2017** benchmark suite that have high conditional branch mis-prediction rates when running in SMT mode on the same core
- Implemented the **branch-alignment algorithm** suggested in Half&Half on top of the **LLVM** compiler to align conditional branches to the appropriate program counter values to ensure that only half of the conditional branch predictor is used
- Working on identifying **prediction-critical workloads** that don't perform well when running concurrently with another process in SMT mode, and will benefit from using a partitioned conditional branch predictor

Secure Cache-line Reallocation in Partitioned Caches (Report) *(Jul 2022 - Nov 2022)*
Prof. Virendra Singh, IIT Bombay

- Studied and implemented the **UCP** and static cache partitioning technique on the **Sniper** multi-core simulator, along with **PASS-P**, which provides security against side-channel attacks for dynamic cache-partitioning techniques
- Analyzed **SPEC2006** benchmark pairs for performance, focusing on clean re-allocated blocks and dead blocks.
- Proposed and **implemented modifications** to PASS-P, based on observing a high dead block percentage, to **preferentially reallocate dead blocks** on every phase change instead of dirty blocks, thereby reducing dead blocks by over **10%**

Honours & Awards

- Won the **Distinguished Artifact Award** at the USENIX Security Symposium (SEC'25) *(2025)*
- Awarded the **Intel India Research Fellowship** 2024-25 with a total grant of INR 800,000 ($9500) *(2024)*
- Ranked **5th** among **99** students enrolled in the Electrical Department Dual Degree program *(2024)*
- Awarded **Undergraduate Research Award** by IIT Bombay for excellence in research and development *(2023)*
- Secured **All India Rank 266** in Joint Entrance Exam, JEE (Advanced) among 160,000 candidates *(2020)*
- Awarded the Kishore Vaigyanak Protsahan Yojana (**KVPY**) fellowship with **All India Rank 337** *(2018)*

Teaching & Mentorship Experience

Graduate Application Assistance Program (GAAP) Mentor *(Sep 2025 - Present)*

- Supported **3** graduate student applicants throughout their application journey and provided **feedback** on materials
- Helped **10+** applicants from **under-represented groups** with doubts about graduate applications via **one-off sessions**

Department Academic Mentor *(May 2024 - Jun 2025)*
Student Mentorship Program, IIT Bombay

- Selected as part of a **54**-member team handpicked after a rigorous process of meticulous interviews and peer reviews
- Appointed to personally mentor **6 sophomores** with their academics, extra-curricular activities, career paths, and research journeys during the rigorous second year in Electrical Engineering at IIT Bombay
- Contributed to the department website blog and collected course feedback, providing academic help to **1300+** students

Teaching Assistant
Served as a TA for Electrical Engineering and Computer Science students in the following courses:

- CS773: Comp. Arch. for Performance and Security (100+ students) Instructor: *Prof. Biswabandan Panda* *(2025)*
- EE789: Algorithmic Design of Digital Systems (80+ students) Instructor: *Prof. Madhav Desai* *(2025)*
- CS683: Advanced Computer Architecture (100+ students) Instructor: *Prof. Biswabandan Panda* *(2024)*
- EE229: Signal Processing (90+ students) Instructor: *Prof. Preeti Rao* *(2024)*
- EE309: Microprocessors (200+ students) Instructor: *Prof. Virendra Singh* *(2022)*

Responsible for creating **assignment problems**, conducting **doubt-solving sessions** to help academically weak students, creating **tutorial solutions**, helping with the **course evaluation**, and academically mentoring students

Professional Experience

Embedded Software Intern *(May 2023 - Jul 2023)*
Texas Instruments India, Bangalore *Internship*

- Created a **driver-monitoring application** for the AM62Ax Sitara MPU, capable of detecting **driver-drowsiness** and **gaze-detection** to ensure that the driver is attentive towards the road, which helps reduce the risk of accidents
- Used the **GStreamer** media framework to create a new media pipeline which enables **stacking of multiple DNN models**, required for using multiple DNN models to efficiently and correctly make classifications using just the driver's face
- Analyzed and documented the **boot flow** of various microprocessors and created a boot loader **porting guide** for the Sitara AM62x MPU, which makes it easier to port user applications from a different microprocessor to the AM62x

Selected Academic Projects (Full list)

Sliced-Out-of-Order Core Implementations (Report) *(Jul 2023 - Nov 2023)*
Prof. Virendra Singh, IIT Bombay *EE748: Advanced Topics in Computer Architecture*

2-way OoO Superscalar Processor Design (Repository) *(Jul 2022 - Nov 2022)*
Prof. Virendra Singh, IIT Bombay *CS683: Advanced Computer Architecture*

24-channel EEG Data Acquisition System (Report, Code) *(Jan 2023 - Nov 2023)*
Prof. Siddharth Tallur, IIT Bombay *Research Exposition & EE344: Electronic Design*

Optimal Device Design for NIPIN Memory Selector (Report) *(Jan 2024 - Apr 2024)*
Prof. Udayan Ganguly, IIT Bombay *EE724: Nanoelectronics*

CMOS Implementation of Low Power Equi-Prop System (Report) *(Jul 2023 - Nov 2023)*
Prof. Udayan Ganguly, IIT Bombay *EE746: Neuromorphic Engineering*

Technical Skills

Languages	C, C++, VHDL, Verilog, Python, Assembly (8085), Algorithmic assembly (Aa), Heptagon
Software	Intel Quartus, Vivado, Fusion360, Cadence Virtuoso, Synopsys Sentaurus, LTSpice
Simulators	ChampSim, gem5, Sniper, GPGPU-Sim, CacheFX, PCACTI

Courses Undertaken (Full list)

Computer Systems: Advanced Computer Architecture - I, Advanced Computer Architecture - II, Operating Systems, High-Performance Scientific Computing, Microprocessors§

Hardware Design: VLSI Design§, Algorithmic Design of Digital Systems, RF Microelectronics Chip Design, Testing & Verification of VLSI Circuits, CMOS Analog VLSI Design, Electronic Design, Neuromorphic Engineering, Foundation of VLSI CAD, Nanoelectronics

Computer Science: Formal Reasoning about Programs†, Data Structure & Algorithms, Design & Analysis of Algorithms, Principles of Data & System Security, Embedded Systems, Discrete Structures

Electrical Engineering: Digital Systems§, Analog Circuits§, Communication Networks, Wireless & Mobile Communication, Information Theory & Coding, Electronic Devices§, Signal Processing§, Control Systems§

†*MIT courses* §*along with a lab component*