Sarabjeet Singh, Ph.D Candidate.

sarab@cs.utah.edu https://www.cs.utah.edu/~sarab/
sarabjeet-singh-1b02b67b sarabjeetsingh007 Google Scholar

I am a fifth-year PhD student at the University of Utah, working on accelerating modern cryptographic primitives, ranging from efficient memory integrity verification to Post Quantum Cryptography to applications of Fully Homomorphic Encryption.

Professional Experience

05/22 – 08/22 **NVIDIA Research,** *Co-op,* Project: Homomorphic Encryption at Modern GPU Datacenter Scale.

05/20 – 08/20 **AMD Research,** *Co-op,* Project: Processing In Memory.

08/19 – · · · · **University of Utah,** *Research/Graduate Assistant,* Advisor: Prof. Rajeev Balasubramonian.

09/18 – 06/19 **Ashoka University,** *Junior Research Fellow,* Project: Design of Main Memory Architectures for Next Generation Datacenter Servers.

01/18 – 08/18 **Indian Institute of Technology, Gandhinagar,** *Junior Research Fellow,* Project: Design of Main Memory Architectures for Next Generation Datacenter Servers.

08/17 – 12/17 **Hexagon Capability Center India Hyderabad,** *Software Analyst,* Project: Oracle Application Express (APEX) platform.

Research Publications

Conference Proceedings

1. **S. Singh**, S. Singh, S. Gudaparthi, X. Fan, and R. Balasubramonian, "Hyena: Balancing Packing, Reuse, and Rotations for Encrypted Inference," in *IEEE Symposium on Security and Privacy (SP)*, IEEE, 2024 (accepted, yet to publish) Outline: Faster Homomorphic Encryption based inference.
2. S. Gudaparthi, **S. Singh**, S. Narayanan, R. Balasubramonian, and V. Sathe, "CANDLES: Channel-aware novel dataflow-microarchitecture co-design for low energy sparse neural network acceleration," in *2022 IEEE International Symposium on High-Performance Computer Architecture (HPCA)*, IEEE, 2022, pp. 876–891.
3. **S. Singh** and M. Awasthi, "Efficacy of statistical sampling on contemporary workloads: The case of SPEC CPU2017," in *2019 IEEE International Symposium on Workload Characterization (IISWC)*, IEEE, 2019, pp. 70–80.
4. **S. Singh** and M. Awasthi, "Memory centric characterization and analysis of spec cpu2017 suite," in *Proceedings of the 2019 ACM/SPEC International Conference on Performance Engineering*, 2019, pp. 285–292.

Journal Articles

1. **S. Singh**, X. Fan, A. K. Prasad, *et al.*, "XCRYPT: Accelerating Lattice Based Cryptography with Memristor Crossbar Arrays," *IEEE Micro*, 2023.
2. **S. Singh**, N. Surana, K. Prasad, P. Jain, J. Mekie, and M. Awasthi, "HyGain: High-performance, Energy-efficient Hybrid Gain Cell-based Cache Hierarchy," *ACM Transactions on Architecture and Code Optimization*, vol. 20, no. 2, pp. 1–19, 2023.
3. S. N. Ved, **S. Singh**, and J. Mekie, "Pane: Pluggable asynchronous network-on-chip simulator," *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, vol. 15, no. 1, pp. 1–27, 2019.

Workshops/Blogs

1. **S. Singh**, S. Singh, and R. Balasubramonian, *EPIC: Efficient Packing for Inference using Cheetah*, 6th Workshop on Cognitive Architectures, hosted in conjunction with HPCA 2022, 2022.
2. **S. Singh**, *Post Quantum Cryptography*, ACM SigArch Computer Architecture Today Blog, 2021.

Ongoing/Past Research Projects

On-going work

01/21 – · · · · **Efficient Integrity Verification using Custom DIMM**, Reducing the cost of integrity verification in trusted environments with near-memory support.

08/23 – · · · · **ZPU: Zero-Knowledge Proof Processing Units**, Novel high throughput Processing units for MSM/NTT kernels to maximize throughput in ZKP.

05/23 – · · · · **Reducing expensive Key movement in FHE using Processing in Memory**, Partitioning FHE kernels on CPU-UPMEM model.

Past Work

08/21 – 06/22 **Secure AI using Samsung's AxDIMM**. Finalists for Samsung AxDIMM contest.

08/20 – 03/21 **Efficient Metadata for Memory Protection**.

03/19 – 08/19 **AMBOP: Adaptive Multiple Best Offset Prefetcher**.

Education

2019 – · · · · **Ph.D., University of Utah**
Thesis title: *Hardware-Software Co-Design to Accelerate Modern Cryptography.*

2013 – 2017 **B.Tech. (Minor), Computer Science and Engineering, Indian Institute of Technology (IIT), Gandhinagar**

B.Tech. (Major), Mechanical Engineering, Indian Institute of Technology (IIT), Gandhinagar

Skills

Programming Languages — High-level programming languages (C, C++, Python), Hardware description language (Verilog), Shell scripting, SQL.

Familiar Tools — Performance Analysis Tools and Instrumentation Tools (Pin, perf, Intel VTune), System Simulators (Sniper, ZSim, Gem5, NVMain, DRAMSim2, USIMM), Interconnection Network Simulators (booksim2, PANE), Design Tools (Cacti, Cadence Spectre/RTL Compiler, Innovus, Virtuoso).

Personal — Boxing (Coach at Legends Boxing Trolley Square), CPR-certified, Snowboarding, Outdoor recreational activities.

Miscellaneous Experience

Awards/Service/Outreach

- One of the finalist for **Samsung's Open Innovation Contest for AxDIMM Technology**.
- **Computer Architecture Student Association (CASA)** Founding Member, Steering Committee (2020-2022).
- **GradSAC, University of Utah** Member (2020-2021).

Miscellaneous Experience (continued)

- **Journal review**: IEEE Micro 2022.
- **Teaching Mentor:** CS 6810 Computer Architecture (Fall 2020), CS 3810 Computer Organization (Spring 2022).

Graduate Coursework

- Neuromorphic Architectures, Modern Cryptography, Advanced Computer Architecture, Parallel and High Performance Computing, Digital VLSI Design, Data Structures & Algorithm for Scalable Computing, Computer Architecture, Distributed Systems, Operating System, Advanced Algorithms

References

Up to 3 references available on request