SERB CRG 2018000864
Microarchitectural techniques to design a secure processor

Summary report

Dr. Nanditha Rao
Assistant Professor, IIIT Bangalore

Feb 25, 2022

Project summary

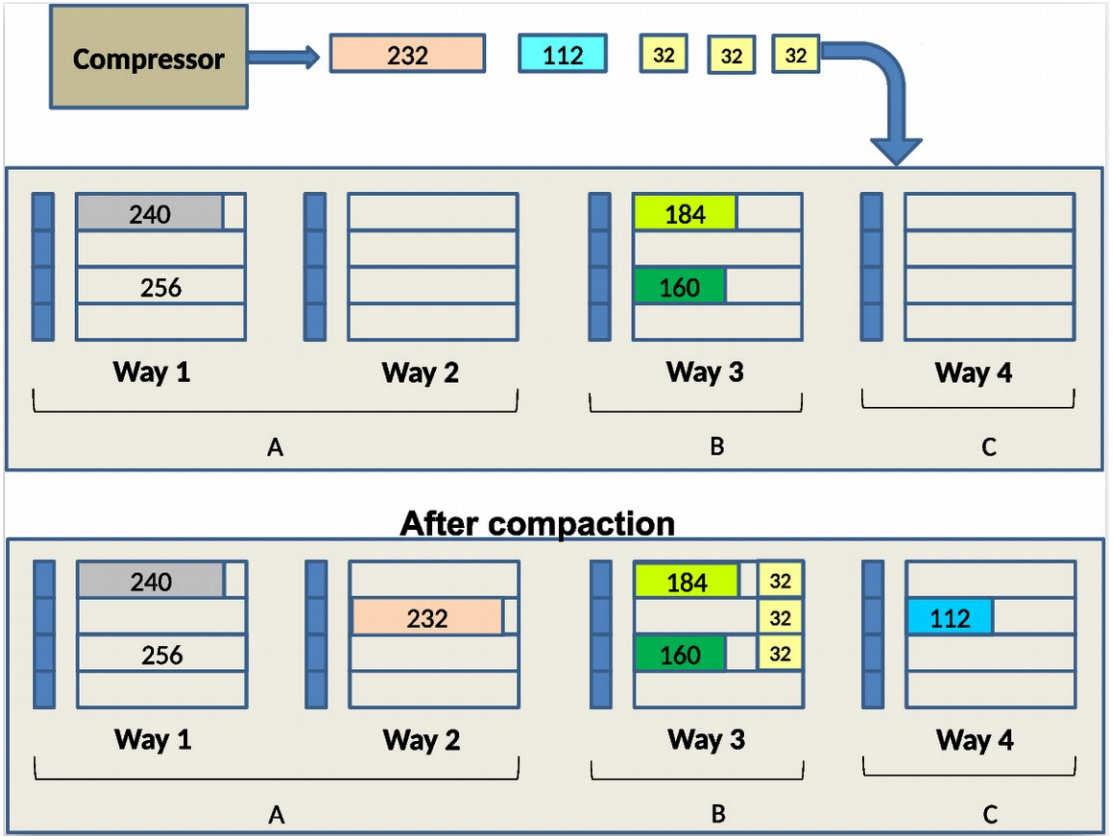
- Title: SERB CRG 2018000864
  Microarchitectural techniques to design a secure processor
- PI: Nanditha Rao, Assistant Professor
- Co-PI: Subir Roy, Professor
- Institution: IIIT Bangalore
- Duration: 2019- 2022
- Cost: Rs. 28,78,914

Objectives of the Proposal and Deliverables

- Detailed study of existing cache varieties
- Detailed study of existing **cache compression methods** and possibilities of data leakage
- Studying and **Implementing data attacks on compressed caches.** Study their vulnerability
- Propose **possible solutions** in terms of cache compression designs. Identify a suitable metric to measure processor security
- Detailed study of speculation engine and branch predictors
- Implementing data attacks on speculative engine and predictors. Studying their shortcomings
- Investigate/Model circuit level aspects that can prevent cache data attacks

Compressed cache with modified BDI

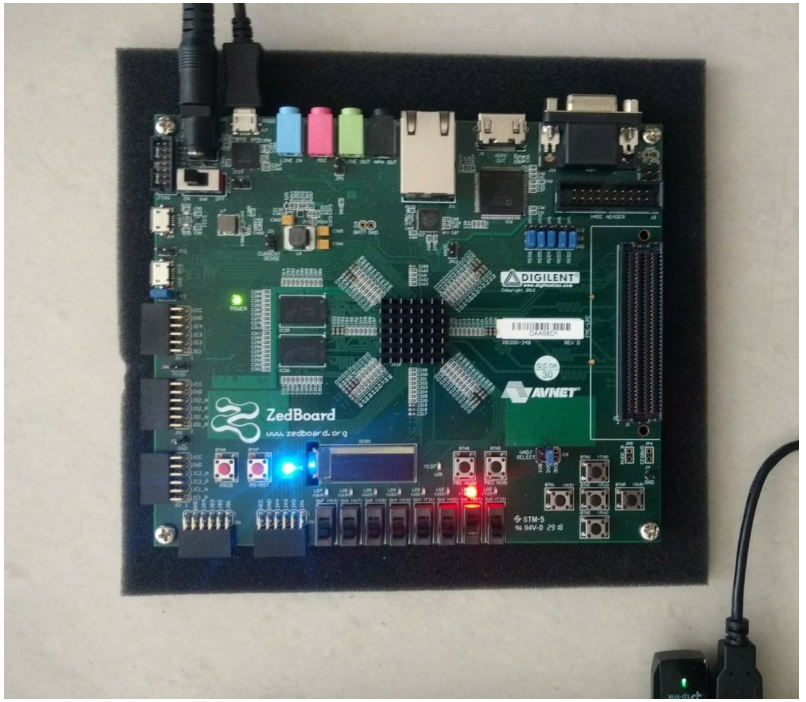
Compression scheme which inherits features from BDI, but uses a dynamic base instead of a fixed base to compress the data.
Tested these algorithms on image workloads : 52.31% improvement in bits reduction over the fixed base method.
Compression factor: 3.95% - 10.5% improvement on an average over fixed base approach.
Saves 8.2% of the cache area



Cache compaction scheme to utilize the B2B4 algorithm
A compressed cache can fit more blocks. Blocks could be compressed to different sizes --> need to assign a compressed block into a certain way of the set-associative cache.
Implemented an 8-way set associative cache architecture

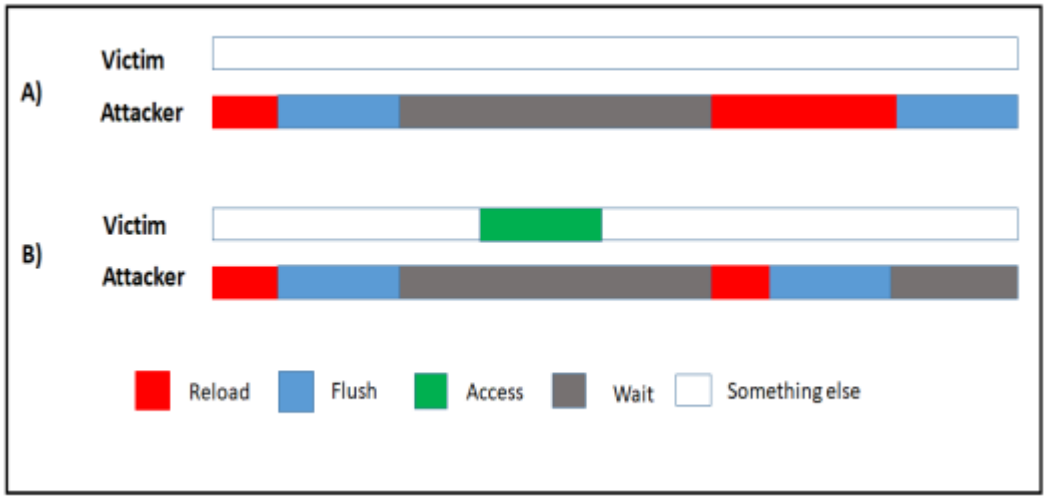
Integration with RISC-V processor

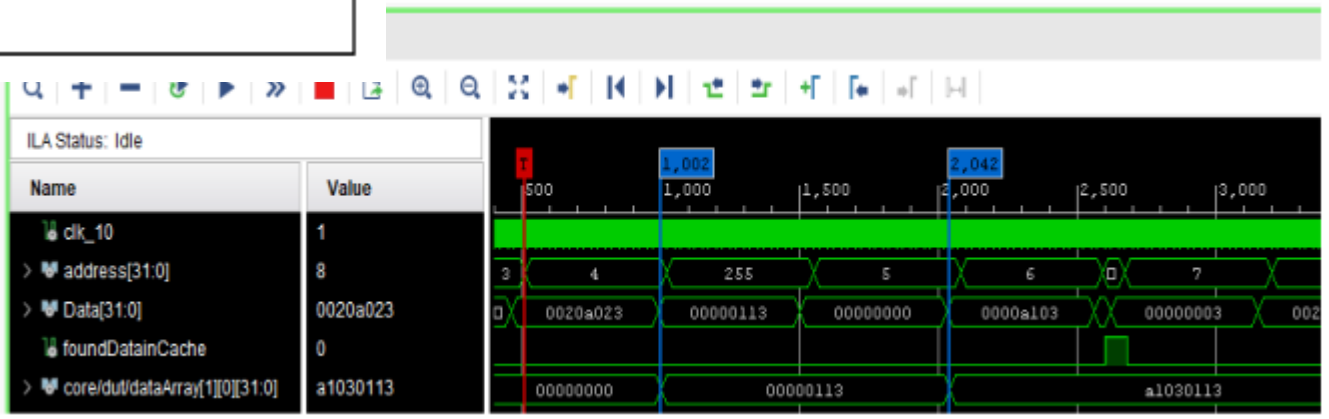
- Not part of initial plan
- Hardware implementation and attacks on compressed caches:
- We have successfully integrated a compressed cache with picoRV32- a RISC-V based processor. We have programmed this on an FPGA board- Zedboard.



Flush- Reload attack on FPGA based compressed cache

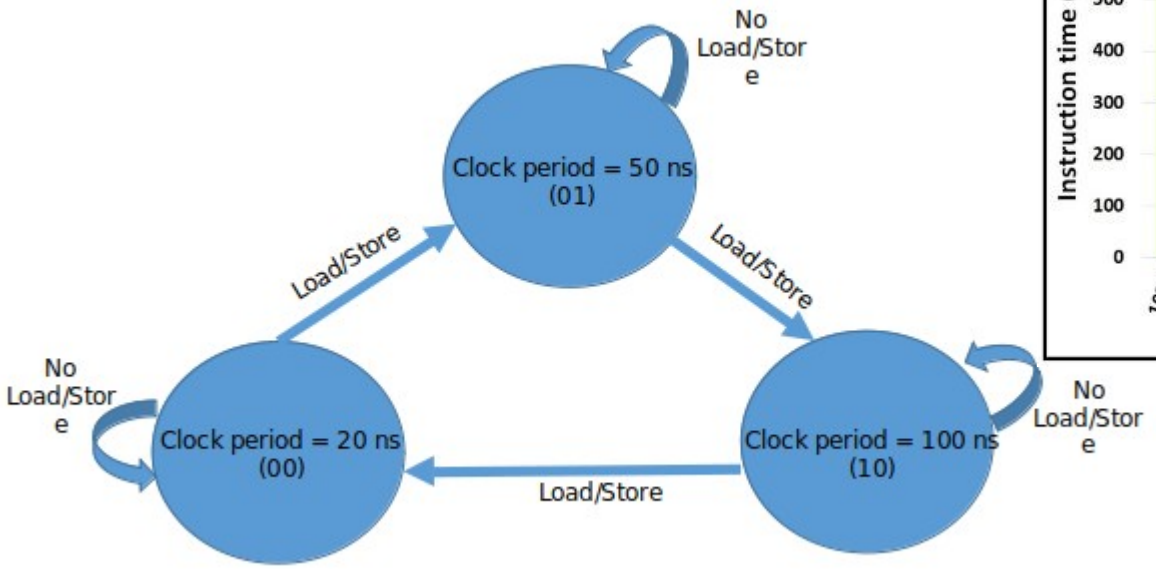
- Hardware implementation of Flush Reload and attacks on compressed caches:
- Successfully integrated a compressed cache with picoRV32- a RISC-V based processor. Programmed this on Xilinx Zedboard.

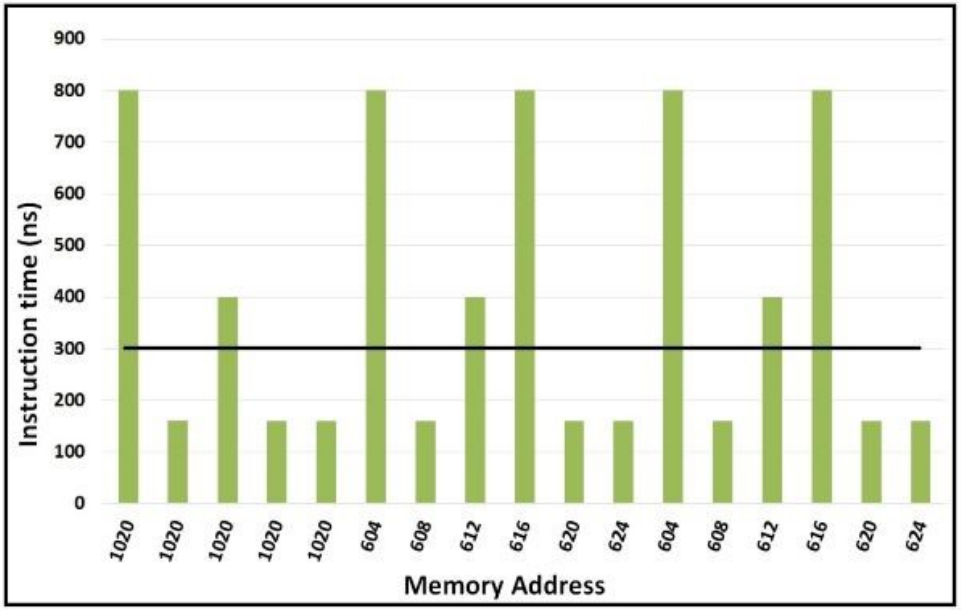




Attack Mitigation by varying clock frequency: on FPGA

- We change the clock frequency whenever the processor executes load or store instruction. 3 clock periods we use in the technique are 20 ns, 50 ns and 100 ns.
- Variation in cache hit time due to change in clock frequency at run time and this misleads the attacker. All memory accesses in graph are cache hits.
- If the attacker assumes here that access time below 300 ns indicates cache hit then the attacker fails 47% of times.



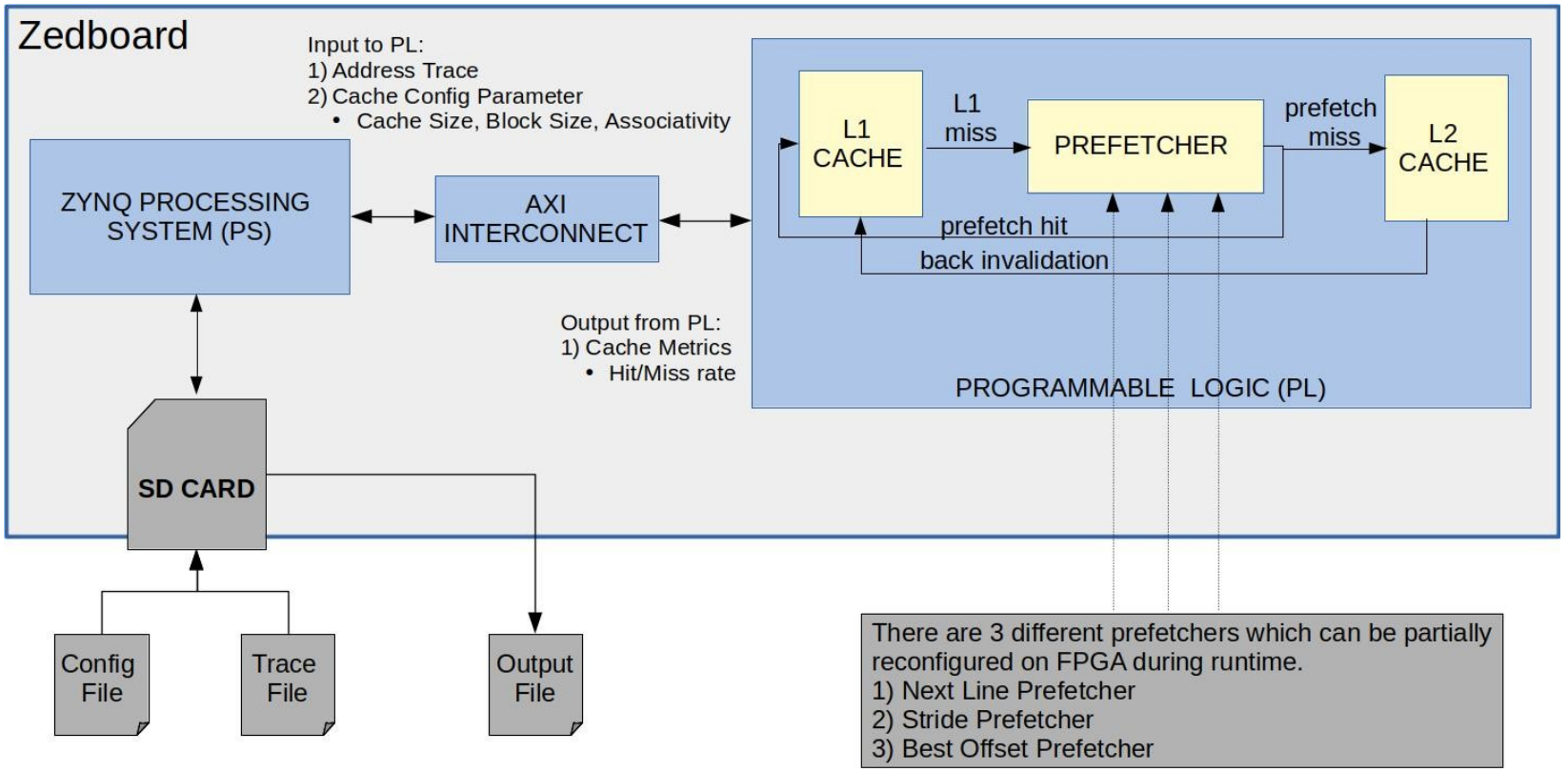


Cache-Accel: FPGA based hardware cache simulator

Implemented an FPGA accelerated parameterized two-level cache simulator called Cache-accel which can be partially reconfigured to include prefetching.

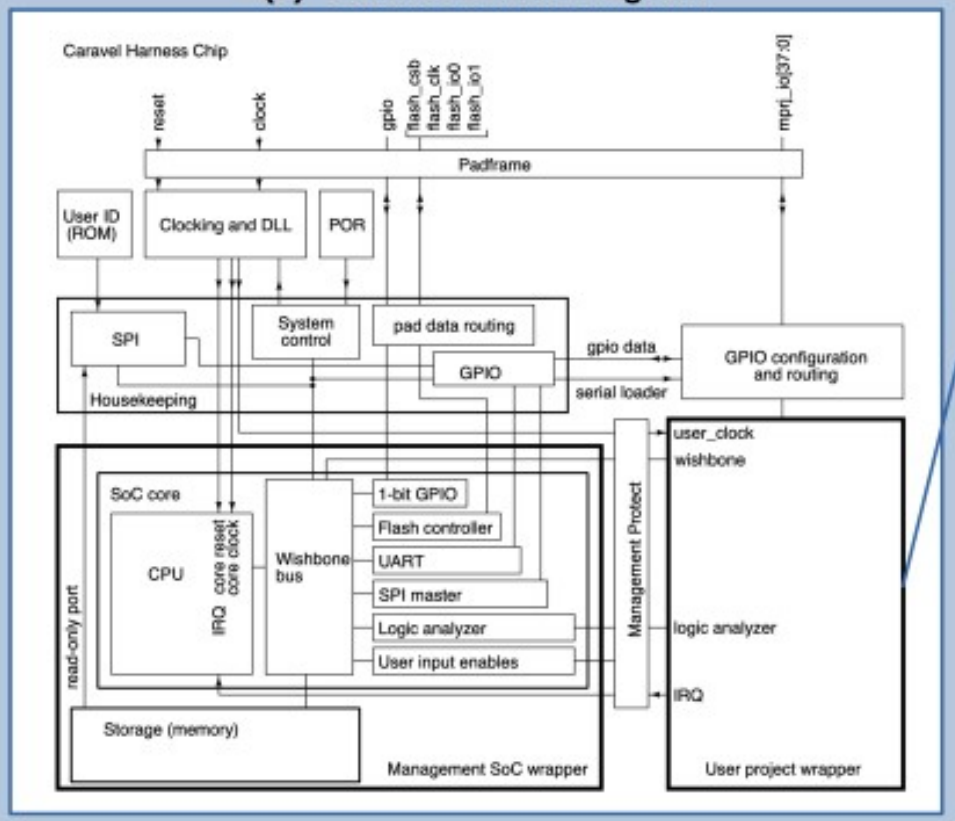
Adopted inclusive properties[I] for sets and ways in second level cache architecture to simulate multiple cache configurations in parallel.

Board used: Zedboard which is based on Zynq-7000 SoC architectures

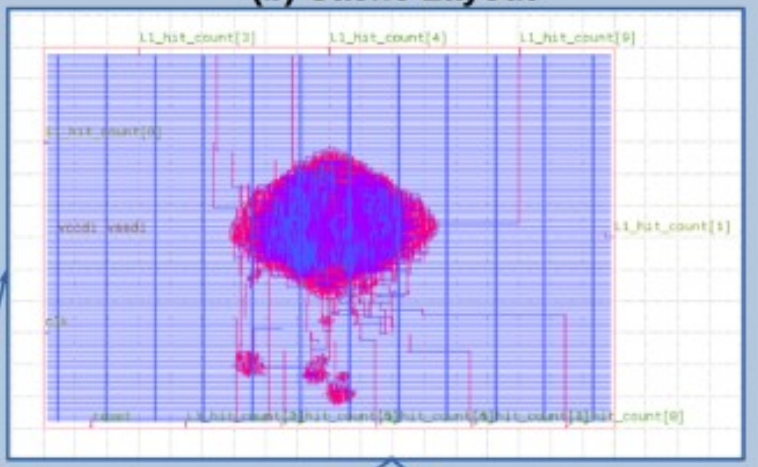


Spectre attack is implemented on a 2-level cache structure using an always-taken branch predictor

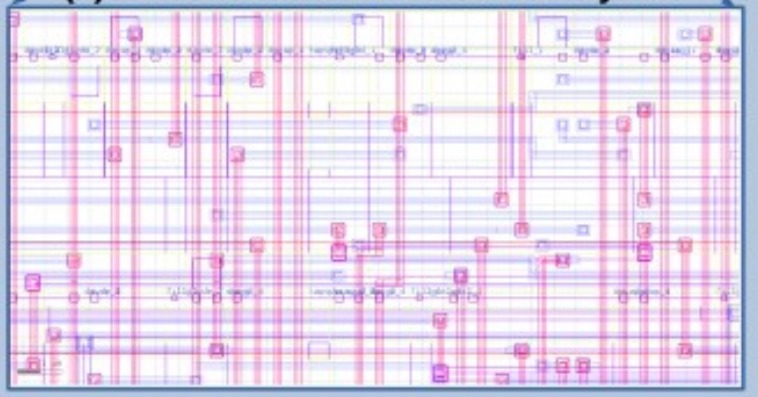
(a) Caravel Block Diagram



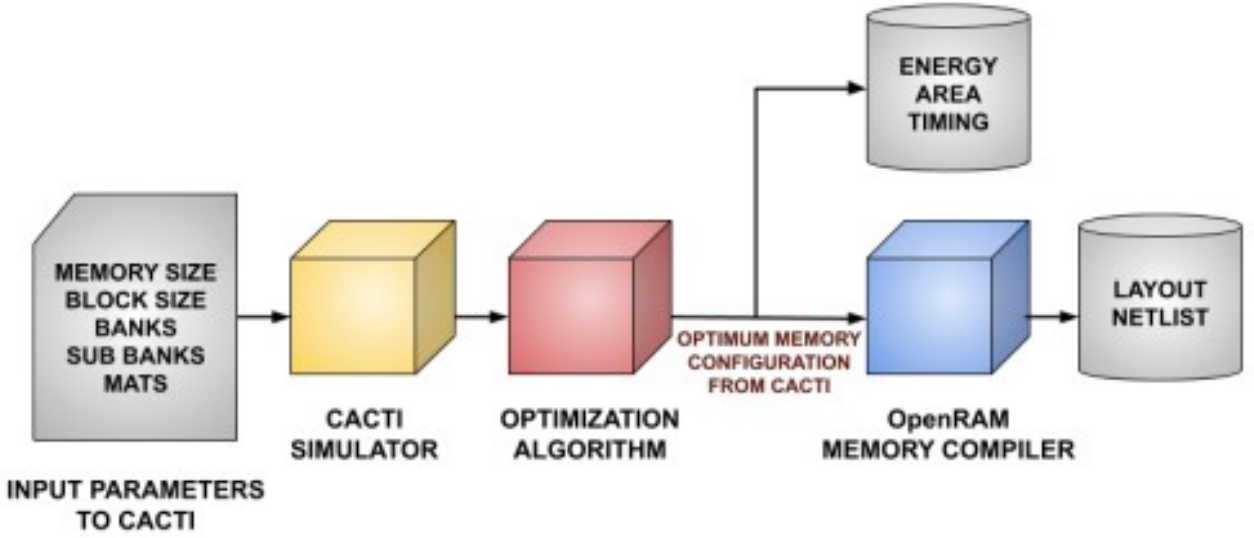
(b) Cache Layout

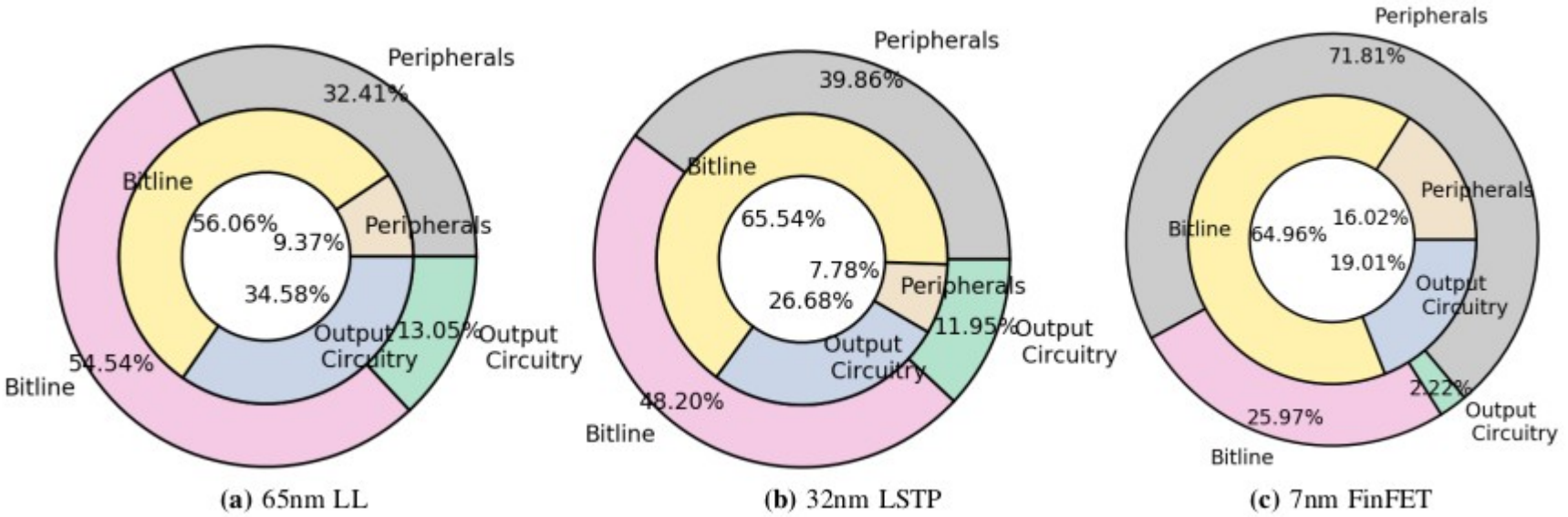


(c) Disectional view of Cache Layout



FastMem: A Fast Architecture-aware Memory Layout Design





We design FastMem to obtain optimal memory configurations for 65nm, 32nm, and 7nm technology nodes. As part of the experiments, we observe that, as technology scales from 65nm to 32nm to 7nm, the contribution of peripherals and interconnects to the access time increases from 32% to 70%. Thus, we need to optimize the peripherals and interconnects at lower technology nodes rather than the actual SRAM cells.

Publications so far

- Journal submitted: 2 (under review)
- Alok Parmar, Kailash Prasad, Nanditha Rao, Joycee Mekie, " An Automated Approach to Compare Bit Serial and Bit Parallel In-Memory Computing for DNNs", IEEE International Symposium on Circuits and Systems (ISCAS 2022)- Accepted
- Alok Parmar, Kailash Prasad, Nanditha Rao, Joycee Mekie, "FastMem: A Fast Architecture-aware Memory Layout Design", International Symposium on Quality Electronic Design (ISQED'22) - Accepted
- Shivani Shah, Vaibhavi Mathur, Sahithi Meenakshi Vutakuru, Kavya Borra and Nanditha P. Rao, “Cache-accel: FPGA Accelerated Cache Simulator with Partially Reconfigurable Prefetcher”, EuroMicro Digital System Design 2021. pp. 97-100, doi: 10.1109/DSD53832.2021.00024.
- P. Mata and N. Rao, "Flush-Reload Attack and its Mitigation on an FPGA Based Compressed Cache Design," 2021 22nd International Symposium on Quality Electronic Design (ISQED), 2021, pp. 535-541, doi: 10.1109/ISQED51717.2021.9424252.
- Shivani Shah, Sahithi Meenakshi Vutakuru, Nanditha Rao, "FPGA Accelerated Parameterized Cache Simulator", 22nd International Symposium on Quality Electronic Design. April 2021 (ISQED'21)

Publications, Patents, and other deliverables so far

- Shreya Joshi, Prashant Mata, Nanditha Rao, “A Dynamic Base Data Compression Technique for the Last-Level Cache” at International conference on Modelling, Simulation and Intelligent computing (MOSICOM), Jan 2020, Dubai and HiPC 2019 Research Symposium
- Shreya Joshi, Subir Roy, Nanditha Rao, “Cache compression using variable base BDI technique for RISC-V processors”, RISC-V-Workshop Zurich, 2019

Students trained

- PhD: Kailash Prasad (IIT Gn) - ongoing
- MS (R): Prashant Mata, Alok Parmar, Shivani Shah
- MTechs: Vaibhavi Mathur, Sahithi Meenakshi Vutakuru, Shreya Joshi
- IMTech: Kavya Borra, Harshith Reddy, Rohit B (ongoing), Mayank Kabra (ongoing)

Plan for the Future

- Extend the Cacti tool to include in-memory compute circuits
  - 7nm FinFET node
  - Bit serial and Bit parallel compute circuits
- Memory management in FPGA implementation of neural network models

Utilisation of funds and budget status, Request to SERB

1-Apr-21 to 21-Feb-22

Particulars	Opening Balance	Debit/ Utilization	Credit/ Receipt	Closing Balance
7123-01 Equipments	363835.00 Dr	*32530.00*		396365.00 Dr
7123-02 Consumables	102788.00 Dr	*3439.00*		106227.00 Dr
7123-03 Travel	6754.00 Dr			6754.00 Dr
7123-04 Manpower	893730.00 Dr	*384400.00*		1278130.00 Dr
7123-05 Contingencies	21116.00 Dr			21116.00 Dr
7123-06 Scientific Social Responsibility		*10000.00*		10000.00 Dr
7123-07 Overhead	140227.00 Dr			140227.00 Dr
7123-08 Conference	14051.00 Dr			14051.00 Dr
7123 SERB Project - Prof. Nandita Rao	1685289.00 Cr		*800000.00*	2485289.00 Cr
Grand Total	**142788.00 Cr**	***430369.00***	***800000.00***	**512419.00 Cr**

Spent since Apr 2021

Received in Apr 2021

Balance remaining

Are we eligible for other grants- such as POWER, Early career research award, having got CRG?

Thank you