Report on Activities of PS-CDISHA (2019-2020)

Prepared by IIT Madras - September 2020

Executive Summary

This report presents the work done by the members of PS-CDISHA in the fields of Microprocessor, Security, Artificial Intelligence, Machine and Reinforcement Learning in the past year. It also provides an outlook of the roadmap for the center in the next 3 years. The report is organized into various areas and the contribution made in those areas by members of PS-CDISHA. It also presents the funding received for projects during the current time period, as well the future funding requirements taking into account the perceived roadmap for the PS-CDISHA center.

Table of Contents

Introduction

A meeting was organized on 4th September 2020, to present the progress of work done at the PS-CDISHA, IIT Madras between 7:30 pm and 9:30 pm IST. Members of PS-CDISHA presented their work done. The following faculty members and their teams made the presentations:

- Arun Rajkumar
- Chester Rebeiro
- Harish Guruprasad
- V. Kamakoti
- Mitesh Khapra
- Pratyush Kumar Panda
- B. Ravindran
- K. C. Sivaramakrishnan

The technical areas that were covered during the presentation includes:

- SHAKTI microprocessor and security extensions
- Edge AI accelerator and SHAKTI extensions
- Machine Learning and Reinforcement Learning at PS-CDISHA
- AI Based Human in the Loop Learning
- Secure Hardware
- 6G Efforts
- Data Libre Open Source Stack

The rest of the report presents the contribution to these areas by the PS-CDISHA team in the past year. Other than the technical achievements this report also presents an overall financial status, and also about the split of personnel at PS-CDISHA as of 4th September 2020.

Personnel

The center has a total of 114 personnel including students, project staff and consultants, whose split up is as follows:

Students

Post Doc	01
PhD	12
MTech	21
MS	12
BTech and Dual Degree	10
Total	**56**

Table 1 : Students at PS-CDISHA

Project Staff and Consultants

Principal Project Officer	01
Senior Project Advisor	05
Senior Project Officer	10
Senior Executive	02
Senior Engineer	01
Senior Project Assistant	01
Project Associate	33
Project Officer	03
Project Attendant	01
Junior Engineer	01
Total	**58**

Table 2: Project Staff at PS-CDISHA

Technical Activities Report of PS-CDISHA

We present the activities being carried out at PS-CDISHA in the various technical areas.

SHAKTI series of Microprocessor

The SHAKTI series of microprocessors are a family of processors, catering to different segments of the market. The series involves a few base core processors and multicore processors. It is an Open-source processor development initiative at IIT-Madras. The aim is to build an ecosystem of production grade processors, SoC's and peripheral IP's.

Aardonyx: Ardruino compatible board

Among the SHAKTI series an improved version of E-Class SHAKTI, code named “MOUSHIK”, had its successful Tape-in at SCL. The chip was fabricated, and it passed its post-silicon testing. Currently, this chip is being integrated with Ardruino compatible boards (designed at PS-CDISHA) so that all Ardruino projects can be executed on this board. An SDK that is indigenously developed is also made available.

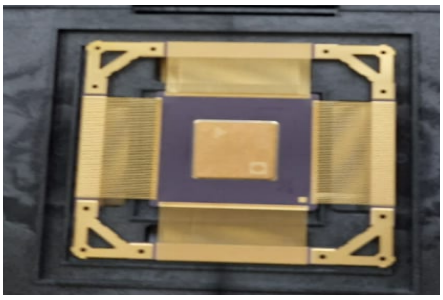

Figure 1: E-Class Moushik Chip

Silicon Details

- Die size - 5.315 X 5.155 sq.mm
- Functional IOs - 103
- Package - 256 pin CQFP package
- Core Voltage - 1.8v
- IO Voltage - 3.3v
- Gate Count - 647k
- Instance Count - 210k
- DFT - SCAN, JTAG

SOC Details

- PWM x 6
- SPI x 3
- GPIO x 16
- UART x 3
- QSPI x 1 (FLASH)
- I2C x 2 (EEPROM/A_H)
- SDRAM 32-bit
- JTAG x 1
- FREQUENCY: 75-100Mhz
- PACKAGE: CQFP
- PIN COUNT MAX:103 + VCC & GND (WITH PINMUX)

The Software Development Kit (SDK) and the Integrated Development Environment (IDE) has also be developed for this project.

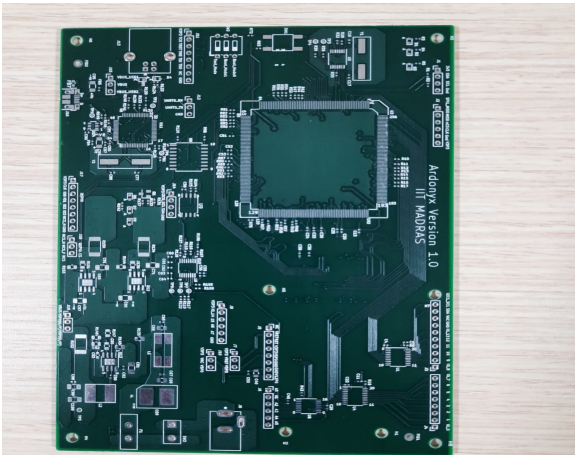

Figure 2: Ardruino Compatible Reference Board Designed at PS-CDISHA

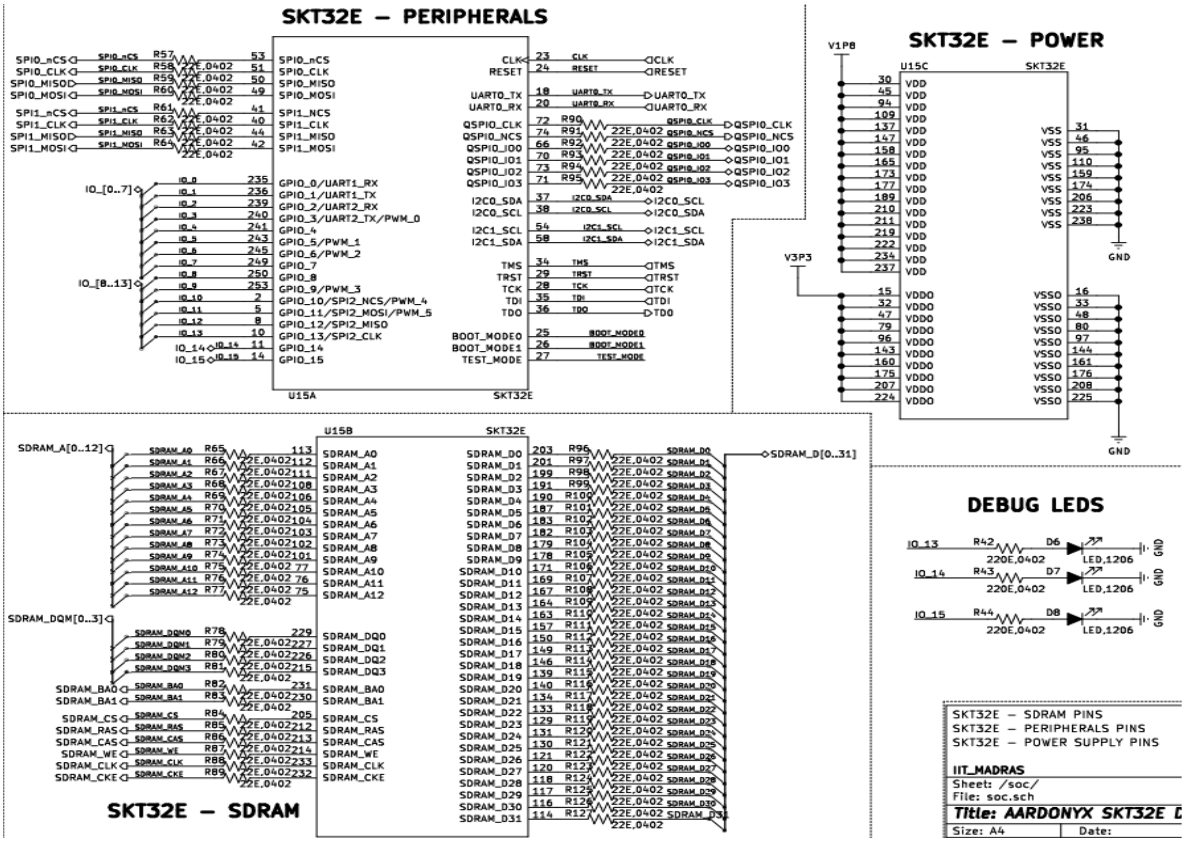

Figure 3: Reference Board Sample Layout Details

Reference Board Details:

- The heart of the board is Shakti Aardonyx SOC (SKT-32E).
- 512Mb (64kBytes) SDRAM support.
- Support added to test peripherals like I2C, QSPI, SPI ADC.
- Core and IO voltage sequencing.
- Ardruino Compatible header (pinout) to interface various daughter cards.
- Level translator to support 5V IO signals.
- I2C Clock multiplier to support multiple system clocks.
- Serial console and JTAG debugging interface with FTDI2232H.
- Switcher ICs are used for power conversion (12V - 5V, 5V - 3.3V & 3.3V to 1.8V conversions).
- Input power 12V @ 2A.
- The PCB will be 4-layer PCB @ 1.6mm thickness FR4 di-electric material.

In order to increase the adoption of the Ardruino compatible board and be cost effective the center is planning to release “Aardonyx”.

The center has built a cost-friendly FPGA kit for students to prototype, experiment and learn about RISC-V and micro-architecture, using the Arty-35T FPGA development board available off the shelf. However the cost of FPGA board is under Rs. 10,000. Based on the volume the Aardonyx board costs can be brought down to under Rs. 5000.

Software Development for SHAKTI

An SDK has been built for SHAKTI with the following features:

- Support for current versions of C and E class.
- **Driver support** for PLIC, CLIC, SPI, QSPI, UART, I2C and PWM.
- Standalone mode supported on E class.
- Multilevel logging, Direct Flash programming, MMU support added.
- ESP8266 & ESP 32, FTDI, External Flashes and many sensors integrated.
- IoT support added and live **temperature** **monitoring** done using SHAKTI.
- **Arduino compatible** board and peripheral support added.

The important highlights of this SDK are its

- Clean separation between drivers, boot, core and application layers
- Easily portable to **any RISC-V based architecture**
- **Multiple sensors** connected and proven with SHAKTI-SDK.

The software team also have ensured porting of Linux, FreeRTOS and Zephyr OS in SHAKTI class of microprocessors.

Education with SHAKTI

The SHAKTI environment has been used for a course curriculum for the computer organization course replacing the traditional X86 processors. The lab portion concentrated on RISC-V open source hardware framework and the SDK developed by the SHAKTI software team. A sample web page is presented below:

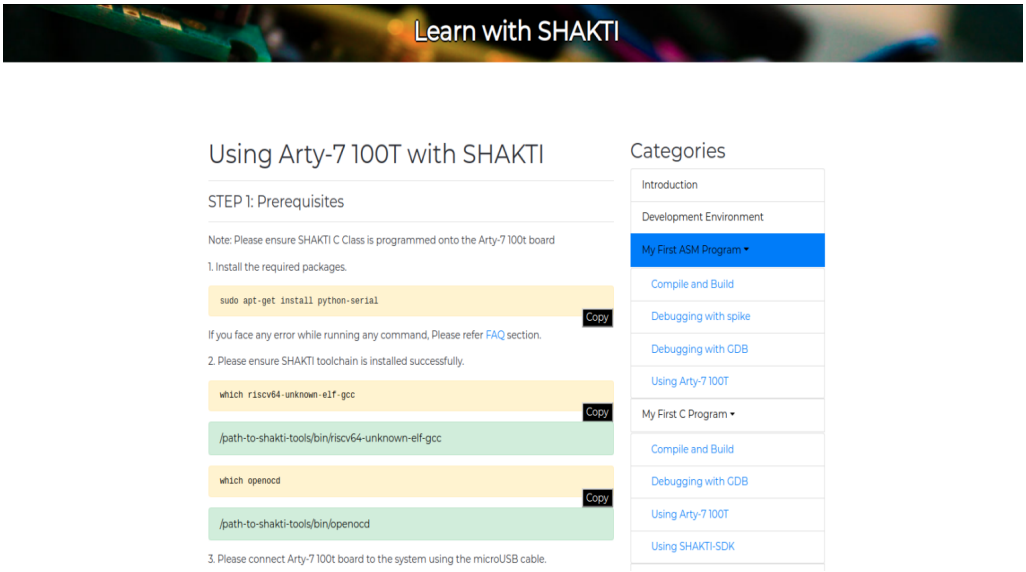

Figure 4: SHAKTI in Education

SHAKI Customer Status - IGCAR

Indira Gandhi Centre for Atomic Research, Kalpakkam, replaced their age-old Motorola based systems/boards with **SHAKTI C-class core (PC-I)**. The reason towards movement to SHAKTI was prioritized due to the

1. Open specification
2. Robust and open Verification plans/platforms
3. Indigenous expertise available

4. Obsolescence free roadmap

Custom FPGA boards with Shakti C-Class have been deployed for **field trials in IGCAR's electrical substation**. Specific customization of the Core - like custom traps and endianness translation were requested and completed. Note that without a proprietary core and with a restricted budget these enhancements would not have been possible. Field trials are currently in progress and deployment is slated for December 2020.

Microprocessor Grand Challenge

SHAKTI is one of the microprocessor that has been chosen for the Atmanirbhar effort of Government of India. This is an effort to provide further impetus to strong ecosystem of start-ups, innovators & researchers in the country. This challenge uses a family of state-of-the-art Swadeshi Microprocessors made available under MDP by IIT Madras (32-bit & 64-bit शक्ति IP variants) and C-DAC (32-bit & 64-bit वेगा IP variants) on XILINX FPGA Boards. The incubation support to winning teams will be provided by an Incubator located at their geographical proximity coordinated by Maker Village. Check https://innovate.mygov.in/swadeshi-microprocessor-challenge/ for more details.

SHAKTI Roadmap

The variants of SHAKTI that are planned to be released are as follows:

C32 - Low Power Processor

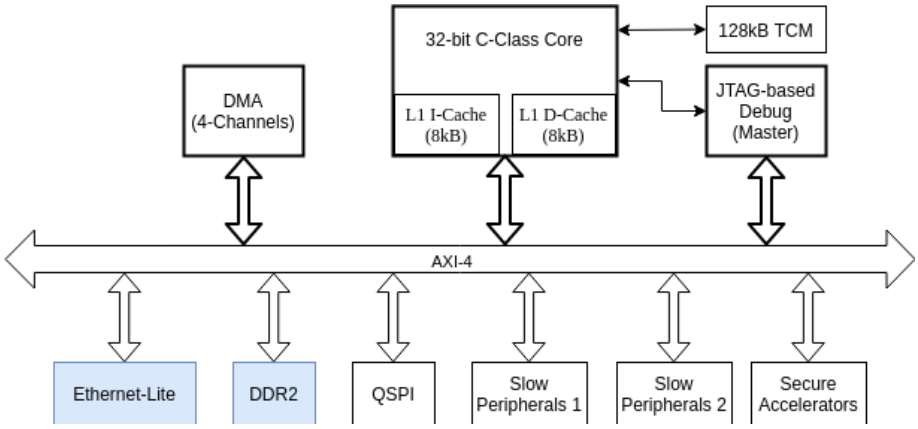

Figure 5: C32 Block Diagram

The core will feature:

1. 6 stage in-order core
2. ISA: RV32IMAFCU
3. 8KiB Instruction Cache and 8KiB Data Cache
4. GShare Branch Predictor
5. Single Precision Floating Point Unit optimized for performance
6. Integrated integer Multiply/Divide units
7. Physical Memory Protection Unit (PMP)
8. DMIPs: ~1.5 DMIPs/MHz
9. Debug Support and Trigger support for data and address.
10. Freq of Operation: 300MHz

The SOC list includes:

1. 4 Channel DMA
2. OCM - 128KiB
3. High Speed Peripherals:
    a. 4-GiB DDR2
    b. 1G Ethernet
4. PLIC: Platform Level Interrupt controller with 7 priority levels
5. Power Management.
6. Secure Accelerators:
    a. RSA-4096, SHA-256, AES 256, TRNG
7. Secure Boot
    a. Hardware assisted authenticated software execution
8. Power Management
9. Slow Peripherals
    a. VGA controller, SPI, I2C, PWMs, WatchDog, GPIOs, Counters/Timers, QSPI Flash

C64 - High Performance Processor

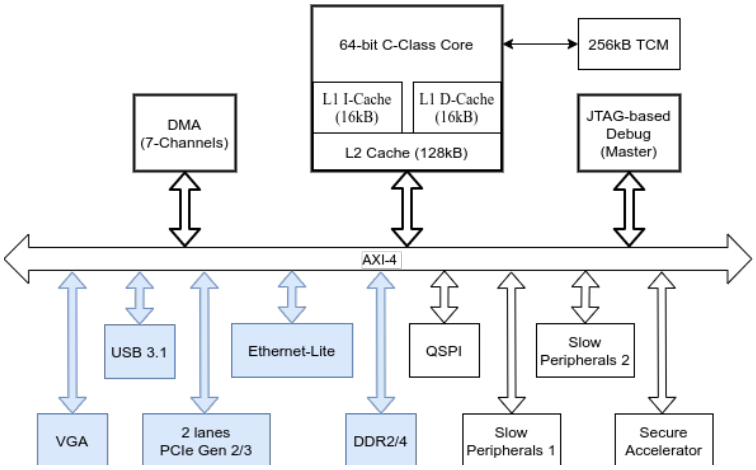

Figure 6: C64 Block Diagram

The core includes:

1. 6 stage in-order core
2. ISA: RV64IMAFDCSU
3. 16KiB Instruction Cache and 16KiB Data Cache
4. GShare Branch Predictor
5. Single Precision Floating point Unit optimized for performance
6. Integrated integer Multiply/Divide units
7. Supports sv39/sv48 supervisor spec.
8. Physical Memory Protection Unit (PMP)
9. DMIPs: ~1.72 DMIPs/MHz
10. Debug Support and Trigger support for data and address.
11. Freq of Operation: 800MHz

The SOC includes:

1. 7 Channel DMA
2. OCM - 128KiB (With ECC)

3. High Speed Peripherals:
    a. DDR2 x 4, USB3.1, PCIe Gen 2/3 (2lanes)
4. 1G Ethernet
5. PLIC: Platform Level Interrupt controller with 7 priority levels
6. Power Management.
7. Secure Accelerators:
    a. RSA-4096, SHA-256, AES 256
8. Secure Boot
    a. With TRNG support
    b. Hardware assisted authenticated software execution
9. Power Management
10. Slow Peripherals
    a. SPI, I2C, PWMs, WatchDog, GPIOs, Counters/Timers, QSPI Flash

Both these variants will be jointly developed by third parties, InCore Semi and IIT Madras with the responsibility split up as follows:

Task	**Responsibility**
Core optimizations	IITM
Verification of Core	IITM + InCore Semi
Secure Accelerators (Design)	IITM
Secure Accelerators (Verification)	IITM
Hardware Assisted Authenticated Software Execution (D&V)	IITM
OpenSBI + Linux with secure boot	IITM
Integrate Power Management	IITM + InCore Semi + 3rd Party
Integrate 3rd party IPs (HW+SW)	InCore Semi + 3rd Party
SoC Design	InCore Semi
SoC Verification	InCore Semi + 3rd Party
Backend	IITM + InCore Semi + 3rd Party

The technology of choice will be 65nm from TSMC. While the C32 is directed towards low power processor, C64 will be high performance processor for compute intensive applications.

IISU Variant

IISU (ISRO Inertial System Unit) will be deploying a variant of SHAKTI. This is a full featured C-class with custom peripherals and performance tuned for specific application. The SOC will consist of:

- Pulse Width Modulators (PWM)
- Tightly Coupled Memory (TCM) with ECC
- Input Qualification Control
- Quadrature Encoder Pulse (QEP)
- MIL1553B Timer
- External Interface
- BootROM
- I/O Qualification Control
- JTAG based debugger
- Custom SPI
- Counters
- Timers
- Watchdog
- UART
- CORDIC
- GPIO
- CLInt
- PLIC

The processor will have an operating frequency of 80 MHz and will have two variants one RAD-HARD version and a normal industry standard version. It will be manufactured at SCL. Currently, the FPGA prototyping is in progress. For this an FMC based generic card has been designed which can be used across FPGA boards The same FMC card will be used for ASIC board prototyping. This will reduce complexity of test-board.

I-Class

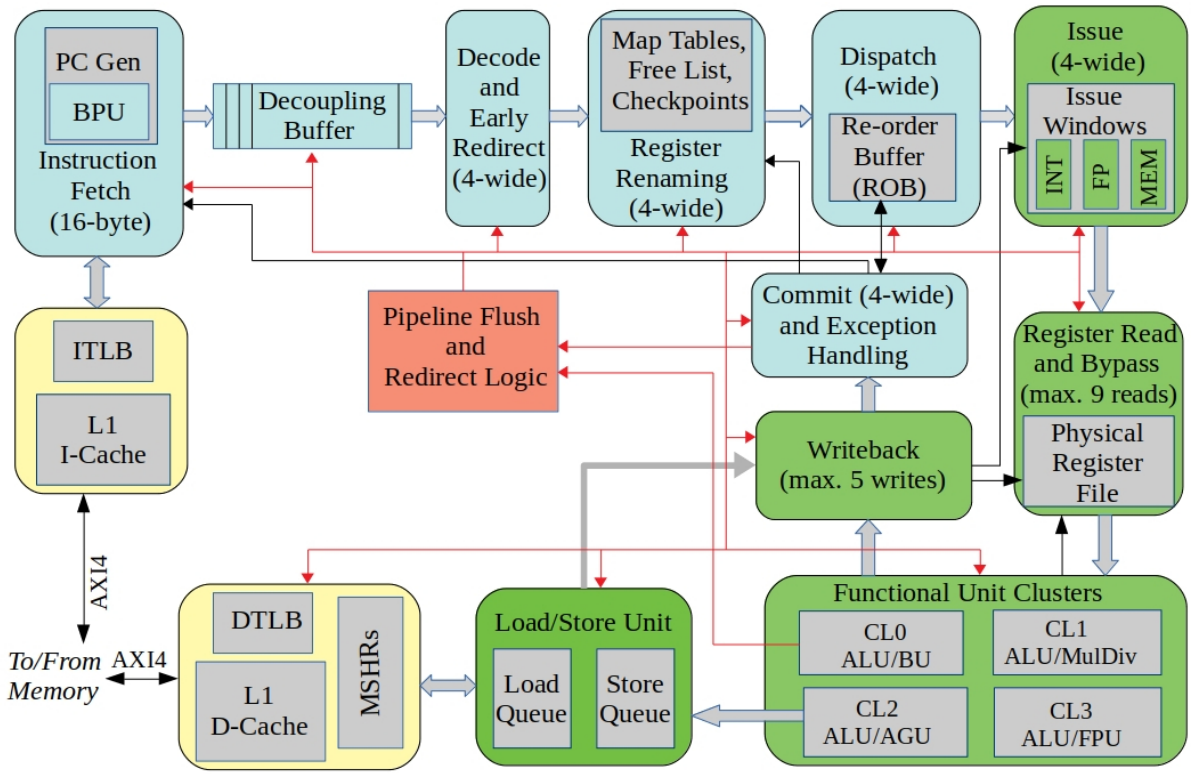

Figure 7: I Class Block Diagram

The I-Class will be a general purpose out-of-order superscalar processor supporting RV64GC with a 12-stage pipeline for simple integer operations. In Figure 7, the In-order pipeline stages (fetch, decode, rename, dispatch, commit) are in **blue**, while the Out-of-order stages (issue, register read, execute, writeback, load/store unit) are in **green.** The flush logic connections are shown in red.

The features of the I-Class include:

- Superscalar out-of-order processor with 4-way fetch, decode, dispatch, issue and commit
- Supports M, A, C, F and D extensions (IEEE compliant)
- Branch predictor sends fetch packet (16-byte) addresses to I-Cache
- Fetch logic extracts 1-8 instructions per cycle from the packet and queues into decoupling buffer
- Early Redirect from Decode handles definite mispredictions
- Register Map checkpoints for fast recovery from mispredictions and pipeline flushes
- Fully pipelined functional units (except for Integer Divide, FP Divide and FP Sqrt)
- Clustered functional unit design with statically assigned register file ports to clusters
- Unified 128-entry Physical Register File (PRF) with 9-read and 4-write ports
- 80-entry Re-order Buffer to maintain sequential semantics
- Load/Store Unit handles memory operation scheduling and interfaces with D-Cache
- Non-blocking D-Cache to support multiple outstanding misses to the next level
- **Max. possible frequency**: 2.2Ghz (on 22nm)
- **Tapeout plans:** Planning to tapeout enhanced version of I-Class in 2021 (on 10nm). Enhancements include improved front-end, split PRF, memory dependence prediction and unified 2nd level cache

SHAKTI Security Variants

A microprocessor attack surface can be found in software, micro-architecture and/or hardware (invasive or non-invasive). Therefore security has to be addressed at all these levels. Some of the hardware attacks include Side Channel Attacks, Fault Injection, Bus Probing etc. Similarly at the micro-architecture level, Cache Timing, Branch prediction and TLB related attacks can be used. At the software level, Memory Vulnerabilities, Overflows and Privilege Escalation are some kinds of attacks that could be used. The aim is to make SHAKTI resilient towards these type of attacks.

In order to make SHAKTI resilient research on security variants is in progress. Some of the related work being carried out are as follows:

- Root of trust using OTP Fuses
- Ensure that only signed binaries can be loaded and executed at boot
- Support for encrypted boot where the binary is encrypted [1]
- Include cryptographic hardware accelerators:
    - AES-128/256/512 with 5 modes
    - RSA 1024/2048/4096
    - SHA256
    - SHA3[1]

[1] Work in Progress

    - Present
    - True Random Number Generator (TRNG) [2]
    - Physically Unclonable Functions (PUFs) [2]
- Secure memory to store public signing key which is used to verify the signature of an image
- Safeguard secret key store table inside the accelerator
- Define APIs that can be called by higher level programs to validate and decrypt a binary

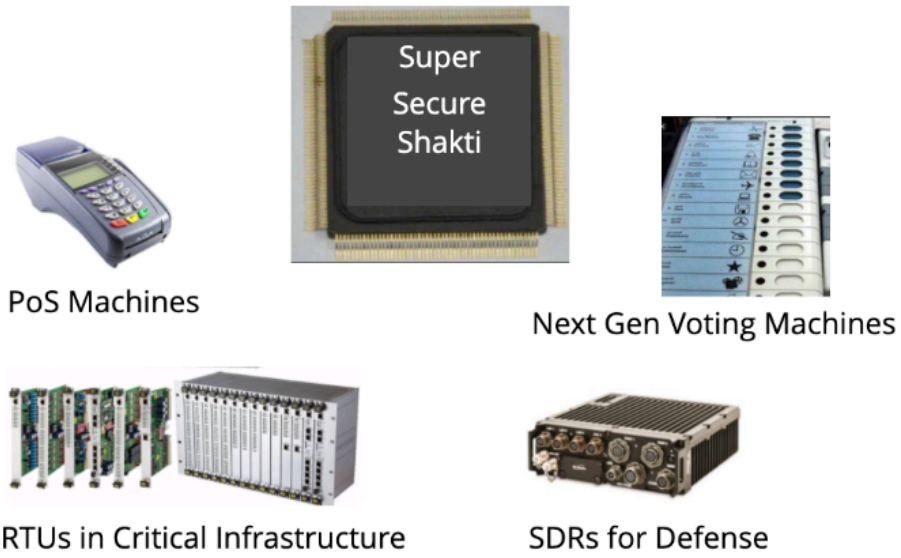

Figure 8: Application Areas for Secure SHAKTI

The application areas envisaged are shown in Figure 8.

Secure Tablet

A prototype that uses ARM to demonstrate the capabilities of Root of Trust and Chain of Trust was also developed. In future the secure SHAKTI will be used for the secure tablet as well as reduced form factor devices. Probable customers include some defence units who want both hardware, software trust and security.

Memory Safety and Secure Programming

Memory safety issues are predominant in software programming languages. For example 70% of all security bugs in Google Chrome are memory safety issues. Therefore there is a need to move software (legacy ones) to be memory safe. One could incrementally swap unsafe code with safe code a few parts at a time. In SHAKTI Trusted Execution Environment we could enforce memory safety with hardware-assisted fat pointers to eliminate memory safety issues. This featured can be turned off dynamically. A hardware enforced compartments for application partitioning will improve security. The current work with OCAML achieves the same (see Figure 9).

[2] Work in Progress

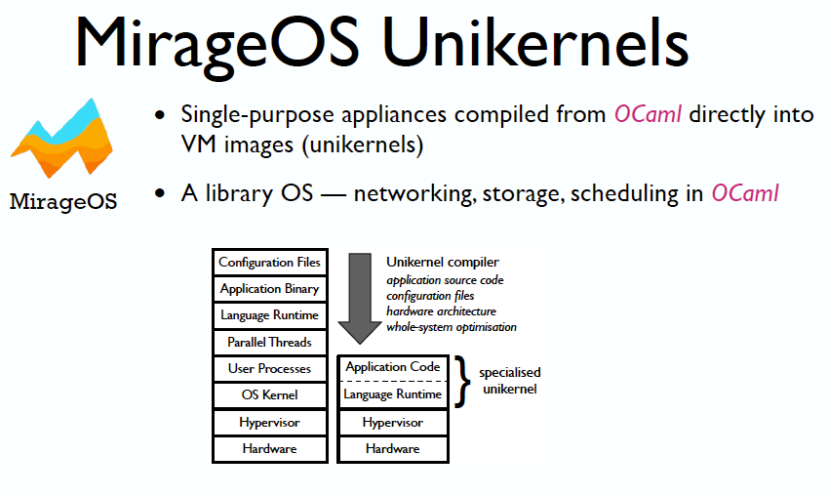

Figure 9: Memory Safety with OCAML

SHAKTI Planned Tapeouts

The following are the planned tapeouts for SHAKTI in the next 2 years.

- C-Class 32 Bit – Commercial Class - Jointly with INCORE (40nm/65nm TSMC)
- C-Class 64 Bit – Commercial Class - Jointly with INCORE (40nm/65nm TSMC)
- I Class – Test Chip (Jointly with Intel - heads on with ARM A75)
- IISU – RAD-HARD + Normal - SCL 180 nm
- IISU – TSMC 65nm - Same design
- NAVIC SOC - SCL 180 nm
- Full Mobile Application Processor
- India Chip Fund and TSMC/GF

NLP Efforts

The current NLP efforts are focused on three areas:

1. Developing robust evaluation metrics for Natural Language Generation
2. Developing NLP tools and technologies for Indian languages
3. Evaluating robustness of NLP systems to adversarial attacks

AI and Deep Learning Focus

The centre is working on 2 important areas in AI - hardware accelerators for deep learning (integrated end-to-end effort) and human learning aspects research.

Hardware Accelerators

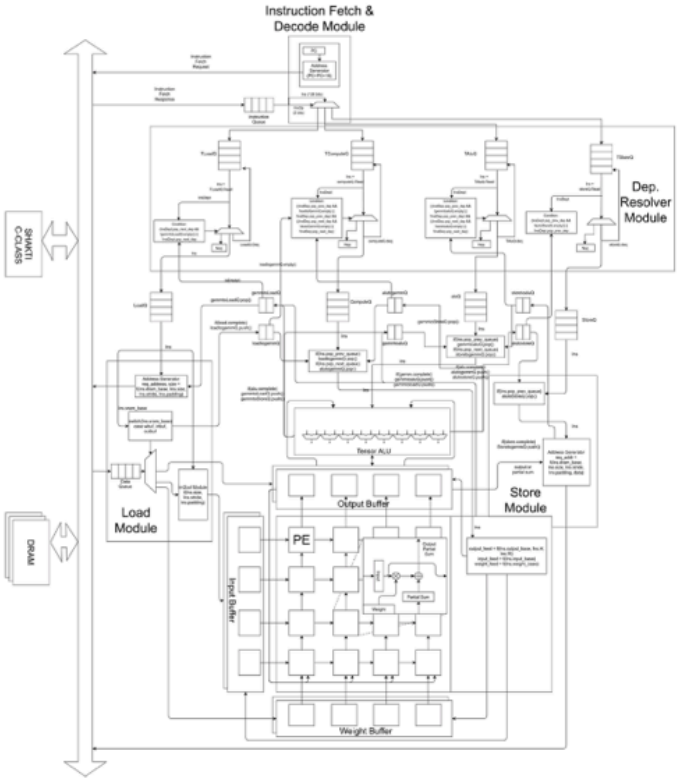

Figure 10: AI/ML Systolic Array Block Diagram

Figure 10 shows the proposed AI/ML hardware accelerator (SHAKTI-MAAN) that uses systolic arrays. The instruction set for these accelerators have also been finalized. Many modules are in the final design stages.

Software

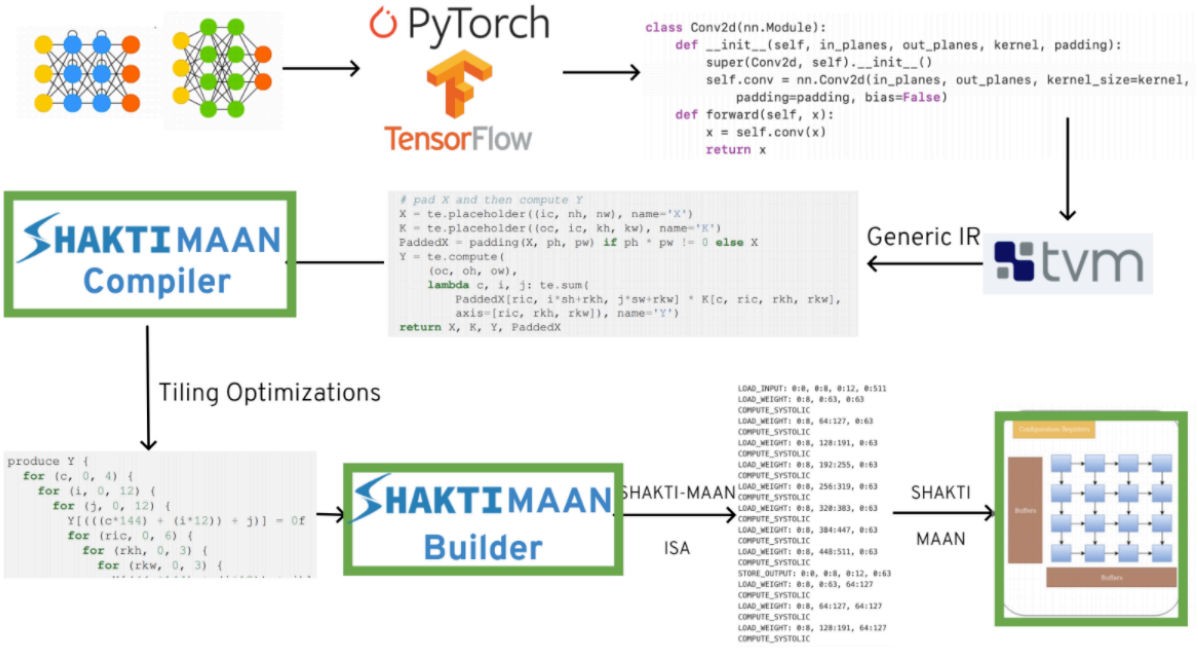

Figure 11: Software for the AI Hardware

The software co-integration is explained in Figure 11. The SHAKTIMAAN compiler and builder takes care of conversion and optimization of the code that will be run in the hardware.

End-to-end integration must also minimize cost of deployment. Therefore cost models have to be developed to show the efficiency of the system. For example, “Can we estimate how fast a network is on a series of hardware devices?”

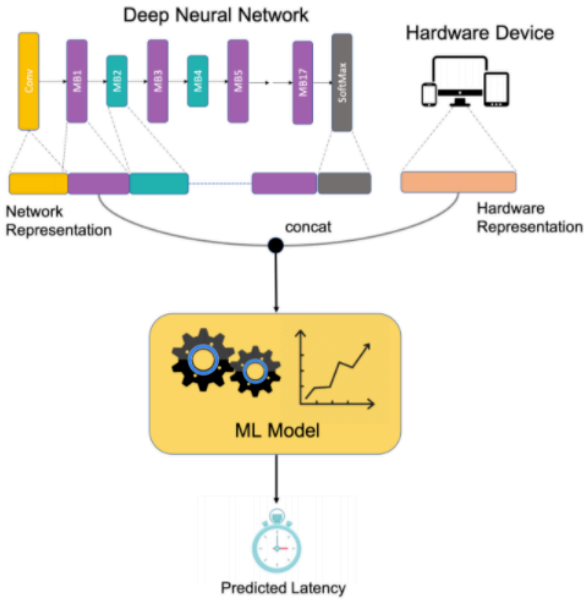

Figure 12: Predicting Latency based on Hardware and DL Network Representation

Results have been validated for real 120 DNNs in 100 mobile models. These can be expanded to ML based compilers to do efficient DNN mapping.

Human Learning

The idea is to use AI to improve human learning. The results obtained through this research will have the following benefits:

- Improving student engagements in learning activities.
- Development of prototypes that can help learning by various age groups
- Exploring Gamification for learning
- Intervention mechanism for dropout prevention

6G Efforts

Active discussions are on with NTT for developing an opensource 6G stack. In the final stages, SHAKTI security features can be incorporated in the RAN hardware as well as the communication equipment.

Data Analytics Stack

A performance analytics tool called Appedo (http://www.resileo-labs.com/load-test) was developed by a start-up Resileo labs (http://www.resileo-labs.com/). In collaboration with PS-CDISHA an opensource data analytics stack (https://www.finlibre.org/) has been developed. This stack has been used in the ITIHAS + Aarogya Setu application for COVID prevention. The performance analysis tool has also become a de facto certifying tool for many government applications from Registration office, treasury, education and also Unnati application.

Startups

Company Name	PS-CDISHA Members	Website
Incore Semi	Students of PS-CDISHA	https://incoresemi.com/
Padhai	Pratyush and Mitesh	https://padhai.onefourthlabs.in
SilInt Consulting	Kamakoti and Ravindran	http://www.sil-int.com

Future Work and Funding Requirements

For the next three years PS-CDISHA is planning to focus on the research and implementation part of the work presented in this document. The research part (building block) budgetary requirement is **USD 6 Million**. This consists of sample tapeouts for C32, C64, valued at USD 1 million, Security and AI/ML research valued at USD 1 Million, and the Mobile SoC, Supercomputer Core RTL for around 4 Million USD, including the Networking - 6G Stack.

For large scale implementation of Mobile SoC Tape Out and HPC – Para SHAKTI – Tape OUT a total of **USD 20 Million** will be required.

PS-CDISHA is working with various funding agencies to generate the required budget.