Side-channel attack hardware detection module added to RISC-V core

Juliette Pottier[1], Bertrand Le Gal[2], Maria Méndez Real[3], Sébastien Pillement[1]

[1]IETR, Nantes Université, Nantes, France

[2]IRISA/INRIA, Université de Rennes, Lannion, France

[3]Lab-STICC, Université de Bretagne Sud, Lorient, France

Contact: juliette.pottier@univ-nantes.fr

Convention: ANR-21-CE-39-0017

Context: SEC-V project

WP 1 – Dynamic code transformation unit

On-the-fly decoding modification/alteration

Dynamic instrumentation

Instruction set tailoring/customization/adaptation

WP 2 – Micro-architectural modifications

Alternative approaches to traditional caches (scratchpads, TCM)

Dynamic cache management

Inserting execution noise (access instructions for example)

WP 3 – Dynamic control of the architecture adaptation

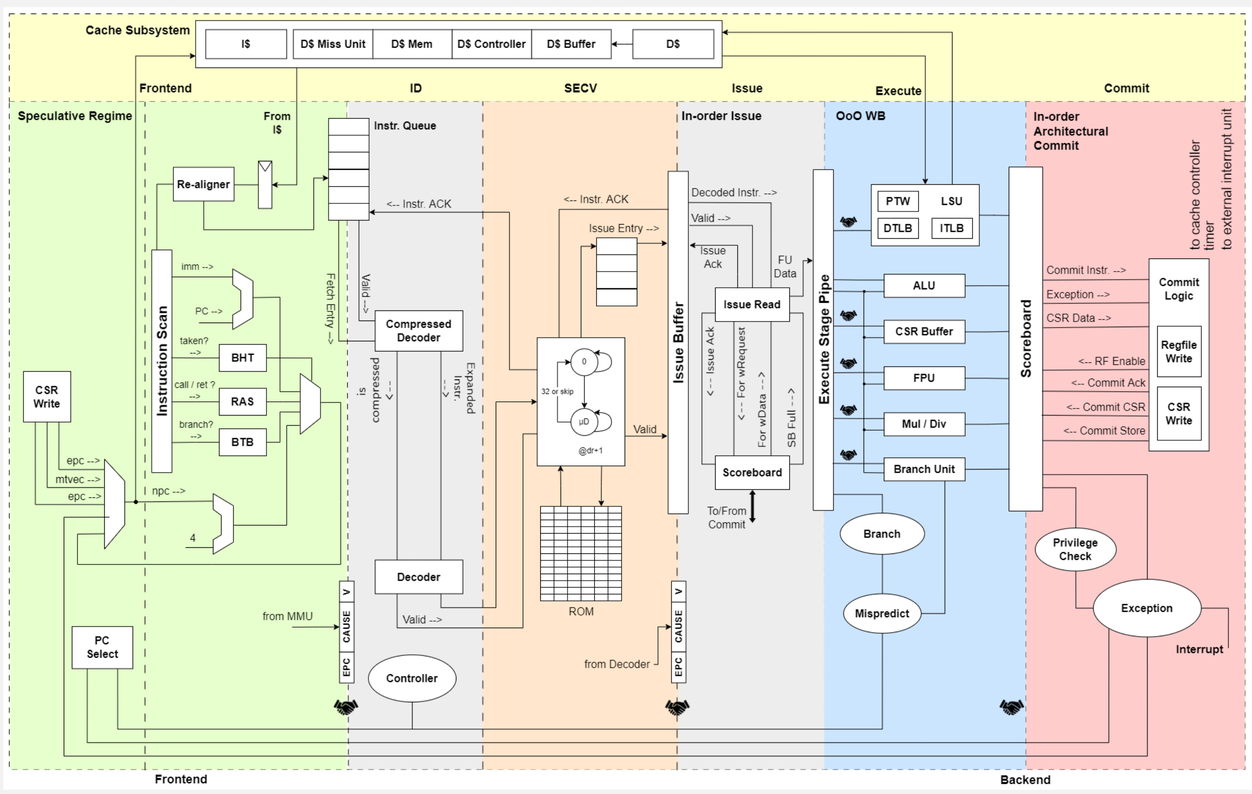
Detection of abnormal behavior

Dynamic code transformation unit control

WP 4 – Prototype and evaluation

Inclusion in the CVA6 core of the OpenHW Group

Assessment (indicators and metrics) of security levels



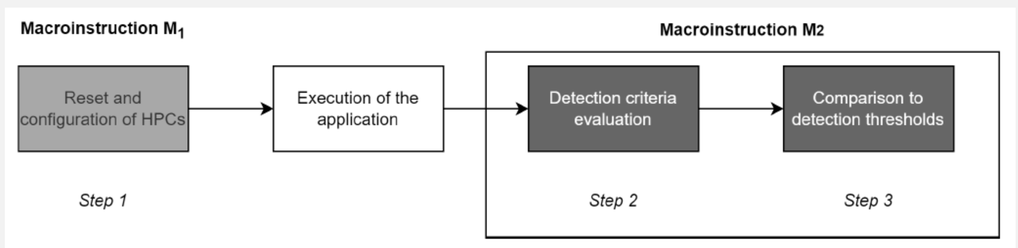
CVA6 enhanced with a µ-decoding unit

- **CVA6's Features [1]:**
  - ISA: RV64GC
  - 6-stage pipeline partially out-of-order (Execute Stage)
  - Single issue
- **Detection module Features:**
  - FSM: Bypass/Microdecoding state
  - ROM: contains 32-bit microinstructions sequences
  - FIFO: interfaces with the Issue stage
  - 5 internal registers dedicated to temporary data storage
- **Hardware cost evalution:**

	LUT	SRL	FF	BRAM36
Baseline	47453	0	24764	36
Enhanced core	49518	0	25636	38
	+4.3%	-	**+3.5%**	**+5.5%**

Detection module

- **Novel approach to monitore HPCs decdicated to side-channel detection**



- **Hardware approach → low timing overhead**

Application name	Overhead (%)
ARC4 enc./dec.	**+0.85%**
AES v1 (128/512) enc./dec.	**+0.01%**
AES v2 (128 from [23]) enc./dec.	**+0.05%**
Engine control	**+0.06%**
Data sorting (bubble)	**+0.06%**
Queens	**+0.01%**
Pattern matching (text)	**+0.01%**
LMS filter processing	**+0.01%**
FIR filter processing	**+0.01%**
Echo cancellation	**+0.06%**
Motion detection	**+0.01%**
Contrast egalization	**+0.04%**
Dhrystone	**+0.09%**

- **Side-channel attacks [2-3] detection accuracy**

Load conditions	Test performed	FP	FN	Accuracy
No noise	-	0.09%	0%	**100%**
1 noisy app	Random app	0.14%	0%	**100%**
	Worst case	0.21%	0%	**100%**
2 noisy apps	Random apps	2.70%	0%	**100%**
	Worst case	0.33%	0.02%	**99.98%**
4 noisy apps	Random apps	5.10%	0%	**100%**
	Worst case	0.35%	0.80%	**99.2%**

Security strategies:

- **Monitoring : detection of contexts favorable to side-channel attacks and/or covert channels**
- **Dynamic management : micro-architectural defenses and micro-decoder**
- **Deployment of a complete solution from detection to countermeasure on target, while preserving performance**

[1] 1F. Zaruba and L. Benini. The cost of application-class processing: Energy and performance analysis of a linux-ready 1.7-ghz 64-bit risc-v core in 22-nm fdsoi technology. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 27(11):2629–2640, Nov 2019.

[2] V. Martinoli, E. Tourneur, Y. Teglia, and R. Leveugle. CCALK: (When) CVA6 Cache Associativity Leaks the Key. Journal of Low Power Electronics and Applications, 2022.

[3] L. Gerlach, D. Weber, R. Zhang, and M. Schwarz. 2023. A security RISC: microarchitectural attacks on hardware RISC-V CPUs. IEEE Symposium on Security and Privacy (SP) (2023).

May 12-15 2025

RISC-V Summit Europe, Paris, 2025