MonitoRISC: Dynamic insertion of instructions dedicated to sidechannel attacks detection

Juliette Pottier, Maria Mendez Real, Bertrand Le Gal, Sébastien Pillement

MonitoRISC: Dynamic insertion of instructions dedicated to side-channel attacks detection

† Juliette Pottier, † Maria Méndez Real, ‡Bertrand Le Gal, † Sébastien Pillement

†IETR, Nantes Université, Nantes, France

‡IRISA/INRIA, Université de Rennes, Lannion, 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

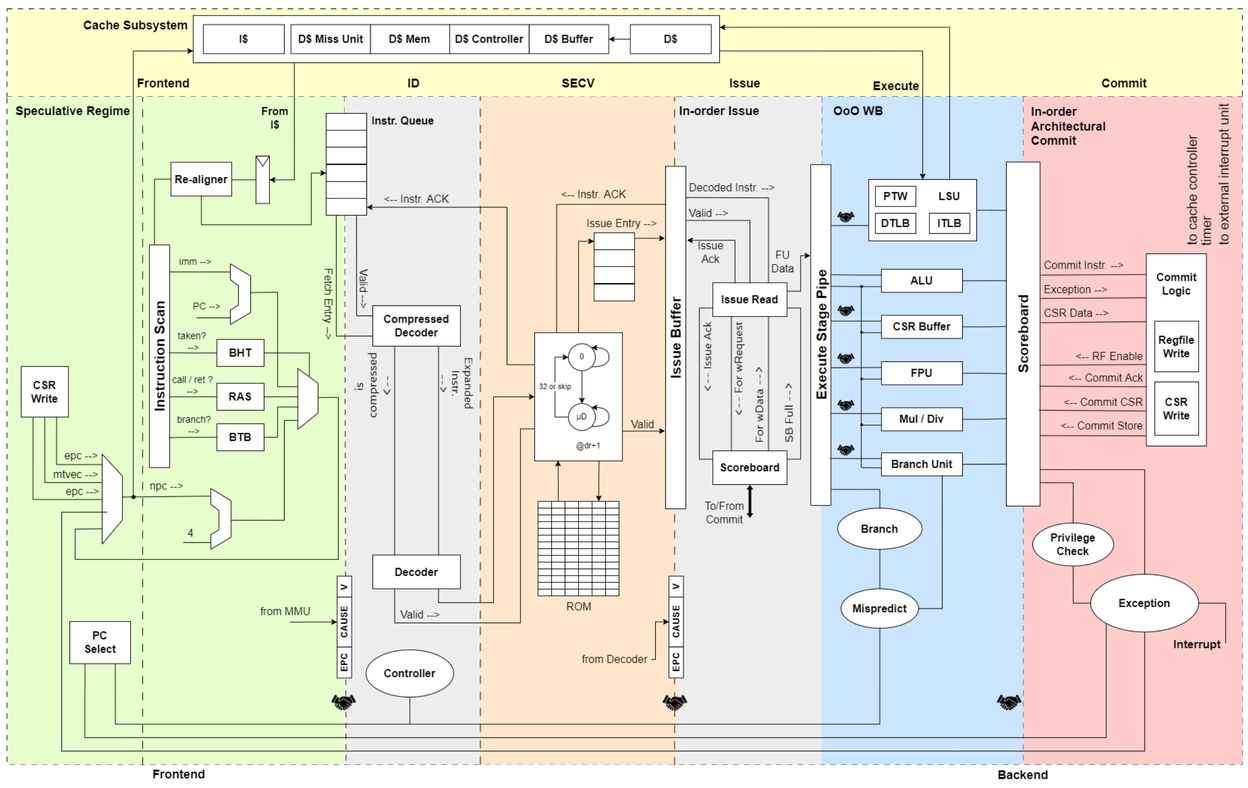
Detection of abnormal behavior

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



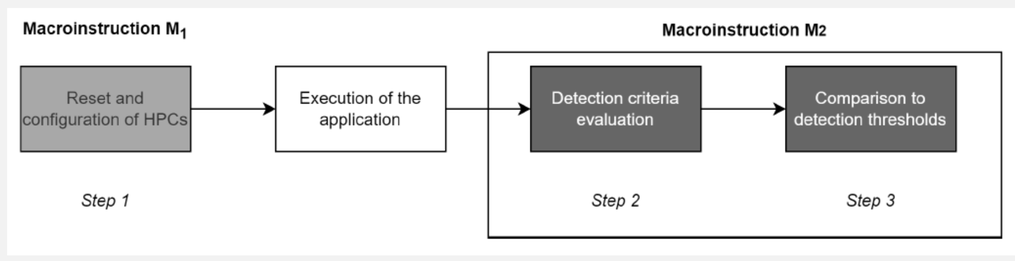
CVA6 Core enhanced with a microdecoding unit

- **CVA6's Features [1]:**
  - ISA: RV64GC
  - 6-stage pipeline partially out-of-order (Execute Stage)
  - Single issue
- **MonitoRISC's Features:**
  - FSM: Bypass/Microdecoding state
  - ROM: contains 32-bit microinstructions sequences
  - FIFO: interfaces with the Issue stage

	LUT	SRL	FF	BRAM36	BRAM18	DSP
baseline	47453	0	24764	36	0	27
With MonitoRISC	49701	0	25718	36	0	27
	+4.7%	-	+3.8%	-	-	-

MonitoRISC

- **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%

- **Prime+Probe attack [2] detection accuracy**

Load conditions	Type of noisy app	Accuracy	False positive	False negative	P+P Sucess rate
Successful P+P attack	(>50% of retrieved bits):				
No noise (NL)	-	100%	0.10%	0%	97%
1 noisy app (AV)	random app	100%	0.14%	0%	73%
	MP3 or random app	100%	0.17%	0%	
	MP3	100%	0.14%	0%	
2 noisy apps (AV)	random apps	100%	0.19%	0%	60%
	MP3 and random apps	99.50%	0.24%	0.50%	
	MP3	99.85%	0.21%	0.15%	
4 noisy apps (FL)	random apps	100%	0.43%	0%	51%
	MP3 and random apps	98.75%	1.92%	1.25%	
	MP3	97.9%	0.21%	2.1%	
Not successful P+P Attack	(<50% of retrieved bits):				
6 noisy apps	random apps	100%	3%	0%	47%
	MP3 and random apps	100%	1.69%	0%	
	MP3	49.5%	0.21%	50.05%	
8 noisy apps	random apps	100%	6.65%	0%	47%
	MP3 and random apps	95.05%	1.44%	39.95%	
	MP3	24.05%	0.20%	75.95%	
10 noisy apps	random apps	99.45%	4.40%	0.55%	47%
	MP3 and random apps	92.20%	1.83%	7.80%	
	MP3	21.6%	0.22%	78.4%	

- **Security strategies:**
  - **Monitoring : detection of contexts favorable to side-channels attacks and/or covert channels**
  - **Dynamic management : micro-architectural defenses and micro-decoder**
  - **Deployment of a complete solution 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.