First analysis and protection of the micro-architecture of a RISC-V core

Juliette Pottier, Maria Mendez Real, Sébastien Pillement

First analysis and protection of the micro-architecture of a RISC-V core

Juliette Pottier, Maria Méndez Real, Sébastien Pillement
IETR, Nantes Université, Nantes, France

Contact: juliette.pottier@univ-nantes.fr

Convention: ANR-21-CE-39-0017
Partners: IETR, IMS, LS2N, Thales

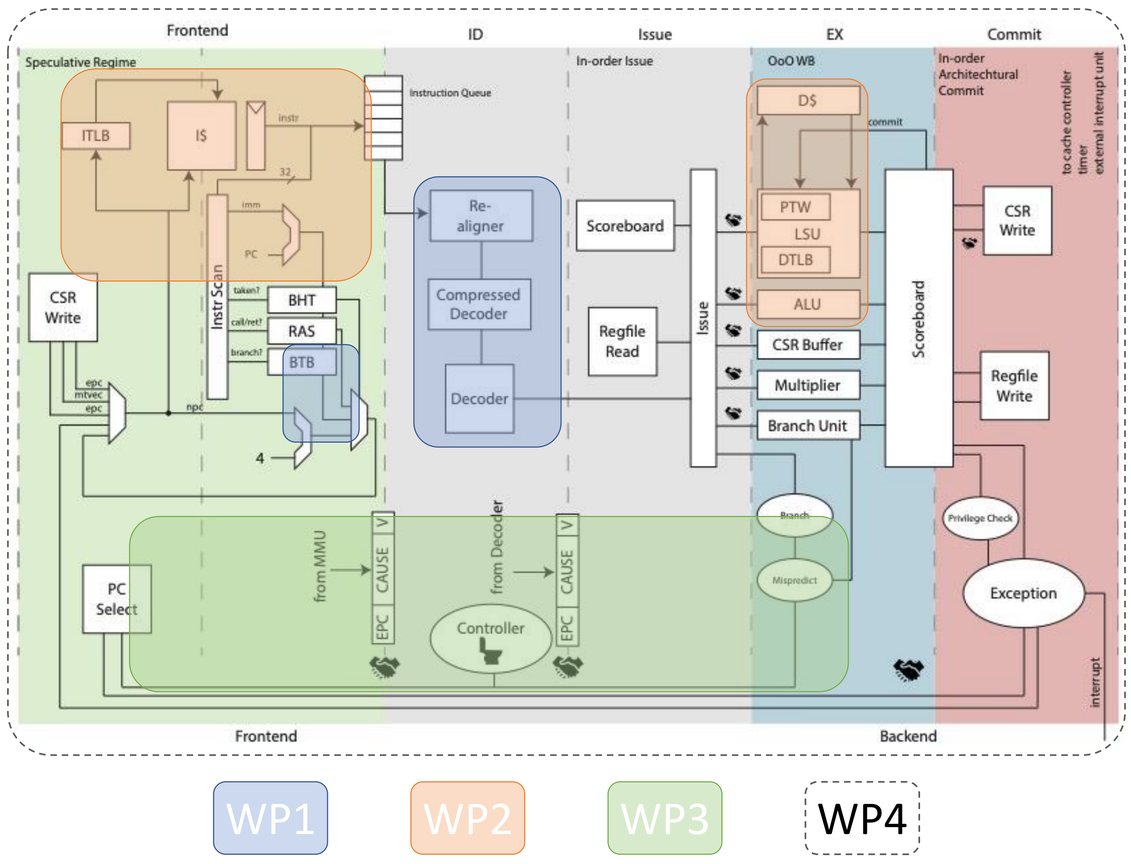
SEC-V Project: Methodology and organization

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



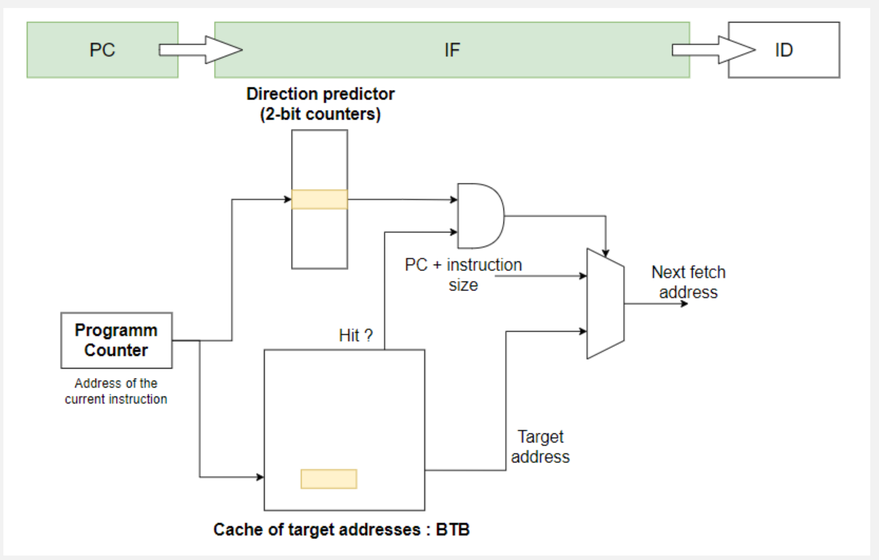
Micro-architecture analysis

- **Vulnerabilities targeted by side-channel attacks and covert channels:**

Principal vulnerabilities	Principal micro-architectural elements involved
Contention Collision Mistraining/poisoning	Branch Predictor (BTB, BHT) Cache memories (I-cache, D-cache) Virtual memory management (TLB)

  - *Kocher, Paul, et al. "Spectre attacks: Exploiting speculative execution. "Communications of the ACM"(2020)*
  - *Ge, Qian, et al. "A survey of microarchitectural timing attacks and countermeasures on contemporary hardware." Journal of Cryptographic Engineering (2018)*

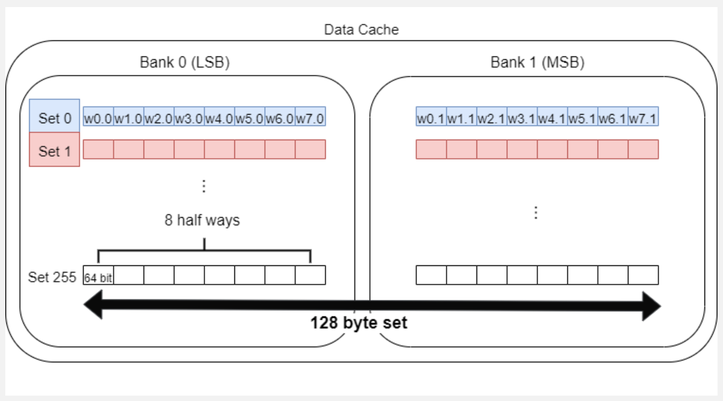
- **2-bit local dynamic Branch Predictor:**



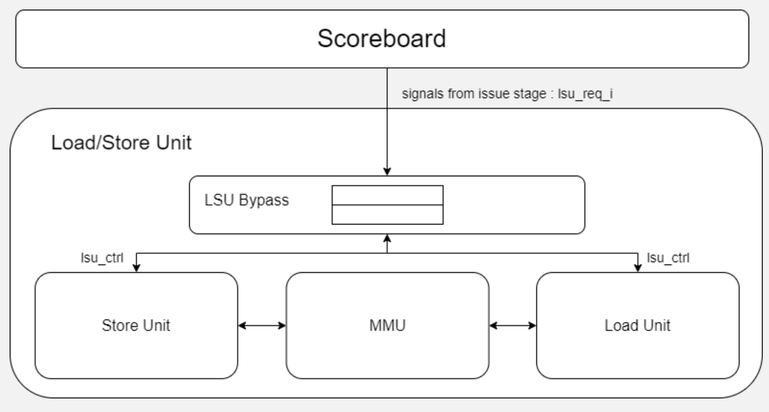
CVA6 Core

- **Features:**
  - ISA : RV64GC
  - 6-stage pipeline partially out-of-order (Execute Stage)
  - Single issue

- **Data cache :**



- **Load-Store Unit and Cache Interface**



- **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**