



HAL
open science

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

Juliette Pottier, Maria Mendez Real, Sébastien Pillement

► To cite this version:

Juliette Pottier, Maria Mendez Real, Sébastien Pillement. First analysis and protection of the micro-architecture of a RISC-V core. Journée Nationale GDR SoC2, Jun 2023, Lyon, France. . hal-04104031

HAL Id: hal-04104031

<https://hal.science/hal-04104031>

Submitted on 6 Jun 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

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

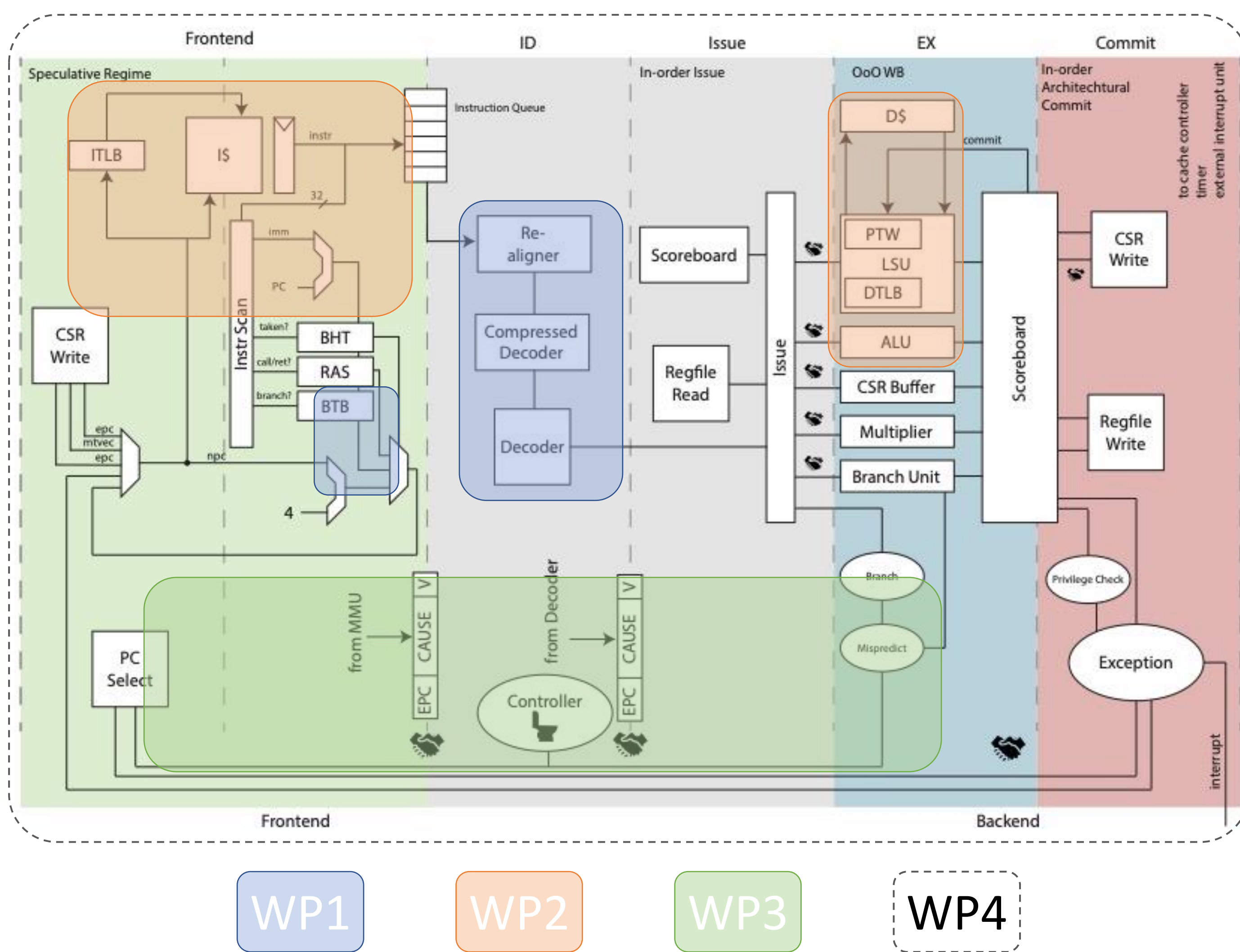
Alternative approaches to traditional caches (scratchpads, TCM)
Dynamic cache management
Inserting execution noise (access instructions for example)

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



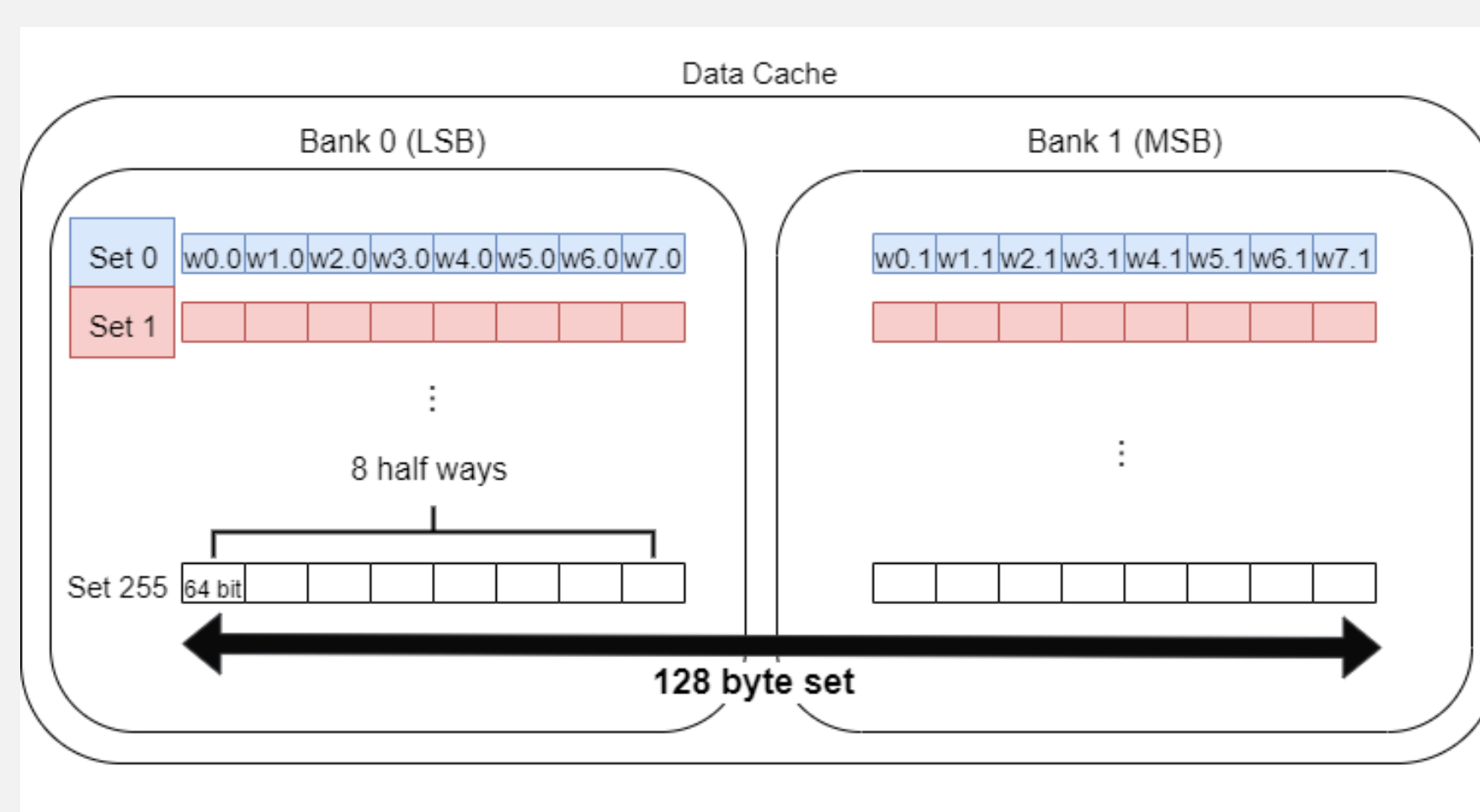
WP1 WP2 WP3 WP4

CVA6 Core

Features:

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

Data cache :



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

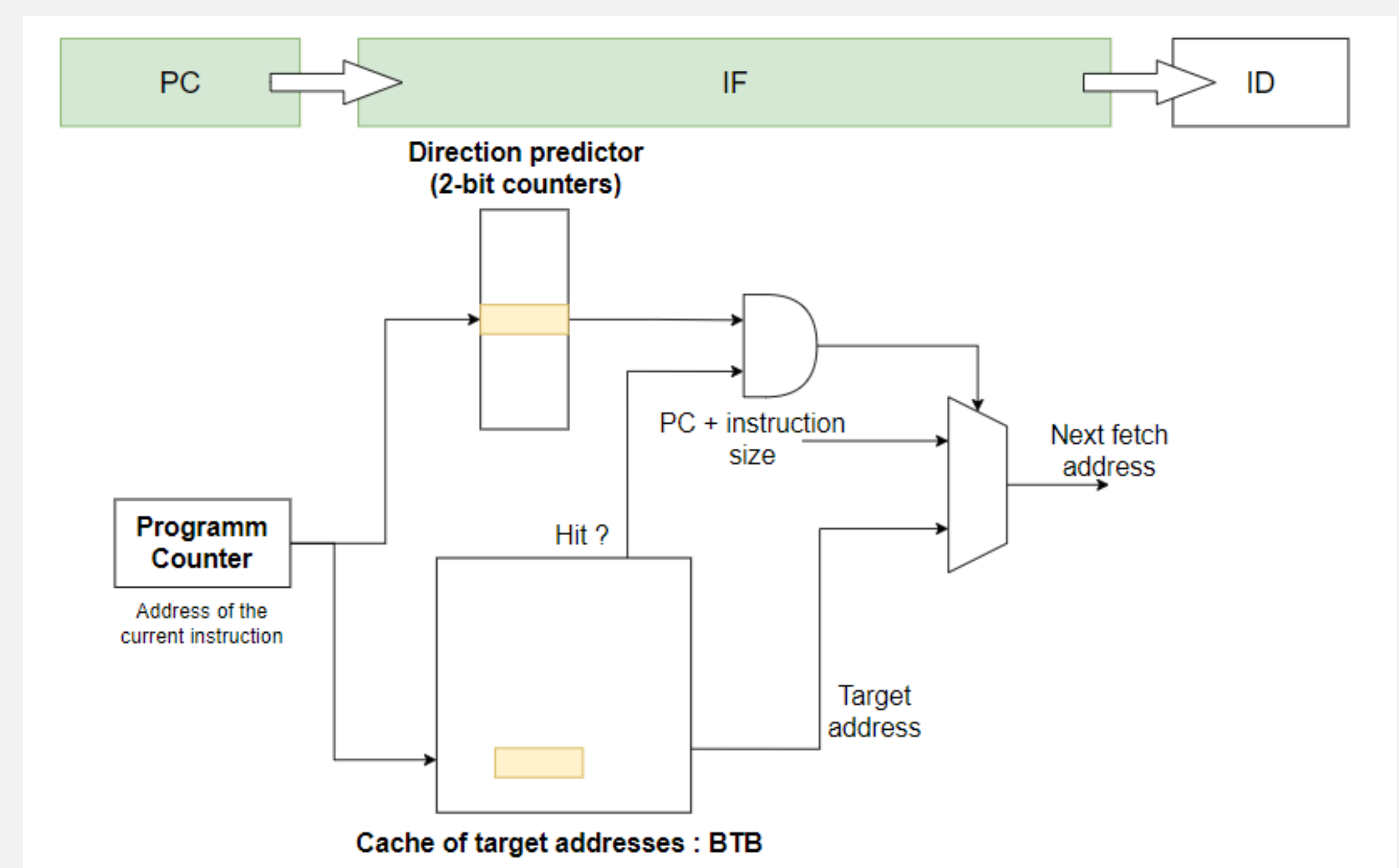
Micro-architecture analysis

- 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:



- Load-Store Unit and Cache Interface

