When in-core DIFT faces fault injection attacks

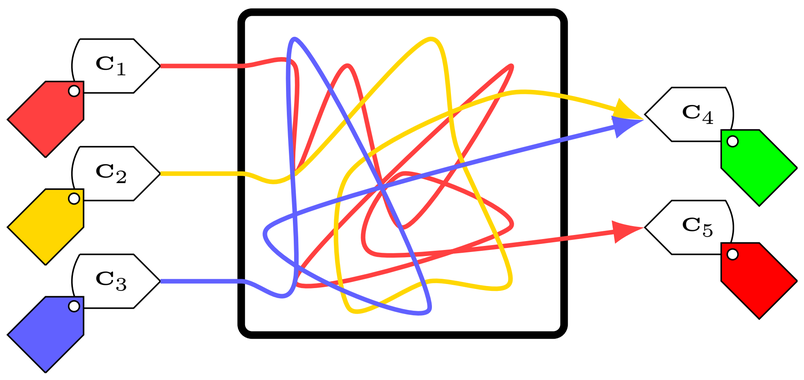
William PENSEC, Vianney LAPÔTRE, Guy GOGNIAT
Lab-STICC, UMR 6285, Université Bretagne Sud, Lorient, France
firstname.lastname@univ-ubs.fr

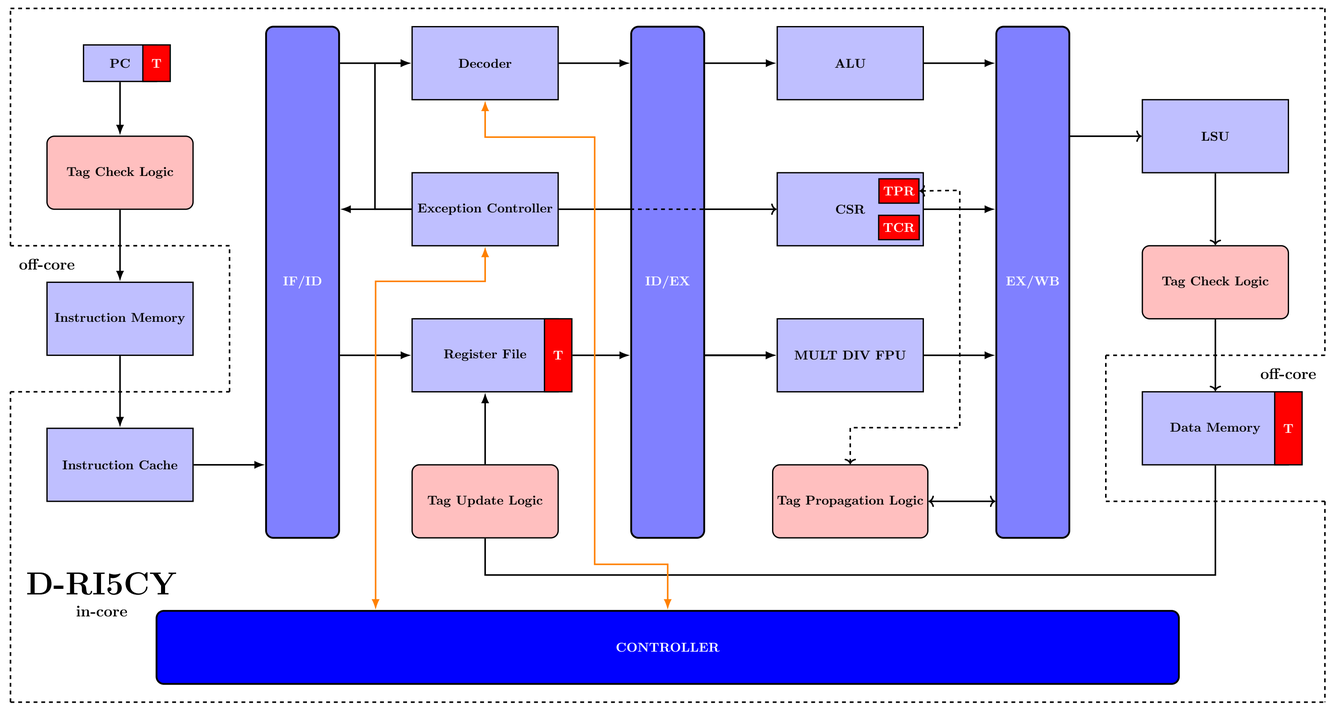
Information Flow Tracking in a RISC-V processor

Different types of IFT [1, 2]:
- Static or Dynamic
- Software, hardware (in-core, off-core [3] (dedicated CPU, co-processor)) or mixed

Three steps
- Tag initialization
- Tag propagation
- Tag verification

Levels of IFT
- OS level
- Application level
- Low level

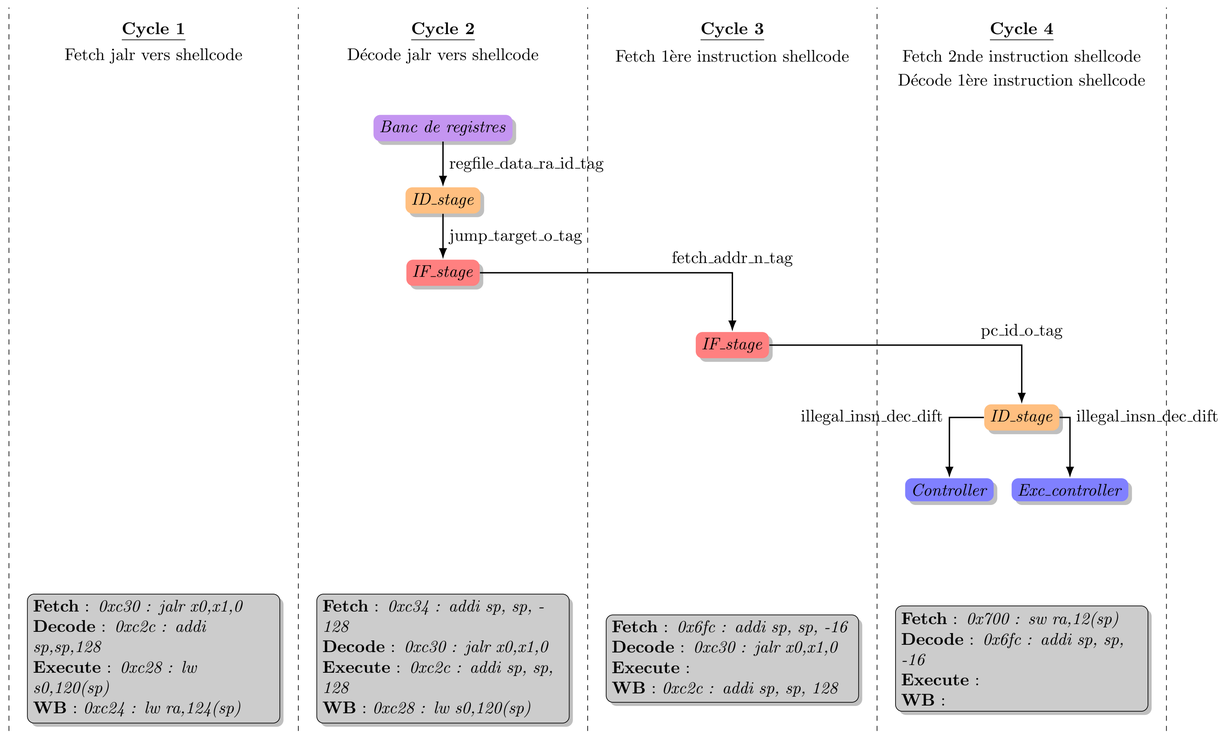




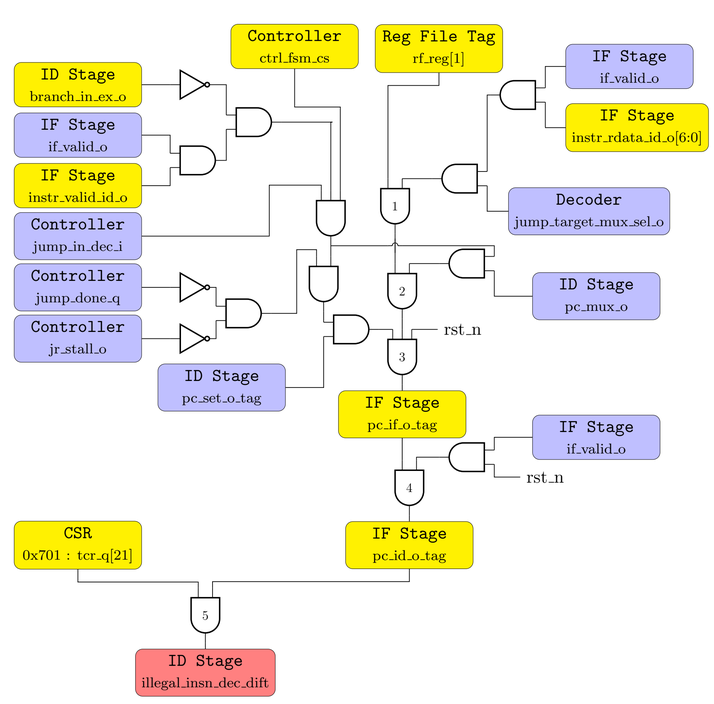
D-RI5CY [4] has been developed by researchers from Columbia University, New York, and University of Turin (Italy).

Physical Attacks against DIFT

We consider an attacker able to:
- combine software and physical attacks to defeat the DIFT mechanism,
- inject faults in registers associated to the DIFT-related components: set to 0, set to 1, a bit-flip at a random position of the targeted register.



Tag propagation in a buffer overflow attack



Logic description of the exception driving in a buffer overflow attack

Results

We used fault injection simulations to evaluate the sensitivity of DIFT at cycle-accurate and bit-accurate levels (CABA).

	Crash	NSTR	Delay	Success	Total
Buffer overflow	0	940	17	15 (1.54%)	972

Fault simulations end status

	137140 ns		137180 ns			137220 ns		137260 ns		137300 ns
	set to 0	set to 1	set to 0	set to 1	bitflip	set to 0	bitflip	set to 0	bitflip	set to 0
pc_if_o_tag						✓		✓	✓	
rf_reg[1]						✓	✓			
tcr_q	✓		✓		✓	✓		✓		✓
tpr_q	✓	✓	✓	✓						

Buffer overflow: success per register, fault type and simulation time

Perspectives

- Implement and evaluate countermeasures taking into account constraints (performance, area, consumption) to protect critical computation related to DIFT.
- Extend the study to the entire D-RI5CY core and a more complex threat model.
- Perform a fault injection campaign targeting a FPGA implementation.

Bibliography

[1] W. Hu *et al.*, "Hardware information flow tracking," *ACM Computing Surveys*, 2021. DOI: 10.1145/3447867.

[2] K. Chen *et al.*, "Dynamic information flow tracking: Taxonomy, challenges, and opportunities," *Micromachines*, 2021. DOI: 10.3390/mi12080898.

[3] H. Kannan *et al.*, "Decoupling dynamic information flow tracking with a dedicated coprocessor," in *International Conference on Dependable Systems & Networks*, IEEE, 2009. DOI: 10.1109/DSN.2009.5270347.

[4] C. Palmiero *et al.*, "Design and implementation of a dynamic information flow tracking architecture to secure a RISC-V core for IoT applications," in *High Performance Extreme Computing*, 2018. DOI: 10.1109/HPEC.2018.8547578.