Exploring Fault Injection Attacks on CVA6 PMP Configuration Flow

Kévin Quénéhervé, William Pensec, Tanguy Philippe, Rachid Dafali, Vianney Lapotre

Exploring Fault Injection Attacks on CVA6 PMP Configuration Flow

Kévin QUÉNÉHERVÉ[£], William PENSEC[£], Philippe TANGUY[£], Rachid DAFALI[†], Vianney LAPÔTRE[£]

[£]Université Bretagne Sud, UMR6285, Lab-STICC, Lorient, France, firstname.lastname@univ-ubs.fr [†]DGA MI, Bruz, France

Context

Fault-Injection Attacks (FIA) [1] are **serious threats** to embedded systems. Nashimoto et al. [2] showed that clock glitching can change the **Physical Memory Protection** (PMP) configuration on RISC-V processors. In [3], we have **characterized** the effects of faults on PMP configuration. To better understand these faults, we used Error-Correction Code (ECC). We modified the `ID` pipeline stage with hardware modules to **filter** single bit-flip faults using **Hamming code**.

Experimental setup

- **Chipwhisperer Lite**
- FPGA Arty A7-100T.
- **Clock glitching** with parameters Figure 2.
- **1,970,001 injections** per campaign
- Target pseudocode, cf. Figure 1.

```
1 TRIGGER high;
2 @ret = (&@base) » 2;
3 @ret &= (size » 3);
4 @ret |= ((size » 3) - 1);
5 csrw pmpaddr0, @ret;
6 csrs pmpcfg0, (0x99);
7 modify the protect value;
```

Figure 1: Target pseudo code

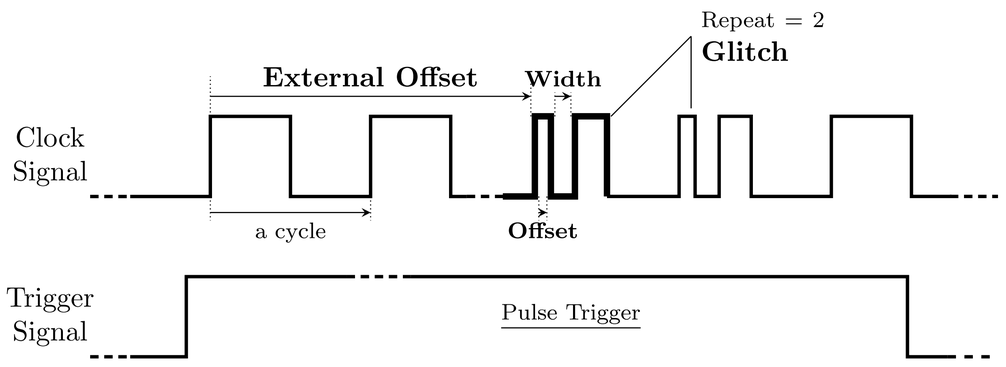
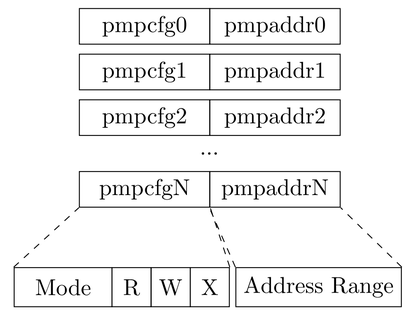
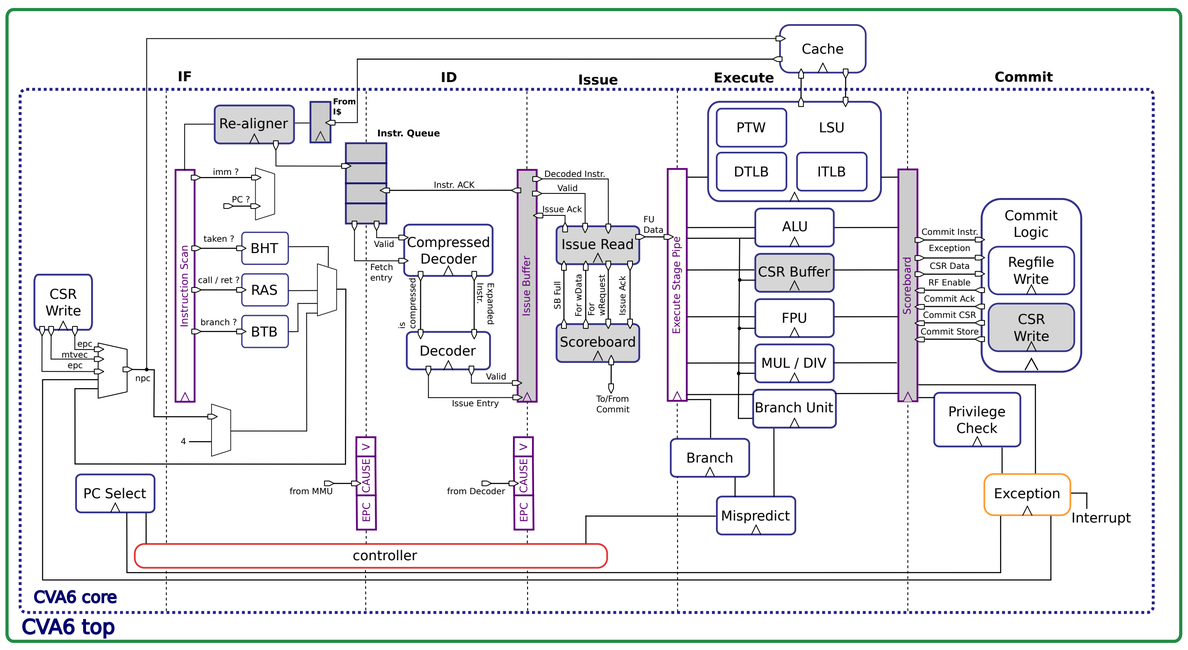


Figure 2: Clock Glitch principles parameters

CVA6 PMP

- **PMP** secures up to 16 memory regions with access permissions.
- Each region uses **two Control Status Registers (CSRs)**.
- In the CVA6 core, PMP configuration is handled in the *CSR Write* module of the *Commit* stage.





Effects of FIA on PMP configuration

5,561 injections modified PMP configuration, enabling write access to protected memory. Figure 3 shows a **correlation** between fault effects and injection parameters, *Width* and *External Offset*.

- **Sensitive** zones can be further divided into sub-zones with specific effects.
- **Single bit-flip effects** mainly occur at zone boundaries.
- **Specific effects** can be targeted by an attacker.

Different impact of `pmpcfg0` & `pmpaddr0` combinations :

- **`G1`** gathers faults that lead to *complex* effects.
- **`G2`** gathers faults that impact either `pmpcfg0` or `pmpaddr0`.
- **`G3`** gathers faults that impact both `pmpcfg0` & `pmpaddr0`.

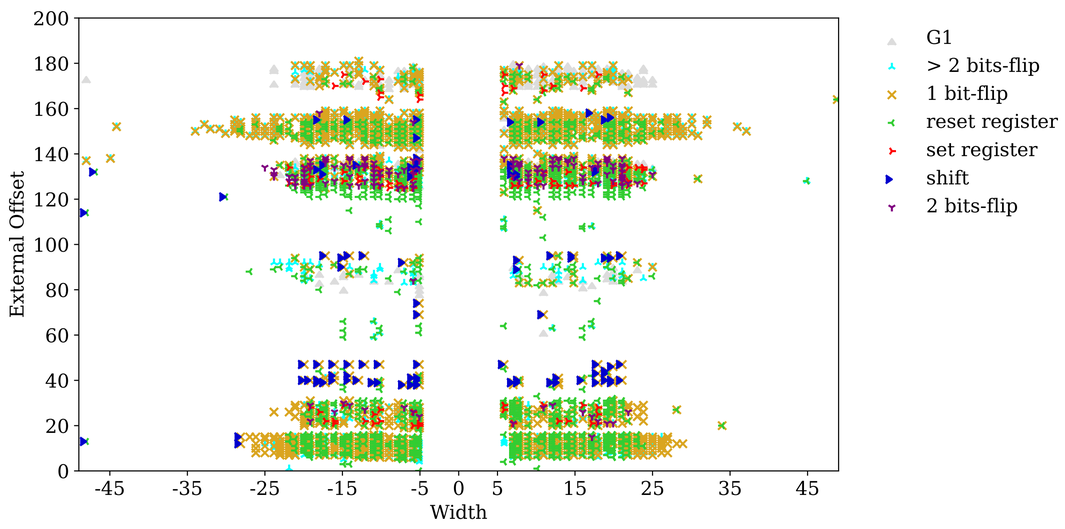


Figure 3: Fault effects about injection parameters

Filters along the PMP configuration flow

- Figure 4 shows **Hamming Code-based filters** that correct **single bit-flips** in PMP registers.
- Table 1 quantifies fault effects for the baseline and **CVA6 core extended with the proposed filters** in the *ID* stage:
- Figure 5 quantifies **the impact of `pmpcfg0` & `pmpaddr0` combinations** in both core versions.

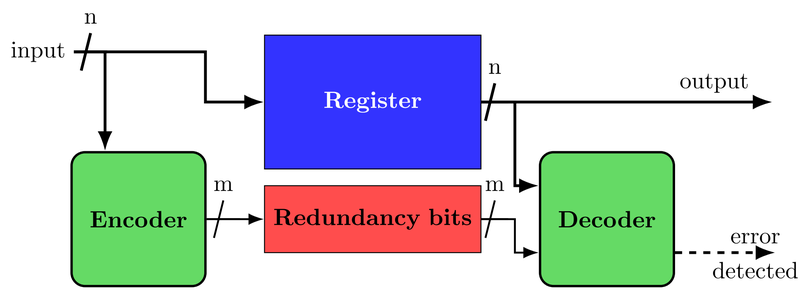


Figure 4: Hamming Code - Filter

Table 1: Results comparison between baseline and filtered

CVA6	Crash	Silent	Faults			
			G1	G2	G3	Total
Baseline	50,146	1,914,294	1,165	2,091	2,305	5,561
ID Filter	122,047	1,846,171	248	487	1,048	1,783

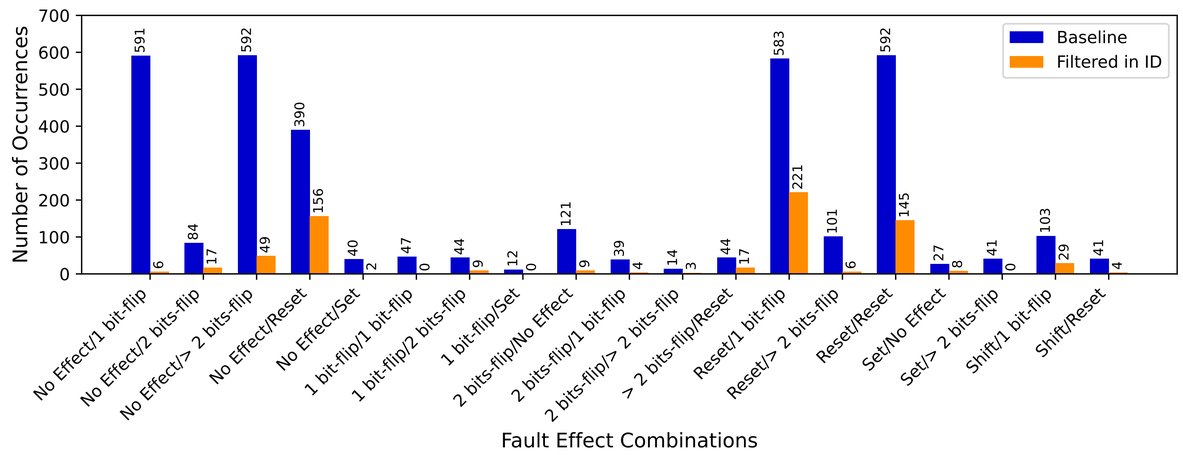


Figure 5: Effects on PMP registers - group G2 & G3 with Hamming Code-based filters in *ID* stage

Conclusion & perspectives

- Shows clock glitch FIA on CVA6 PMP configuration, **identifying exploitable effects**.
- Attackers can adjust injection parameters for **desired effects** with high success.
- Filter helps in **characterizing multiple fault effects**.
- Approach can be applied to **other pipeline stages**.
- Consider **different processor** cores and implementations.

Bibliography

[1] H. Bar-El *et al.*, "The sorcerer's apprentice guide to fault attacks," *Proceedings of the IEEE*, 2006.
[2] S. Nashimoto *et al.*, "Bypassing Isolated Execution on RISC-V using Side-Channel-Assisted Fault-Injection and Its Countermeasure," *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*, 2021.
[3] K. Quénéhervé *et al.*, "Exploring Fault Injection Attacks on CVA6 PMP Configuration Flow," in *27th Euromicro Conference Series on Digital System Design (DSD)*, 2024.