CVA6 RISC-V PMP Vulnerabilities against FIA

Kévin QUÉNÉHERVÉ[£], Philippe TANGUY[£], Rachid DAFALI[†], Vianney LAPÔTRE[£]
[£]Université Bretagne Sud, UMR6285, Lab-STICC, Lorient, France, firstname.lastname@univ-ubs.fr [†]DGA MI, Bruz, France

Context

The **Physical Memory Protection** (PMP) mechanism, crucial for system security and integrated into TEEs, is vulnerable to Fault Injection Attacks (FIA) [1], such as voltage pulses, electromagnetic pulses, and clock glitching. Nashimoto et al. [2], have shown that **clock glitching** can manipulate PMP configuration registers on RISC-V processors. Although most systems use integrated clocks to complicate direct access, clock glitching remains a key method for **exploring fault vulnerabilities** and designing countermeasures.

Experimental setup

- **Chipwhisperer Lite**
- FPGA Arty A7-100T.
- **Clock glitching** with parameters Figure 3.
- **836,381 injections** per campaign
- Target pseudocode, cf. Figure 2.

```
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 2: Target pseudo code

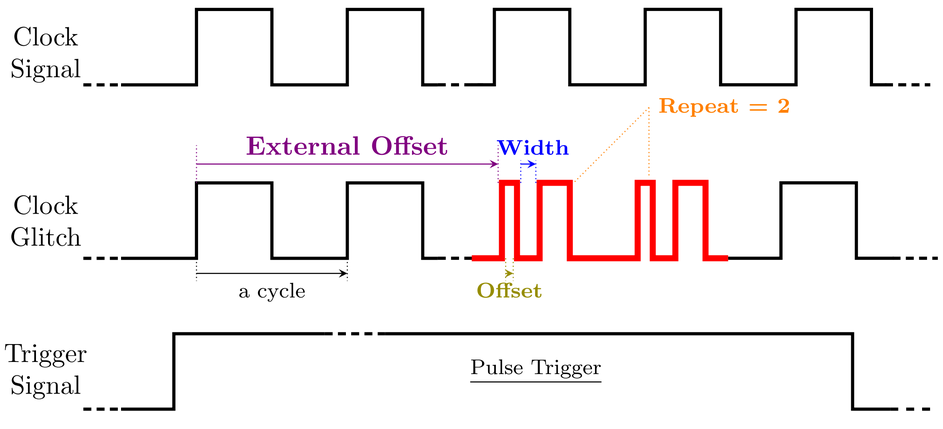
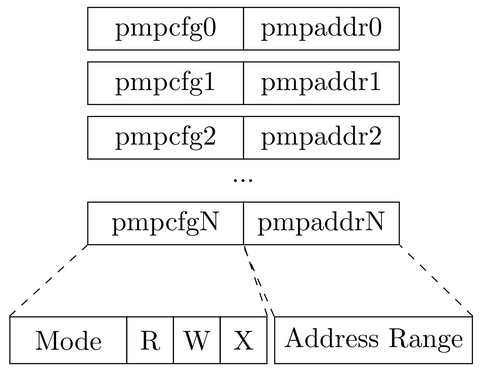


Figure 3: Clock Glitch principles parameters

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 Figure 1.
- Various addressing modes (**NAPOT**, TOR, NA4) in `pmpaddr`*N*



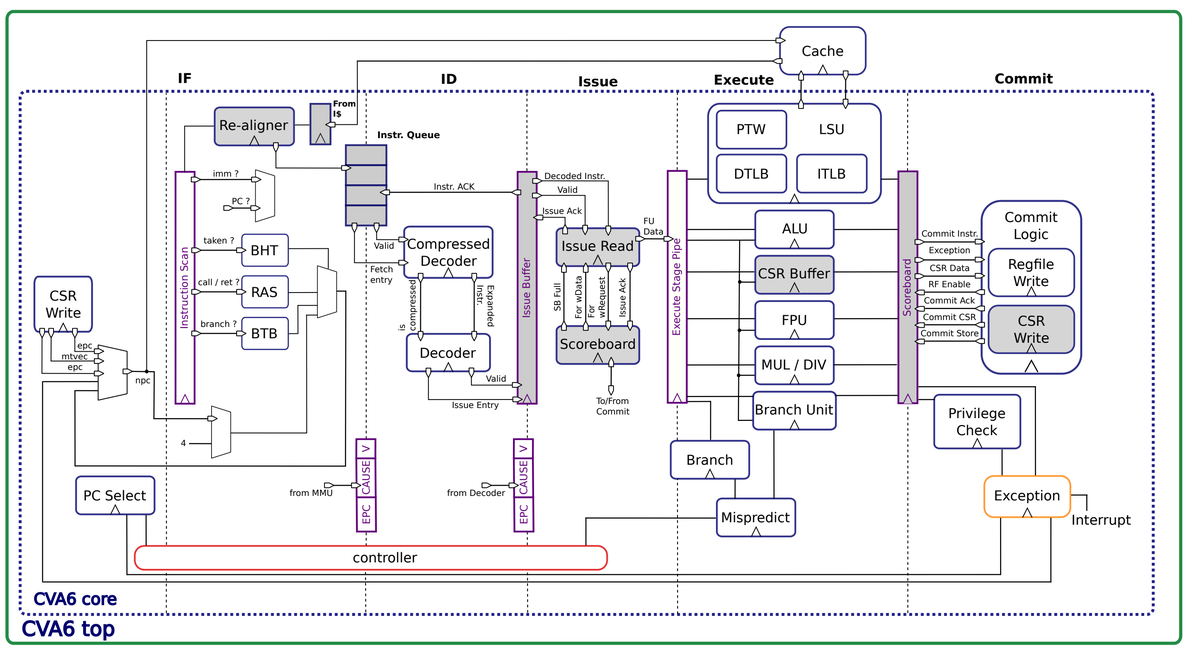


Figure 1: CVA6 RISC-V Core

Effects of FIA on PMP configuration

2,126 injections modified PMP configuration, enabling write access to protected memory. Figure 4 shows different impact of `pmpcfg`*0* & `pmpaddr`*0* combinations :

- **G1** gathers faults that lead to *complex* effects.
- **G2** gathers faults that impact either `pmpcfg`*0* xor `pmpaddr`*0*.
- **G3** gathers faults that impact both `pmpcfg`*0* & `pmpaddr`*0*.

Table 1: Results comparison between baseline and filtered

CVA6	Crash	Silent	Faults			
			G1	G2	G3	Total
Baseline	51,996	782,259	23	1,708	395	2,126

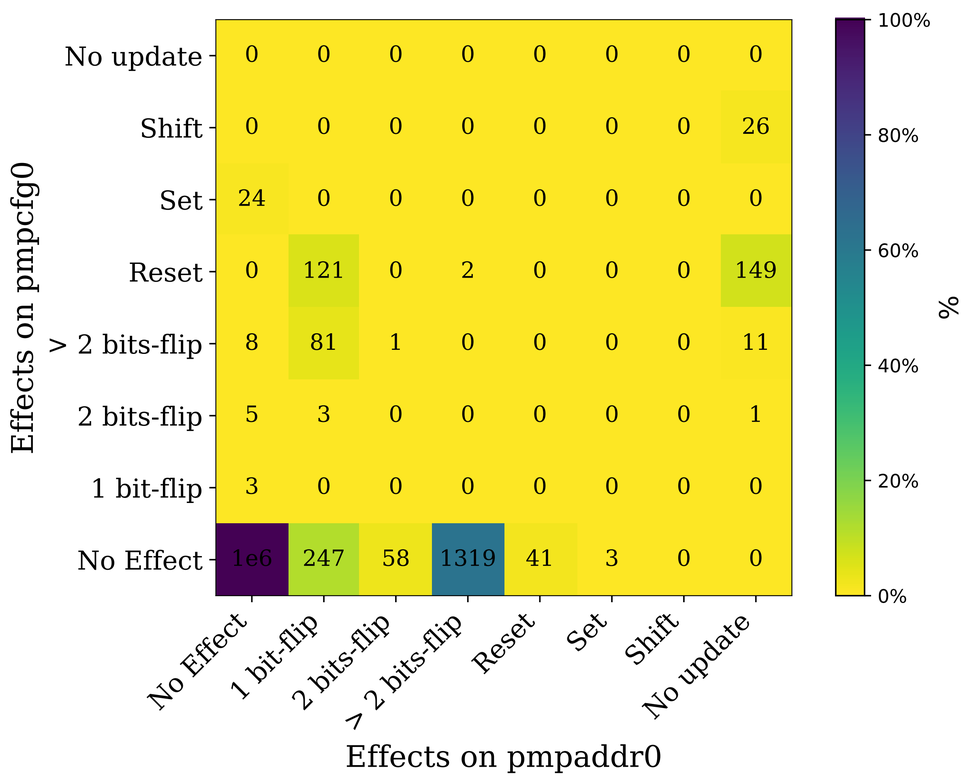


Figure 4: Observed combinations of fault injection effects in G2 & G3

Figure 5 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.
- **Specific effects** can be targeted by an attacker.
- **External Offset** correlates with the instructions in the PMP Library.

The effects of vulnerabilities follow **a structured pattern**, allowing attackers to **fine-tune injections** for precise manipulation of the PMP.
Stronger countermeasures are needed to mitigate targeted attacks.

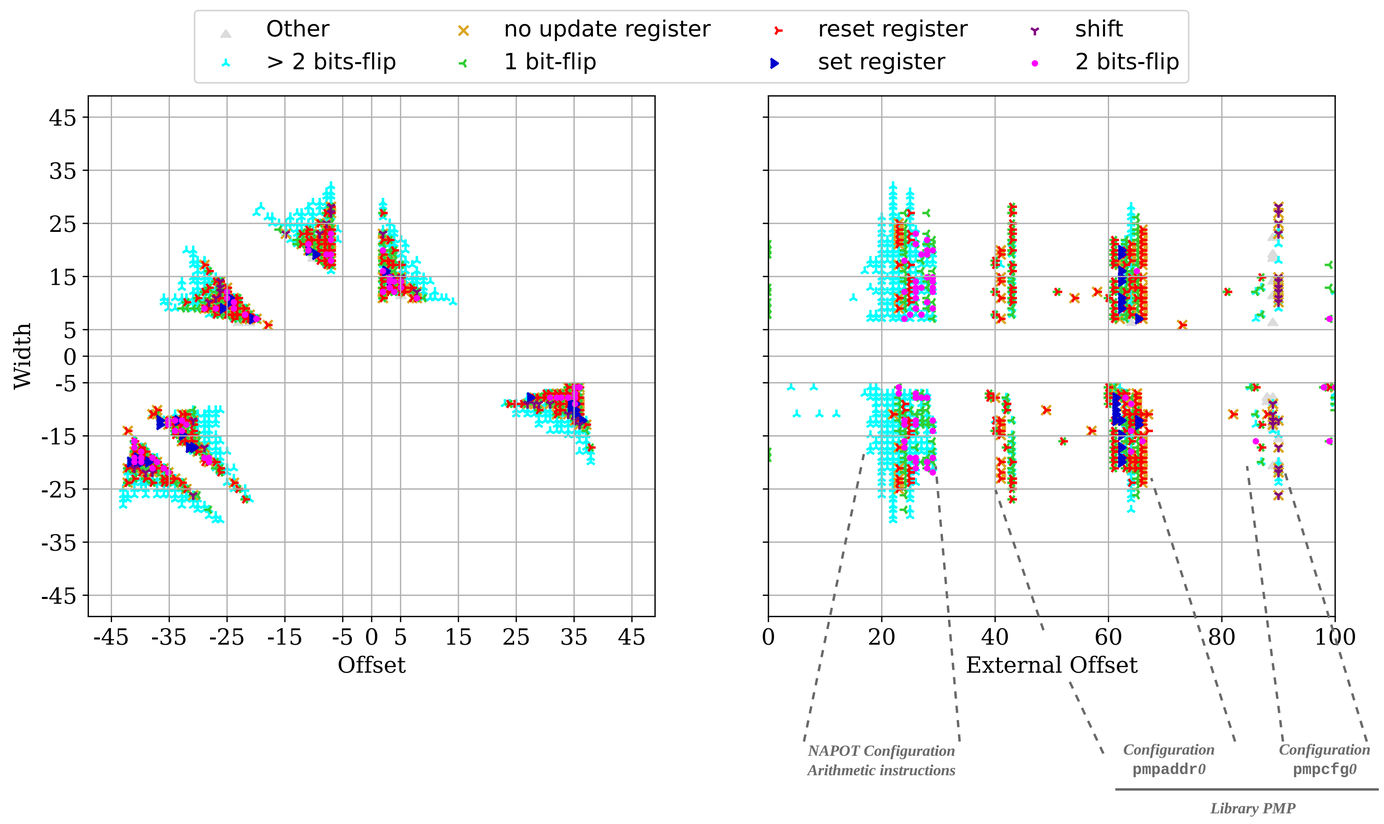


Figure 5: Types of fault effect on PMP registers Vs. Clock fault injection parameters: *Width*, *Offset* and *External Offset*

Conclusion & perspectives

- Attackers can adjust injection parameters for **desired effects**.
- Allows targeting **specific instructions** via *External Offset*.
- Analysis of the **location of fine-grained fault** in the RISC-V pipeline.
- Analysis of the fault effect in **different processor** RISC-V cores.

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.