New issue

Jump to bottom

[Bug Report] incorrect SFENCE.VMA decoder #876

Closed **Phantom1003** opened this issue on May 15 · 1 comment

Phantom1003 commented on May 15 Contributor

Hi, we are currently doing some co-simulation with cva6 and spike, and we found the decoder has an incorrect behavior when meeting a sfence.vma with non-zero rd field.

According to the ISA Specification (Volume II: RISC-V Privileged Architectures V20211203 Page 152) for the SFENCE.VMA format, instr[11:7] should be 5'b00000.

When modified instr[11:7] to 5'b00001. cva6 treats this instruction as SFENCE.VMA as well. No exception occurred. The implementation is missing a check for this field.

cva6/core/decoder.sv
Lines 152 to 165 in 44a89b9

```
152     // SFENCE.VMA
153     default: begin
154         if (instr.instr[31:25] == 7'b1001) begin
155             // check privilege level, SFENCE.VMA can only be executed in M/S mode
156             // otherwise decode an illegal instruction
157             illegal_instr    = (priv_lvl_i inside {riscv::PRIV_LVL_M, riscv::PRIV_LVL_S})
158             instruction_o.op = ariane_pkg::SFENCE_VMA;
159             // check TVM flag and intercept SFENCE.VMA call if necessary
160             if (priv_lvl_i == riscv::PRIV_LVL_S && tvm_i)
161                 illegal_instr = 1'b1;
```

In the following test case, there is an invalid sfence.vma at 0x80000190, whose rd field is 1, cva6 execute it as normal instruction, while spike throws an excaption.

```
[cva6] 532890ns    26637 M 000000008000018c 0 12000073 sfence.vma
[spike] core   0: 0x000000008000018c (0x12000073) sfence.vma zero, zero
[cva6] 534950ns    26740 M 0000000080000190 0 120000f3 sfence.vma
[spike] core   0: 0x0000000080000190 (0x120000f3) unknown
[spike] core   0: exception trap_illegal_instruction, epc 0x0000000080000190
[spike] core   0:           tval 0x0000000000000000
```

cva6-0.zip

> @LuminaDCIX helps reproduce the problem

Phantom1003 commented on Jun 7 — Contributor — Author

cc to **@zarubaf**

Phantom1003 mentioned this issue on Jun 23

fix sfence.vma decoder #921

Merged

Phantom1003 closed this as completed on Jul 8

Gchauvon mentioned this issue on Jul 19

decoder.sv: fix sfence.vma when rs1 != 0 #933

Merged

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant