Sensitive Instructions on ARM

Coprocessor Access Instructions

`MRC` – Move to ARM register from coprocessor
`MCR` – Move to coprocessor from ARM registers

```
LDR r1, =0x00C00000
MCR p15, 0, r1, c13, c3, 4
MRC p15, 0, r0, c13, c1, 0
```

```
IN:
0x00000000: mov r1, #12582912 ; 0xc00000
0x00000004: mcr 15, 0, r1, cr13, cr3, {4}

OP:
 movi_i32 tmp8,$0xc00000
 mov_i32 r1,tmp8
 movi_i32 tmp8,$0xee0d1f93
 mov_i32 tmp9,r1
 movi_i32 tmp10,$set_cp15
 call tmp10,$0x0,$0,env,tmp8,tmp9
 movi_i32 pc,$0x8
 exit_tb $0x0
OUT: [size=60]
0x01000000: e1a00007 mov r0, r7
0x01000004: e3a01093 mov r1, #147 ; 0x93
0x01000008: e3811c1f orr r1, r1, #7936 ; 0x1f00
0x0100000c: e381180d orr r1, r1, #851968 ; 0xd0000
0x01000010: e38114ee orr r1, r1, #-301989888 ; 0xee000000
0x01000014: e3a02000 mov r2, #0 ; 0x0
0x01000018: e38228c0 orr r2, r2, #12582912 ; 0xc00000
0x0100001c: e3a03000 mov r3, #0 ; 0x0
0x01000020: e38338c0 orr r3, r3, #12582912 ; 0xc00000
0x01000024: e5873004 str r3, [r7, #4]
0x01000028: ebc5e16e bl 0x1785e8
0x0100002c: e3a00008 mov r0, #8 ; 0x8
0x01000030: e587003c str r0, [r7, #60]
0x01000034: e3a00000 mov r0, #0 ; 0x0
0x01000038: eac8336a b 0x20cde8

----------------

IN:
0x00000008: mrc 15, 0, r0, cr13, cr1, {0}

OP:
 movi_i32 tmp8,$0xee1d0f11
 movi_i32 tmp10,$get_cp15
 call tmp10,$0x0,$1,tmp9,env,tmp8
 mov_i32 r0,tmp9

OUT: [size=52]
0x01000040: e1a00007 mov r0, r7
0x01000044: e3a01011 mov r1, #17 ; 0x11
0x01000048: e3811c0f orr r1, r1, #3840 ; 0xf00
0x0100004c: e381181d orr r1, r1, #1900544 ; 0x1d0000
0x01000050: e38114ee orr r1, r1, #-301989888 ; 0xee000000
0x01000054: ebc5e01b bl 0x1780c8
0x01000058: e5870000 str r0, [r7]
```

CDP – Coprocessor data operations

CDP p1,10,c1,c2,c31

```
IN:
0x00000000:  fdvs       f1, f2, f3

OP:
 movi_i32 pc,$0x0
 movi_i32 tmp8,$0x1
 movi_i32 tmp9,$exception
 call tmp9,$0x0,$0,tmp8
 exit_tb $0x0

OUT: [size=24]
0x01000000:  e3a00001  mov     r0, #1   ; 0x1
0x01000004:  e3a01000  mov     r1, #0   ; 0x0
0x01000008:  e587103c  str     r1, [r7, #60]
0x0100000c:  ebc5cfdf  bl      0x173f90
0x01000010:  e3a00000  mov     r0, #0   ; 0x0
0x01000014:  eac83373  b       0x20cde8
```

`LDC,STC` – Transfer data between memory and coprocessor

```
LDC  p1,c2,[R5,#24]
STC  p1,c2,[R5,#24]
```

Assertion fault