

RNDR, Random Number

The RNDR characteristics are:

Purpose

Random Number. Returns a 64-bit random number which is reseeded from the True Random Number source at an implementation defined rate.

If the hardware returns a genuine random number, PSTATE.NZCV is set to 0b0000.

If the instruction cannot return a genuine random number in a reasonable period of time, PSTATE.NZCV is set to 0b0100 and the data value returned is 0.

Configuration

This register is present only when FEAT_RNG is implemented or FEAT_RNG_TRAP is implemented. Otherwise, direct accesses to RNDR are undefined.

Attributes

RNDR is a 64-bit register.

Field descriptions

63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32
RNDR																															
RNDR																															
31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

RNDR, bits [63:0]

Random Number. Returns a 64-bit Random Number which is reseeded from the True Random Number source at an implementation defined rate.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

Accessing RNDR

Accesses to this register use the following encodings in the System register encoding space:

MRS <Xt>, RNDR

op0	op1	CRn	CRm	op2
0b11	0b011	0b0010	0b0100	0b000

```
if PSTATE.EL == EL0 then
    if IsFeatureImplemented(FEAT_RNG_TRAP) &&
        SCR_EL3.TRNDR == '1' then
        if Halted() && EDSCR.SDD == '1' then
            UNDEFINED;
        else
            AArch64.SystemAccessTrap(EL3, 0x18);
        elsif !IsFeatureImplemented(FEAT_RNG) then
            UNDEFINED;
        else
            X[t, 64] = RNDR;
    elsif PSTATE.EL == EL1 then
        if IsFeatureImplemented(FEAT_RNG_TRAP) &&
            SCR_EL3.TRNDR == '1' then
            if Halted() && EDSCR.SDD == '1' then
                UNDEFINED;
            else
                AArch64.SystemAccessTrap(EL3, 0x18);
            elsif !IsFeatureImplemented(FEAT_RNG) then
                UNDEFINED;
            else
                X[t, 64] = RNDR;
    elsif PSTATE.EL == EL2 then
        if IsFeatureImplemented(FEAT_RNG_TRAP) &&
            SCR_EL3.TRNDR == '1' then
            if Halted() && EDSCR.SDD == '1' then
                UNDEFINED;
            else
                AArch64.SystemAccessTrap(EL3, 0x18);
            elsif !IsFeatureImplemented(FEAT_RNG) then
                UNDEFINED;
            else
                X[t, 64] = RNDR;
    elsif PSTATE.EL == EL3 then
        if IsFeatureImplemented(FEAT_RNG_TRAP) &&
            SCR_EL3.TRNDR == '1' then
            AArch64.SystemAccessTrap(EL3, 0x18);
        elsif !IsFeatureImplemented(FEAT_RNG) then
            UNDEFINED;
        else
            X[t, 64] = RNDR;
```

[AArch32
Registers](#)

[AArch64
Registers](#)

[AArch32
Instructions](#)

[AArch64
Instructions](#)

[Index by
Encoding](#)

[External
Registers](#)

28/03/2023 16:01; 72747e43966d6b97dcbd230a1b3f0421d1ea3d94

Copyright © 2010-2023 Arm Limited or its affiliates. All rights reserved. This document is Non-Confidential.