THALES
Building a future we can all trust

SP 800-90B Non-Proprietary Public Use Document
Thales RO_TRNG Version 2.2

SEPTEMBER 12, 2023, Rev. B

Revision History

Version	Change
September 12, 2023, Rev.B	Addressed comment in Section 7
April 17, 2023, Rev.A	Initial release

Table of Contents

1. Description

The Thales RO_TRNG Version 2.2 is a physical entropy source. Entropy is provided by eight ring oscillators (RO), whose period is affected by thermal noise. Two flip-flops for each RO acquire one bit per RO. The bits are combined to produce a single output random bit. The clk_smp signal comes from a specific ring oscillator named SAMPLER, whose output is divided by a software configurable factor KD, and clocks the entire digitization process at a low frequency.

This is a Non-IID source.

2. Security Boundary

Figure 2-1 presents the noise source architecture.

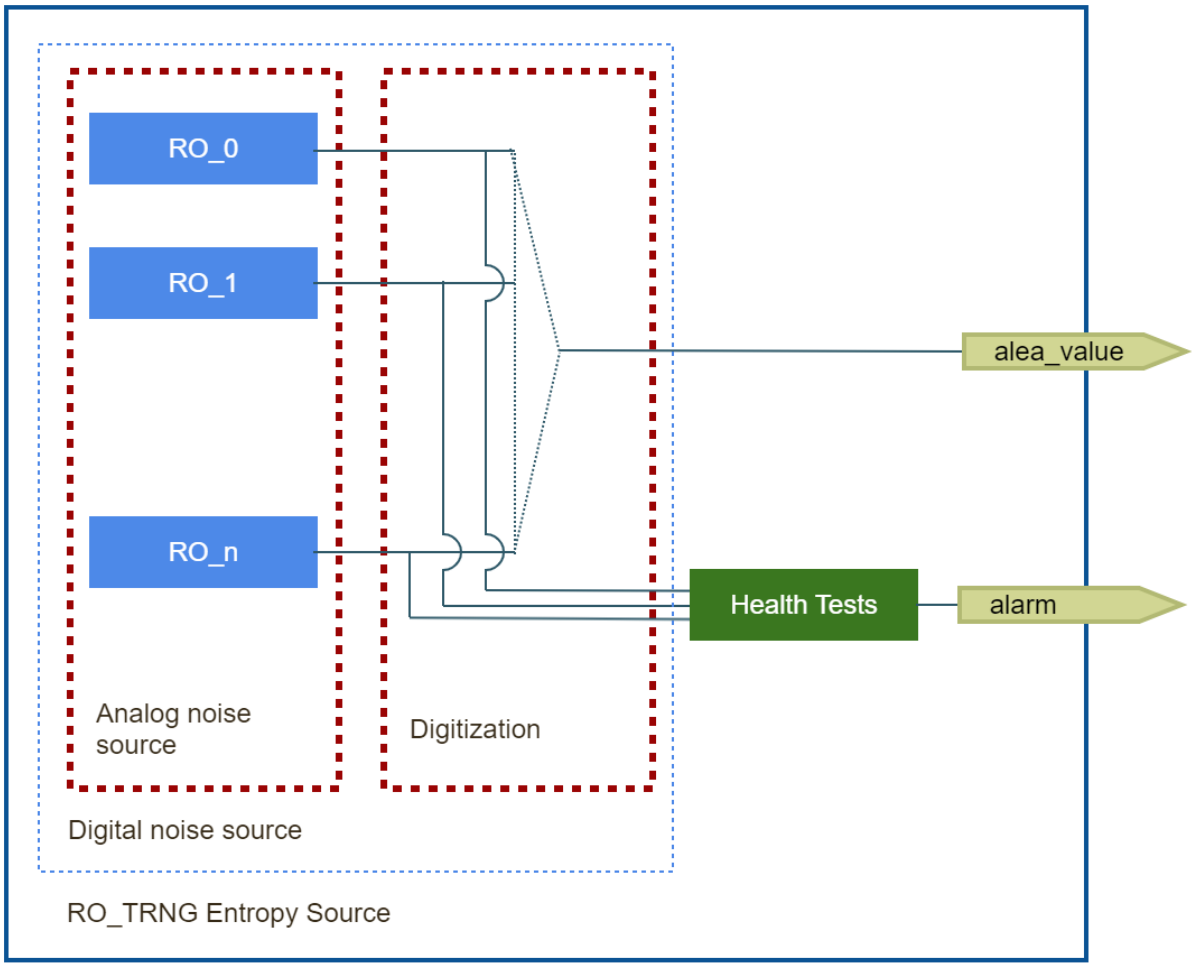

Figure 2-1: Entropy Source Architectural Representation

3. Operating Conditions

Entropy is not expected to vary across the range of operating conditions for the entropy source. The entropy source is therefore valid for the full range of conditions.

The range of operating conditions is as follows:

Operating condition	Min	Typical	Max	Unit
FPGA junction temperature	0	25	80	°C
FPGA core voltage	0.87	0.9	0.93	V

Table 3-1: Operating conditions range

4. Configuration Settings

The entropy source RO_TRNG must be properly configured before use. The following procedures provide an exhaustive description of the parameters to be configured.

1. Set registers.
   The following steps may be performed in any order.
   - Enable sampler and set KD with **REG_CFG_SMP**
   - Enable the contributing ROs 0 to 7 by setting **REG_SEL_RO_0_31**
   - Configure Sampler Frequency Test in **REG_CFG_FENETRE_SMP** , **REG_CFG_SMP_MIN** and **REG_CFG_SMP_MAX**
   - Configure APT and RPT thresholds for the full source in **REG_CFG_TEST_TOP**
   - Configure APT and RPT thresholds for each activated RO in registers **REG_CFG_TEST_RO_0** to **REG_CFG_TEST_RO_7**
   - Ensure alarms are not masked by setting **REG_ALARM_MASK**
2. Then, activate alea generation by setting **REG_CMD**.

These configuration settings are summarized by the following register write operations, with:

- Step: the indicative order of the step. The order does not matter, except for the last step (which is the final step)
- Register name: mnemonic of the written register
- Address: byte address to set on the APB bus to access the register
- Value: value to write to the register

Step	Register name	Address	Value
1	**REG_CFG_SMP**	0x0000_0008	0x8000_1517
2	**REG_SEL_RO_0_31**	0x0000_0010	0x0000_00FF
3	**REG_CFG_FENETRE_SMP**	0x0000_0018	0x0004_0953
4	**REG_CFG_SMP_MIN**	0x0000_001C	0x0000_0008
5	**REG_CFG_SMP_MAX**	0x0000_0020	0x0000_0024
6	**REG_CFG_TEST_TOP**	0x0000_0024	0x0028_0319
7	**REG_CFG_TEST_RO_0**	0x0000_0100	0x0054_0398
8	**REG_CFG_TEST_RO_1**	0x0000_0104	0x0074_03BB
9	**REG_CFG_TEST_RO_2**	0x0000_0108	0x00B9_03DB

Step	Register name	Address	Value
10	**REG_CFG_TEST_RO_3**	0x0000_010C	0x00D0_03E1
11	**REG_CFG_TEST_RO_4**	0x0000_0110	0x0168_03F4
12	**REG_CFG_TEST_RO_5**	0x0000_0114	0x01F7_03FA
13	**REG_CFG_TEST_RO_6**	0x0000_0118	0x0165_03F3
14	**REG_CFG_TEST_RO_7**	0x0000_011C	0x01B0_03F8
15	**REG_ALARM_MASK**	0x0000_002C	0x0000_0000
16	**REG_CMD**	0x0000_000C	0x0000_0001

Table 4-1: Configuration settings – registers access

Below is a more detailed description of the required register settings. The tables provide the following information:

- Field – the name of the register field
- Bits – the location of the field of the 32 bits of the register. The lowest index bit corresponds to the least significant bit
- Access – details the access rights to the field
- Value – the value of the field to be set

REG_CFG_SMP – Sampler Configuration Register

Field	Bits	Access	Description	Value
EN_SAMPLER	31	Read Write	Activation of the sampler ring with the configured KD parameter.	1
KD	15 - 0	Read Write	Parameterization of the KD factor. The clk_sampler clock is derived from clk_sampler_ndiv by a division factor equal to KD+1.	0x1517

Table 4-2: REG_CFG_SMP Register

REG_SEL_RO_0_31: RO Activation Registers

Field	Bits	Access	Description	Value
SEL_RO_i	31 - 0	Read Write	When bit i of the register is set to 0, ring i is deactivated and does not contribute to the entropy. Rings 0 to 7 must be activated.	0x0000_00FF

Table 4-3: REG_SEL_RO_0_31 Register

REG_CFG_FENETRE_SMP – Configuration of the SAMPLER test window

Field	Bits	Access	Description	Value
WINDOW_SMP	31_0	Read Write	Configures the window size (expressed in number of clk system clock edges) for the sampler frequency test.	0x0004_0953

Table 4-4: REG_CFG_FENETRE_SMP Register

REG_CFG_SMP_MIN – Configuration of the SAMPLER minimum threshold

Field	Bits	Access	Description	Value
F_MIN_SMP	31_0	Read Write	Configures the minimum threshold of clk_sampler edges to detect during the duration of WINDOW_SMP.	0x8

Table 4-5: REG_CFG_SMP_MIN Register

REG_CFG_SMP_MAX – Configuration of the SAMPLER maximum threshold

Field	Bits	Access	Description	Value
F_MAX_SMP	31_0	Read Write	Configures the maximum threshold of clk_sampler edges to detect during the duration of WINDOW_SMP.	0x24

Table 4-6: REG_CFG_SMP_MAX Register

REG_CFG_TEST_TOP – Full source online test setup

Field	Bits	Access	Description	Value
ADA_TOP	25 - 16	Read Write	Configures the threshold for the *adaptive proportion test* for the complete physical source.	0x028
REP_TOP	9 - 0	Read Write	Configures the threshold for the *repetition count test* for the complete physical source.	0x319

Table 4-7: REG_CFG_TEST_TOP Registers

REG_ALARM_MASK – Alarm masking

Field	Bits	Access	Description	Value
MSK_ADA_TOP	20	Read Write	When this bit is at 1, the ALR_ADA_TOP alarm is masked at 0.	0
MSK_REP_RO	19	Read Write	When this bit is at 1, the ALR_REP_RO alarm is masked at 0.	0
MSK_SMP	18	Read Write	When this bit is at 1, the ALR_SMP alarm is masked at 0.	0
MSK_ADA_RO	17	Read Write	When this bit is at 1, the ALR_ADA_RO alarm is masked at 0.	0
MSK_REP_TOP	16	Read Write	When this bit is at 1, the ALR_REP_TOP alarm is masked at 0.	0

Table 4-8: REG_ALARM_MASK Registers

REG_CFG_TEST_RO_0 – Ring online test setup

Field	Bits	Access	Description	Value
ADA_TOP	25 - 16	Read Write	Configures the threshold for the *adaptive proportion test* for the ring 0.	0x054
REP_TOP	9 - 0	Read Write	Configures the threshold for the *repetition count test* for the ring 0.	0x398

Table 4-9: REG_CFG_TEST_RO_0 Register

REG_CFG_TEST_RO_1 – Ring online test setup

Field	Bits	Access	Description	Value
ADA_TOP	25 - 16	Read Write	Configures the threshold for the *adaptive proportion test* for the ring 1.	0x074
REP_TOP	9 - 0	Read Write	Configures the threshold for the *repetition count test* for the ring 1.	0x3BB

Table 4-10: REG_CFG_TEST_RO_1 Register

REG_CFG_TEST_RO_2 – Ring online test setup

Field	Bits	Access	Description	Value
ADA_TOP	25 - 16	Read Write	Configures the threshold for the *adaptive proportion test* for the ring 2.	0x0B9
REP_TOP	9 - 0	Read Write	Configures the threshold for the *repetition count test* for the ring 2.	0x3DB

Table 4-11: REG_CFG_TEST_RO_2 Register

REG_CFG_TEST_RO_3 – Ring online test setup

Field	Bits	Access	Description	Value
ADA_TOP	25 - 16	Read Write	Configures the threshold for the *adaptive proportion test* for the ring 3.	0x0D0
REP_TOP	9 - 0	Read Write	Configures the threshold for the *repetition count test* for the ring 3.	0x3E1

Table 4-12: REG_CFG_TEST_RO_3 Register

REG_CFG_TEST_RO_4 – Ring online test setup

Field	Bits	Access	Description	Value
ADA_TOP	25 - 16	Read Write	Configures the threshold for the *adaptive proportion test* for the ring 4.	0x168
REP_TOP	9 - 0	Read Write	Configures the threshold for the *repetition count test* for the ring 4.	0x3F4

Table 4-13: REG_CFG_TEST_RO_4 Register

REG_CFG_TEST_RO_5 – Ring online test setup

Field	Bits	Access	Description	Value
ADA_TOP	25 - 16	Read Write	Configures the threshold for the *adaptive proportion test* for the ring 5.	0x1F7
REP_TOP	9 - 0	Read Write	Configures the threshold for the *repetition count test* for the ring 5.	0x3FA

Table 4-14: REG_CFG_TEST_RO_5 Register

REG_CFG_TEST_RO_6 – Ring online test setup

Field	Bits	Access	Description	Value
ADA_TOP	25 - 16	Read Write	Configures the threshold for the *adaptive proportion test* for the ring 6.	0x165
REP_TOP	9 - 0	Read Write	Configures the threshold for the *repetition count test* for the ring 6.	0x3F3

Table 4-15: REG_CFG_TEST_RO_6 Register

REG_CFG_TEST_RO_7 – Ring online test setup

Field	Bits	Access	Description	Value
ADA_TOP	25 - 16	Read Write	Configures the threshold for the *adaptive proportion test* for the ring 7.	0x1B0
REP_TOP	9 - 0	Read Write	Configures the threshold for the *repetition count test* for the ring 7.	0x3F8

Table 4-16: REG_CFG_TEST_RO_7 Register

REG_CMD – Start / Stop alea generation

Field	Bits	Access	Description	Value
REP_TOP	0	Write	Writing a 1 starts the alea generation process. Writing a 0 stops the process and halts data ROs.	1

Table 4-17: REG_CFG_TEST_RO_0 Register

5. Physical Security Mechanisms

The physical security is provided by the Arria10 FPGA and the computing platform on which it is installed.

6. Conceptual Interfaces

Output from the noise sources is available exclusively from the alea_value output pin.

7. Min-Entropy Rate

The min-entropy figure of $H_{submitter}$ = 0.50922269 has been selected to be a conservative estimate. In accordance with Section 3.1.4.2 of SP800-90B, H_{min} = 0.50922269. The output at alea_value provides 0.5 bits of entropy per bit output. This is the $H_{submitter}$ value, rounded down.

8. Health Tests

The entropy source performs the health tests mandated by Section 4.4 of SP 800-90B. The source conducts Start-up Health Tests on initiation of the entropy source. Continuous Health Tests consist of a Repetition Count Test and an Adaptive Proportion Test. On-demand Health Tests are initiated by restarting the entropy source. Failure of any of these tests is indicated by an alarm raised on the alarm pin.

9. Maintenance

No maintenance activities are prescribed for this entropy source.

10. Required Testing

The Thales RO_TRNG entropy source was tested in accordance with SP 800-90B requirements. Observation pins were used to collect raw unconditioned noise. These interfaces are not available in all implementations; therefore, the user must rely on health tests to ensure that the entropy source is configured correctly and is working as expected.

No further testing is required.