SP 800-90B Non-Proprietary Public Use Document for Samsung TRNG

Document Version: 1.1

Document Date: 2023-07-20

Prepared by:
atsec information security corporation
9130 Jollyville Road, Suite 260
Austin, TX 78759
www.atsec.com

Table of Contents

1 Description

The Samsung TRNG is a physical (P) entropy source based on Meta-RO (metastable ring oscillator). The entropy source version is hard macro: sf_crypt_samsung_trng_ln08lpp_306000_v2.00e and soft macro: sf_crypt_samsung_trng_system_sss_ln08lpp_v8.20e.

Table 1 provides details of the Operational Environment of the entropy source.

Model	Processor
S4LV006 S01	ARM SC000

Table 1: Operational Environment

2 Security Boundary

The Security Boundary of the entropy source is depicted in Figure 1:

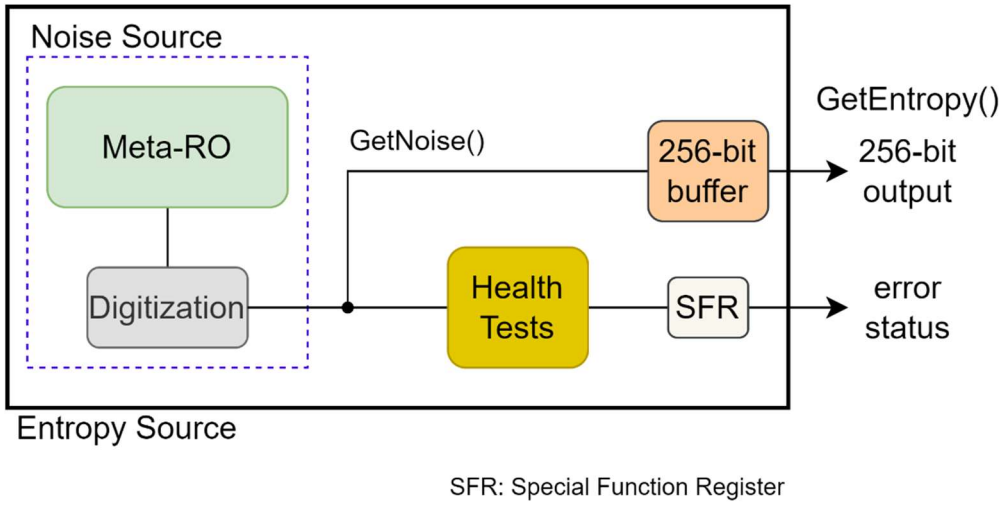

Figure 1: Security Boundary

The noise source includes the Ring Oscillator and digitization circuitry. Health tests are applied to the output of the digitization circuitry and an error status is returned.

3 Operating Conditions

The entropy source operating conditions are provided in Table 2:

Parameter	Value
Operating Temperature Range	-25°C to 105°C
Operating Voltage Range	0.75 V ±10%

Table 2: Operating Conditions

4 Configuration Settings

The customer does not have the ability to modify the entropy source configuration settings.

5 Physical Security Mechanisms

The entropy source resides within the Elan Controller chip, which is a single-chip cryptographic module enclosed in an opaque package. The chip contains other hardware and firmware components besides the entropy source. The packaging is of type FCPBGA with solder ball, production grade. This package cannot be removed or penetrated without causing serious damage to the chip.

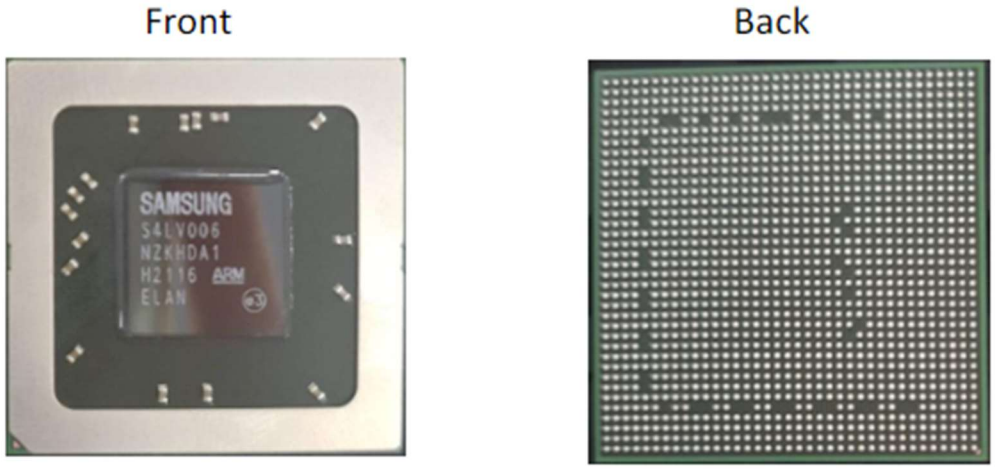

Figure 2: Chip front and back views

6 Conceptual Interfaces

There are two conceptual interfaces as shown in Figure 1:

a) GetNoise() which receives entropy and fills a 256-bit buffer

b) GetEntropy() which receives entropy from the 256-bit buffer. The entropy source can provide outputs of one single bit, or 256 concatenated samples in an output of 256 bits.

7 Min-Entropy Rate

The entropy source provides min-entropy rate of 0.5 bits per one-bit sample. The entropy source does not implement a conditioning function.

8 Health Tests

The entropy source implements both the approved Repetition Count Test (RCT) and Adaptive Proportion Test (APT).

The startup health tests are executed automatically after a reset or power-up. During startup, the health test unit collects 1024 samples of raw data and performs RCT and APT on this data. The collected data samples are discarded and not used for random number generation.

The continuous tests implement both the RCT and APT.

The on-demand health tests are activated by a request of the user or caller by setting the flag TRNG_STARTUP_CTRL.STARTUP_HTPASS to 1'b1. This triggers the execution of the startup health tests. The samples for those tests are discarded upon completion.

8.1 Repetition Count Test (RCT)

The entropy source implements the RCT as specified in SP 800-90B.

To comply with the recommendation in IG D.K [2], the RCT uses $\alpha = 2^{-40}$, which lies within the required range of $2^{-20} \leq \alpha \leq 2^{-40}$.

The cut-off value is given by the equation in Section 4.4.1 in SP 800-90B:

$$C = 1 + \left\lceil \frac{-\log_2 \alpha}{H} \right\rceil = 81$$

where,

$$\alpha = 2^{-4} \ ;$$

$$H = 0.5$$

8.2 Adaptive Proportion Test (APT)

The entropy source implements the APT as specified in SP 800-90B. The APT is computed over a window size of 1024 samples. The cut-off value is defined as $C = 824$ per the computation of the inverse cumulative binomial distribution and significance level $\alpha = 2^{-40}$ (Section 4.4.2 in SP 800-90B).

8.3 Status and Error Codes

The health test unit provides the following status codes.

Flag	Value	Description
TRNG_TEST_DONE.HTDONE	1'b0	Startup health test not yet completed.
TRNG_TEST_DONE.HTDONE	1'b1	Startup health test completed.
TRNG_TEST_STAT.HTERR	1'b0	No failure found in health tests.
TRNG_TEST_STAT.HTERR	1'b1	Failure found in health tests.

Table 3: Status and Error Codes

9 Maintenance

There are no maintenance requirements.

10 Required Testing

In order to test the entropy source, raw data samples must be collected when the entropy source is in test mode, in which case the health tests are disabled so that the noise data can be collected as is from the GetNoise() interface, with or without failures. This test mode is not available in the user mode of the entropy source.

Raw noise data samples consisting of at least 1,000,000 bits must be collected from the operational environment at is normal operating conditions and processed by the SP 800-90B

entropy tool that is provided by NIST. The expected min-entropy rate must approach the one in Section 7.

Restart data must be collected at normal operating conditions when the entropy source is in test mode via the GetNoise() interface following the restart procedure specified in SP 800-90B. (i.e. 1,000 samples from 1,000 restarts each). The restart data must be processed by the SP 800-90B entropy tool. The minimum of the row-wise and column-wise entropy rate must be more than half that of the raw noise entropy rate.

11 Vendor Permissions and Relationship

The ESV certificate is “Reuse restricted to vendor”. Someone other than the vendor can only use the certificate with written and signed permission from the vendor’s point of contact (as indicated on the ESV certificate).