SAMSUNG

SP 800-90B Non-Proprietary Public Use Document

[Samsung Elan TRNG]
Document Version 1.0

Hard macro Version:
sf_crypt_samsung_trng_ln08lpp_306000_v2.00e
Soft macro Version:
sf_crypt_samsung_trng_system_sss_ln08lpp_v8.20e
Tested Platform:
S4LV006X02

Samsung Electronics Co., Ltd.
1-1 Samsungjeonja-ro
Hwaseong-si Gyeonggi-do 18448
KOREA

January 19, 2023

Revision History

Version	Change
1.0	Initial Draft

Table of Contents

Description 4
Security Boundary 4
Operating Conditions 4
Configuration Settings 5
Physical Security Mechanisms 5
Conceptual Interfaces 5
Min-Entropy Rate 5
Health Tests 5
Maintenance 6
Required Testing 6

Description

Samsung Elan TRNG *(hereinafter referred to as Samsung TRNG)* is an entropy source compliant to the NIST SP 800-90A/B and FIPS 140-3 standard, designed and validated by Samsung (Foundry). Samsung TRNG is a physical entropy source based on Ring oscillators.

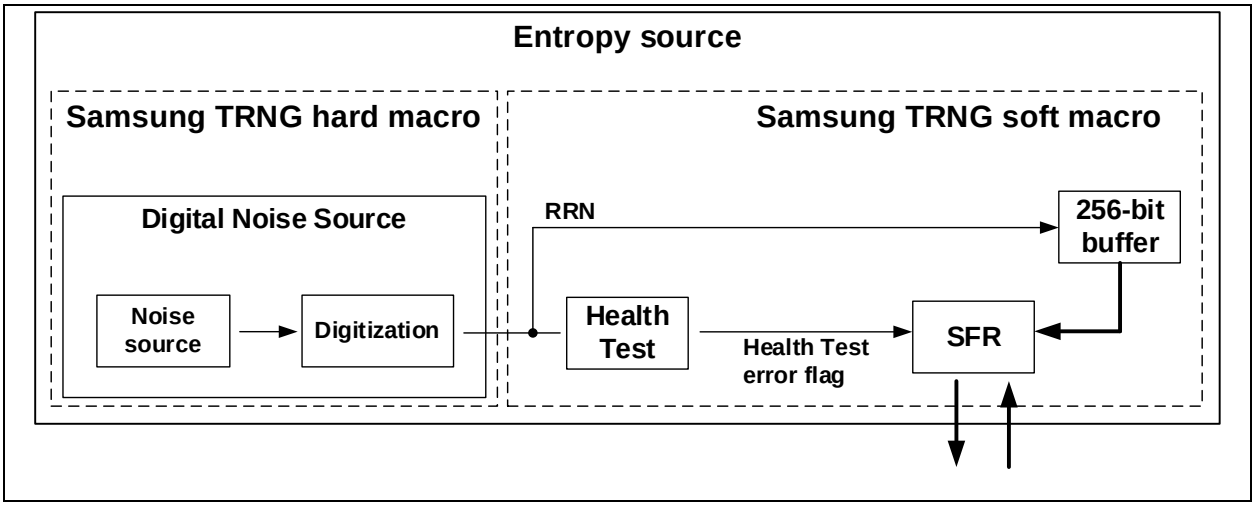
Samsung TRNG is composed of the TRNG hard macro and the TRNG soft macro. The TRNG hard macro implements digital noise source and the TRNG soft macro includes the health test, a 256-bit buffer, and an SFR (Special Function Register). The main function of the implemented entropy source is to generate bits of raw random numbers (RRN) with entropy.

Detailed component version used for this certification is listed as following:

- Hard macro Version: sf_crypt_samsung_trng_ln08lpp_306000_v2.00e
- Soft macro Version: sf_crypt_samsung_trng_system_sss_ln08lpp_v8.20e
- Tested Platform: S4LV006X02

Security Boundary

The security boundary of Samsung TRNG, the entropy source, contains Samsung TRNG hard-macro as a digital noise source and health tests included in Samsung TRNG soft-macro, and no conditioning component is employed. The entire entropy source is implemented in a single chip.



Operating Conditions

Samsung TRNG supports stable entropy extraction in the following operating conditions:

- Voltage 0.75V ± 10 %
- Temperature -25℃ ~ 105℃

Configuration Settings

The implemented TRNG soft-macro will handle other details based on given configuration settings from user.

- The frequency of the entropy source is automatically configured after the reset and cannot be changed by the user
- The health tests are enabled in a default configuration and cannot be changed by the user
- The cutoff values for the health test are configured by default and cannot be changed by the user

Physical Security Mechanisms

Samsung TRNG is embedded in the single-chip embodiment which encases in opaque package within the visible spectrum. A strong removal resistant and penetration resistant IC packaging technique is applied to the single-chip to prevent and detect the physical access.

Conceptual Interfaces

The GetEntropy interface is implemented by the GenerateRandomNumber function in the cryptographic module FW which controls the Samsung TRNG to provide 512 bits of entropy input and 256 bits of nonce to construct a seed for a DRBG.

The GetNoise interface has been used for ESV purpose only. There is no implementation to use the raw data of the noise source directly in the cryptographic module FW.

The HealthTest interface is implemented to monitor the SFR at every calling of GenerateRandomNumber function in the cryptographic module FW whether there is a health tests failure or not.

Min-Entropy Rate

Samsung TRNG generates 1 bit per sample, which is credited with a min-entropy of H=0.5 bits/ bit.

Health Tests

The health test, implemented in Samsung TRNG soft-macro, includes start-up, continuous, and on-demand tests.

The health test error flag is raised when the bits of RRN do not meet the threshold in the implemented health test (i.e. an error is detected). Bits of RRN are not in use when the health test error flag is raised. When the health test error is detected, the error counter is incremented and the start-up health test is activated. System reset is requested to the entropy source when 3 health test errors occur in a row.

Maintenance

For Samsung TRNG, there is no special maintenance required to guarantee its min-entropy rate or performance.

Required Testing

The entropy source does not provide an operator-accessible mechanism for outputting raw samples. No testing other than the implemented health tests is required for obtaining assurance that the entropy source is operating correctly.