SAMSUNG

SP 800-90B Non-Proprietary Public Use Document

[Samsung TRNG]
Document Version
1.01

Hard macro Version:
sf_crypt_samsung_trng_ln05lpe_v2.10
Soft macro Version:
sf_crypt_samsung_trng_system_sss_v8.63

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

May 18, 2023

Revision History

Version	Change
1.00	Initial Draft
1.01	Updated

Table of Contents

Description

Samsung TRNG is NIST SP 800-90B and FIPS 140-3 standard compliant entropy source, designed and validated by Samsung (Foundry). Samsung TRNG is categorized as P, the physical entropy source and claims Non-IID track for the validation.

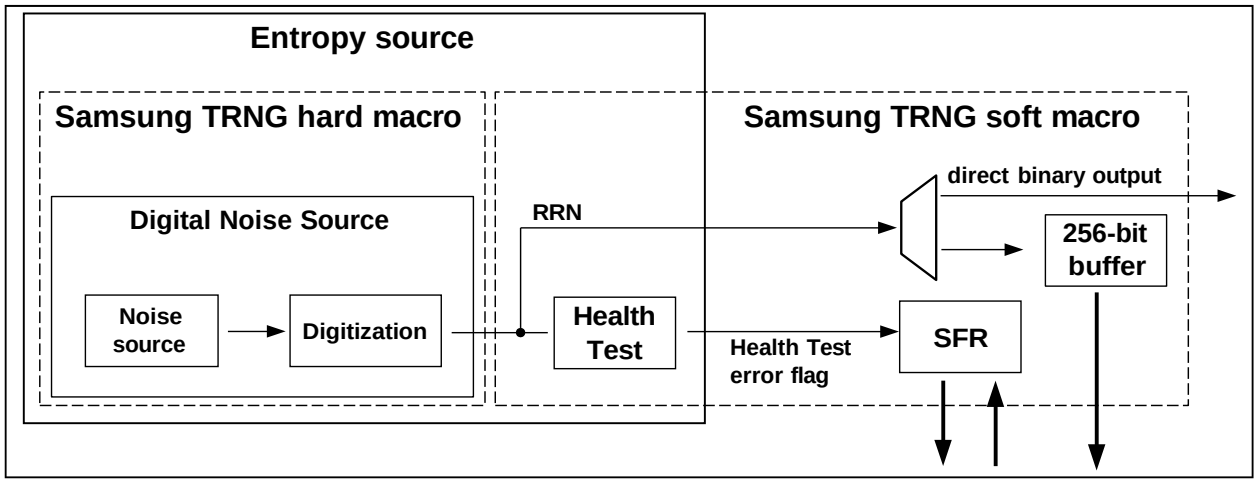
Samsung TRNG is composed of the TRNG hard macro and the TRNG soft macro. TRNG hard macro implements digital noise source and TRNG soft macro that includes the health test, 256-bit buffer, and SFR. The main function of the implemented entropy source is to generate bits of raw random numbers (RRN) with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

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

- Hard macro: sf_crypt_samsung_trng_ln05lpe_4007000_v2.10
- Soft macro: sf_crypt_samsung_trng_system_sss_v8.63
- Tested Platform: S4LY011A01

Security Boundary

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. 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

Implemented FW to control TRNG soft-macro is automatically handle the configuration settings for entropy source after the power up or after the reset events. The end user is not able to change the configuration settings. The entropy source is ready after the automated startup health testing.

Physical Security Mechanisms

Samsung TRNG is embedded in the single-chip embodiment which encases in opaque package within the visible spectrum. And 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 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 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 healthtests failure or not.

Min-Entropy Rate

The claimed $\boldsymbol{H}_{\text{submitter}}$ is 0.5 bits of min-entropy per bits.
Samsung TRNG generates 1 bit per sample and the confirmed min-entropy per bit $H = 0.5$ refers to the initial entropy estimation and confirmation by restart testing.
The GetEntropy request receives 768 (512 + 256) bits of RRN (raw random number) from Samsung TRNG, which corresponds to 768*0.5 = 384 of entropy bits per request.

Health Tests

The approved health tests (the Repetition Count test and the Adaptive Proportion test) were implemented in Samsung TRNG soft-macro to proceed with the start-up, the continuous and the on-demand health tests on random output (bits of RRN) of the entropy source. The start-up health test is automatically activated on power-on or reset events, and bits of RRN are not available until the successful completion of start-up health test. The continuous health test is constantly monitoring bits of RRN.
The on-demand health test can be called any time (either the health test error is detected or not). When the on-demand health test is called, the bits of RRN are not available until the successful completion.
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 health test is restarted. 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

Testing is not required given the entropy source can only be used by Samsung. During original validation, Samsung collected Raw noise data (bits of RRN) from 10 randomly selected chips and under the product corner voltage/temperature conditions (sequential 5Mbits for $H_{original}$ estimation and 1024*1024bits to construct restart data). Statistical testing by SP800-90B tool confirms the initial entropy of 0.5 bits of min-entropy per bit. The pre-collected raw noise data is available for the end user on request.
The end user can refer to the health test error report (see the Health Tests part) if during operation any errors were detected.

Vendor Permissions and Relationship

Samsung TRNG will be embedded on Samsung Products. Samsung plans to restrict the use of this entropy source to Samsung only.