SP 800-90B Non-Proprietary Public Use Document

Infineon Memory Solutions TRNG

Document Version 1.1

Hardware version:
2A190F0390A1 /A2
2A180F0390A1 /A2

Firmware Version:
9.10.02.02

Cypress Semiconductor – An Infineon Technologies Company
198 Champion Court,
San Jose, California,
U.S.A. 95134

July 19, 2024

Revision History

Version	Change
0.1	Initial Draft
0.2	Updated based on entropy assessment
0.3	Updated with review feedback
1.0	Updated for Final HW version
1.1	Updated based on NIST feedback.

Table of Contents

Description 4

Security Boundary 4

Operating Conditions 5

Configuration Settings 5

Physical Security Mechanisms 5

Conceptual Interfaces 5

Min-Entropy Rate 6

Health Tests 6

Maintenance 6

Required Testing 6

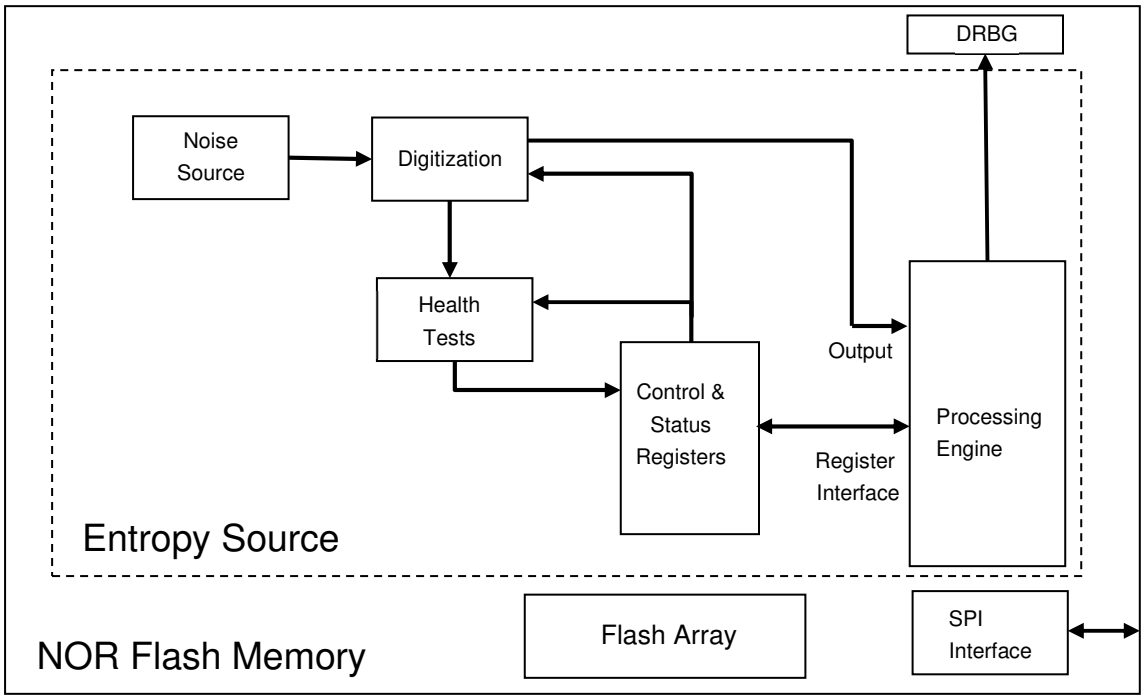
Description

The Infineon Memory Solutions TRNG is a physical entropy source, complaint to SP800-90B with Hardware versions: 2A190F0390A1 /A2, 2A180F0390A1 /A2 and Firmware Version: 9.10.02.02. It makes no IID claims. It was tested on PCB: CYPESS-16-P-271-REV1.3, Device Name: Semper Secure NOR Flash, Part Number: S35Hx256Txxxx, S35Hx128Txxxx.

Security Boundary

The security boundary is depicted in the figure below and includes the noise source, digitization, health tests and the control and status registers. The noise source consists of 6 ring oscillators. The digitization step samples the noise source outputs and computes an XOR of the samples to provide the output. The output of the Entropy Source is accumulated by the processing engine and provided to the DRBG. The Entropy Source control and status registers can only be accessed by the internal processing engine for configuration and monitoring.

Direct access to the raw data is only available through the processing engine in test units and is not available in production units.



Operating Conditions

The Entropy Source has been validated for the following operating conditions and will produce the assessed entropy for the entire range of values in the table below. The identified worst case condition is high voltage, low temperature, and fast process. The entropy data files were collected for this condition.

Parameter	Value	Description
Temperature	-40C to 125 C	Entropy Source was tested for -40C, 25C, and 125C
Voltage	Range 1: 2.7V to 3.6V Range 2: 1.7 to 2 V	Range1 is for 3.3V devices and Range2 is for 1.8V devices
Process	Slow, Typical and Fast	Entropy Source was tested for all the process corners

Configuration Settings

The applicable configuration settings for the Entropy Source are listed below.

Parameter	Value
Initial Delay	256 (First 256 samples are dropped)
Sampling rate	156 KHz
Conditioning component	off
RCT cutoff	37
APT cutoff	618

Physical Security Mechanisms

The Entropy Source is embedded in the NOR Flash Memory chip which is packaged in either a BGA24 or SOIC package designed to meet industrial/automotive grade 3 and above for temperature, power, and reliability.

The Entropy Source is only accessible to the processing engine. There is no other option for a direct access to the entropy source.

Conceptual Interfaces

The Entropy Source outputs 32 bits of data at a time, that can be requested and then read by the processing engine.

Min-Entropy Rate

Min-entropy rate is the same as H_submitter and is equal to 0.7218 per bit. For every request the entropy source outputs 32 bits and is unconditioned.

Health Tests

The Entropy Source performs the required health tests of section 4.4 of SP 800-90B namely:

- RCT
- APT

These tests are run at startup and continuously and on demand. On demand tests are run via a reset which triggers the startup health tests. A failure of the health tests causes an error condition, and no data is output. If the health tests start passing after new data is acquired, the data output is re-enabled.

Maintenance

There are no maintenance requirements for the Entropy Source.

Required Testing

The Entropy Source compliance to SP 800-90B was validated using the testing interface (not available to production units, as mentioned in Security Boundary Section) and the SP 800-90B entropy assessment tool.

To validate the theoretical assumptions about the noise source, data was collected from the device in its designated operational range; the following tests were performed according to Section 3 of SP 800-90B:

• Raw Noise samples comprising of at least 1,000,000 bits were collected via the raw noise source interface and processed by the NIST SP800-90B tool. The entropy rate was above the min-entropy rate defined in Section 'Min-Entropy Rate'.

• Restart data was collected in accordance with the procedure specified in SP800-90B (in the format of 1,000 samples from 1,000 restarts) through the raw noise source interface and processed by the NIST SP800-90B tool. The restart sanity tests all passed and the minimum of the row-wise and column-wise entropy rate was above the min-entropy rate defined in Section 'Min-Entropy Rate'.

No further testing is required on the Entropy Source.