SP 800-90B Non-Proprietary Public Use Document

secr_trngab_5nm (5ff)

Document Version 1.1

Advanced Products Division
Broadcom Inc.
270 Innovation Dr.
San Jose CA 95134

April 14, 2023

Revision History

Version	Change
1.0	First draft for secr_trngab_5nm (5ff)
1.1	Updated Required Testing section

Table of Contents

Description

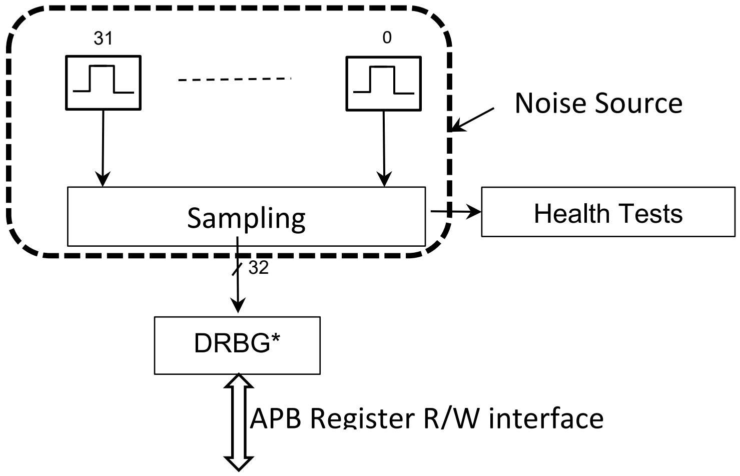
The Broadcom entropy source P/N: secr_trngab_5nm (5ff) is a hardware implemented, physical (ENT (P)) entropy source consisting of 32 individual ring oscillators concatenated to produce 32-bit raw data output, which is provided with no conditioning. The entropy source was tested by collecting data from multiple process, voltage, and temperature (PVT) operational conditions from a test card.

The test card specifics are:

- PCBA: Squid MCM
- ASIC: Squid
- FW: Arctic v12

Security Boundary

The entropy source is depicted in Figure 1, showing a high-level design of the basic layout of the module. Output from sampling the ring oscillators is provided to SP 800-90B compliant health tests and an SP 800-90A compliant DRBG.



**SP800-90A compliant DRBG with derivation function*

Figure 1. Entropy Source

The security boundary is depicted in Figure 2, showing the data control of the entropy source. Access and control of the entropy source and raw data is restricted to the on-chip support processor running authenticated code. Direct access to the entropy source is not possible from any other interface. The external entropy source data interface shown is used for raw data collection, for use in testing, and is not accessible in non-test units.

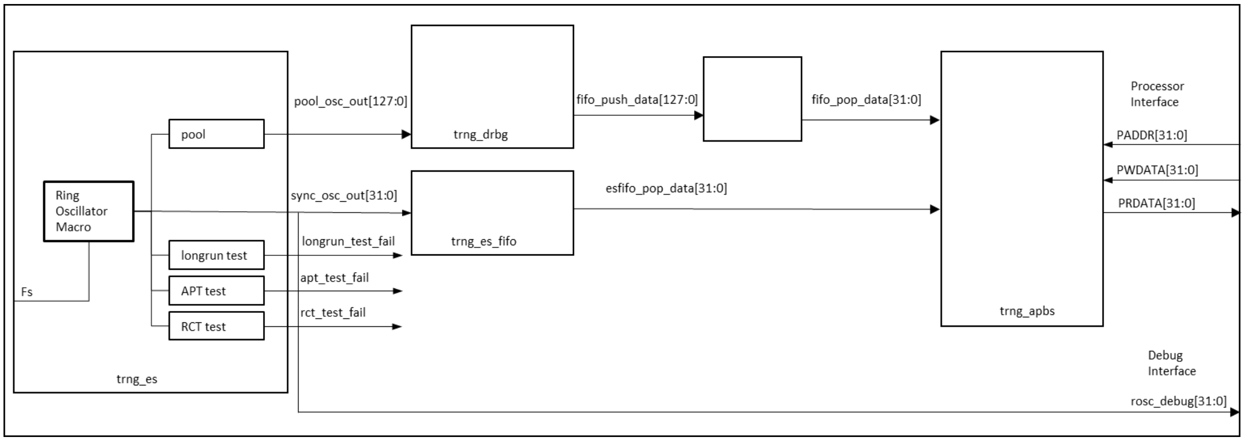


Figure 2. Ring Oscillator Data Flow Diagram

Operating Conditions

The entropy source was tested under several different PVT corners. Table 1 contains the operational conditions in which the entropy source will operate in and maintain entropy production at the assessed value.

Table 1. Entropy-Relevant Parameters

Parameter	Value	Description
Temperature	Min: -40C; Typical: 25C; Max: 125C	Operating Temperature Range
Voltage	Min: 0.67V; Typical: 0.76V; Max: 0.83V	Operating Voltage Range
Sampling Frequency	5MHz	Ring Oscillator Sampling Frequency

Configuration Settings

The following Configuration settings are required for the correct operation of the Entropy Source

Table 2. Entropy-Relevant Parameters

Parameter	Value	Description
Sampling Frequency (Fs)	5MHz	Ring Oscillator Sampling Frequency (Fs) Derived from clock Input (clk) using divisor input rosc_sampling_rate[15:0]
Min Entropy	4	Set by APB min_entropy[15:0] register. Sets Cutoff value for Health tests

Physical Security Mechanisms

The Entropy source is embedded in the ASIC that is covered by a Heat Sink. The Entropy source is only accessible by the on-chip support processor running authenticated code. Direct access to the entropy source is not possible from any other interface.

Conceptual Interfaces

In Operational Mode the Entropy source generates 32bit of raw Entropy data every sampling clock and provides 128bits of pooled data to the SP 800-90A complaint DRBG.

Min-Entropy Rate

The TRNG provides 4 bits of entropy per 32-bit sample output. These samples are provided unconditioned to a SP 800-90A complaint DRBG.

Health Tests

The TRNG performs all required health tests of Section 4.4 of SP 800-90B. This includes startup, continuous, and on-demand health tests.

Health tests are set to flag errors with a false positive probability of 2^{-40}. Health test failures will be flagged by the source and the module will immediately stop producing entropy data and enter an error state. The device requires reset commands to leave the error state.

Maintenance

There are no specific maintenance requirements for the entropy source.

Required Testing

The TRNG entropy source was tested in accordance with all SP 800-90B requirements. Raw and restart noise data was collected through a debug interface not available outside of test units. Test data was collected following the requirements of Section 3 of SP 800-90B. All tested data was evaluated at a higher entropy than the defined entropy of the assessment, and all restart sanity checks were passed.

Built-in Health Tests described in the Health Tests section constantly check the validity of the noise source. Therefore, no further testing is required.