SP 800-90B Non-Proprietary Public Use Document

Cisco TRNG Core Entropy Source
Document Version 0.4

Firmware Version: TAm2.0 v1
Hardware Version: Microsemi SmartFusion2 SOC FPGA

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
September 30, 2022

Revision History

Version	Change
0.1	Initial draft
0.2	Updates to versions, entropy source name, page numbers, min-entropy and final edits.
0.3	Updated OE information and changed entropy source name
0.4	Minor updates to sections Security Boundary (to match EAR) Health Tests (error handling) and Required Testing (reduced decimal value)

Table of Contents

Description 4

Security Boundary 4

Operating Conditions 4

Configuration Settings 5

Physical Security Mechanisms 5

Conceptual Interfaces 6

Min-Entropy Rate 6

Health Tests 6

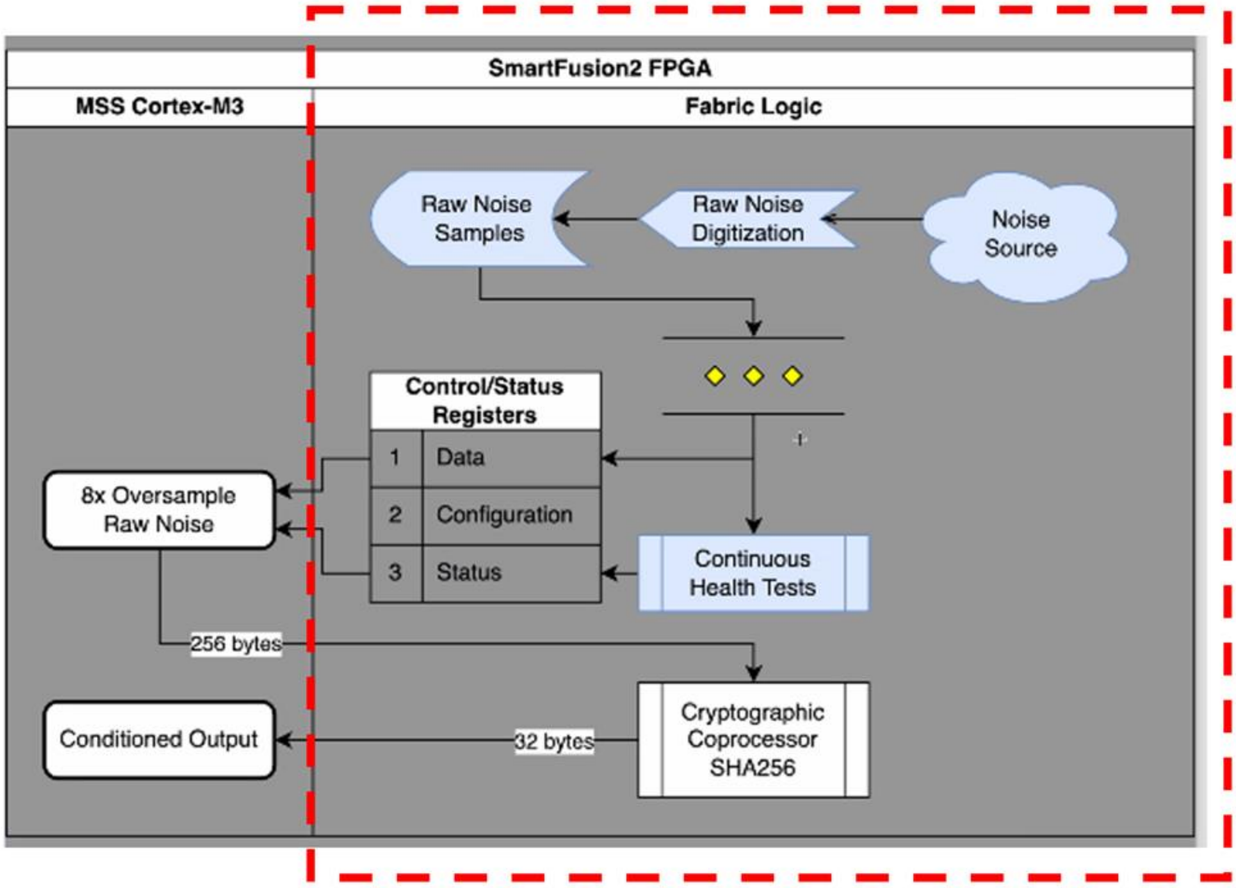
Maintenance 7

Required Testing 7

Description

The Cisco TRNG Core (CTC) Entropy Source is a physical entropy source. It makes no IID claim and thus meets all the requirements for non-IID compliance.

Security Boundary



The security boundary of the CTC entropy source surrounds the Fabric Logic as seen in the figure above. This boundary includes the entropy source, the digitization, the health tests, and the conditioning function.

The MSS Cortex-M3 contains APIs that can be used to request entropy to seed the DRBG. The TRAND family of APIs can be used directly to seed an external SP 800-90A compliant DRBG because the TRAND API returns the seeding material directly from the SHA2-256 conditioning function.

Operating Conditions

Table 1 Operating Conditions

Parameter	Value
Operating temperature	32 to 104°F (0 to 40°C)
Storage temperature	-40 to 150°F (-40 to 70°C)

Parameter	Value
Voltage – Direct Current (DC) core supply	1.14 to 1.26 Volts
Voltage – Power supply for charge pumps	3.15 to 3.45 Volts

Configuration Settings

Table 2 Configuration Settings

Parameter	Value
$H_{submitter}$	0.25
n_{in}	2048
n_{out}	256
nw	256
h_{in}	512
h_{out}	256
APT cutoff value	921
RCT cutoff value	97
Noise source independence claim	Non-IID
Length of conditioning chaining	1
Vetted conditioner	SHA2-256

Physical Security Mechanisms

The CTC entropy source relies on the built-in physical security measures provided by the SmartFusion2 (SF2) device. The SF2 incorporates differential power analysis (DPA) countermeasures to protect the bitstream keys from discovery using side-channel analysis. It provides tamper detection and tamper response (including zeroization).

The SF2 device has a number of tamper detection flags, described in the following table.

Flag	Generated by	Description
JTAG_ACTIVE	Hardware	This flag is asserted when the device is programmed using JTAG. It is also asserted whenever the JTAG TAP controller enters the Run-Test-Idle state.
LOCK_TAMPER_DETECT	Hardware	A parity error has been detected in the security segment where access control configuration bits (Lock bits) are stored.
MESH_SHORT_ERROR	Hardware	An error has been detected in the metal mesh. This allows protection against invasive attacks, like cutting and probing of traces using focused ion beam (FIB) technology with an active metal mesh on one of the higher metal layers.
CLK_ERROR	Hardware	A clock monitor that compares the frequency of the two on-chip system controller clocks (1 MHz and 50/25 MHz). If the discrepancy over a number of clock cycles is too great, this flag is set (-60, -90 and -150 devices only).
DETECT_CATEGORY[3:0] DETECT_ATTEMPT DETECT_FAIL	Firmware	Ability to detect the programming port activity. DETECT_CATEGORY: Indicates the category of detectable crypto activity type. DETECT_ATTEMPT: Indicates that an activity type in DETECT_CATEGORY has been attempted. DETECT_FAIL: Indicates that an activity type in DETECT_CATEGORY has failed.
DIGEST_ERROR	Firmware	A user-initiated digest request has detected an error.
POWERUP_DIGEST_ERROR	Firmware	An error has been detected during the power-up digest check.
SC_ ROM_DIGEST_ERROR	Firmware	An error has been detected in the system controller metal mask ROM digest.
TAMPER_CHANGE_STROBE	Firmware	Active high strobe pulse to indicate state changes of any outputs on the Tamper Macro.

Conceptual Interfaces

GetEntropy is implemented by the TRAND instructions in the TAM FW. The DRBG specifies how much entropy it needs from the CTC entropy source, and the entropy source returns the requested amount.

Min-Entropy Rate

$H_{submitter}$ is claimed to be a very conservative 0.25 bits of entropy per bit of raw noise data. The CTC entropy source with vetted conditioning returns 256 bits of data which contain 256 bits of entropy, or full entropy

Health Tests

The CTC entropy source performs three health tests:

- Repetition Count Test (RCT)
- Adaptive Proportion Test (APT)
- Dead Ring Test (DRT)

These three tests are run at start up and then are run continuously during the operation of the entropy source. They are run on demand by power-cycling the CTC SF2 FPGA. The health tests are implemented in the fabric logic of the SF2 and are performed on the raw data before it's sent to the conditioning function.

The RCT and APT tests comply with the requirements in section 4.4 of SP 800-90B. The DRT is a vendor-defined health test that was designed to identify a failure mode specific to the CTC entropy source.

The DRT checks that the generated clock sample captured by the tapped delay line contains a rising edge of the clock. The noise source will not output any random bit if it cannot locate a rising clock edge in a sample, so the entropy generation throughput will be reduced, possibly to 0 bits per second. Such an event could indicate the ring oscillator performance has been altered to the point that the clock is either too fast or too slow for the digitization circuit to capture a suitable representation of the waveform. Given the engineering margins added to the design of the circuit, neither case is considered likely. Therefore, this continuous health test is referred to as the Dead Ring Test because it is meant to detect a ring oscillator that has suffered a catastrophic failure and is no longer toggling. The DRT error flag is set to indicate that no random bit has been returned. The DRT cutoff threshold value (which corresponds to the number of consecutive invalid samples allowed before the health test fails) is typically set to 1.

If any health test fails, an error flag is set and passed to the consuming application.

Maintenance

There are no maintenance actions required by the CTC entropy source.

Required Testing

The NIST non-IID statistical tests for raw data were run on the 1,000,000 samples of raw data collected by the test harness. The tests calculated a min-entropy of 0.76 bits of entropy per 1-bit symbol. Thus:

$H_{original}$ = 0.76 bits of entropy per bit of data
$H_I = \min(H_{submitter}, H_{original}) = 0.25$

The results support the claim that $H_{submitter}$ is a very conservative estimate of the entropy produced by the CTC entropy source. As expected, the measured min-entropy was considerably higher than $H_{submitter}$.

The NIST non-IID tests were also run on the restart data that was collected as required by SP 800-90B (1000 bits collected over 1000 restarts). The tests calculated the following:

H_r: 0.768694
H_c: 0.794638

```
H_I: 0.250000

Validation Test Passed...
```

The testing passed, and the entropy from both the columns and the rows were very close to the min-entropy calculations from the raw data. The minimum of H_r and H_c was almost identical to the min-entropy calculated by the raw noise tests, thus far exceeding the requirement that the minimum be more than half of the min-entropy of the raw data.