SP 800-90B Non-Proprietary Public Use Document

TRNG Entropy Source

Document Version 0.1

Hardware Version: 1.0

Google, LLC

1600 Amphitheatre Parkway
Mountain View, CA 94043

March 29, 2024

**Revision History**

|  |  |
| --- | --- |
| Version | Change |
| 0.1 | Initial Draft |
|  |  |

Table of Contents

[Description 4](#_Toc150937624)

[Security Boundary 5](#_Toc150937625)

[Operating Conditions 6](#_Toc150937626)

[Configuration Settings 7](#_Toc150937627)

[Physical Security Mechanisms 7](#_Toc150937628)

[Conceptual Interfaces 8](#_Toc150937629)

[Min-Entropy Rate 8](#_Toc150937630)

[Health Tests 8](#_Toc150937631)

[Maintenance 9](#_Toc150937632)

[There are no maintenance requirements. 9](#_Toc150937633)

[Required Testing 9](#_Toc150937634)

# Description

The Google entropy source P/N: TRNG Entropy Source, version 1.0, is a hardware-based, physical (ENT (P)) entropy source. It is a non-IID entropy source. It does not require firmware or software to operate.

This assessment was conducted on various listed device in Table 1.

Table 1: Evaluated Entropy Source Specification

|  |  |  |  |
| --- | --- | --- | --- |
| Part Number | Stepping | Entropy Category | Entropy Estimation Track |
| Intel® IPU ES2000CC | B | Physical | Non-IID |

# Security Boundary

The TRNG Entropy Source consists of a noise source, conditioning component, and continuous health testing as shown in Figure 1. The noise source consists of bit generators which are based on a set of two ring oscillators per generator. The Entropy Source permits reads of the raw (unconditioned) output of the noise source only when in test mode. The vetted conditioning component is a AES-128 block\_cipher\_df (CAVP Certificate #A1714). The conditioned output is also available for input into a hardware-based DRBG (not shown) or may be read directly via registers. Continuous health tests are run on the raw noise data.

The security boundary is depicted in Figure 1 as well.

Figure 1: Google TRNG Entropy Source Block Diagram



The noise source itself consists of 6 bit-generators which are based on ring oscillators. Each bit generator comprises two ring oscillators and a digitizer. There is a single bit collector in the noise source.

Figure 2: Noise Source Block Diagram



# Operating Conditions

Table 2: Operating Conditions

|  |  |  |  |
| --- | --- | --- | --- |
| Part Number | Temperature | Voltage | System Activity |
| Intel® IPU ES2000CC | Min: 0C; Typical: 30C; Max: 105C | Range: 0.7V to 0.82V\* | Range: 0 to 100% |

\* The TRNG is on a fixed voltage supply per individual SOC, externally regulated and internally specified. So, voltage cannot be varied. During manufacturing, the test program searches for the minimum voltage (within reliability guardrails) necessary for that device to operate – this accounts for temperature and process corner. That minimum voltage is fused into the part. Testing occurred at this specific per-SOC voltage. For the aggregate of all SOCs, the voltage may range from 0.7V to 0.82V.

# Configuration Settings

The entropy source does not require configuration of entropy-relevant parameters. Settings such as sample interval, startup delay, health test enable, etc. are all statically configured at build time and cannot be changed in the hardware.

There is the ability to adjust the ring length in the clock ring in each bit generator. The MAX\_REJECTS field dictates the maximum number of consecutive bit rejections that must occur within a single bit generator before the ring feedback control system dynamically adjusted the frequency of the affected bit generator. There is usually no need to adjust this register. It is primarily for test purposes.

# Physical Security Mechanisms

The TRNG Entropy Source is embedded in the system on chip (SOCs) listed above. The SoCs are single-chip embodiments of production-grade components that include standard passivation. The SOCs are only usable when soldered to printed circuit board and are typically packaged using a ball grid array (BGA) package. The entropy source operates within the physical protections of the associated device package. This is capable of meeting FIPS 140-3 Level 1 or 2 requirements without additional security measures. Any required additional security measures such as tamper seals, etc. exist outside the package at the enclosure level. Any module integrating an SOC with the Intel entropy source included within their boundary must fulfill the physical security requirements appropriate to the targeted module type and security level.

The entropy source is only accessible by the internal processor which is typically running authenticated code. Direct access to the entropy source is not possible from any other interface. Zeroization of the TRNG including the entropy source occurs after reset and is available upon demand and may be triggered by internal processor within the SOC.

# Conceptual Interfaces

The Generate Noise command is issued via a control register which causes the entropy source inside the TRNG to provide a new 384-bit full-entropy seed for the DRBG available in the Conditioned Output Register. Once the GEN\_NOISE command is issued, the noise source generates a 512-bit block of noise and passes that through the conditioning component to generate 128-bits of the final seed. GEN\_NOISE repeats this operation 3 times to produce a complete 384-bit seed (output of conditioning component).

# Min-Entropy Rate

The H\_submitter is 0.989 min-entropy per bit of any contiguous 512-bit output sample.

The H\_out with the vetted conditioning component is 127.9999999999996732 based on n\_in: 512, n\_out: 128, nw: 128 and h\_in: 170. The within 512 bits that are input to the conditioner for each seed is required to be > 170/512 bits or H= 0.33.

# Health Tests

The TRNG Entropy Source performs the NIST SP800-90B required health tests on the entropy source. One round of Known Answer Test (KAT/CAST) on the conditioning component plus a full round of statistical tests on the noise source are performed as the start-up test after reset. The number of noise bits that are generated and tested as part of the start-up test is 1024-bits. All bits generated and tested during the start-up test are discarded after the test regardless of the success or failure of the test. The entropy health test block receives bits coming out of the noise source and performs continuous statistical tests on those bits.

The continuous NIST SP800-90B health tests include:

* Repetition Count Test (RCT)
* Adaptive Proportion Test (APT)

The health tests always run during mission mode of operation. Health tests can only be individually disabled at runtime when the core is in test mode. In mission mode, health tests cannot be disabled. Any transition between test and mission modes, enable all health tests.

The following parameters are used for the RCT:

|  |  |
| --- | --- |
|  Parameter | Value |
| Sample size  | 1 bit |
| Min-Entropy | H=50% |
| Cutoff value | C=41 |
| Window Size | w=1024 |
| False positive error rate | Alpha = 2-20 |

The following parameters are used for the APT:

|  |  |
| --- | --- |
| Parameter | Value |
| Sample size  | 8 bits |
| Min-Entropy | H=50% |
| Cutoff Value | C=793 |
| Window Size | w=1024 |
| False positive error rate | Alpha = 2-20 |

When a health test fails, whether it is statistical or KAT and whether during the start-up test, continuous statistical checks or on-demand testing, a non-maskable alarm raises and the core zeroizes itself. The cause of failure can be read from ALARMS register.

While the start-up test is ongoing, the core is in busy state and remains unfunctional until the start-up test is finished. If the test finishes successfully, the core is ready to be used.

If the start-up test fails, the TRNG issues an alarm and zeroizes itself. However, by default, thehardware comes out of the busy state and is ready to be used. It is the responsibility of the application software to take proper action upon failure. The software resets the core to kick-off a new round of start-up test if desired.

On-demand statistical test is possible by rebooting the core. Note that resetting, rebooting, or powering up are acceptable methods for initiating an on-demand test since the procedure results in the immediate execution of the start-up tests. Samples collected from the noise source during on demand health tests at startup time are discarded. Continuous statistical testing continues after the startup tests providing that there are no errors.

# Maintenance

# There are no maintenance requirements.

# Required Testing

The TRNG Entropy Source was tested by placing the TRNG in test mode and collecting raw noise data through the raw noise data register. The non-IID SP800-90B tests using the most recent update of the NIST 90B test implementation were run over data collected. The non-restart assessment was run as well as the restart assessment. 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 min entropy rate, all restart sanity checks passed, and both the row and column-wise entropy were nearly identical to the non-restart entropy value. No additional testing is required.