



**SP 800-90B Non-Proprietary Public Use
Document**

**Tensor G5 Google security core Entropy
Source**

Prepared for:

*Google LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043*

Prepared by:

*atsec information security corporation
4516 Seton Center Parkway, Suite 250
Austin, TX 78759*

*Document Version 1.1
Date: May 2025*

Table of Contents

1. DESCRIPTION.....	3
2. SECURITY BOUNDARY.....	3
4. CONFIGURATION SETTINGS.....	4
5. PHYSICAL SECURITY MECHANISMS.....	4
6. CONCEPTUAL INTERFACES.....	4
7. MIN-ENTROPY RATE.....	5
8. HEALTH TESTS.....	5
9. MAINTENANCE.....	5
10. USER VERIFICATION.....	5
11. VENDOR PERMISSIONS AND RELATIONSHIP.....	5

1. Description

The Tensor G5 Google security core Entropy Source is a sub-chip physical entropy source validated as conformant to to SP 800-90B (January 2018), FIPS 140-3 IG D.J (November 5, 2021), and FIPS 140-3 IG D.K (March 17, 2023). The noise generation of this entropy source is based upon “Bit Generators”, each of which consists of two Free Running Oscillators (FROs) and a sampler (D flip-flop). A simplified diagram of a Bit Generator is shown in Figure 1.

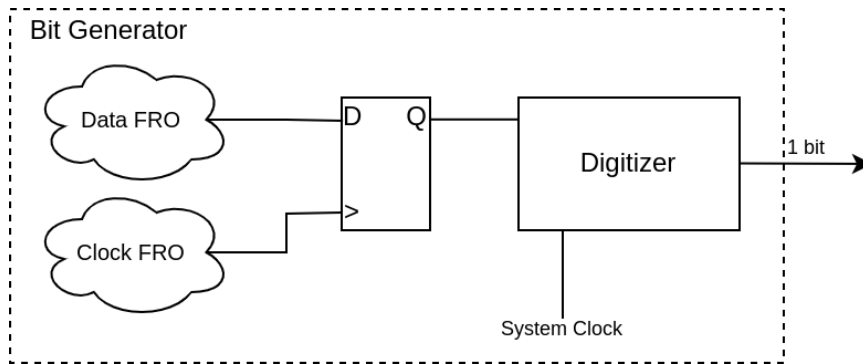


Figure 1: Simplified diagram of the Bit Generator Architecture

The output of the noise source is assumed to be non-IID. The entropy source was tested on the hardware platforms listed in Table 1.

Name	Version
Google Tensor G5	1.0

Table 1: Tested Operational Environments

2. Security Boundary

The security boundary is defined by the outer dashed line in Figure 2. The entropy source boundary contains the following components: physical noise source (eight Bit Generators and the digitization & bit collection logic), SP 800-90B health tests, a 1536-bit FIFO, a vetted Block_Cipher_df conditioning component, and a vendor-defined health test.

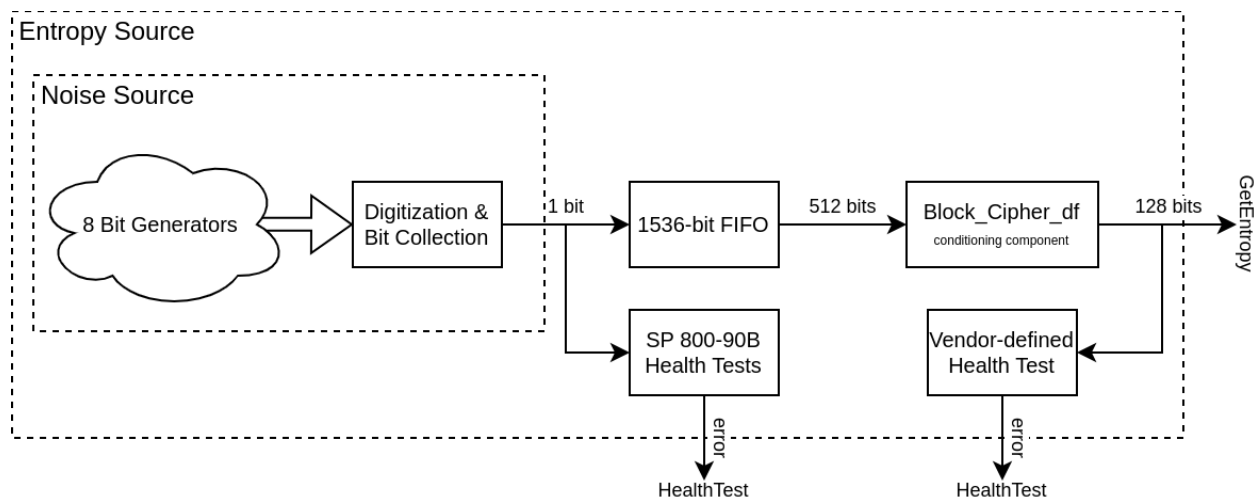


Figure 2: Block Diagram of the entropy source with the Bit Generator physical noise source

3. Operating Conditions

The entropy source is claimed to operate correctly under the inherent operating conditions of the hardware platforms:

- Temperature range: -25° C to 125° C
- Voltage range: 0.750V +/- 10%

4. Configuration Settings

The entropy source provides the following configuration settings in the SMODE register:

- NOISE_COLLECT (bit 31): enable raw noise collection in TEST mode = 0
- INDIV_HT_DISABLE (bits 23:16): disable individual health tests in TEST mode = 0
- MAX_REJECTS (bits 9:2): number of rejections before tweaking FRO = 10
- MISSION_MODE (bit 1): whether MISSION or TEST mode is enabled = 1
- NONCE (bit 0): whether nonce seeding mode is enabled = 0

These configuration settings cannot be changed by the user. Any such changes would invalidate the ESV entropy certificate.

5. Physical Security Mechanisms

The noise source is physical. The entropy source is embedded in the systems on chip (SoCs) listed in Table 1. The SoCs are single-chip embodiments of production-grade components that include a standard sealing coating. The coating is opaque within the visible spectrum.

6. Conceptual Interfaces

The entropy source provides the following interfaces:

- **GetEntropy:** by invoking the GEN_NOISE command, which will write the conditioned entropy data to the SEEDx registers.
- **GetNoise:** this interface is only accessible in TEST mode SoCs.
- **HealthTest:** health test errors are signaled through the O_alarm I/O port. More details are available in bits 0 through 5 of the ALARMS register.

7. Min-Entropy Rate

The entropy source provides 128 bits of entropy per 128-bit conditioned output block (i.e., full entropy).

8. Health Tests

The vendor implemented the approved Repetition Count Test (RCT) and Adaptive Proportion Test (APT) as defined in SP 800-90B, which are performed on the full 1-bit noise source sample. In addition, the vendor defined the conditioned RCT, a variant of the SP 800-90B RCT performed on 4-bit blocks of conditioned output.

Following the NIST SP 800-90B requirements, three sets of health tests are performed:

- **Start-up tests.** The start-up tests run the SP 800-90B health tests over 1024 consecutive samples. The data generated during the start-up tests is discarded after the tests, regardless of the result of the test. If any of the start-up tests fail, an alarm will be raised, the internal state is zeroized, and the caller is responsible to deal with the failure (e.g., by resetting the hardware).
- **Continuous tests.** The SP 800-90B and developer-defined health tests are performed continuously when samples are collected from the noise source. If any of these tests fail, an alarm will be raised to the caller, the internal state is zeroized, and the entropy source stops generating entropy.
- **On-demand tests.** The on-demand tests can be performed by rebooting the entropy source, which results in the immediate execution of the start-up tests.

9. Maintenance

There are no maintenance requirements.

10. User Verification

Raw noise data is not available on production (non-Test mode) SoCs. The user must therefore rely upon the included health tests described in Section 8 to detect any loss of entropy.

11. Vendor Permissions and Relationship

This entropy source validation is “Reuse restricted to vendor”.