SP 800-90B Non-Proprietary Public Use Document

AMD TRNG Entropy Source for RDSEED

Prepared for:

Advanced Micro Devices (AMD)
2485 Augustine Drive
Santa Clara, CA 95054

Prepared by:

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

Document Version 1.0
Date: June 2024

Table of Contents

1. Description

The AMD TRNG Entropy Source for RDSEED is a physical entropy source validated as conformant to SP 800-90B by the Entropy Source Validation Program. The noise generation of this entropy source is based upon Free Running Oscillators (FROs). 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
EPYC EIOD2.0	2.0-55cc84d4
Ryzen RIOD2.0	2.0-55cc84d4
Strix1 OPN 100-000001569	2.0-55cc84d4

Table 1: Tested Operational Environments

2. Security Boundary

The security boundary is defined by the outer dashed line in Figure 1. The entropy source boundary contains the following components: physical noise source (16 FROs and sampler), SP 800-90B and developer-defined health tests, a 128-bit FIFO, a vetted AES-256 CBC-MAC conditioning component, a 2048-bit FIFO, an external FIFO, and the microcode for RDSEED. This microcode will filter out all 32-bit blocks of zeroes obtained from the external FIFO, thereby reducing the entropy rate at the output of the entropy source. Consequently, the RDSEED microcode acts as a non-vetted conditioning component.

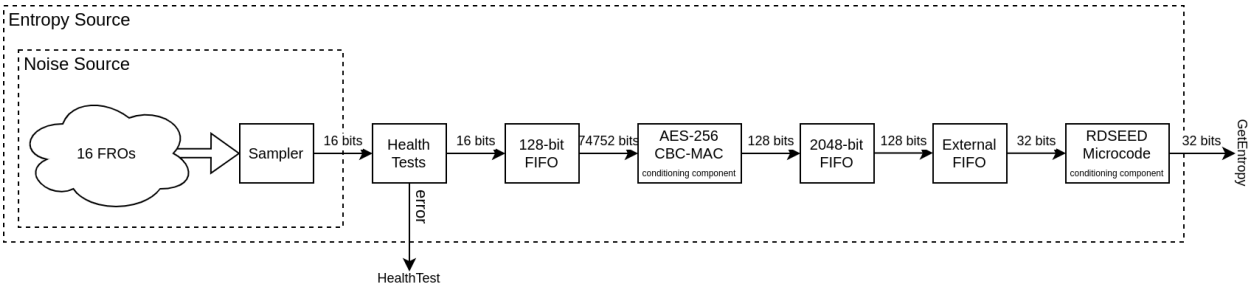

Figure 1: Block Diagram of the entropy source with the FRO physical noise source

3. Operating Conditions

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

- Temperature range: 0°C to 100°C
- Voltage range: -0.3 V to 1.3 V relative to VSS

4. Configuration Settings

There are no configurable settings for the entropy source.

5. Physical Security Mechanisms

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 calling the RDSEED instruction, which outputs the entropy in the destination register if CF=1. If CF=0, no valid entropy output is available, and any data in the destination register must not be used by the caller.
- GetNoise: this interface is only accessible on development SoCs.
- HealthTest: health test errors are signaled through bits 18 and 19 of the Trng_Control register, which respectively indicate if an SP 800-90B or developer-defined health test failed (Section 8).

7. Min-Entropy Rate

The H_submitter is 0.2373797 bits per 16-bit sample. The min-entropy rate at the output of this entropy source is 29.06 bits per 32-bit output.

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 16-bit noise source sample. In addition, the vendor defined the single-bit RCT and the two-bit APT, variants of the SP 800-90B health tests with a reduced sample size. The Trng_Control register contains the results of these health tests: bit 18 and 19 respectively indicate a failure in the SP 800-90B or developer-defined health tests.

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 and developer-defined health tests over a minimum of 4096 consecutive samples. If any of these tests fail, the sampled bits will be discarded, and the start-up tests are performed on the next 4096 samples. There is no output available from the entropy source before the successful completion of the start-up tests.
- Continuous tests. The SP 800-90B health tests and developer-defined health tests are performed continuously when samples are collected from the noise source. If any of these tests fail, all noise and entropy data is discarded, and an error is signaled to the caller.
- 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. Required Testing

To test the entropy source, noise source samples must be collected using development SoCs (used for assessment testing purposes), and a test harness that can collect outputs from the RO-OUT register. The 16-bit samples from the noise source must be reduced to 8 bits for testing purposes, due to restrictions on the SP 800-90B entropy tool that is provided by NIST.

One million consecutive samples must be collected from the operational environment at its normal operating conditions and processed using the NIST SP 800-90B entropy tool. The results must be at least as high as the H_submitter.

Restart data must be collected at normal operating conditions following the restart procedure specified in SP 800-90B (i.e., 1,000 samples from 1,000 restarts each) and processed by the NIST SP 800-90B entropy tool. The sanity test must pass, and the minimum of the row-wise and column-wise entropy rate must not be less than half of the H_submitter.

11. Vendor Permissions and Relationship

The entropy source status is indicated as "Open for reuse".