[Public]

AMD RNG ESV Public Use Document

Document Version 0.4

January 26, 2023

Advanced Micro Devices, Inc. (AMD)
2485 Augustine Dr.
Santa Clara, CA 95054
USA

Table of Contents

References

Ref.	Full Specification Name	Date
[90A]	NIST, SP 800-90A Rev. 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators	24-Jun-2015
[90B]	NIST, SP 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation	10-Jan-2018
[140]	NIST, FIPS PUB 140-3, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES	22-Mar-2019
[140IG]	NIST, Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program	7-Oct-2022

1 Description

This document provides the information required by the NIST Entropy Source Validation (ESV) program.

This assessment was conducted using data and parameters measured in the evaluated version and configurations described in Table 1. The AMD RNG design is described in Section 2.

Table 1: Evaluated Entropy Source Specification

Identifier	EPYC 7xx2 Family	EPYC 7xx3 Family	Ryzen V3xxx Family
Entropy Source Name	AMD RNG	AMD RNG	AMD RNG
Part Numbers	AMD EPYC 7xx2/7xx2P	AMD EPYC 7xx3/7xx3P	AMD Ryzen Embedded V3xxx/V3xxxI
Vendor ID	AuthenticAMD	AuthenticAMD	AuthenticAMD
CPU Family	23	25	25
Model	49	1	68
Model Name	AMD EPYC 7742 64-Core Processor	AMD EPYC 7713 64-Core Processor	AMD Ryzen Embedded V3C48 8-core Processor
Stepping	0	1	0
Entropy Category	Physical	Physical	Physical
Entropy Estimation Track (per SP 800-90B §3.1.2)	Non-IID	Non-IID	Non-IID

2 Security Boundary

The AMD RNG design (depicted in Figure 1) comprises a noise source, optional conditioning function and health testing. The noise source is based on a set of ring oscillators. The RNG subsystem permits reads of the raw (unconditioned) output of the ring oscillators or the use of the RDSEED instruction, inclusive of conditioning.

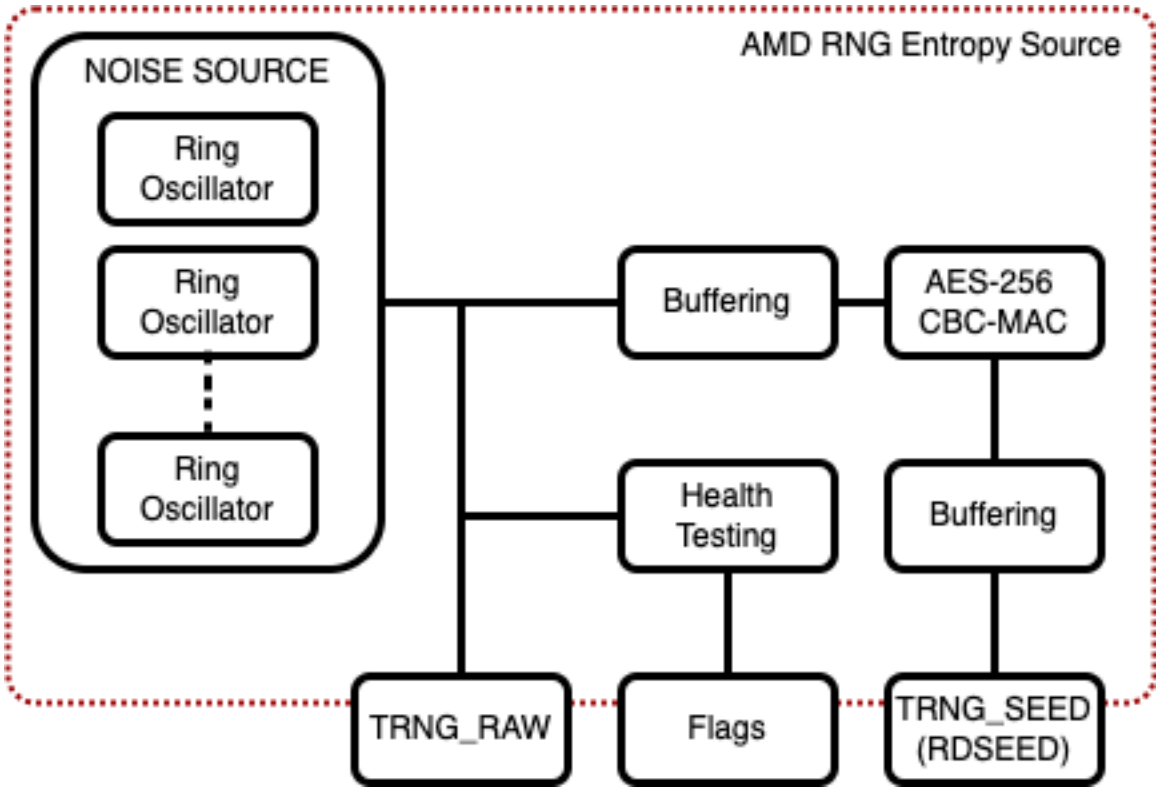

Figure 1: RNG Entropy Source

3 Operating Conditions

The entropy-relevant operating conditions for all entropy source variants listed in Table 1 are given in Table 2.

Table 2: Entropy-Relevant Operating Conditions

Parameter	Value
Temperature	0 to 100 C
Voltage	-0.3 V to 1.30 V (relative to VSS)

4 Configuration Settings

The AMD RNG does not require configuration of entropy-relevant parameters. However, use of the AMD RNG to seed SP 800-90A compliant DRBGs is expected to adhere to the recommendations of Sections 6 and 7 of this document.

5 Physical Security Mechanisms

The AMD RNG entropy source operates within the physical protections of the associated device package; these would typically be capable of meeting FIPS 140-3 Level 2 or Level 3 physical security requirements without additional measures. In addition, the AMD part families listed in this document are usable only when mounted onto PCBs, protecting access to the integrated circuit package.

The AMD RNG does not impose any physical security requirements beyond the nominal FIPS 140-3 requirements. Modules undergoing FIPS 140-3 validation that incorporate the AMD RNG into their boundary must fulfill the physical security requirements appropriate to the targeted module type and security level.

6 Conceptual Interfaces

The AMD RNG provides access to conditioned data (RDSEED) as well as raw data (TRNG_RAW) and flags.

The RDSEED instruction provides error signaling via the CF flag. If CF = 1, the RDSEED return value is valid. If CF = 0, the value is invalid. Software must test the state of the CF flag prior to using the value returned in the destination register to determine if the value is valid. If the returned value is invalid, software must execute the instruction again. Software should implement a retry limit to ensure forward progress of code. If any of the health tests fails, as signaled by checking the CF upon executing RDSEED, the RNG should be restarted to resume normal operation.

The customer also has the option to use the output of the noise source - the ring oscillators - directly to gather the needed entropy. In that case, entropy samples will be collected from the read-only TRNG_RAW register, which is accessible through the AMD-SP MMIO space for x86 software. The output of the ring oscillators is 16 bits.

APIs are available, through the AMD Secure RNG library, to verify support for the RDSEED instruction as well as retrieving 16-bit, 32-bit or 64-bit segments of the 128-bit conditioned output using the RDSEED instruction. The customer can then build their own software blocks for the other components if needed (like the DRBG) or use a cryptographic library that includes an implementation for a software DRBG that will use the entropy collected from the noise source as its own seed.

7 Min-Entropy Rate

Table 3 summarizes the results of the entropy assessment performed for the output of RDSEED.

Table 3: Min Entropy Per 128-Bit RDSEED Output

Part	Min Entropy
7xx2/7xx3	0.312358
V3xxx	0.293746

If the RDSEED output of this entropy source is used to seed a compliant DRBG, then the seeding requirements summarized in Table 4 and Table 5 must be met.

Table 4: 7xx2/7xx3 RDSEED Seeding Requirements for Security Strengths

DRBG Security Strength	128-bit Blocks Required (Nonce Provided)	128-bit Blocks Required (Random Nonce)
112	359	538
128	410	615
192	615	923
256	820	1230

Table 5: V3xxx RDSEED Seeding Requirements for Security Strengths

DRBG Security Strength	128-bit Blocks Required (Nonce Provided)	128-bit Blocks Required (Random Nonce)
112	382	572
128	436	654
192	654	981
256	872	1308

For RDSEED, the conditioned output from the entropy source is the full 128-bit CBC MAC output from the conditioner, and only this full 128-bit block can be credited as containing entropy. The conditioner is considered as a non-vetted conditioning component, so truncation of its output is prohibited by the requirements of SP 800-90B. The RDSEED instruction has variants that return 16, 32, and 64 bits of conditioned data, so multiple RDSEED calls must be used to extract the full 128-bit value.

Table 6 summarizes the results of the entropy assessment performed for the output of raw data.

Table 6: Min Entropy Per 16-Bit Raw Output

Part	Min Entropy
7xx2/7xx3	0.312364
V3xxx	0.293751

If the raw output of this entropy source is used to seed a compliant DRBG, then the seeding requirements summarized in Table 7 and Table 8 must be met. The entropy is associated with the full 16-bit output, so these values only apply when using the full 16-bit samples. No entropy claim is made for sub-portions of these raw symbols.

Table 7: 7xx2/7xx3 Raw Data Seeding Requirements for Security Strengths

DRBG Security Strength	16-bit Blocks Required (Nonce Provided)	16-bit Blocks Required (Random Nonce)
112	359	538
128	410	615
192	615	923
256	820	1230

Table 8: V3xxx Raw Data Seeding Requirements for Security Strengths

DRBG Security Strength	16-bit Blocks Required (Nonce Provided)	16-bit Blocks Required (Random Nonce)
112	382	572
128	436	654
192	654	981
256	872	1308

8 Health Tests

The AMD RNG implements the following health tests:

- APT (Adaptive Proportion Test) and RCT (Repetition Count Test) are performed on start-up and as continuous tests.
- On-demand health tests are fulfilled by the start-up health tests triggered by a reset.

In the event that some number of rings fail to oscillate, then the bits in the output become fixed. The symbols with these fixed bits then become dramatically more likely, which will (given sufficient failures) necessarily trigger an APT failure.

9 Maintenance

The AMD RNG does not require maintenance.

10 Required Testing

The AMD entropy source was tested by collecting raw noise data through the raw noise source interface, which was then processed by the SP 800-90B tool. Restart noise data was also collected through the raw noise source interface and processed by the SP 800-90B tool. 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.

An end user can confirm that the noise source is working by gathering a sample set of 1000000 16-bit samples from the raw output from the noise source. The most straight-forward way to assess this data is using the NIST `ea_non_iid` tool in its conditioning mode, so that the full set of 16 rings can be simultaneously assessed. If the assessed entropy is less than 6.5, then this result is inconsistent with the analysis present in the current entropy assessment.