[Public]

AMD RNG ESV Public Use Document

Document Version 0.7

October 24, 2024

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

Copyright 2024 AMD - may be reproduced only in its original entirety (without revision)

Table of Contents

References 2
1 Description 3
2 Security Boundary 4
3 Operating Conditions 5
4 Configuration Settings 5
5 Physical Security Mechanisms 5
6 Conceptual Interfaces 5
7 Min-Entropy Rate 6
8 Health Tests 9
9 Maintenance 9
10 Required Testing 9

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	23-Oct-2024

AMD Public Material – may be reproduced only in its original entirety (without revision)

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	Entropy Source Name	Part Numbers	Vendor ID	CPU Family	Model	Tested Part	Stepping	Entropy Category	Entropy Estimation Track[1]
EPYC Series									
EPYC 7xx2 Family	AMD RNG	AMD EPYC 7xx2/7xx2P	AuthenticAMD	23 (17h)	49 (31h)	AMD EPYC 7742 64-Core Processor	0	Physical	Non-IID
EPYC 7xx3 Family	AMD RNG	AMD EPYC 7xx3/7xx3P	AuthenticAMD	25 (19h)	1 (1h)	AMD EPYC 7713 64-Core Processor	1	Physical	Non-IID
EPYC 9xx4/8xx4 Family	AMD RNG	AMD EPYC 9xx4/9xx4P/ 8xx4P	AuthenticAMD	25 (19h)	17 (11h)	AMD EPYC 9654 96-Core Embedded Processor	1	Physical	Non-IID
EPYC 3xxx Family	AMD RNG	AMD EPYC 3xxx	AuthenticAMD	23 (17h)	1 (1h)	AMD EPYC 3451 16-Core Processor	2	Physical	Non-IID
Ryzen Embedded Series									
Ryzen V1xxxx Family	AMD RNG	AMD Ryzen Embedded V1xxxx	AuthenticAMD	23 (17h)	24 (18h)	AMD Ryzen Embedded V1500B	1	Physical	Non-IID
Ryzen V3xxx Family	AMD RNG	AMD Ryzen Embedded V3xxx/V3xxxI	AuthenticAMD	25 (19h)	68 (44h)	AMD Ryzen Embedded V3C48 8-Core Processor	0	Physical	Non-IID
Ryzen V2xxx Family	AMD RNG	AMD Ryzen Embedded V2xxx	AuthenticAMD	23 (17h)	96 (60h)	AMD Ryzen Embedded V2546 with Radeon Graphics	1	Physical	Non-IID
Ryzen 5xxxE Family	AMD RNG	AMD Ryzen Embedded 5xxxE	AuthenticAMD	25 (19h)	33 (21h)	AMD Ryzen Embedded R5000 16C	0	Physical	Non-IID

[1] Per SP 800-90B §3.1.2 *Determining the track: IID track vs. non-IID track*

AMD Public Material – may be reproduced only in its original entirety (without revision)

[Public]

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.

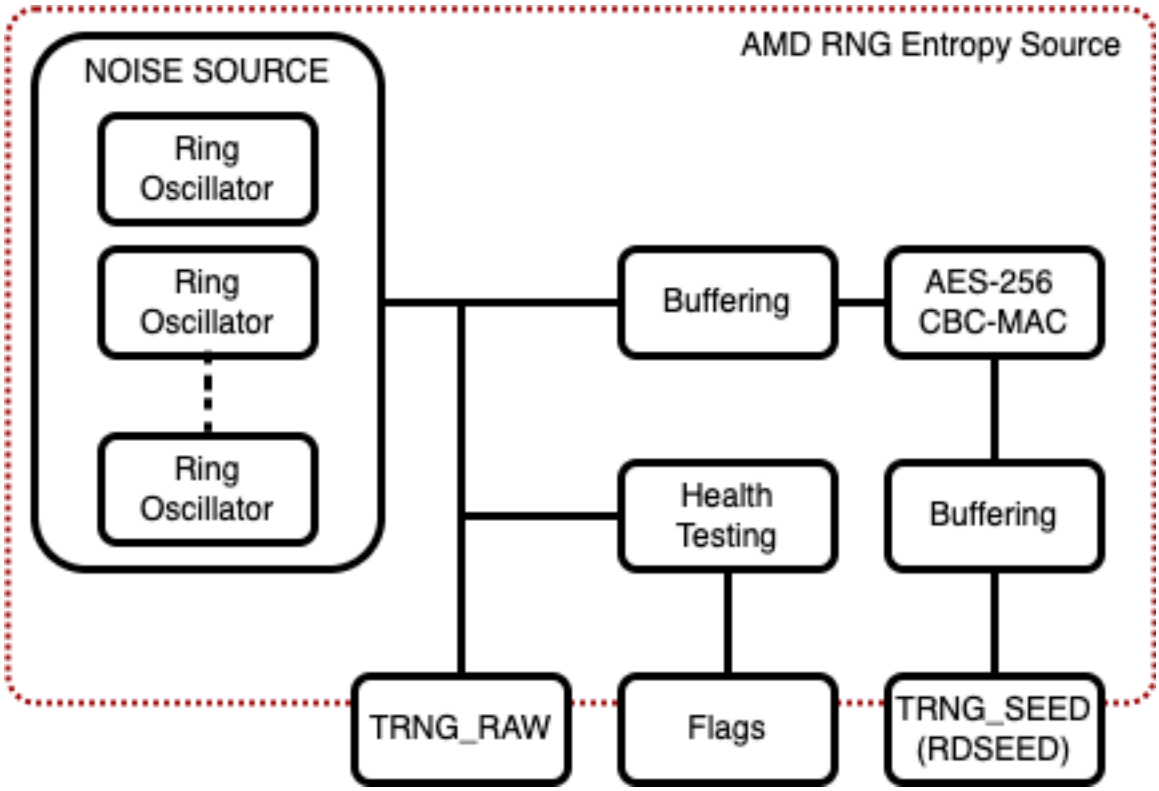

Figure 1: RNG Entropy Source

AMD Public Material – may be reproduced only in its original entirety (without revision)

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

Products Covered	Temperature	Voltage
EPYC Series		
EPYC 7xx2/7xx2P Family	0 to 100 C	-0.3 V to 1.30 V (relative to VSS)
EPYC 7xx3/7xx3P Family	0 to 100 C	-0.3 V to 1.30 V (relative to VSS)
EPYC 9xx4/9xx4P/8xx4P Family	0 to 100 C	-0.3 V to 1.30 V (relative to VSS)
EPYC 3xxx Family	0 to 95 C	-0.3 V to 1.30 V (relative to VSS)
Ryzen Series		
Ryzen V1xxxx Family	0 to 100 C	-0.3 V to 1.30 V (relative to VSS)
Ryzen V3xxx/V3xxxI Family	0 to 100 C	-0.3 V to 1.30 V (relative to VSS)
Ryzen V2xxx Family	0 to 105 C	-0.3 V to 1.30 V (relative to VSS)
Ryzen 5xxxE Family	0 to 85 C	-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.

AMD Public Material – may be reproduced only in its original entirety (without revision)

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
EPYC 7xx2/7xx3	1.31221
EPYC 9xx4/8xx4	1.07355
EPYC 3xxx	0.796275
Ryzen V1xxxx	0.656040
Ryzen V3xxx	1.63007
Ryzen V2xxx	1.02913
Ryzen 5xxxE	1.32622

If the RDSEED output of this entropy source is used to seed a compliant DRBG, then the seeding requirements summarized in Table 4 through Table 10 must be met.

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

DRBG Security Strength	128-bit Blocks Required (Nonce Provided)	128-bit Blocks Required (Random Nonce)
112	86	129
128	98	147
192	147	220
256	196	293

Table 5: EPYC 9xx4/8xx4 RDSEED Seeding Requirements for Security Strengths

DRBG Security Strength	128-bit Blocks Required (Nonce Provided)	128-bit Blocks Required (Random Nonce)
112	105	157
128	120	179
192	179	269
256	239	358

Table 6: EPYC 3xxx RDSEED Seeding Requirements for Security Strengths

DRBG Security Strength	128-bit Blocks Required (Nonce Provided)	128-bit Blocks Required (Random Nonce)
112	141	211
128	161	242
192	242	362
256	322	483

Table 7: Ryzen V1xxxx RDSEED Seeding Requirements for Security Strengths

DRBG Security Strength	128-bit Blocks Required (Nonce Provided)	128-bit Blocks Required (Random Nonce)
112	171	257
128	196	293
192	293	439
256	391	586

Table 8: Ryzen V3xxx RDSEED Seeding Requirements for Security Strengths

DRBG Security Strength	128-bit Blocks Required (Nonce Provided)	128-bit Blocks Required (Random Nonce)
112	69	104
128	79	118
192	118	177
256	158	236

Table 9: Ryzen V2xxx RDSEED Seeding Requirements for Security Strengths

DRBG Security Strength	128-bit Blocks Required (Nonce Provided)	128-bit Blocks Required (Random Nonce)
112	109	164
128	125	187
192	187	280
256	249	374

Table 10: Ryzen 5xxxE RDSEED Seeding Requirements for Security Strengths

DRBG Security Strength	128-bit Blocks Required (Nonce Provided)	128-bit Blocks Required (Random Nonce)
112	85	127
128	98	147
192	147	220
256	196	293

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

Table 11: Min Entropy Per 16-Bit Raw Output

Part	Min Entropy
EPYC 7xx2/7xx3	1.31225
EPYC 9xx4/8xx4	1.073578
EPYC 3xxx	0.796292
Ryzen V1xxxx	0.656053
Ryzen V3xxx	1.630126
Ryzen V2xxx	1.02916
Ryzen 5xxxE	1.32626

If the raw output of this entropy source is used to seed a compliant DRBG, then the seeding requirements summarized in Table 12 through Table 18 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.

AMD Public Material – may be reproduced only in its original entirety (without revision)

Table 12: EPYC 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	86	129
128	98	147
192	147	220
256	196	293

Table 13: EPYC 9xx4/8xx4 Raw Data Seeding Requirements for Security Strengths

DRBG Security Strength	16-bit Blocks Required (Nonce Provided)	16-bit Blocks Required (Random Nonce)
112	105	157
128	120	179
192	179	269
256	239	358

Table 14: EPYC 3xxx Raw Data Seeding Requirements for Security Strengths

DRBG Security Strength	16-bit Blocks Required (Nonce Provided)	16-bit Blocks Required (Random Nonce)
112	141	211
128	161	242
192	242	362
256	322	483

Table 15: Ryzen V1xxxx Raw Data Seeding Requirements for Security Strengths

DRBG Security Strength	16-bit Blocks Required (Nonce Provided)	16-bit Blocks Required (Random Nonce)
112	171	257
128	196	293
192	293	439
256	391	586

Table 16: Ryzen V3xxx Raw Data Seeding Requirements for Security Strengths

DRBG Security Strength	16-bit Blocks Required (Nonce Provided)	16-bit Blocks Required (Random Nonce)
112	69	104
128	79	118
192	118	177
256	158	236

Table 17: Ryzen V2xxx Raw Data Seeding Requirements for Security Strengths

DRBG Security Strength	16-bit Blocks Required (Nonce Provided)	16-bit Blocks Required (Random Nonce)
112	109	164
128	125	187
192	187	280
256	249	374

Table 18: Ryzen 5xxxE Raw Data Seeding Requirements for Security Strengths

DRBG Security Strength	16-bit Blocks Required (Nonce Provided)	16-bit Blocks Required (Random Nonce)
112	85	127
128	97	145
192	145	218
256	194	290

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 5 bits per byte, then this result is inconsistent with the analysis present in the current entropy assessment.

AMD Public Material – may be reproduced only in its original entirety (without revision)