SP 800-90B Non-Proprietary Public Use Document
PS1010 And PS1030 NVMe Opal SEDs

Document Version 1.1

Hardware Part Numbers

HFS1T9GFJCX142N
HFS3T8GFJCX142N
HFS7T6GFJCX142N
HFS15T3FJCX142N
HFS1T6GFJCX142N
HFS3T2GFJCX142N
HFS6T4GFJCX142N
HFS12T8FJCX142N
HFS1T9GEJVX142N
HFS3T8GEJVX142N
HFS7T6GEJVX142N
HFS15T3EJVX142N
HFS1T6GEJVX142N
HFS3T2GEJVX142N
HFS6T4GEJVX142N
HFS12T8EJVX142N

SK hynix Memory Solutions America
3103 North First Street, San Jose, CA, 95134

December 14, 2023

Template Revision History

Version	Date	Change
V1.0		Initial release
V1.1	3/9/23	Updated Required Testing section to match CMVP expectations. Removed some the IID or non-IID classification on the Description section. Stated that the Operating Conditions and Physical Security Mechanisms are not always required based on the entropy source. Added Vendor Permissions and Relationship section.

Revision History

Version	Date	Change
V0.1	09/22/23	Initial draft
V1.0	10/03/23	Final
V1.1	12/14/23	Corrected the Entropy Source name in the Min Entropy section.

Table of Contents

[Note: Some sections in this document may be pared down or excluded when the entropy source is validated as reuse restricted to vendor.]

Description

SK hynix PS1010 and PS1030 NVMe Opal SED's (referred to as The Module hereafter) TRNG/NDRNG Physical Entropy module IP is from Synopsys. Synopsys calls the IP DesignWare® Cores (DWC) True Random Number Generator (TRNG) NIST SP800-90C (DWC TRNG NIST SP800-90C). v3.00a of the DWC TRNG NIST IP is used. The IP comprises of synthesizable source code and testbenches in Verilog HDL and configuration tools.

Table 1. Description

Identifier	Version
Part Number and Product ID	dwc_trng_nist_sp800_90c B227-0
Hardware Revision	Version 3.00a

The DesignWare® Cores True Random Number Generator (TRNG) NIST SP800-90 (DWC TRNG NIST SP800- 90C) circuit is comprised of a physical entropy source, a NIST SP 800-90A DRBG, and health-check blocks that perform continuous statistical health tests and on-demand Known Answer Tests (KAT).

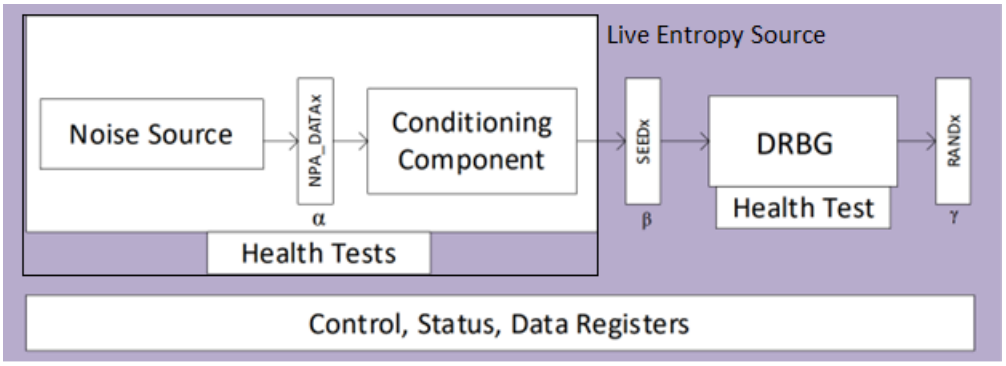

Figure 1. High-Level Design of the DWC TRNG NIST SP800-90C

The noise source sends a non-Independent and Identically Distributed (non-IID) noise stream to the conditioning component to produce an entropy seed which is then fed into the approved DRBG to generate random bits. A health-test block is included to perform Known Answer Tests (KAT) and statistical tests required by NIST SP800-90A/B/c and BSI AIS 20/31. The health test block performs start-up, on-demand, and continuous tests.

The TRNG has been fully verified at the IP And system integration levels. Testing of the IP instance has been carried out in RTL simulations, on FPGA and then on silicon. Silicon testing is used to characterize the raw noise entropy source.

Security Boundary

The Security Boundary is used to assess the random number provided by the output values from an entropy source. The entropy assessment is performed under the assumption that any observer (including any adversary) is outside of that boundary.

The entropy source security boundary is the boundary surrounding the noise source, digitizer, conditioner, online health test SP 800-90A DRBG, and self-tests. Other logic components (bus interfaces, power negotiation, clock management, DFx logic) exist outside this boundary.

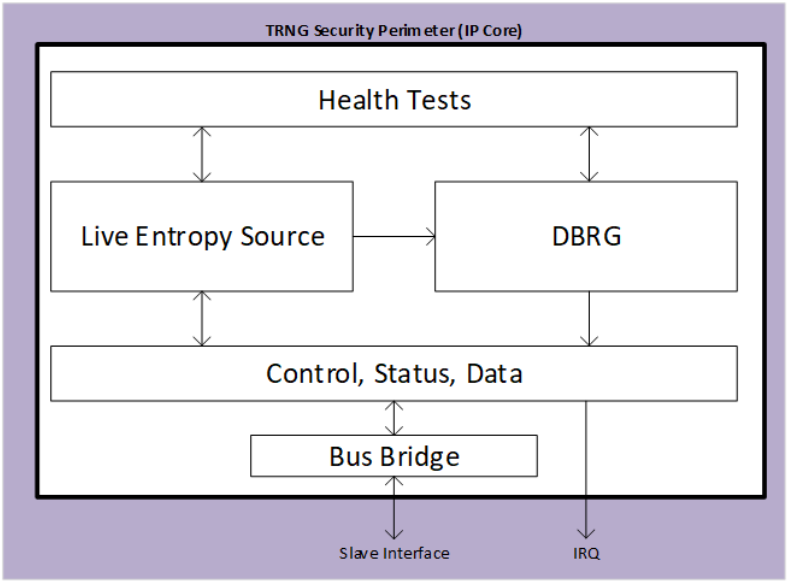

Figure 2. Security Boundary

Operating Conditions

Operating Conditions under which the entropy source is claimed to operate correctly are itemized in the following table.

Table 2. Operating Conditions

Parameter	Value	Description
Temperature	0 – 125C	Operating temperature range
Voltage	0.75V +/- 10%	Operating voltage range
Clock speed	550MHz	Operating frequency

Physical Security Mechanisms

The Module implements the following physical security mechanisms to meet FIPS 140-3 level 2:

- An aluminum alloy enclosure that protects the production-grade components of the Module. The enclosure is opaque within the visible spectrum.
- Two (2) opaque tamper-evident seals that are affixed on the sides of the Module. These two (2) seals are required to ensure the detection of tamper attempt. These seals cannot be removed or reapplied without tamper evidence.

Configuration Settings

The finalized DWC TRNG NIST SP800- 90C does not require any additional configurations of entropy-relevant parameters.

Conceptual Interfaces

Raw noise output is available in the TRNG registers. The noise source output is not available during regular operation. Only in test mode, the noise source output, TRNG registers are available to be read externally to enable the collection of noise source output for statistical testing.

Min-Entropy Rate

The following table summarizes the results of the entropy assessment performed for the output of the DWC TRNG NIST SP800-90C Entropy Source.

Table 3. Claimed Min-Entropy

Min-Entropy
1 bit/bit

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

Table 4. Seeding Requirements

	Nonce NOT Provided by This Source		Nonce Provided by This Source	
DRBG Security Strength (bits)	1-Bit Blocks Required	Bytes Required	Bits Required	Bytes Required
128	128	16	192	24
256	256	32	384	48

Health Tests

The following figure shows the different tests which are present in the design and their monitoring location:

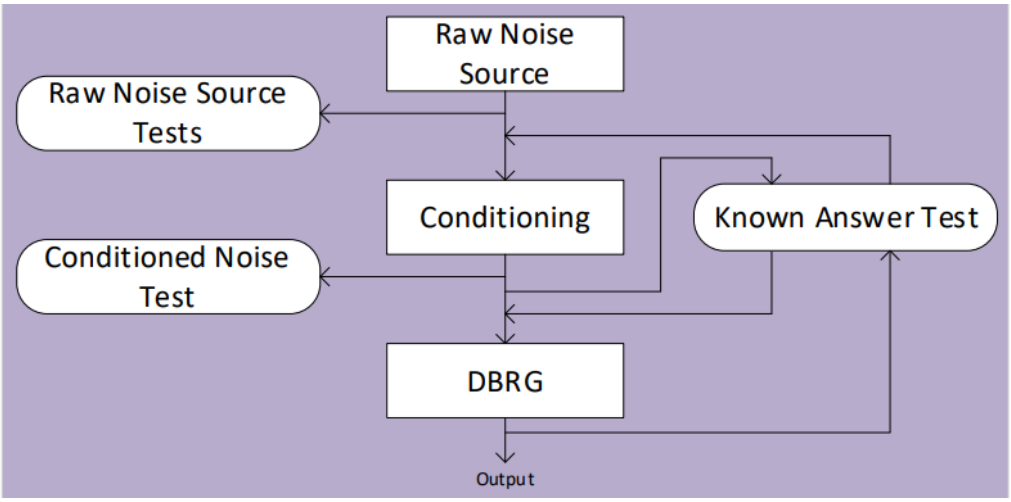

Figure 3. Health Tests

Raw Noise Source Tests - Repetition Count and Adaptive Proportion tests.

Conditioned Noise Test - Repetition Count test.

Known Answer Tests - A known input to the block is provided and the result is checked. This test is run on-demand by the application software and after the core comes out of reset.

Failure modes of the noise source in the TRNG-NIST Core are characterized by one of the following:

- High bias (many more 1s than 0s)
- Low bias (many more 0s than 1s)
- High positive binary serial correlation coefficient (many more 00 and 11 patterns than 01 and 10 patterns)
- High negative binary serial correlation coefficient (many more 01 and 10 patterns than 00 and 11)
- High rate of limit cycles (many more 0110, 1001 patterns than 0101 or 1010)

Anticipated Failure Modes

Limit cycles result from the alignment of the feedback step points with the Markov probability curve mode. A slight increase in the rate of limit cycles present in the noise source output data is expected. A failure leading to excessive negative feedback will result in a more significant number of limit cycle patterns (00110011…) if the alignment of the peak of the metastable curve is centered on a step point of the feedback. An asymmetric failure in the feedback paths will lead to high or low bias. In comparison, a symmetric failure in the feedback path will lead to high or low serial correlation. The presence of limit cycles is tightly related to the bias and serial correlation. The definitions are redundant because the bias and correlation can be explained in limit cycles and visa-versa.

All such known noise source failure modes are detected by the implemented health tests.

Health Test Failures and Responses

A non-maskable alarm is raised and the TRNG-NIST core zeroizes itself 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. The cause of failure can be deduced by reading a TRNG 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-NIST core issues an alarm and zeroizes itself. However, by default, the hardware comes out of the busy state and is ready to be used. The application software takes necessary action upon failure, for e.g., by resetting the core to kick off a new round of the start-up test. The TRNG-NIST core works alongside a carefully written software to be NIST SP 800-90A/B/c compliant. This allows some tasks including re-run of the startup test to be handed out to software to allow more flexibility. Both hardware and software are expected to reside in the same secure boundary.

Similarly, when a continuous health test or KAT fails, a non-maskable alarm raises and the core zeroizes itself. The cause of failure can be read from a TRNG register.

Module enters Self_Test_Error state if Health Tests fail. In this error state, the module outputs the error status message via NVMe Identify Controller command word at offset 4092, bit 0 will be 1. Otherwise, it indicates successful completion by bit 0 will be 0.

Maintenance

There are no specific maintenance requirements.

Required Testing

Raw noise is not available to be collected for statistical tests on production modules. The user must rely on the health tests to detect any drops in entropy.

For ESV, the test modules with a debug interface running a debug firmware allow raw noise collection.

The NDRNG/TRNG hardware module generates 192 bytes of noise for one Noise Generation request i.e. 48 32-bit dwords. Firmware issues the below command sequence to the hardware for one Noise Generation request. The sequence is repeated by the firmware to collect as many samples as needed.

Table 5: Noise Generation Sequence

Step #	Description
1	Issue Zeroize cmd
2	Wait for Zeroized flag to be set indicating Zeroize cmd processing is completed.
3	Clear Zeroized flag.
4	Select AES-256 algorithm
5	Write default settings for this register i.e. Nonce Seeding Mode and Test Mode.

6	Clear NOISE_RDY bit
7	Issue GEN_NOISE cmd
8	Wait for NOISE_RDY bit to be set
9	Read 16 32-bit dwords of raw noise
10	If all 48 32-bit dwords of noise are read, quit. Else, go to step 8.