SP 800-90B Non-Proprietary Public Use Document

Ultrastar® DC SN650
Document Version 1.1

Hardware Model Number WUS5BB1A1E9ELE7
Firmware Image Release Version LA204108
Security Firmware Release Version TB.039.007.A

Western Digital Corporation
5601 Great Oaks Parkway, San Jose, California 95119

October 19, 2022

Revision History

Version	Change
1.0	Initial Draft
1.1	Updates to address CMVP's comments

Table of Contents

Description

The entropy source of the Western Digital Ultrastar DC SN650 is a hardware implemented, physical (ENT (P)) entropy source consisting of 32 individual ring oscillators concatenated to produce 32-bit raw data output, which is provided with no conditioning. The entropy source was tested by collecting data from multiple process, voltage, and temperature (PVT) operational conditions from a test card. The hardware noise source is essentially the noise source of Broadcom's design secr_trng_800_90a_vb1 and is claimed to produce non-IID outputs. The health tests are within the security firmware library, which is stored in NAND memory within the SSD module. The overall firmware image release version is LA204108, and the security firmware library release version is TB.039.007.A. The security firmware library release utilizes API calls to retrieve raw entropy data from the entropy source.

Security Boundary

The entropy source is depicted in Figure 1, showing a high-level design of the basic layout of the module. Output from sampling the ring osculators is provided to SP 800-90B compliant health tests and an SP 800-90A compliant DRBG.

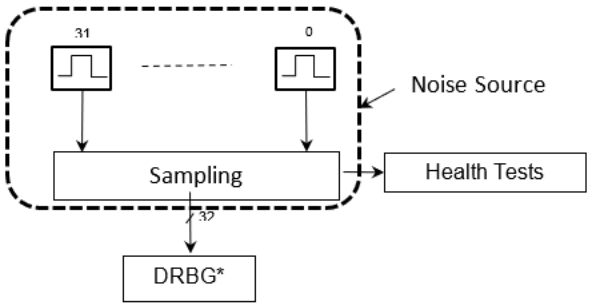

Figure 1. High-level Block Diagram of the Entropy Source

*SP800-90A-compliant DRBG with derivation function

The security boundary is depicted in Figure 2. The entire TRNG IP module, which is implemented within the Western Digital SoC9 ASIC and contains the noise source, constitutes the security boundary.

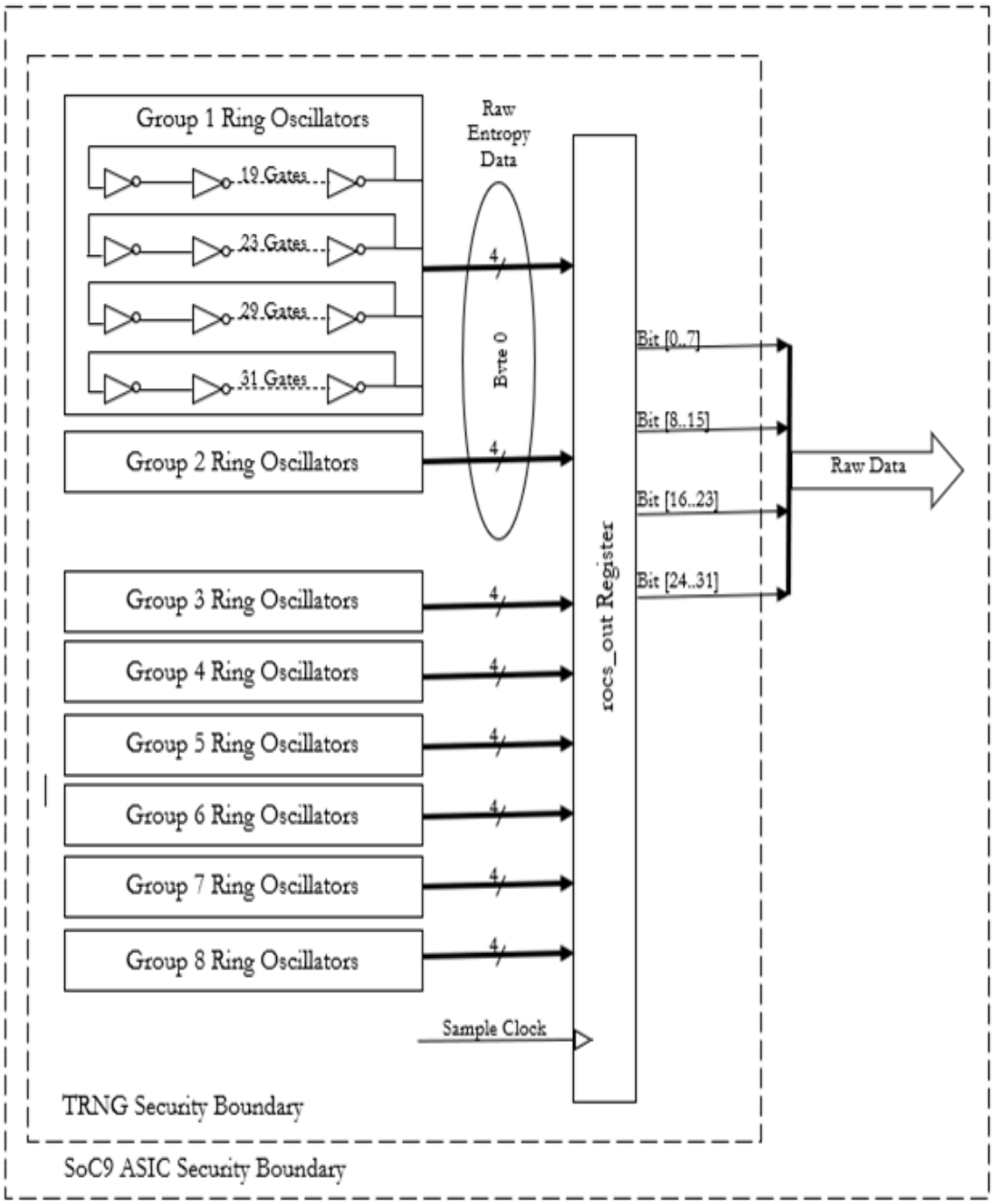

Figure 2. Physical Boundary of the Entropy Source

Operating Conditions

The entropy source was tested under several different PVT corners. Table 1 contains the operational conditions in which the entropy source will operate in and maintain entropy production at the assessed value.

Table 1. Operational Conditions

Parameter	Value	Description
Temperature	Min: -40C; Typical: 27C; Max: 125C	Operating Temperature Range
Voltage	Min: 0.72V; Typical: 0.83V; Max: 0.96V	Operating Voltage Range
Clock speed	200Khz	System Clock Frequency

Configuration Settings

The entropy-relevant configuration settings are summarized in Table 2.

Table 2. The Setting of Entropy-Relevant Parameters

Entropy-Relevant Parameters	Configurations
Size of the health testing block	1024 bits
Sampling Frequency	12.5 MHz
Bounds for each of the health tests	RCT's cutoff = 15, APT's cutoff = 384

Physical Security Mechanisms

The Cryptographic Module does not make claims in the Physical Security area beyond FIPS 140-3 Security Level 1.

- All components are production-grade materials with standard passivation.
- The Cryptographic Module enclosure is opaque and enclosed within a host system.

Conceptual Interfaces

At power up, the security firmware calls EntropySource::Initialize to test the health of the ENT(P) entropy source. From within EntropySource::Initialize, calls to Get32bitsFrmNDRNGNoiseSrc, APT::CheckSample, and RCT::CheckSample harvest raw entropy data and test the health of the harvested data.

If the ENT(P) entropy source is deemed healthy, the security firmware discards the harvested data and calls EntropySource::GetEntropy to generate a DRBG seed. From within EntropySource::GetEntropy, calls to Get32bitsFrmNDRNGNoiseSrc, APT::CheckSample and RCT::CheckSample harvest new raw entropy data and test the health of the harvested data. If the ENT(P) entropy source is deemed healthy the security firmware seeds the DRGB with the harvested entropy data.

Min-Entropy Rate

The entropy source embedded in the Western Digital Ultrastar DC SN650 provides 2.69 bits of min-entropy per 32-bit sample output. This is also equal to H_submitter. One hundred sixty (160) 32-bit samples are provided unconditioned to an SP 800-90A complaint DRBG with a security strength of 256 bits.

Health Tests

On power up, the cryptographic module executes the entropy source initialization sequence shown in Figure 3. The sequence collects 1024 consecutive samples of raw noise to verify the health of the ENT (P) noise source. The sequence consists of a Repetition Count Test (RCT) and Adaptive Proportion Test (APT). On demand testing requirements are satisfied by the RCT and APT health tests executed during that power up sequence. If the initialization sequence returns false, the cryptographic module transitions to an error state that blocks the execution of all security services.

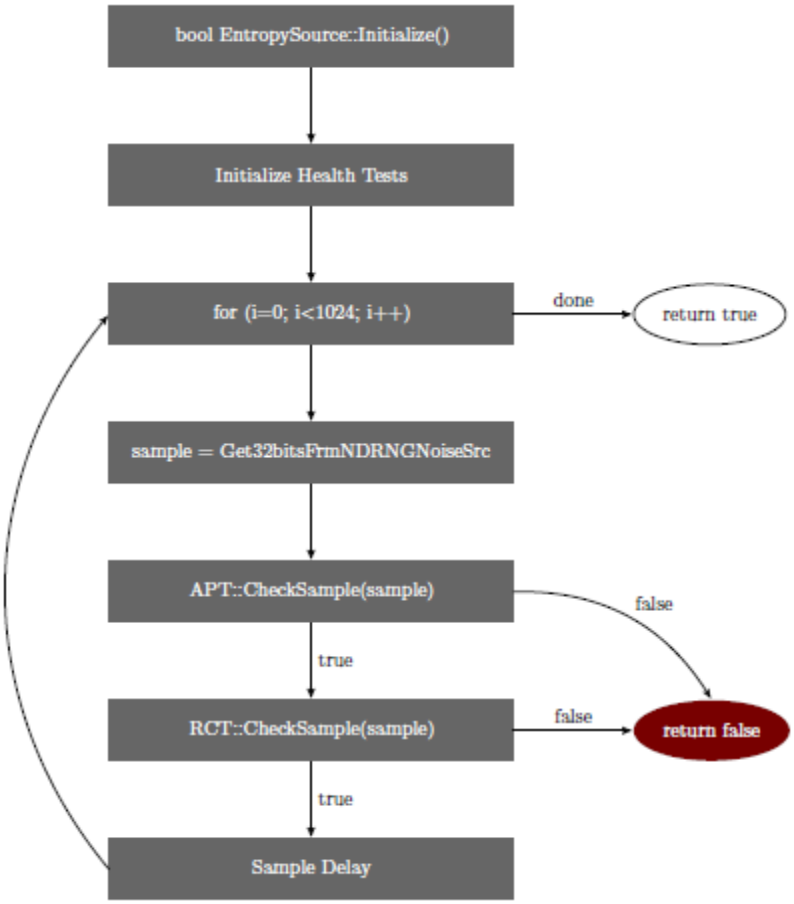

Figure 3. Entropy Source Initialization Sequence

Prior to seeding the DRBG, the module tests the health of the harvested entropy. Figure 4 illustrates the harvesting and health test sequence. If either continuous health fails, the DRBG seeding operation aborts and the cryptographic module transitions to an error state that blocks the execution of all security services.

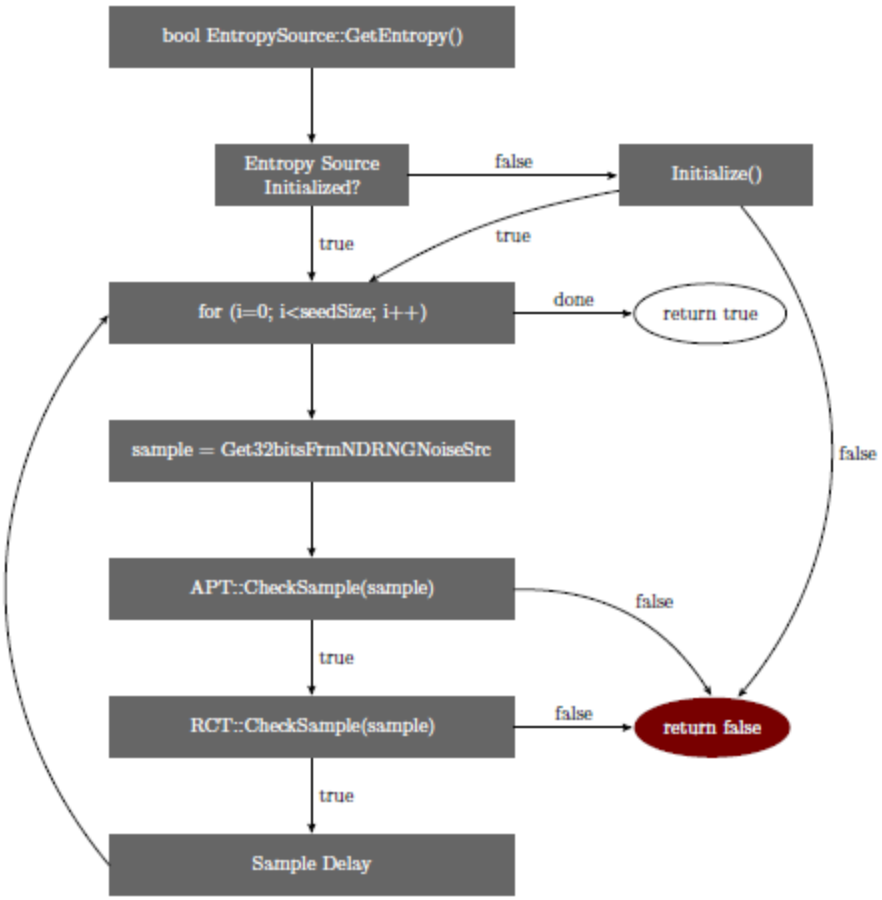

Figure 4. Entropy Source Harvest Sequence

Maintenance

No maintenance requirements must be executed for the entropy noise source to remain healthy.

Required Testing

The entropy source embedded in the Western Digital Ultrastar DC SN650 was tested by collecting 32-bit data, as the concatenation of 32 ring oscillators' output bits, which was then processed with the SP 800-90B tool. Raw and restart noise data was collected through a debug interface not available outside of test units. 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.