SP 800-90B Non-Proprietary Public Use Document

SOC9B ASIC, Rev 2.1,
ARM Cortex M3 & ARM Cortex R8

Hardware Model Number 0L23689

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

February 13, 2024

Revision History

Version	Change
1.0	Initial Draft
2.0	Correct to provide a more accurate vendor reuse reference data

Table of Contents

Description 4

Security Boundary 4

Operating Conditions 5

Configuration Settings 6

Physical Security Mechanisms 6

Conceptual Interfaces 6

Min-Entropy Rate 6

Health Tests 6

Maintenance 8

Required Testing 8

Description

The entropy source of the Western Digital SoC9B ASIC is a hardware implemented, physical 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 implementation utilizes the Broadcom's design secr_trng_800_90a_vc1 TRNG IP and is claimed to produce non-IID outputs. The health tests within the security firmware library are entirely implemented within the entropy_source.hpp and entropy_source.cpp source code files. The integrity of the health test source code is verified during the build process by comparing a known SHA-256 hash digest of entropy_source.hpp and entropy_source.cpp against a digest calculated during the build process. The binary equivalent of the health tests resides within non-volatile memory. Utilizing a SHA-256 hash digest to assure the integrity of the health tests allows the health test to be ported to multiple security library version. All security firmware library releases that incorporate the health tests utilize 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.

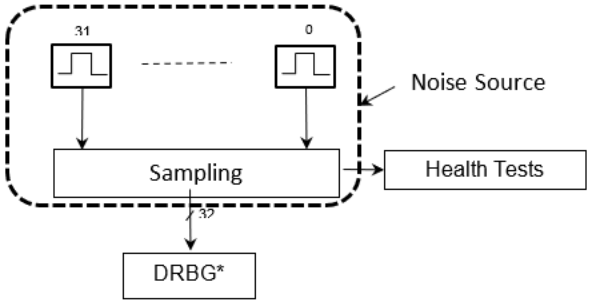

Figure 1: High-level Block Diagram of the Entropy Source

*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 SoC9B ASIC and contains the noise source, constitutes the security boundary.

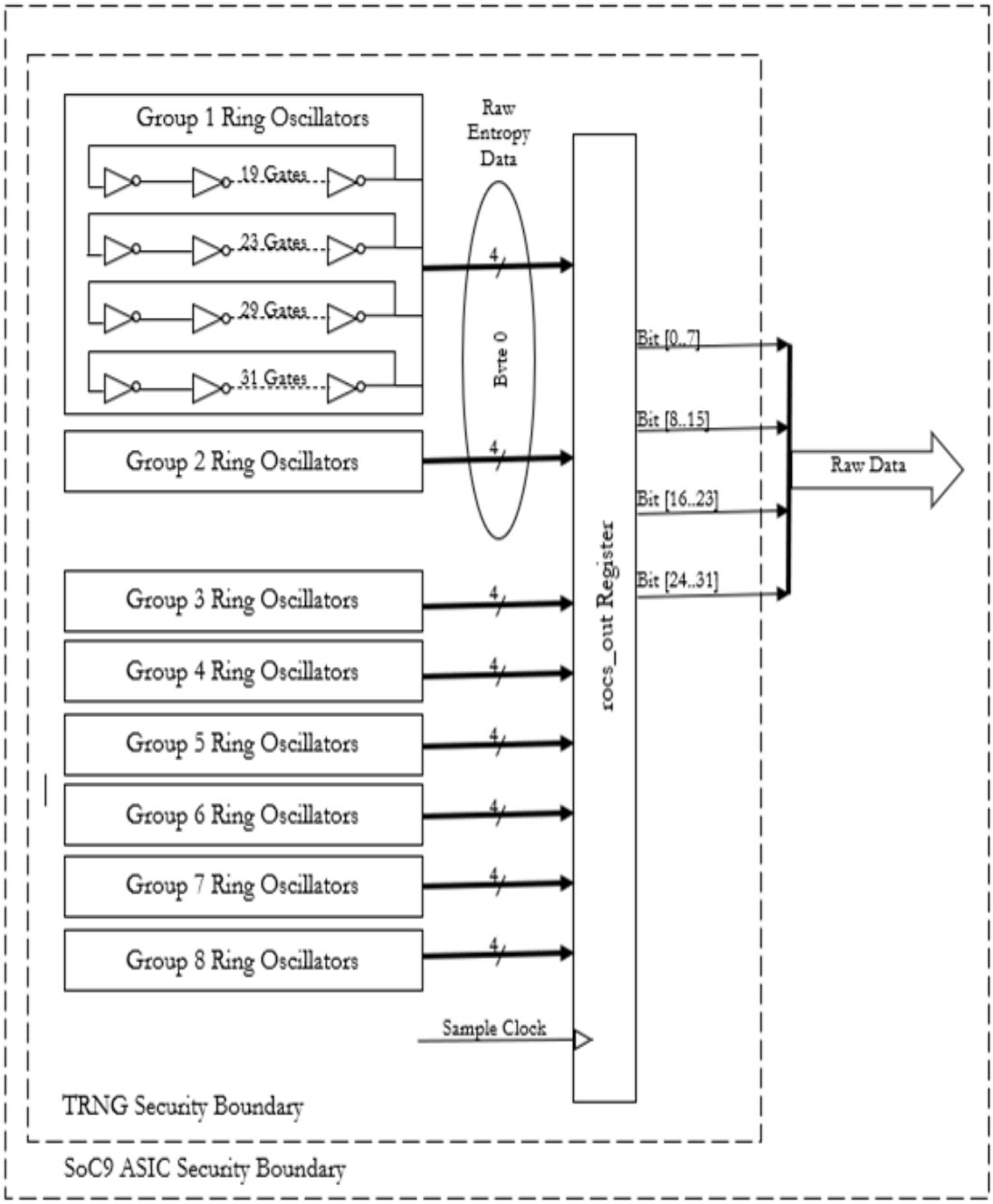

Figure 2: Physical Boundary of the Entropy Source

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: 0.76 V; Typical: 0.85 V; Max: 0.99 V	Operating Voltage Range
Clock speed	260 MHz	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	10 MHz
Bounds for each of the health tests	RCT's cutoff = 15, APT's cutoff = 384

Physical Security Mechanisms

The SoC9B ASIC 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 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 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 SOC9B ASIC provides 2.7 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 compliant 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 noise source. The sequence consists of an Adaptive Proportion Test (APT) and Repetition Count Test (RCT). On demand testing requirements are satisfied by the RCT and APT health tests

executed during the 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.

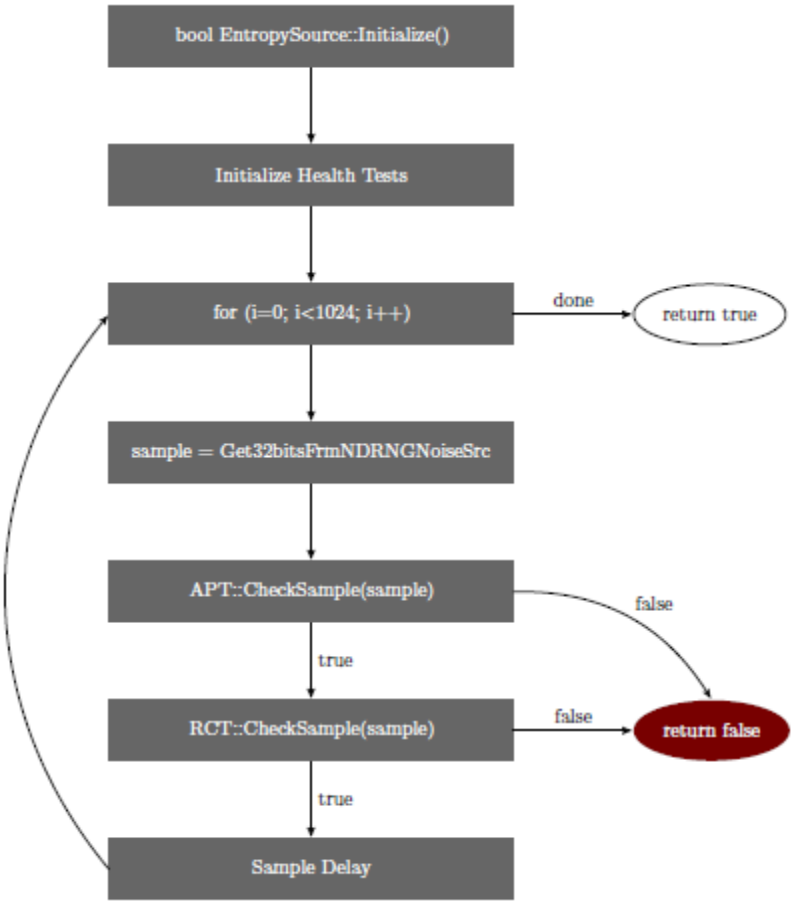

Figure 3: Entropy Source Initialization Sequence

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.

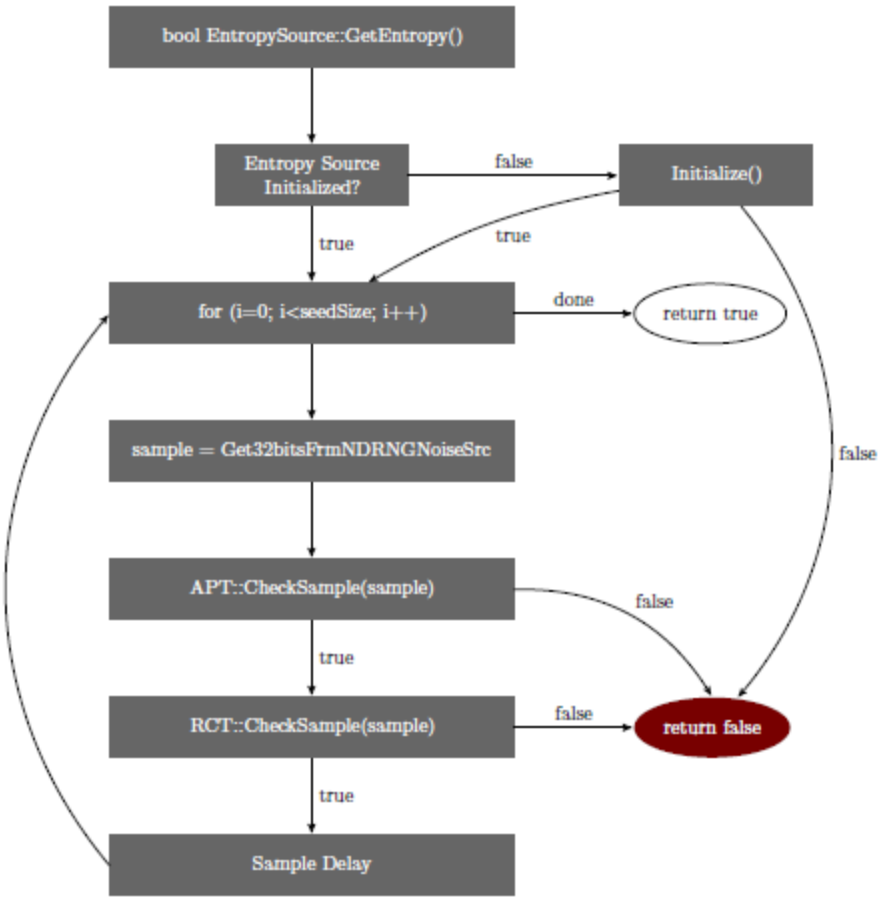

Figure 4: Entropy Source Harvest Sequence

Maintenance

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

Required Testing

Built-in Health Tests described in the Health Tests section constantly checks the validity of the noise source. No additional testing is required.