



SP 800-90B Non-Proprietary Public Use Document for the Entropy Source of the Qualcomm® Pseudo Random Number Generator

Hardware Version: 3.4.0

Document Version: 1.3

Document Date: 2026-09-01

Prepared for:
Qualcomm Technologies, Inc.
5775 Morehouse Dr
San Diego, CA 92121
USA

Prepared by:
atsec information security Corporation
4516 Seton Center Parkway, Suite 250
Austin, TX 78759
USA

Table of Contents

1 Description..... 3

2 Security Boundary 3

3 Operating Conditions..... 4

4 Configuration Settings..... 4

5 Physical Security Mechanisms 4

6 Conceptual Interfaces 4

7 Min-Entropy Rate 4

8 Health Tests 4

9 Maintenance 5

10 User Verification 5

11 Vendor Permissions and Relationship 5

1 Description

This document describes the design aspects of the Qualcomm® Pseudo Random Number Generator entropy source (referred to as the TRNG or as the entropy source in the rest of this document). The TRNG is a physical entropy source whose noise generation is based upon timing variations of the periods of the included ring oscillators (ROs). These timing variations are caused by underlying thermal and shot noise. The TRNG was tested on the operational environments listed in Table 1 under the assumption that the TRNG's output is non-IID.

The entropy source is validated as conformant to SP 800-90B (January 2018), FIPS 140-3 IG D.J (April 16, 2026), and FIPS 140-3 IG D.K (April 16, 2026).

Table 1: Operational environment and versions.

Hardware Version	Hardware Platform	Embodiment
3.4.0	Snapdragon 7 Gen 4 Mobile Platform	Single-chip
3.4.0	Qualcomm Dragonwing™ Q-7790	
3.4.0	Snapdragon 8s Gen 4 Mobile Platform	

2 Security Boundary

Figure 1 below depicts the entropy source boundary with its enclosing box.

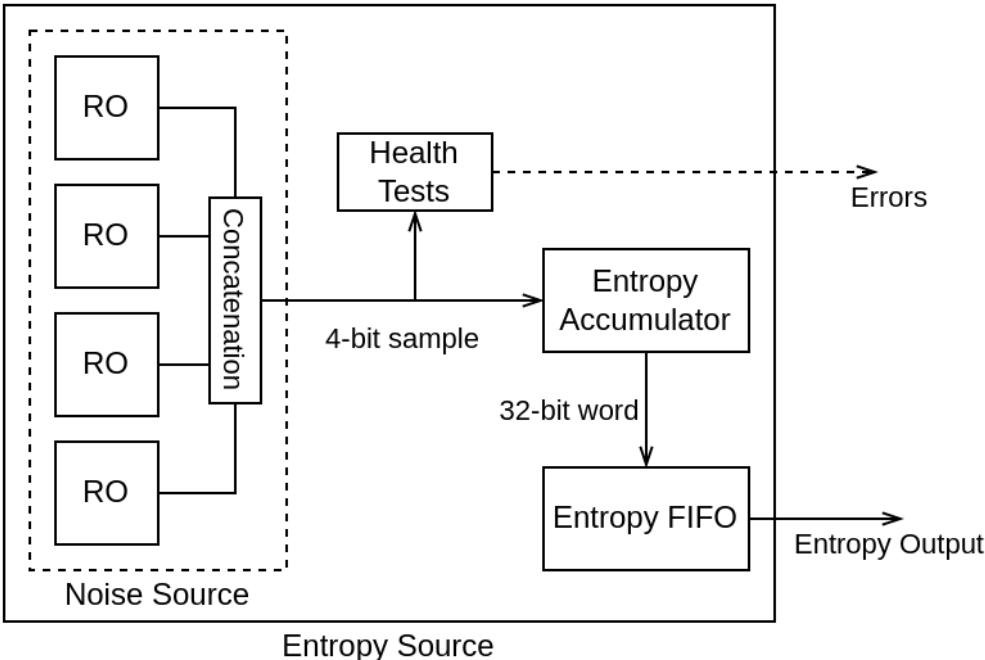


Figure 1: Block diagram of the entropy source

The entropy source boundary contains the following components:

- the physical noise source,
- the SP 800-90B health tests,

- the Entropy Accumulator, and
- the Entropy FIFO, which holds the data from the Entropy Accumulator and is accessible via the Entropy Output interface.

The TRNG does not include a conditioning component.

3 Operating Conditions

The entropy source is implemented as a part of a hardware platform and is therefore subject to the same environmental conditions as its SoC (System-on-Chip). The SoC's enclosure provides stabilized voltages and temperatures which are guaranteed to stay within the entire SoC's limits.

The operating temperature and voltage range of the Snapdragon 7 Gen 4 Mobile Platform and Qualcomm Dragonwing Q-7790, and thus of the TRNG in these platforms, is as follows:

- Temperature Range of [-30°C, 95°C]
- Voltage Range of [0.485V, 0.974V]

The operating temperature and voltage range of the Snapdragon 8s Gen 4 Mobile Platform, and thus of the TRNG in this platform, is as follows:

- Temperature Range of [-30°C, 105°C]
- Voltage Range of [0.485V, 1.018V]

4 Configuration Settings

The TRNG has no operator-configurable parameters.

5 Physical Security Mechanisms

At the time of manufacturing, the die containing the TRNG is embedded within a printed circuit board (PCB), which prevents visibility into the internal circuitry of the TRNG. The layering process used to embed the die into the PCB prevents tampering of the physical components without leaving tamper evidence.

The TRNG is further protected by being enclosed within a commercial off-the-shelf mobile device that utilizes production-grade components. The mobile device enclosure physically surrounds the TRNG.

6 Conceptual Interfaces

The TRNG provides its entropy output interface (the GetEntropy() interface) to an SP 800-90A compliant DRBG running on the same platform. In the production environment, only the DRBG can directly access the entropy source output.

7 Min-Entropy Rate

The entropy source provides 0.4 bits of entropy per 4-bit output sample.

8 Health Tests

The TRNG performs the required health tests per section 4.4 of SP 800-90B. There are two types of health test failures: intermittent failure and permanent failure. When a health test fails, this is initially marked as an intermittent failure and the entropy source is automatically reset, causing the start-up health tests to run. When three intermittent failures are detected, the entropy source enters a permanent failure state.

Recovery from the permanent failure state requires that an external entity either perform a hard reset of the entire chip or assert the reset signal of the entropy source.

There are three health test methods: Repetition Count Test (RCT), Adaptive Proportion Test (APT), and Health Monitoring Test. The RCT and APT are the approved methods per SP800-90B. The Health Monitoring test monitors the individual ring oscillators for failure to oscillate events.

The entropy source performs health tests at the following conditions:

- Start-up tests are performed after start-up, reboot, or reset, before the first use of the entropy source. The start-up tests consist of both the RCT and APT, run over 1024 consecutive 4-bit samples, as well as the continuous Health Monitoring. Upon failure, all collected entropy is discarded and the start-up tests are performed again on the next 1024 4-bit samples. The APT window size is 512 samples.
- Continuous tests consist of both the RCT and APT, run over 4-bit samples, as well as the continuous Health Monitoring. The APT window size is 512 samples.
- On-demand tests are performed by rebooting the hardware platform, initiating the previously mentioned start-up tests.

9 Maintenance

The TRNG has no maintenance requirements.

10 User Verification

In normal operation, an arbitrary user does not have access to the output of the TRNG – only the DRBG can access it – as described in Section 6. The testing thus must rely on the health tests discussed in Section 8 to detect anomalies in the expected entropy and failures.

To identify the version of the entropy source, the operator can read the register `RNG_CM_PRNG_HW_VERSION` and verify its value is `0x00030400`.

To identify the hardware platform, the operator can physically inspect the package of the SoC which contains the entropy source: 'SM7750' is printed on the package of Snapdragon 7 Gen 4 Mobile Platform, 'CQ7790M' is printed on the package of Qualcomm Dragonwing™ Q-7790, and 'SM8735' is printed on the package of Snapdragon 8s Gen 4 Mobile Platform.

11 Vendor Permissions and Relationship

This entropy source validation is “Reuse restricted to vendor”.

Snapdragon and Qualcomm branded products are products of Qualcomm Technologies, Inc. and/or its subsidiaries.