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

Hardware Version: 3.0.0

Document Version: 1.04

Document Date: 2023-11-02

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

Prepared by:
atsec information security Corporation
9130 Jollyville Rd, Suite 260
Austin, TX 78759
USA

©2023 Qualcomm Technologies, Inc. and/or its subsidiaries. All rights reserved.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Table of Contents

©2023 Qualcomm Technologies, Inc. and/or its subsidiaries. All rights reserved.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

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.

Table 1: Operational environment and versions.

Hardware Version	Hardware Platform
3.0.0	Qualcomm QCM6490
3.0.0	Qualcomm QCS6490

2 Security Boundary

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

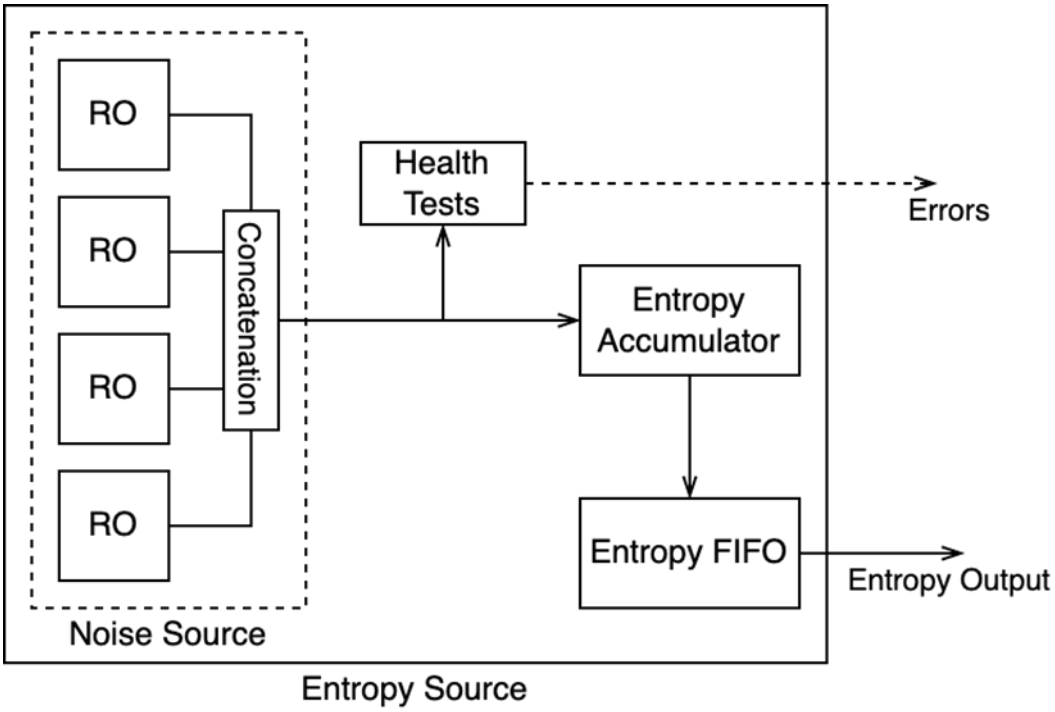

Figure 1: Block diagram of the entropy source.

The entropy source boundary contains the following components:

- The physical noise source.
- The SP 800-90B health tests.
- The Entropy Accumulator.

©2023 Qualcomm Technologies, Inc. and/or its subsidiaries. All rights reserved.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

- 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 environment of the SoC, and thus of the TRNG, is as follows:

- Temperature Range of [-30°C, 95°C]
- Voltage Range of [0.47V, 1.027V]

4 Configuration Settings

The TRNG has no operator-configurable or controllable 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 circuity 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 in commercial off the shelf mobile device utilizing production grade commercially available components and that the mobile device enclosure surrounds the TRNG.

6 Conceptual Interfaces

The TRNG provides its entropy output interface (the GetEntropy() interface) to a SP 800-90A compliant DRBG running on the same platform. In the production environment, there is no interface to access the entropy source output directly for an arbitrary user but to the attached DRBG.

7 Min-Entropy Rate

The H value is 0.420625 per 4-bit sample, which is the sum of the assessed ring oscillator entropies.

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. To recover from a permanent error state, the operator must explicitly reset 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 test at following conditions:

©2023 Qualcomm Technologies, Inc. and/or its subsidiaries. All rights reserved.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

- Start-up tests.
    - Performed after start-up, reboot, or reset.
    - Performed before the first use of the entropy source.
    - consist of both RCT and APT runs 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.
- Continuous tests.
    - consist of RCT, APT and Health Monitoring runs over 4-bit samples.
    - APT has a window-size of 512 samples.
- On-demand tests.
    - performed by rebooting the hardware platform, initiating the previously mentioned start-up tests.

9 Maintenance

The TRNG has no maintenance requirements.

10 Required Testing

In normal operation, an arbitrary user does not have access to the output of the TRNG but the attached DRBG, 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.

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

©2023 Qualcomm Technologies, Inc. and/or its subsidiaries. All rights reserved.

This document can be reproduced and distributed only whole and intact, including this copyright notice.