SP 800-90B Non-Proprietary Public Use Document for IBM Power10 RNG

Entropy Source Version: 1.0

Document Version: 1.1

Document Date: 2023-12-07

Prepared by:

atsec information security corporation

9130 Jollyville Road, Suite 260

Austin, TX 78759

www.atsec.com

Table of Contents

1. Description

The IBM Power10 RNG is a physical entropy source that resides on the Power10 Microprocessor. The noise generation of this entropy source is based upon the principle of Ring Oscillators. The noise source was tested under the assumption that its output is non-IID. The entropy source was tested on the operational environment ranges listed in Table 1 and thus the entropy source is certified only for those operational environments and specified ranges.

Table 1: Operational Environments

Entropy Source Name	**Operational Environment**
IBM Power10 RNG	Power10 Microprocessor Frequency Range: 2000MHz, to 4400MHz OE Operating temperature range: 15°C to 95°C RNG Operating temperature range: 15°C to 75°C Voltage range: 0.60V to 1.2V *Note: The OE temperature range is wider than that of the RNG. However, even if the OE temperature exceeds that of the RNG range, the RNG temperature will remain within its range, under standard operating conditions.*

2. Security Boundary

The Power10 RNG security boundary corresponds to the RNG components implemented on the Power10 Microprocessor.

Figure 1 depicts the security boundary of the entropy source and the components therein, such as Ring Oscillator Blocks, Noise Source and Health Tests. There are two Ring Oscillator (RO) blocks that act independently, with the 64-bit output of each block alternating with the 64-bit output of the other block. The raw noise samples of a given block are passed to the health tests. If the health tests fail, the data is discarded. If the health tests pass, the output of the healthy 64-bit samples will be provided to the DARN instruction.

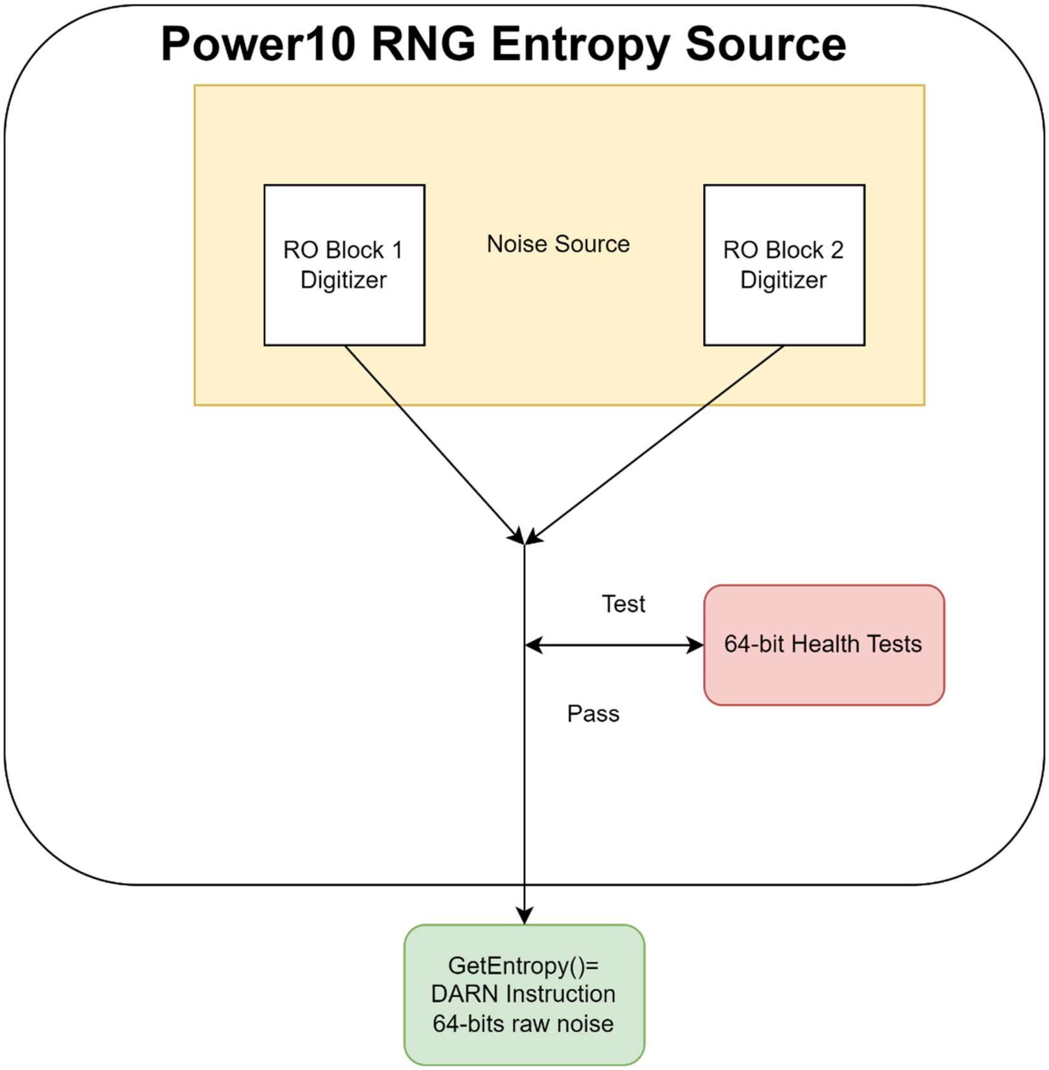

Figure 1: Security boundary of the Power10 RNG entropy source.

3. Operating Conditions

The operating conditions of the entropy source RNG are different than those of the Power10 Microprocess on which it resides, as specified in Table 1.

4. Configuration Settings

The entropy source does not have any user-configurable parameters or settings.

5. Physical Security Mechanisms

The noise source is physical in nature and so it inherits the physical security mechanisms of the Power10 Microprocessor that it resides in.

6. Conceptual Interfaces

The output of the entropy source is 64-bits in length, and produces at least 32-bits of entropy. The output is provided from the entropy source by calling the DARN instruction which returns 64-bits of healthy entropy data to the caller. The DARN instruction corresponds to both the GetNoise() and GetEntropy() interfaces.

7. Min-Entropy Rate

$H_{submitter}$ = 32 bits per 64-bit sample or equivalently 0.5 bits per 1-bit.

8. Health Tests

There are two RO blocks that are independent of each other and whose outputs are passed to the health tests. The outputs of each block are independently tested and if an RO block's output fails a health test, that RO block is disconnected and prevented from producing any further output. If the health tests pass, then the healthy 64-bits of raw noise data are passed as output to the DARN instruction.

The entropy source implements the following continuous health tests:

- Repetition Count Test conforming to SP 800-90B section 4.4.1:
    - $H = 32$ bits of entropy per 64-bit sample.
    - alpha value: $\alpha = 2^{-40}$.
    - Cutoff value: $C = 3$.
- Adaptive Proportion test conforming to SP 800-90B section 4.4.2:
    - $W = 512$.
    - $H = 32$ bits of entropy per 64-bit sample.
    - alpha value: $\alpha = 2^{-40}$.
    - Cutoff value: $C = 51$.
- Sample Rate Test – counts number of times a bit value changes when compared to the next bit:
    - $H = 0.5$ bits per 1-bit sample.
    - $W = 64000$ bits.
    - Minimum Threshold 28,000[1] bits.
    - Maximum Threshold 36,000 bits.
- Bias Test – counts number of 0s and 1s:
    - $W = 512$.
    - Minimum Threshold 100[2] bits.
    - Maximum Threshold 415 bits.

The startup tests run the four continuous tests: RCT, APT, Samples Rate Test, Bias Test.

[1] Thresholds are used to indicate a Fail event

[2] Thresholds are used to indicate a Fail event

The Failure Conditions are:

a) RCT failure - discards failed data. The result is a Fail event.

b) APT failure – discards failed data. Three failures in a 1-hour period results in a Fail event.

c) Sample Rate Test – discards failed data. If either threshold is surpassed, results in a Fail event.

d) Bias Rate Test – discards failed data. If either threshold is surpassed, results in a Fail event.

On-demand health tests are run by powering the Power10 RNG off and on. This operation will then trigger the startup tests.

Whenever health tests fail, there are three failure bits that can be set:

1. RNG0 noise source failed.
2. RNG1 noise source failed.
3. RNG recoverable error (e.g., a soft error).

9. Maintenance

There are no maintenance requirements applicable to this entropy source, except that if there is a Fail event, the entropy source needs to be rebooted.

10. Required Testing

To test the entropy source, 64-bit samples must be collected using the DARN instruction that is capable of accessing the raw noise interface of the entropy source.

Raw noise data samples consisting of at least 1,000,000 64-bit samples must be collected from the operational environment at its normal operating conditions, mapped down to 8-bit samples and processed by the SP 800-90B entropy tool that is provided by NIST. The expected min-entropy rate must approach the one in Section 7

Restart data must be collected at normal operating conditions through the raw noise source interface using the DARN instruction, following the restart procedure specified in SP 800-90B (i.e., 1,000 samples from 1,000 restarts each) and processed by the NIST SP 800-90B entropy tool. The minimum of the row-wise and column-wise entropy rate must be more than half that of the raw noise entropy rate.

11. Vendor Permissions and Relationship

The ESV certificate is “Reuse restricted to vendor”. Someone other than the vendor can only use the certificate with written and signed permission from the vendor’s point of contact (as indicated on the ESV certificate).