

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

**(With Conditioning Component)
Entropy Source Version: 1.0**

**Document Version: 1.8
Document Date: 2025-06-23**

IBM Corporation
1 New Orchard Road
Armonk, NY 10504-1722

Prepared by:
atsec information security corporation
4516 Seton Center Parkway, Suite 250
Austin, TX 78759
www.atsec.com

Table of Contents

1 DESCRIPTION 3

2 SECURITY BOUNDARY 3

3 OPERATING CONDITIONS 4

4 CONFIGURATION SETTINGS 5

5 PHYSICAL SECURITY MECHANISMS 5

6 CONCEPTUAL INTERFACES.....5

7 MIN-ENTROPY RATE 5

8 HEALTH TESTS 6

8.1 CONTINUOUS HEALTH TESTS..... 6

8.1.1 Repetition Count Test (RCT) 6

8.1.2 Adaptive Proportion Test (APT) 6

8.1.3 Sample Rate Test 6

8.1.4 Bias Test 7

8.2 STARTUP HEALTH TESTS 7

8.3 ON-DEMAND HEALTH TESTS 7

8.4 ERRORS..... 7

9 MAINTENANCE 8

10 USER VERIFICATION 8

11 VENDOR PERMISSIONS AND RELATIONSHIP 8

1 Description

The information about the entropy source described in this document is contained in Table 1.

Table 1: Entropy source and operational environment information.

Characteristic	Description
Entropy source name	Power10 RNG
Standard, IGs	SP800-90B (2018) IG D.J, IG D.K, IG D.O (April 18, 2025)
Entropy category	Physical (P)
Entropy source version	1.0
Operational environment	Power10 Power11
Embodiment	Single chip

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.

2 Security Boundary

The Security Boundary of the entropy source is depicted in Figure 1.

There are two Ring Oscillator (RO) macros (rng0 and rng1) that act independently, wherein the 64-bit output of one macro alternates with the 64-bit output of the other macro as the actual output of the noise source. The raw noise samples are passed to the health tests. If the health tests fail, the data is discarded. If the health tests pass, the noise data continues to the non-vetted conditioning component. The conditioning component then outputs 64-bits of conditioned data, which is the output of the entropy source.

Power10 RNG Entropy Source

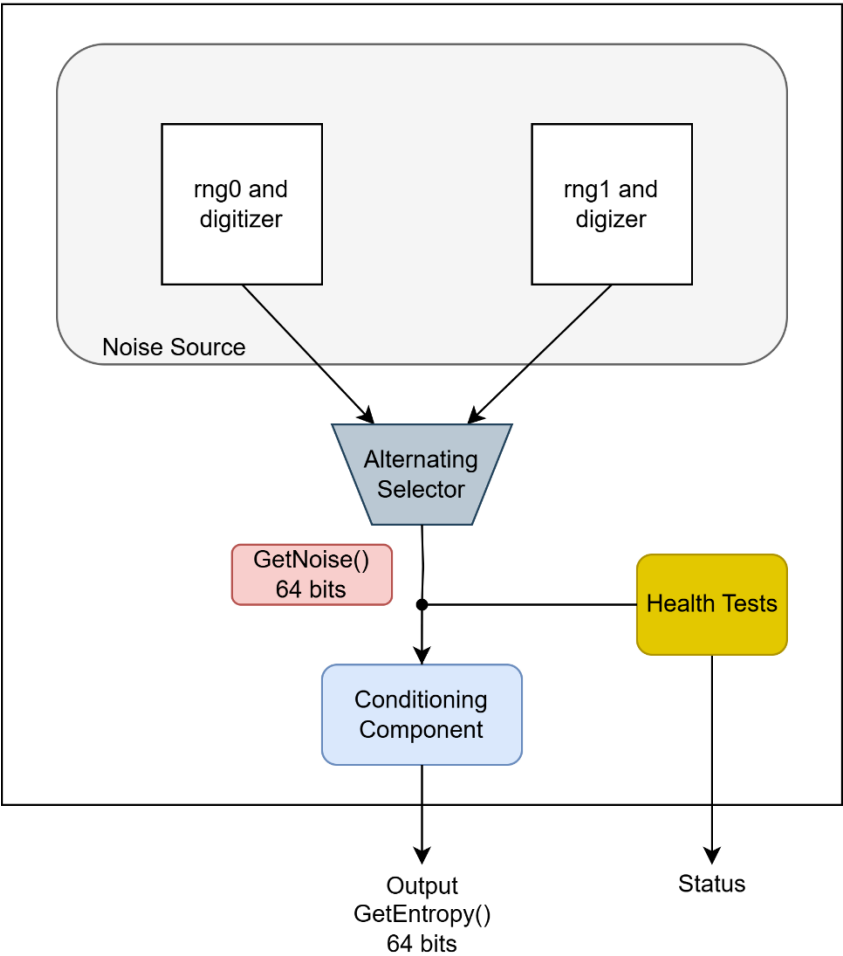


Figure 1: Security boundary.

3 Operating Conditions

The entropy source operating conditions are provided in Table 2:

Table 2: Operating conditions.

OE Name	Operating Conditions
Power10	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 <i>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.</i>
Power11	Power11 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 <i>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.</i>

4 Configuration Settings

The operator of the entropy source does not have the ability to modify any of the entropy source configuration settings.

5 Physical Security Mechanisms

The entropy source resides within the operational environments identified in Table 1, characterized as multi-chip standalone enclosed in an opaque package. The packaging of the chip is production grade and cannot be removed or penetrated without causing serious damage to the chip.

6 Conceptual Interfaces

There are three conceptual interfaces as shown in Figure 1:

- GetNoise(): outputs raw noise data. This interface is not available in the production version of the entropy source.
- GetEntropy(): outputs conditioned data from the non-vetted conditioning component, which is the actual output of the entropy source.
- Status: reports status of health tests (pass or fail).

7 Min-Entropy Rate

The entropy source provides min-entropy rate of 0.5 bit/bit at its output, or 32 bits per 64-bit output.

8 Health Tests

There are two RO macros that are independent of each other and whose outputs are passed to the health tests. The outputs of each macro are independently tested and if an RO macro's output fails a health test, that RO macro is disconnected and prevented from producing any further output. If the health tests pass, then the 64 bits of raw noise data are transferred to the conditioning component.

The entropy source implements the following continuous health tests:

- Continuous health tests.
- Startup health tests.
- On-demand health tests.

8.1 Continuous Health Tests

8.1.1 Repetition Count Test (RCT)

The entropy source implements the RCT as specified in SP 800-90B.

The parameters for the health tests are given in Table 3.

Table 3: Parameters for RCT.

Parameter	Value
Sample size	64 bits
Cut off	3
Alpha	2^{-40}
Entropy H	32 bits

8.1.2 Adaptive Proportion Test (APT)

The entropy source implements the APT as specified in SP 800-90B.

The parameters for the health tests are given in Table 3.

Table 4: Parameters for APT.

Parameter	Value
Sample size	64 bits
Cut off	51
Alpha	2^{-40}
Entropy H	32 bits
Window Size	512

8.1.3 Sample Rate Test

The custom sample rate test counts number of times a bit value changes when compared to the next bit.

The parameters for the health tests are given in Table 3. The thresholds are used to detect a fail event.

Table 5: Parameters for Sample Rate test.

Parameter	Value
Sample size	64 bits
Minimum threshold	28000 bits
Maximum threshold	36000 bits
Entropy H	32 bits
Window Size	64000 bits

8.1.4 Bias Test

The custom bias test counts number of 0s and 1s.

The parameters for the health tests are given in Table 3. The thresholds are used to detect a fail event.

Table 6: Parameters for Sample Rate test.

Parameter	Value
Sample size	64 bits
Minimum threshold	100 bits
Maximum threshold	415 bits
Window Size	512 bits

8.2 Startup Health Tests

The startup health tests are executed automatically after a reset or power-up. During startup, the health test unit collects millions of samples of raw data (far exceeding the minimum 1024 samples) and performs the continuous health tests on this data. The collected data samples are available for use if the health tests pass.

8.3 On-Demand Health Tests

The on-demand health tests may be invoked by resetting the entropy source, which will automatically invoke the startup health tests.

8.4 Errors

Whenever health tests fail, there are three failure bits that can be set, indicated from the status interface:

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 User Verification

To test the entropy source, raw noise data samples consisting of at least 1,000,000 64-bit samples must be collected from GetNoise() interface at 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 be compatible with the one in Section 7.

Restart data must be collected at normal operating conditions through the GetNoise() interface, 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.

For conditioned output assessment, 1,000,000 64-bit conditioned data samples must be collected from the output of the entropy source and assessed by the NIST SP 800-90B entropy tool. The entropy rate must approach the one in Section 7.

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).