SP 800-90B Non-Proprietary Public Use Document for IBM Capri ASIC Entropy Source

Document Version: 1.0

Document Date: 2022/11/01

Hardware Versions/Part Numbers: 02WP146, 02WP147

Firmware Version: 8.0.37z

IBM

2455 South Rd

Poughkeepsie, NY 12601

Prepared by:

atsec information security Corporation

9130 Jollyville Rd, Suite 260

Austin, TX 78759

Table of Contents

1 Description

The IBM Capri ASIC Entropy Source with hardware versions 02WP146, 02WP147 and firmware version 8.0.37z is a physical entropy source. The creation of entropy in the noise source within this entropy source is based upon the principles of variations of the oscillating period of ring oscillators. The entropy source meets all of the requirements of SP 800-90B and the associated FIPS 140-3 IGs D.J, D.K and D.O.

The entropy source was tested on the configurations listed in Table 1.

Table 1: Operational environments and versions.

ASIC #	Component Version
IBM Capri ASIC 02WP146/02WP147	Hardware Versions/Part Numbers: 02WP146 and 02WP147 Firmware: 8.0.37z

The entropy source is identical for both ASICs and the only different characteristic between the two is that they run at slightly different power bins determined during manufacturing of the ASIC. The Capri ASIC (02WP146) is Low Power and the Capri ASIC (02WP147) is Standard Power. See Section 3 for details on the operating conditions.

The noise source was tested under the assumption that its output is non-IID.

2 Security Boundary

Figure 1 shows the high-level design of the entropy source. The raw noise source consists of ring oscillators whose digitized outputs are XORed and sent to one entropy pool. The health tests apply to the noise samples while they are being fed to the entropy pool. If the health tests pass, the entropy pool is then filled with noise data.

Upon requests for entropy, and only when the entropy pool is completely filled with noise data, the entire contents of the entropy pool is input to the SHA2-512 vetted conditioning function. The output of the conditioning component (512-bit length), which is the output of the entropy source, contains 512 bits of entropy.

The conditioning component used for this design was tested with CAVP. The algorithm testing was conducted for the part numbers listed in Table 1 separately, even though the actual entropy source and conditioning component implementation are essentially the same in those two part numbers. The algorithm certificate numbers are:

- Capri ASIC RNG (02WP147): Certificate C1248
- Capri ASIC RNG (02WP146): Certificate C1247

If the health tests fail, then the noise data is discarded, the entropy source halts without outputting any data, and a failure code is returned to the caller (Section 6).

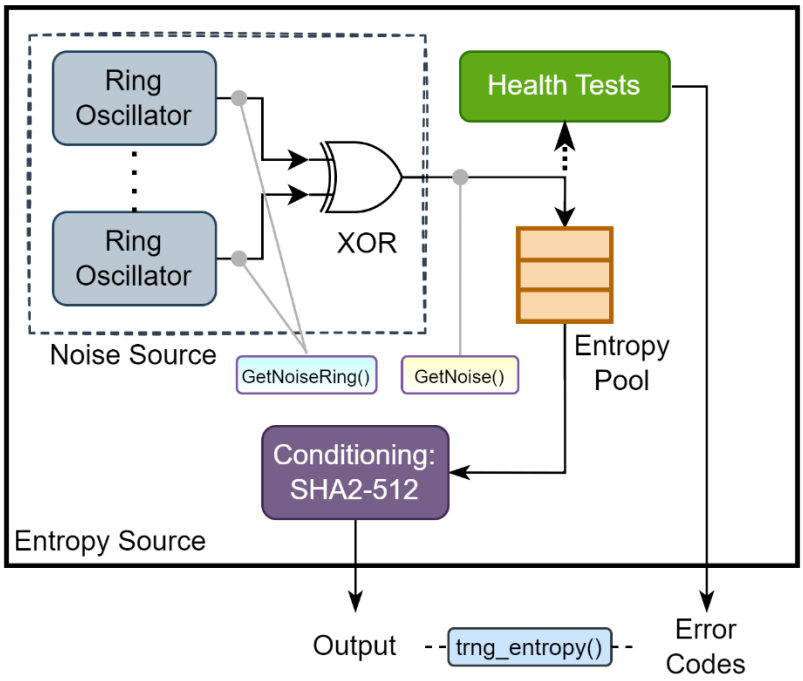

Figure 1: Security boundary of the entropy source.

3 Operating Conditions

The operating temperature range for the ASICs and the entropy source is 5 °C to 40 °C.

The ASIC chips come from the same die and are fabricated on the same wafer board. The ASIC voltages values vary slightly due to ordinary manufacturing process, but those voltages are still within the defined normal operating conditions. There are two voltages of interest: VDD, the voltage drain; and VCS, the voltage control. The operating ranges of each are:

- VDD: 0.833 V to 0.93 V.
- VCS: 0.943 V to 1.021 V.

The voltages are divided into 16 bins during manufacturing. The ASIC is assigned a part number either to the Low Power category (02WP146) or Standard Power category (02WP147) based on a complex analysis of the binning procedure. The part numbers still contain the exact same entropy source design, and both operate within the normal operating conditions for voltage and temperature.

Within these operating condition ranges, the entropy source will operate normally.

4 Configuration Settings

There are no configuration settings for the entropy source that are available to the operator.

5 Physical Security Mechanisms

The Capri ASIC containing the entropy source is implemented in a FIPS validated cryptographic module which is validated at FIPS Security Level 4 and includes tamper response zeroization. This is triggered by the module hardware in response to tamper attempts. In the event of tamper, the cryptographic module stops operating and therefore, so does the entropy source.

6 Conceptual Interfaces

The entropy source provides the following entropy interfaces (Figure 1):

a. trng_entropy(): requests entropy from the entropy source and returns status from the entropy source and result code from the call.

b. GetNoiseRing(): collects noise data directly from a ring oscillator. This interface is not available to an operator of the entropy source and can only be enabled by the vendor for testing purposes.

c. GetNoise(): collects noise data directly from the output of the noise source, which is the XOR of groups of ring oscillators. This interface is not available to an operator of the entropy source and can only be enabled by the vendor for testing purposes.

The trng_entropy() interface returns codes to indicate whether the request for entropy was successful, and error status codes otherwise. Table 2 shows the return codes, the reason for the return, and the behavior of the entropy source upon the return of those codes.

Table 2: Error codes.

Return Code	Reason Code	Entropy Source Behavior
SUCCESS,0	Requested entropy data returned	Wait for new requests
ERROR_RANDOM_NUMBER,975	0x185 Error reading entropy pool	Immediate halt
ERROR_RANDOM_NUMBER,974	0x185 Repetition Count Limit hit or Minimum Entropy Test failed	Immediate halt
ERROR_RANDOM_NUMBER,979	0x185 Error in Continuous testing (Repeated data)	Immediate halt
ERROR_RANDOM_NUMBER,978	0x185 Error in Continuous testing (Repeated data)	Immediate halt
ERROR_RANDOM_NUMBER,977	0x185 Error in Continuous testing (Repeated data)	Immediate halt
ERROR_RANDOM_NUMBER,976	0x185 Error in Continuous testing (Repeated data)	Immediate halt
ERROR_RANDOM_NUMBER, 0x80000000	0x185 Error in RN processing, HT_error	Immediate halt
ERROR_RANDOM_NUMBER, 0x40000000	0x185 Error in RN processing, Invalid command	Immediate halt
ERROR_RANDOM_NUMBER, 0x20000000	0x185 Error in RN processing, Invalid command length	Immediate halt
ERROR_RANDOM_NUMBER, 0x10000000	0x185 Error in RN processing, Invalid reseed counter	Immediate halt
ERROR_RANDOM_NUMBER, 0x08000000	0x185 Error in RN processing, Invalid user length	Immediate halt
ERROR_RANDOM_NUMBER, 0x04000000	0x185 Error in RN processing, Invalid conditioned entropy	Immediate halt

Return Code	Reason Code	Entropy Source Behavior
ERROR_RANDOM_NUMBER, 0x02000000	0x185 Error in RN processing, Invalid Unconditioned entropy	Immediate halt
ERROR_RANDOM_NUMBER, 0x01000000	0x185 Error in RN processing, Invalid user entropy	Immediate halt
ERROR_RANDOM_NUMBER, 0x00800000	0x185 Error in RN processing, Invalid Fmax value	Immediate halt
ERROR_RANDOM_NUMBER, 0x00400000	0x185 Error in RN processing, Invalid Drain value	Immediate halt
ERROR_RANDOM_NUMBER, 0x00200000	0x185 Error in RN processing, Invalid Requested bytes	Immediate halt
ERROR_RANDOM_NUMBER, 0x00100000	0x185 Error in RN processing, Invalid characterization requested bytes	Immediate halt

In case any error is found during operation, such as health tests errors, the entropy source will indicate its code through the return status of the function. The entropy source will then not return any entropy data and will halt further operation. The caller must attempt to reset or reboot the entropy source or consider permanent failure.

7 Min-Entropy Rate

For this entropy source, $H_{submitter} = 1.0\ bit/byte$. The noise source sample size is 8 bits or 1 byte.

The entropy source provides an output of 512 bits. This output provides 512 bits of entropy, or 1 bit/bit of entropy.

8 Health Tests

IBM has implemented the following continuous health tests:

- Repetition Count Test conforming to SP 800-90B section 4.4.1.
  - $H = 1$ bit of entropy per 8-bit sample.
  - alpha value of $\alpha = 2^{-20}$.
  - Cutoff value $C = 21$.
- Adaptive Proportion test conforming to SP 800-90B section 4.4.2.
  - $W = 512$.
  - $H = 1$ bit of entropy per 8-bit sample
  - alpha value of $\alpha = 2^{-20}$.
  - Cutoff value $C = 311$.
- Min-entropy estimator health test.
  - This health test consists of computing the min-entropy over the entire contents of the entropy pool just before the contents are conditioned to create the output of the entropy source. If that min-entropy value falls below 2 bits/byte, then a permanent failure is signaled to the caller, and the entropy source halts operation.

The continuous health tests are applied to each new sample obtained from the noise source. Whenever a failure is detected during the health testing, entropy data is not returned to the caller; instead, a failure code is returned to enable the caller to determine the reason for the failure (Table 2). The entropy source then halts and will refuse new requests for entropy. Upon return of the failure code, the caller shall attempt to reset or reboot the entropy source or return an error to its own operator.

Startup tests conduct the same set and parameters of the continuous health tests on 32,768 bits of noise data. The data is discarded after the startup tests complete successfully.

The entropy pool is refreshed between entropy requests (since the conditioning process consumes the whole entropy pool as input) so that the entropy pool always consists of fresh entropy data.

On-demand health tests of the noise source may be performed by rebooting the cryptographic module containing the entropy source, which results in the immediate execution of the start-up tests. Similarly, the data used for the on-demand health tests are discarded after successful completion.

9 Maintenance

There are no specific maintenance procedures for the entropy source outside of the ones required for the module to which the entropy source is bound.

10 Required Testing

To test the entropy source, raw data samples must be collected using a special characterization mode of the ASIC that allows access to the entropy samples via the enabled GetNoise() interface, before the conditioning function. This configuration of the ASIC is only available to IBM and is not available to the customer.

Raw noise data samples consisting of at least 1,000,000 bits must be collected at 25 °C 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 25 °C 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.