SP 800-90B Non-Proprietary Public Use Document for M1244265 Entropy Source Product Version: 1.0

Document Version: 1.1

Document Date: 2024-08-02

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

Table of Contents

1 Description

This document describes the design aspects of the M1244265 Entropy Source (referred to as the “entropy source” in the rest of this document). The noise generation of the entropy source is due to the jitter in the oscillation period of the ring oscillator which makes it a physical noise source. The entropy source was tested on the operational environments listed in Table 1 under the assumption that the entropy source's output is non-IID.

Table 1: Operational Environments.

HW Platform	Operating System	Processor
M1244265	N/A	N/A

2 Security Boundary

The entropy source boundary is show in Figure 1. The design is composed of the noise source (one single ring oscillator and digitization component), the health test control, and auxiliary components such as a shift register and two FIFO (First-In First-Out) queues to accumulate outputs and transform them into larger, concatenated blocks of bits. There is no conditioning component.

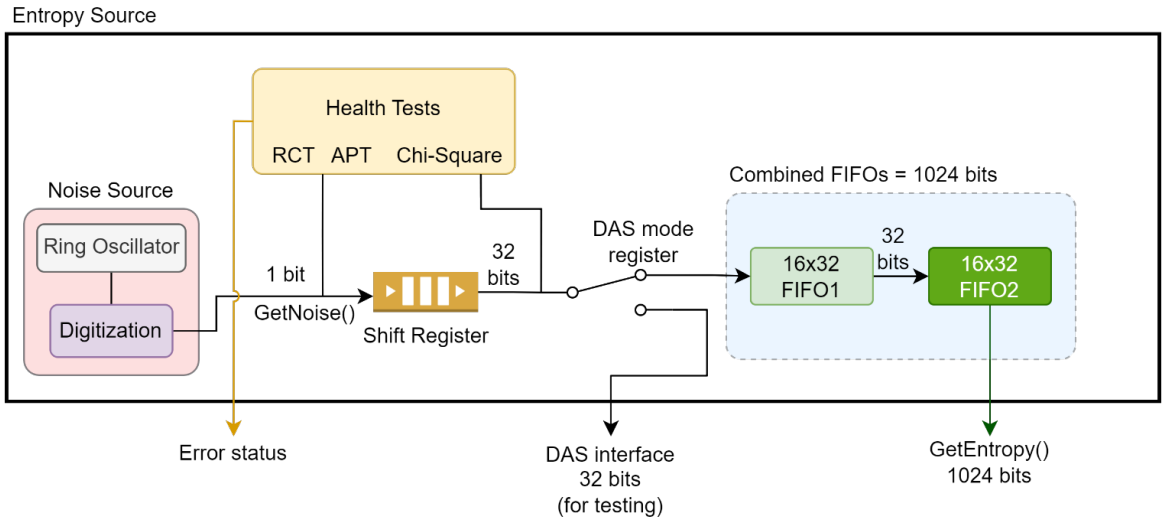

Figure 1 Entropy Source boundary.

3 Operating Conditions

Table 2 lists the operating conditions for the entropy source,

Table 2: Operating conditions.

Parameter	Value
Normal Operating Temperature	25°C
Nominal Operating Voltage	0.83 V
Operating Temperature Range	0°C to 105°C

Parameter	Value
Operating Voltage Range	0.83 V ±3%

4 Configuration Settings

The entropy source has no operator-configurable or controllable parameters.

5 Physical Security Mechanisms

The entropy source resides within the M1244265 chip, which is a single-chip enclosed in an opaque package. The package is production grade and cannot be removed or penetrated without causing serious damage to the chip. Therefore, the physical security of the entropy source relies on the physical protections provided by the chip.

6 Conceptual Interfaces

The GetEntropy() conceptual interface corresponds, to the output of the combined 1024-bit FIFO queue, wherein individual 1-bit samples from the noise source are stored. Thus, the output of the combined queue is composed of 1024 bits.

The GetNoise() conceptual interface is the direct output of the noise source. This interface is only available internally to the health test unit and shift register.

The error status interface provides information about health test failures to the caller.

7 Min-Entropy Rate

Min-entropy rate at the output of the entropy source is 0.5 bit per bit.

8 Health Tests

Following the NIST SP 800-90B requirements, the vendor has implemented the three sets of health tests in this product:

- Start-up tests -performed at power-on on 1024 samples.
- Continuous tests – run continuously on the data being generated.
- On-demand tests – can be invoked by entropy source reset.

The entropy source implements the continuous health tests as such:

- Repetition Count Test (RCT) with cut-off value of 51.
- Adaptive Proportion Test (APT) with cut-off value of 802.
- Chi-Square test with cut-off (χ^2) value of 269.5 and 15 degrees of freedom.

The error status interface provides status codes as shown in Table 3.

Table 3: Error codes.

Flag	Description
repcnt_fault_error	RCT failure
apt_fault_error	APT failure

Flag	Description
chisq_fault_error	Chi-square test failure

9 Maintenance

There are no requirements here.

10 Required Testing

The output of the entropy source is used to seed the DRBG running on the same operating environment and the user does not have access to the entropy source directly. Therefore, no explicit testing is required as it is handled by the entropy source health test.

11 Vendor Permissions and Relationship

The entropy source reuse is restricted to vendor.