SP 800-90B Non-Proprietary Public Use Document

TC58NC1137GTC/TC58NC1138GTC-0002 Entropy Source

Document Version 1.0.0

Hardware Version: 0001
Firmware Version: EntropyDriver-r73863

KIOXIA Corporation
1-21, Shibaura 3-chome
Minato-ku, Tokyo 108-0023
Japan

April 25, 2024

Revision History

Version	Change
1.0.0	Initial version

Table of Contents

Description 4
Security Boundary 4
Operating Conditions 5
Configuration Settings 5
Physical Security Mechanisms 5
Conceptual Interfaces 5
Min-Entropy Rate 6
Health Tests 6
Maintenance 6
Required Testing 6

Description

TC58NC1137GTC/ TC58NC1138GTC-0002 Entropy Source is a hardware implemented, physical noise source consisting of a fast ring oscillator and a slow ring oscillator which provides with no conditioned raw data. TC58NC1137GTC/ TC58NC1138GTC-0002 is a controller embedded in a Solid State Drive (SSD) and has a module that provide various security functions including random number generation (TC58NC1137GTC/TC58NC1138GTC CRPT module). The entropy source was tested by collecting data from multiple process, voltage, and temperature (PVT) operational conditions from implementation on a silicon substrate. The hardware noise source is claimed to produce non-IID outputs. Health tests are executed by firmware component of the TC58NC1137GTC/TC58NC1138GTC CRPT module which is loaded into the module. The firmware component provides the entropy output which passed the health tests to the DRBG algorithm. TC58NC1137GTC/TC58NC1138GTC-0002 Entropy Source is used embedded in SSDs and is not intended to be implemented in any other execution environment.

Security Boundary

Block diagram of the entropy source is shown below.

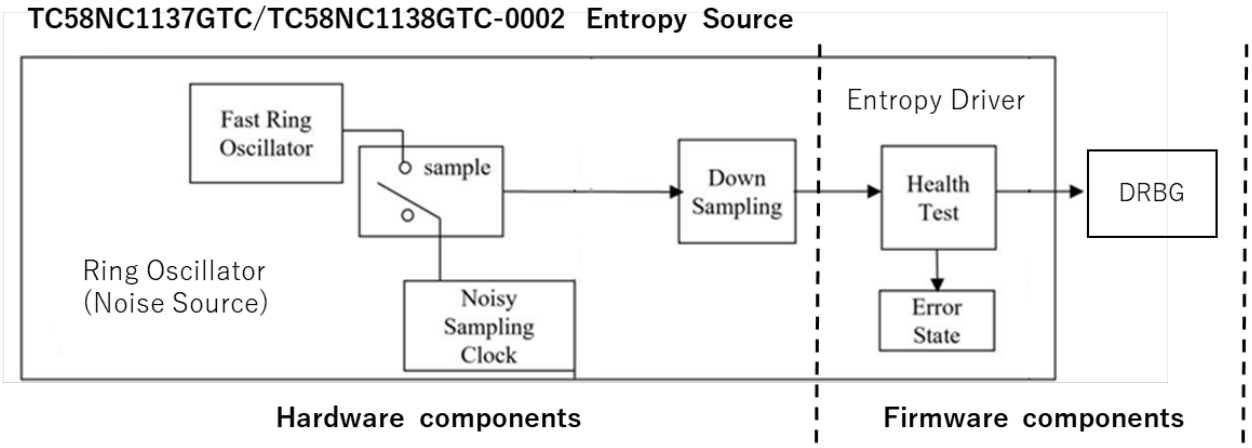


Figure 1. Block diagram of the Hardware Noise Source + Firmware components

The security boundary includes Hardware components such as ring oscillators and registers, as well as Firmware component which perform health tests in accordance with SP800-90B and access registers to change configuration (Entropy Driver). Direct access to the entropy source is only permitted to the firmware of the TC58NC1137GTC/TC58NC1138GTC CRPT module.
The fast ring oscillator and the slow ring oscillator (as Noisy Sampling Clock written in Figure1) are standalone and oscillate independently. The fast ring oscillator output is captured fixed interval rising edge of the slow ring oscillator, and the sampled result is reduced to a certain rate by Down Sampling block. Because the slow ring oscillator rising edge is affected by unpredictable jitter derived from the device noise, the jitter would randomly sample the fast oscillator output, whose samples are the random number source output.

The sampling data is input directly into the firmware components of Health test, which means that the Health tests is performed to the entropy output sampled from a ring oscillator which is not conditioned.

Operating Conditions

The entropy source was tested under several different PVT corners. Table 1 shows the environmental conditions range within which the entropy source operate correctly is guaranteed.

Table 1. Operational Conditions

Parameter	Condition	Description
Temperature (C)	Min: 0 , Typical: 25, Max: 70	Ambient temperature - Operating range of the embedded SSD
Voltage (V)	Min: 0.72, Typical: 0.80, Max: 0.88	Operating voltage

Configuration Settings

The entropy-relevant configuration settings are summarized in Table 2.

Table 2. Configuration Settings

Entropy-Relevant Parameters	Configurations
Fast Ring Oscillator Frequency	1,600 MHz
Slow Ring Oscillator Frequency	182 MHz
Size of the health testing block	1024 bits
False-positive probability of the health tests	2^{-40}
Cut-off value of the health tests	RPT = 60, APT = 744

Physical Security Mechanisms

The entropy source is hardware implemented to the TC58NC1137GTC/TC58NC1138GTC CRPT module. This module is enclosed in a single chip that is covered with opaque package which is used standard passivation techniques. Physical access to the internal components is impossible without forcing the package to open. In this case, it can be confirmed package damage as a tamper-evidence.

Conceptual Interfaces

In the Entropy Source, entropy output acquisition is performed at module's startup or random number generation (only when a reseeding is required). At these timings, the module's firmware requests entropy output (GetEntropy) and the Entropy Source stores the sampled data in the Data Out Reg (GetNoise). The firmware obtains these data up to 1024 bits for running the Health Tests. Entropy output is export to the firmware implemented DRBG algorithm, only if the Health Tests are passed.

Min-Entropy Rate

The Entropy Source provides 5.39 bits of entropy per 8 bits. This result indicates that the entropy rate is 690 bits per 1024 bits of sampled data. It is sufficient to generate 256 bits of strength keys with a SP800-90A compliant DRBG algorithm.

Health Tests

Table 3. Health Tests execution

Health tests Type	Testing condition
Start-up	Module's power-on
Continuous	Required to reseed from DRBG algorithm
On-demand	Any Module's power-off and reboot

When Health Tests are failed, the Entropy Source reports the error to the TC58NC1137GTC /TC58NC1138GTC CRPT module. The module receiving the result will transition to error state and cannot execute any security relevant command including entropy output acquisition. To recover from the error state, the module need to be rebooted and pass the Health Tests to be performed again.

Maintenance

No maintenance requirements for the entropy source.

Required Testing

TC58NC1137GTC/TC58NC1138GTC-0002 Entropy Source has been tested for case of continuous sampling and case of sampling across the module restarts to confirm an entropy rate must be near equal to or the defined min-entropy. In these tests, special test command is used to obtain entropy output that would normally be input to firmware implemented DRBG algorithm. An obtained entropy output data is processed with the SP800-90B tool and calculated Min-Entropy

rate. Moreover, in the restart sampling case the sanity test which confirm the restart sampling data is not be less than half of the entropy rate from continuous one is also performed.