SP 800-90B Non-Proprietary Public Use Document

Entropy Source NVS-RNG

Hardware Version: 1.0

Firmware Version: 1.0

Software Version: (N/A)

Document Version: 1.0

Prepared by:

Novachips Co., Ltd.

#510, 46 Dallaenae-ro, Sujeong-gu

Gyeonggi-do, 13449

Republic of Korea

Release Date: Jan 3rd, 2023

Change History

Report Version	Change Description	Date	Author
1.0	Initial Release	Jan 3rd, 2023	SJ Yoo

Distribution and Ownership

Novachips Co., Ltd has granted the authorization to distribute unmodified copies of this report. This report contains both NIST's IP (the entropy source design and the portions of the analysis which are described as originating from NIST documentation) and Novachips's IP (the portions of the analysis which are not described as originating from NIST documentation).

Table of Contents

• Description

The NVS-RNG (Hardware Version: 1.0 / Firmware Version: 1.0 / Software Version: N/A)) is hardware-based physical (ENT (P)) entropy source developed for SSD (Solid-State Drives) and other flash storage applications by utilizing NAND flash noisy bits. The entropy source is composed of a few major sections, which map to the conceptual components contained within an SP 800-90B entropy source. The NVS-RNG entropy source contains:

1. Flash memory cells (at least more than four silicon die chips) as a raw noise source.
2. Flash memory controller hardware to detect error bits and to run conditioning components.
3. Flash memory controller firmware to digitize noisy bits and to perform health tests.

The validation of NVS-RNG used Non-IID (independent and identically distributed) track, and multiple implementations are tested in different operation environments with varying different ranges of entropy-relevant parameters such as temperature, input voltage, clock speeds, Program/Erase cycle, and data retention factors within the industrial or military-grade SSD specification and 5 years warranty use.

Flash-based TRNG design already has been studied, validated, and proposed by the previous works[1] [2] [3]. The main idea of flash-based TRNG is digitizing non-deterministic noisy bits from flash cells by performing multiples of program and read operations with flash controller, so it requires two components to implement this design, flash memories as raw noise source component and the flash controller as digitizing/harvesting/conditioning component. Hence the boundary of NVS-RNG is limited to flash storage device or system which involves at least those two components, and SSD (solid-state drives) is the optimal reference application for this NVS-RNG design.

Using NVS-RNG in SSD applications has several advantages, compared to other hardware-based random number generators. First, plenty of flash memory cells are available in the SSDs as a noise source to achieve required target bandwidth. Second, the raw error bits from NAND are quantum-level noise, and the quality of the random bits will not be compromised at different temperature or by wear-out factors. Third, this design is independent from CPU, operating system, or IC design platform which makes it as an useful source of random seeds for IoT, bootloader, and other primary booting drives.

[1] Wang, Yinglei, Wing-kei Yu, Shuo Wu, Greg Malysa, G. Edward Suh, and Edwin C. Kan. "Flash memory for ubiquitous hardware security functions: True random number generation and device fingerprints." In 2012 IEEE Symposium on Security and Privacy, pp. 33-47. IEEE, 2012.

[2] Ray, Biswajit, and Aleksandar Milenković. "True random number generation using read noise of flash memory cells." IEEE Transactions on Electron Devices 65, no. 3 (2018): 963-969.

[3] Yan, Wei, Huifeng Zhu, Zhiyuan Yu, Fatemeh Tehranipoor, John Chandy, Ning Zhang, and Xuan Zhang. "Bit 2 rng: Leveraging bad-page initialized table with bit-error insertion for true random number generation in commodity flash memory." In 2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 91-101. IEEE, 2020.

- **Security Boundary**

The security boundary of NVS-RNG is limited to flash storage device or system which involves at least those two components, flash memories as raw noise source component and the flash controller as digitizing/harvesting/conditioning component, so the SSD(solid-state drives) is the optimal reference application for this NVS-RNG design. The security boundary of NVS-RNG is depicted in Figure 1.

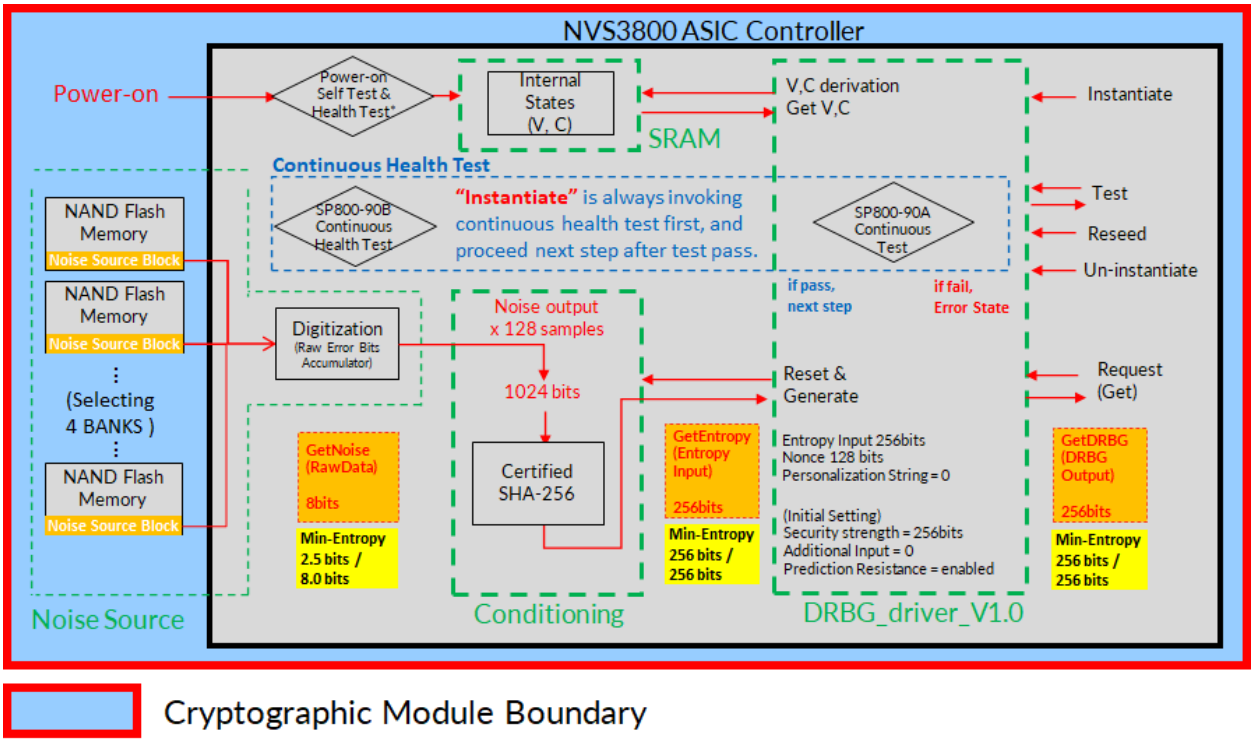

Figure 1. Entropy Source and Overall Block Design of SSD module

• Operating Conditions

The operating condition is described in Table 1.

<table>
<tr><th>Configuration Parameter</th><th>Value</th><th>Description</th></tr>
<tr><td>Temperature</td><td>-40 ~ +85° C</td><td>The entropy outputs are tested and verified from -40 to +85°C with stepping at each +10 °C.</td></tr>
<tr><td>Voltage</td><td>+3.1 ~ +3.5V
+4.5 ~ +5.5V
+10.8 ~ +13.2V</td><td>The input voltage of the module is various per below different form factors, but input voltage is consistent by regulating with power ICs.
M.2 FF : +3.3V with ranging +3.1 ~ +3.5V
2.5” SATA : +5.0V with ranging +4.5 ~ +5.5V
2.5” U.2 : +12V with ranging +10.8 ~ 13.2V</td></tr>
<tr><td>System Clock speed</td><td>200 ~ 266MHz</td><td rowspan="3">The modules are operating under various clock setting of system, NAND, and DRAM as below. (Note: Only NAND clock speed can be related with this RNG design, and RNG design are independent from the two other clock speed.)

<table><tr><th>SSD Module Part Number</th><th>System clock</th><th>NAND clock</th><th>DRAM Clock</th></tr><tr><td>NS361N500GCCR-1F</td><td>200MHz</td><td>200MHz</td><td>800MHz</td></tr><tr><td>NS371N04T0CC1-1F</td><td>266MHz</td><td>533MHz</td><td>533MHz</td></tr><tr><td>NS371N08T0CC0-1F</td><td>266MHz</td><td>533MHz</td><td>533MHz</td></tr><tr><td>NS371N10T0CC0-1F</td><td>266MHz</td><td>533MHz</td><td>533MHz</td></tr><tr><td>NS561N125GCM7-1F</td><td>222MHz</td><td>222MHz</td><td>666MHz</td></tr><tr><td>NS561N500GCE7-1F</td><td>240MHz</td><td>240MHz</td><td>480MHz</td></tr><tr><td>NS571N08T0CC0-1F</td><td>266MHz</td><td>533MHz</td><td>533MHz</td></tr></table></td></tr>
<tr><td>NAND Clock Speed</td><td>200 ~ 533MHz</td></tr>
<tr><td>DDR Clock Speed</td><td>480 ~ 800MHz</td></tr>
<tr><td>NAND Program/Erase cycle</td><td>1 ~ 3,000 cycles</td><td>Error bits from NAND flashes are known to be increasing as NAND P/E cycle increases, and this will also cause positive feedback (+) on min-entropy output result. The tested modules are less than 10 P/E cycles to measure min-entropy.</td></tr>
<tr><td>Data Retention factor</td><td>0 ~ 43,800 hours</td><td>Error bits from NAND flashes are known to be increasing as retention period increases, and this will also cause positive feedback (+) on min-entropy output result. The tested modules are less than 100 hours to measure min-entropy.</td></tr>
</table>

Table 1. Operating Conditions

- ## Configuration Settings

The security-relevant configuration settings (noise source output size, symbol width, conditioning output size, health test cutoff value) are fixed by developer, and the user does not require any additional configuration for the entropy source.

• Physical Security Mechanisms

The NVS-RNG entropy source operates within the physical protection of the device modules, and these devices would typically be capable of meeting FIPS-140-3 Level2 or Level3 physical security requirements without additional measures.

The NVS-RNG does not impose any physical security requirement beyond the nominal FIPS-140-3 requirements. Modules undergoing FIPS 140-3 validation that incorporate NVS-RNG into their boundary must fulfill the physical security requirements appropriate to the targeted module type and security level.

- ## Conceptual Interfaces

The conceptual interface inside of NVS-RNG is described in previous section, Security Boundary Figure 1, and the conceptual interface between the module and the host is described in Figure 3.

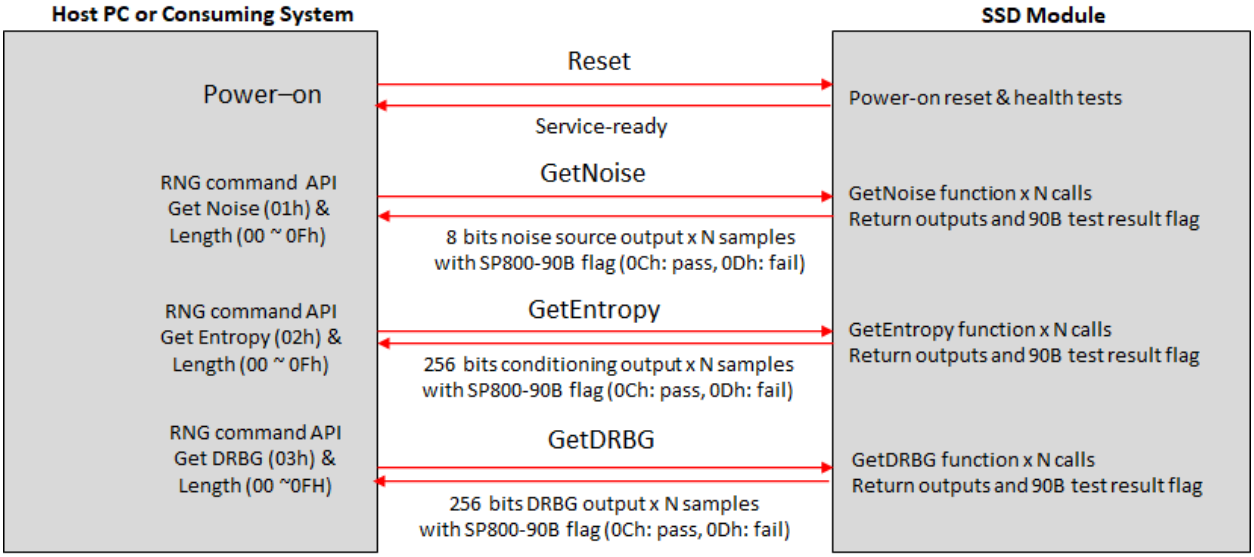

Figure 3. Conceptual Interface

NVS-RNG command guidance document and reference API can be available for the customer of Novachips SSD. This API is useful for the application where NIST-approved random seed is necessary for the cryptographic functions required in the software encryption layer, the preboot-authentication, or the embedded system.

More details on Error State and SP800-90B flag are described in the health tests section.

Please contact to sales representative or Novachips Sales team, if the customer needs to get the related the RNG command guidance document and reference codes.

- ## Min-Entropy Rate

The noise source has been validated in a broad range of operating environments (variant form factors, production lots, and conditions) since 2018. The lowest record of min-entropy of NIST non-IID testing is 2.580118 bits per 8 bits, and we're using 2.5 bits per 8 bits as H_submitter by rounding down to one decimal place.

Concatenated 128 samples of 8 bits noise source are provided to vetted conditioning component, and 256-bit entropy source output samples from the conditioning component have 256 bit min-entropy (full entropy). These outputs are provided to an SP800-90A compliant DRBG with a security strength of 256 bits

• Health Tests

Below are health test items performed by NVS-RNG.

- **SP800-90B Repetition Count test** is performed on noise source outputs at power-on and continuously before using RNG output, and the purpose of this test is to quickly detect catastrophic failures that cause the noise source to become “stuck” on a single output value for a long period time. The test fails if the noise source output is same value for consecutive (C: cutoff value) times. In this case, the module enters an Error state immediately.

  Min-entropy (H) : 2.5
  Acceptable false-positive probability (α) = 2^(-20)
  Cutoff value (C) : 1+(-LOG(α,2))/H = 9

- **SP800-90B Adaptive Proportion test** is performed on noise source outputs at power-on and continuously before using RNG output, and the purpose of this test is to detect a large loss of entropy that might occur as a result of some physical failure or environmental change affecting the noise source. The test fails if same value of noise source is counted over than (C: cutoff value) times within total (W-1) times output result. In this case, the module enters an Error state immediately.

  Min-entropy (H) : 2.5
  Window size (W) : 512 (non-binary data)
  Acceptable false-positive probability (α) = 2^(-20)
  Cutoff value (C) : 1+CRITBINOM(W, 2^(-H), 1- α) = 135

- **SP800-90A Known Answer Test** is performed on DRBG at power-on and continuously before using RNG output, and the purpose of this test is to make sure on all DRBG sub-functions are in order by determining if the calculated output equals the expected output (the known answer). The test fails if the calculated output does not equal the known answer. In this case, the module enters an Error state immediately.

- **FIPS-140-2/3 Continuous test** is performed on Entropy Input and DRBG output at power-on and continuously before using RNG output, and the purpose of this test is to prevent the catastrophic failures that overall RNG operation to become “stuck” on a single output value. The test fails if the 256 bits size output value is same with previous 256 bits output value. In this case, the module enters an Error state immediately.

The entropy source enters Soft Error State when it fails from SP800-90B repetition count or adaptive proportion test. Soft Error indicator and requirements to consuming system are:

- NVS-RNG keeps providing outputs with setting SP800-90B health test fail flag.
- NVS-RNG can go back to normal state mostly at the next power cycling after passing power-on health tests.
- The consuming system requires giving power cycling to NVS-RNG or inducing power reset of itself by sending soft error signal the user or the operator.

The entropy source module enters Hard Error State when it fails from SP800-90A or FIPS-140-2/3 continuous test. Hard Error indicator and requirements to consuming system are:

- NVS-RNG stops the operation immediately without providing any outputs.
- NVS-RNG will not go back to normal state at next power cycling, and this hard error state is permanent.
- The consuming system requires replacing NVS-RNG or inducing RMA process of itself by sending hard error signal to the user or the operator.

On-demand power-on and health test can be performed by giving power cycling or triggering equivalent hard reset command to the module.

- ## Maintenance

NVS-RNG does not require any other maintenance.

- ## Required Testing

The entropy source in Novachips SSD was tested by collecting outputs of noise source and conditioning component from seven different operating environments and processed with the SP800-90B tool. Raw and restart data of noise source and conditioning output was collected through vendor-specific ATA or NVM command interface available outside of test units. Test data was collected following the requirement of Section 3 of SP800-90B. All tested data was evaluated at a higher entropy than the defined entropy of the assessment, and all restart sanity checks were passed.

Health Tests described in section “Health Tests” constantly check the validity of the noise source. Therefore, no further testing is required by the consuming application.

- ## Vendor Permission and Relationship

The usage of this entropy source is not resticted to Novachips Co., Ltd. The customer who owns Novachips SSD which contains NVS-RNG inside of the module can access the entropy source directly via vendor-specific ATA or NVM command. Please contact sales@novachips.com for more information.

