SP 800-90B Non-Proprietary Public Use Document
iStorage® Entropy Source
Document Version 1.0
iStorage® Limited
August 26th, 2024

Revision History

Document Version	Date	Change Description
V1.0	08/26/2024	Initial Release

Table of Contents

Description

iStorage® Entropy Source is an SRAM PUF-based entropy source. This is a physical (P) entropy source consisting of an integrated noise source, health tests and a conditioning function. The considered entropy source is certified under the January 2018 version of NIST Special Publication 800-90B and the March 26, 2024 version of the FIPS 140-3 Implementation Guidance.

Table 1 describes the evaluated version of the entropy source.

Table 1: Evaluated Version

Name	Version
iStorage® Entropy Source	1.0

Table 2 describes the operating environment for the entropy source.

Table 2: Operating Environment

Operating Environment
IS24781

Security Boundary

The security boundary of the entropy source includes the digital noise source, the health tests, and the conditioning component. Figure 1 shows the security boundary of the iStorage® Entropy Source.

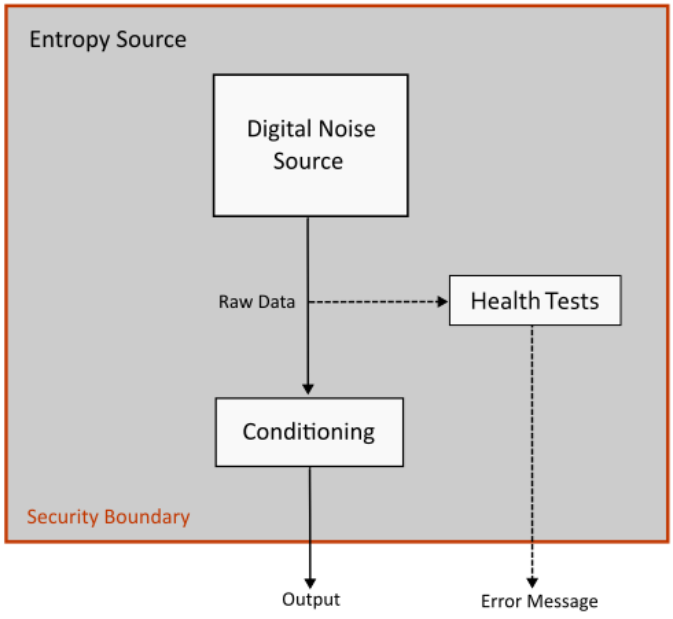

Figure 1: Security Boundary of the iStorage® Entropy Source

Operating Conditions

This section has been omitted, as the entropy source is restricted to the vendor.

Configuration Settings

The entropy source is fully and statically preconfigured and does not require configuration.

Physical Security Mechanisms

This section has been omitted, as the entropy source is restricted to the vendor. Refer to the iStorage® Security Policy for physical security mechanisms.

Conceptual Interfaces

Interface	**Function**
GetNoise	iid_zrng_ltm_get_noise() (test interface to access noise source for entropy validation)
GetEntropy	Only available internally in the product for instantiating the embedded DRBG
HealthTest	All implemented health tests are executed as part of a call to the iid_zrng_initialize() function which starts the entropy source and executes the start-up tests. On-demand health tests are supported by repowering the entropy source and rerunning the start-up tests in this manner.

Min-Entropy Rate

The entropy source, post-conditioning, provides full-entropy outputs.

Health Tests

Table 3 lists the health tests implemented in the entropy source. All health tests are performed at start-up. Since the entropy source is of a 'one-shot' type (only evaluated once per power-cycle of the device), start-up and continuous health tests are equivalent.

All health tests are executed as part of the product's initialization process, triggered by calling the iid_zrng_initialize() function.

Table 3: Health Tests

Health test	**Tests**
PUF_RCT: Repetition count test	Default RCT on the noise sample bits
PUF_APT: Adaptive proportion test	Default APT on the noise sample bits

PUF_NRCT: Nibble-based RCT	Modified RCT for nibbles (quadruplets) of noise sample bits
PUF_NPT: Nibble-based proportion test	Modified (non-adaptive) proportion test for nibbles of noise sample bits
PUF_BRCT: Byte-based RCT	Modified RCT for bytes of noise sample bits
PUF_BAPT: Byte-based APT	Modified APT for bytes of noise sample bits
PUF_WRCT: Word-based RCT	Modified RCT for words (32-bit) of noise sample bits

All health tests have their own failure return code for the iid_zrng_initialize() function.

Known failure modes are:

- Device power-up happened under extreme outlier conditions, leading to extreme bias (and low noise) in the noise source
- Illegal process overwrites original noise samples in the physical SRAM, leading to structured (e.g., zeroized) noise samples

All implemented health tests target one or more variations of these known failure modes. A failing health test always requires at least a repower of the device. Depending on the failure mode, the power-up process and conditions of the device need to be improved, and processes illegally accessing the noise source SRAM should be removed.

Maintenance

The nature of the noise source only allows for the generation of a limited amount of entropy, sufficient for instantiating the coupled DRBG once. Further use of the entropy source requires a repower of the device.

Required Testing

iStorage® Entropy Source provides a test interface for accessing the noise source (iid_zrng_ltm_get_noise()) intended for entropy testing. Data collected through this interface can be compiled into data sets which can be processed by the SP800-90B tool. The entropy estimates produced by the tool should (for the sequential datasets) be near equal to, or exceeding, the defined min-entropy rate of the noise source (3.0%).

It is noted that the nature of the SRAM PUF-based noise source is such that the produced noise samples will with high likelihood fail the sanity check performed on the restart data set generated from the noise samples. The reason for this is that the noise source will generate several samples which are stable over restarts (in addition to many samples which are unstable). The restart test sanity check fails because of these stable samples. However, there is strong argumentation that the unstable noise samples contribute more than sufficient entropy for generating a full-entropy output post-conditioning. The failure of the restart test is not a critical issue, as this is allowed under FIPS IG 140-3 IG D.J. additional comment 4.