SP 800-90B Non-Proprietary Public Use Document

EIP130 TRNG Entropy Source [ES]

Hardware Version 4.1.0

Document Version 1.0

September, 2023

Prepared by:

atsec information security corporation
9130 Jollyville Road, Suite 260
Austin, TX 78759
www.atsec.com

Prepared for:

Rambus Inc.
North First Street, Suite 100
San Jose, CA 95134
United States of America
https://www.rambus.com

Table of Contents

1. Description

The EIP130 TRNG Entropy Source (ES) (also called "ES" in this document) utilizes the EIP-76A IP which is a physical entropy source built upon Free Running Oscillators (FROs). The EIP130 TRNG hardware version is 4.1.0.

The EIP130 TRNG ES is tested on VaultIP and configured in a Xilinx Zynq XC7Z045 Field-Programmable Gate Array (FPGA) embedded in a Xilinx ZC706 base board. The ES raw data samples are tested using the non-IID track to estimate the min-entropy.

2. Security Boundary

The ES boundary is defined by the blue box in Figure 1. The ES boundary contains the following components: physical noise source (eight FROs), Digital logic, SP800-90B health tests and a SHA-256 vetted conditioning function.

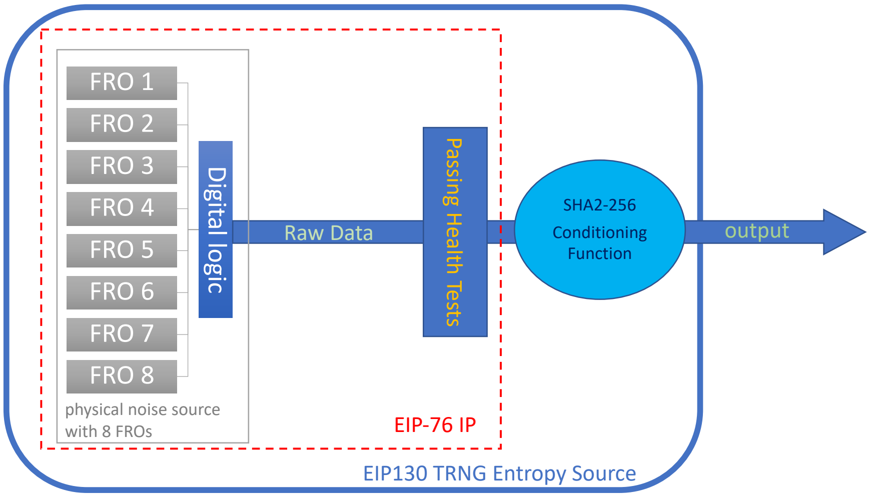

Figure 1: Block Diagram of the ES with the FRO physical noise source

3. Operating Conditions

The entropy source configured in the Xilinx Zynq XC7Z045 FPGA is claimed to operate correctly under the inherent operating conditions of the FPGA:

- temperature range [0°C; 85°C].
- voltage range [1.2V; 3.3V].

4. Configuration Settings

For the EIP130 TRNG ES tested in the FPGA, the operator does not have the ability to modify the ES configuration settings.

5. Physical Security Mechanisms

The EIP130 TRNG ES is configured in the FPGA. The FPGA is a single chip that includes standard passivation provided by the dielectric film at the silicon die level. The integrated heat spreader (IHS) serves as a protective shell around the processing silicon, a pathway for heat to be exchanged between the SoC and SoC cooler. The IHS lid and the substrate with solder ball grid array provide opacity in the visible spectrum and prevent any access to the interior of the chip.

6. Conceptual Interfaces

The entropy source provides the following interfaces:

- The *TRNG Get Random Number* service provides a random number from the ES. This is the function from the entropy source that shall be used to request entropy data. The entropy gathering logic creates 256 bits per invocation. This interface corresponds to the GetEntropy() conceptual interface from SP800-90B. It is possible to provide a specific parameter to this service ('RawKey' field of input token of this service, see VaultIP_FW4.2_Firmware-Reference-Manual_RevA.pdf). In this case, this interface corresponds to the GetNoise() conceptual interface from SP800-90B.
- The *TRNG Configuration* service allows to tune some parameters of the ES. This service is available but not used in mission mode (the Vault-_FW4.2_Firmware-Reference-Manual_RevA.pdf states to "never run the TRNG-Configuration token explicitly", except for re-seeding purpose). It is reserved for characterization services. It allows to tune several parameters like sampling rate, or health test parameters (e.g., cutoff values). Regarding parameter tuning for characterization, it is also possible to use direct register R/W services to modify and access some TRNG registers (see section 10 below).

7. Min-Entropy Rate

The H_submitter is 0.125 bit /bit.

The bits per request sample is 4096 at the input of the vetted conditioning function.

The min-entropy rate at the output of the entropy source the H_out for the output of the conditioning function per section 3.1.5 of SP800-90B, is 256 bits per 256-bit output sample.

8. Health Tests

Rambus has designed the health tests to detect failures of the Noise Source, or to detect a deviation from the expected entropy rate during the correct operation of the Noise Source before the raw data is conditioned. Following the NIST SP 800-90B requirements, the vendor has implemented three types of health tests in this product:

- Start-up Test. The Start-up test runs over a minimum of 1024 consecutive 8-bit samples cumulated into sixteen 512-bit noise blocks. The Start-up tests comprises the Repetitive Count Test (RCT) and Adaptive Proportion Test (APT). If any of these test fails, the sampled bits will be discarded, and the Start-up test is performed on the next 1024 8–bit samples. There is no output available from the entropy source before successful completion of the start-up tests.
- Continuous Tests. The entropy source implements 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 $\alpha= 2^{-30}$.
    - Cutoff value C=31.

  - 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 $\alpha= 2^{-30}$.
    - Cutoff value C=325.

- When any of the health tests fail, ES discards the raw entropy data and move on to the next set of raw entropy data subject to the health tests. If the failure persists, the ES enters in error state.
- On-Demand Test. The On-Demand health tests are performed of the physical entropy source output by rebooting the FPGA which results in the immediate execution of the Start-up Test which includes the health tests described in Section 2.3.1 SP 800-90B.

9. Maintenance

There are no maintenance requirements.

10. Required Testing

The entropy source continuously runs the SP 800-90B health tests and will produce an error upon failure.

- The ES is configured on Xilinx Zynq XC7Z045 FPGA to comply with SP800-90B at the first start of the FPGA. The approved parameters are stored in OTP. Any misuse of the *TRNG Configuration* service would cause the ES to provide entropy that cannot be used by FIPS approved security services. Therefore, the *TRNG Configuration* service is conceptually disabled for the EIP130 TRNG ES configured on the FPGA on mission mode (see also above sections 4 and 6). There is no required testing in this configuration.
- For configuring the EIP130 TRNG ES in other chips or systems, the TRNG configuration parameters shall be adjusted to provide a full entropy rate. ES configuration document (True Random Number Generator Noise & Entropy Discussion) is then provided by Rambus to the customer to get correct parameters. By following the raw data collection procedure described in section 6 of Security VaultIP_HW4.1_Integration-Manual_RevA.pdf (procedure that requires direct read/write of some TRNG registers described in VaultIP_HW4.1_Hardware- Reference-Manual_RevA.pdf), the integrator using this ES in a module should gather:

    - one million consecutive raw physical noise samples at runtime. The results obtained from the NIST SP800-90B tool must be at least as high as the H_submitter (see this document section 7).
    - 1000 raw physical noise samples after 1000 restarts for assessment that (1) the sanity test passes and (2) the minimum of the row-wise and column-wise entropy rate shall not be less than half of the entropy rate from 1 above.

11. Vendor Permissions and Relationship

The EIP130 TRNG status is indicated as "Open for Reuse".