SP 800-90B Non-Proprietary Public Use Document

EIP130 TRNG Entropy Source [ES]

Hardware Version 4.3.1

Firmware Version 4.6.3

Document Version 1.0

April, 2024

Prepared by:

atsec information security corporation
4516 Seton Center Parkway, Suite 250
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 ES has a hardware version 4.3.1 and a firmware version 4.6.3.

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 with eight FROs, Digital logic, no_whitening=1 in the TRNG control register, SP800-90B health tests and a SHA-256 vetted conditioning function. The operator can request unconditioned data (i.e. temporarily disable the conditioning function) by providing the "RawKey" parameter to the RNG Get Random Number service.

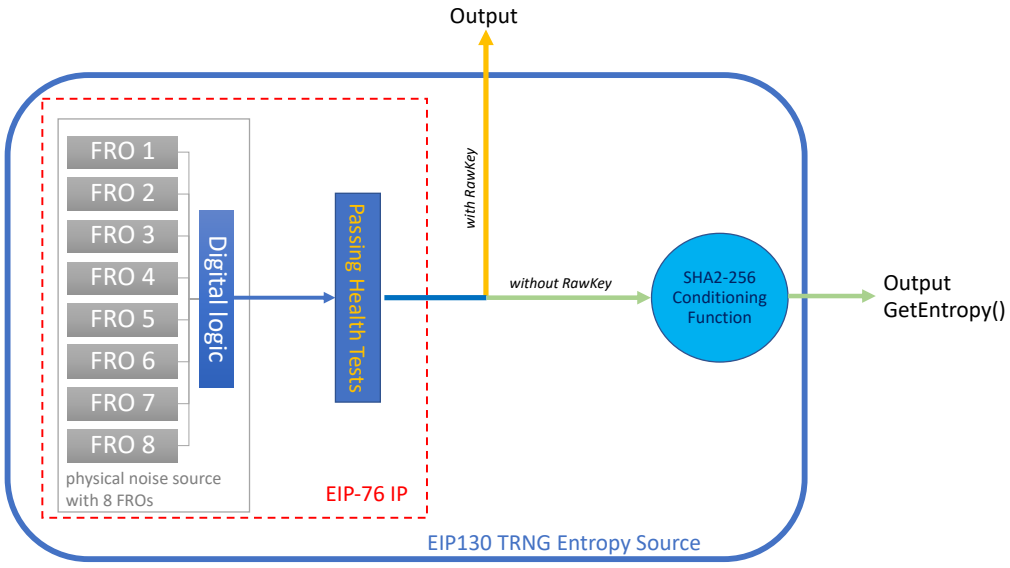

Figure 1: Block Diagram of the ES with the FRO physical noise source

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

The configuration options for the entropy source are defined by the following technology parameters:

- No_whitening=1: disable the toggle flip-flop based whitening of the noise source.
- SampleDiv, SampleCycles, Scale: in no_whitening=1 mode, the number of clocks specified by SampleDiv multiplied by the factor specified in SampleCycles (and Scale) is the sampling interval.
- AdaptProp512Cutoff - The cutoff value for the APT with W = 512, AdaptProp64Cutoff - The cutoff value for the APT with W = 64 (only W=512 is SP800-90B section 4.4.2 compliant)
- RepCntCutoff - The cutoff value for the RCT
- NoiseBlocks - The number of 512-bit noise blocks used as input to the SHA-256 conditioning function (from 1 and 31 inclusive), if the conditioning function is enabled.

For the EIP130 TRNG ES tested in the FPGA, the configuration options are not accessible by the operator. The configurable parameters can be modified from the default values for other environments not covered by the current ESV certificate.

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

When the operator calls the RNG Get Random Number without "RawKey", the ES provides its entropy output interface (the GetEntropy() interface) to a DRBG running on the same platform through the NrbgCondOut register. In the production environment, there is no interface to access the entropy source output directly for an arbitrary user but to the DRBG. This case corresponds to the ES with conditioning function enabled.

When the operator calls RNG Get Random Number with the "RawKey" parameter, the service returns unconditioned data (i.e. raw data at the output of the XORed FROs). This case corresponds to the ES with conditioning function disabled.

7. Min-Entropy Rate

The H_submitter is 0.125 bit/bit.

For the case with conditioning function enabled, 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.

For the case with conditioning function disabled, the min-entropy rate at the output of the entropy source is 0.125 bit/ bit.

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 concatenated 1-bit samples cumulated into sixteen 512-bit noise blocks (NoiseBlocks). The Start-up tests comprises the Repetition 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 concatenated 1-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 concatenated 1-bit samples.
        - alpha value of $\alpha = 2^{-30}$.
        - Cutoff value C (RepCntCutoff)=31.
    - Adaptive Proportion test conforming to SP 800-90B section 4.4.2.
        - W=512
        - H=1 bit of entropy per 8 concatenated 1-bit samples
        - alpha value of $\alpha = 2^{-30}$.
        - Cutoff value C (AdaptProp512Cutoff)=325.

- On-Demand Test. The On-Demand health tests are performed 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.

If any of the health tests fail, the ES discards the raw entropy data and moves on to the next set of raw entropy data subject to the health tests. If the failure persists, the ES enters in error state.

9. Maintenance

There are no maintenance requirements.

10. Required Testing

The Entropy Source was tested in accordance with NIST SP 800-90B requirements. Both raw and restart data were collected by the vendor. No further testing is required.

11. Vendor Permissions and Relationship

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