HEALTH TESTS HARDWARE IMPLEMENTATION FOR ENTROPY SOURCES

Burko L., Kaiky M., Ivaniuk A.
Department of Informatics, Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus
E-mail: {burkoliana, kaikymykhailo}@gmail.com, ivaniuk@bsuir.by

The work discusses the process of synthesizing a microprogrammed machine for testing the suitability of physical sources of entropy in accordance with the NIST SP 800-90B standard. A comparison was made of the hardware costs and performance of the resulting microprogrammed machine and standard implementations of the selected tests. The developed firmware makes it possible to reduce hardware costs for hardware implementation of tests for true random number generators.

Introduction

The topic of random number generation is relevant in the modern world. There are millions of transactions every second that require encryption. To create true random number generator is a non-trivial problem. Most higl-level programming languages use pseudo-random modules for number generation. For example they use system time as seed. Such modules can be susceptible to hacking or failures. To solve this problem there are various methods of testing random number sources in real time. For exapmle NIST Special Publication 800-90B [1], BSI AIS20/31 compliant tests.

I. Entropy source structure

In modern True Random Number Generators entropy sources are implemented as a set of physically unclonable functions that form N-channel sequences of random bits. Each channel requires a separate block of health tests for correct operation according to NIST 800-90B [1]. The entropy source model is represented in figure 1 in detail.

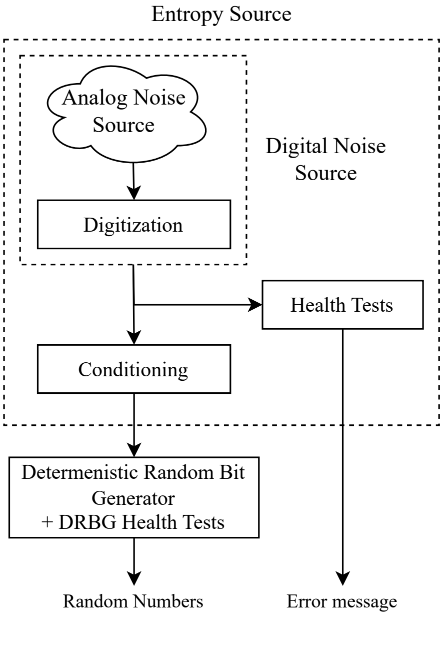

Figure 1 – Entropy Source model

The noise source is the root of security for the entropy source and for the Random Bit Generator as a whole. This is the component that contains the non-deterministic, entropy-providing process that is ultimately responsible for the uncertainty associated with the bitstrings output by the entropy source.

The optional conditioning component is a deterministic function responsible for reducing bias and/or increasing the entropy rate of the resulting output bits (if necessary to obtain a target value).

Health tests are an integral part of the entropy source design that are intended to ensure that the noise source and the entire entropy source continue to operate as expected.

II. Health tests description

There are 3 types of tests.

1. *Start-up health tests* are designed to be performed after powering up, or rebooting, and before the first use of the entropy source. They provide some assurance that the entropy source components are working as expected before they are used during normal operating conditions, and that nothing has failed since the last time that the start-up tests were run.

2. *Continuous health tests* are run indefinitely on the outputs of the noise source while the noise source is operating. Continuous tests focus on the noise source behavior and aim to detect failures as the noise source produces outputs. The purpose of continuous tests is to allow the entropy source to detect many kinds of failures in its underlying noise source.

3. *On-demand health tests* can be called at any time. NIST 80-900B [1] does not require performing testing during operation.

NIST 80-900B provides two approved health tests: *the Repetition Count test* and *the Adaptive Proportion test.* If these two health tests are included among the continuous health tests of the entropy source, no other tests are required.

The goal of *the Repetition Count Test* is to quickly detect catastrophic failures that cause the noise source to become "stuck" on a single output value for a long period of time. A variable C - considered critical.

$$C = 1 + \left\lceil \frac{-log_2(a)}{H} \right\rceil \quad (1)$$

where H – the min-entropy of the samples from a (digitized) noise source or of the output from an entropy source, a – The probability of falsely rejecting the null hypothesis (type I error).

The Adaptive Proportion test checks the ratio of zeros and ones in each window.

Like all statistical tests, both of these tests have a false positive probability – the probability that a correctly functioning noise source will fail the test on a given output. In many applications, a reasonable choice for the probability of type I error is $a = 2^{-20}$.

For example, for $a = 2^{-20}$, an entropy source with H = 2.0 bits per sample would have a repetition count test cutoff value of $1 + 20/2 = 11$.

III. Practical results

Dataset, that comes on Health tests stand divided into blocks with size W. According to Health tests all blocks are checked separately and the validity result is issued within each block. The window size W is selected based on the alphabet size, and shall be assigned to 1024 if the noise source is binary and 512 if the noise source is not binary. In this work was decided to check also $W = 4096$. P will be used as the evaluation parameter, that shows amount of windows processing per second.

$$P = f_{CLK} \cdot W, \quad \text{[Giga Windows/s]} \quad (2)$$

where W – window size, f_{CKL} – maximum synchronization frequency.

Table 1 – Health Tests Hardware Utilization and Performance

Name	Resources				
	W	LUT	FF	f_{CLK}[MHz]	P
Adaptive	512	15	10	246	125
Repetition Count	512	21	13	239	122
Adaptive	1024	17	11	241	244
Repetition Count	1024	27	16	232	237
Adaptive	4096	21	14	238	974
Repetition Count	4096	34	30	230	934

IV. Conclusion

During the work, standards for constructing Health Tests for hardware true random number generators were studied, two single-channel hardware tests for the entropy source and a specialized stand for their validation on a Xilinx FPGA were designed. Prototyping stand is in figure 2. The results are presented in table 1. Dependences of hardware costs on the size of the working window for Health Tests were obtained. With an increase in the number of random bit channels, it is necessary to ensure that Health Tests operates in multi-channel mode, which entails an increase in hardware costs and power consumption of the chip. Further research involves studying methods for processing random sequences of multi-channel entropy sources to implement multi-channel Health Tests with reduced hardware costs and power consumption.

V. Bibliography

1. NIST Special Publication, NIST SP 800-90B 3pd, Recommendation for the Entropy Sources Used for Random Bit Generation – NIST,January 2018. [Electronic resource] – Mode of access: `https://csrc.nist.rip/external/nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf`. – Date of access: 15.10.2023.

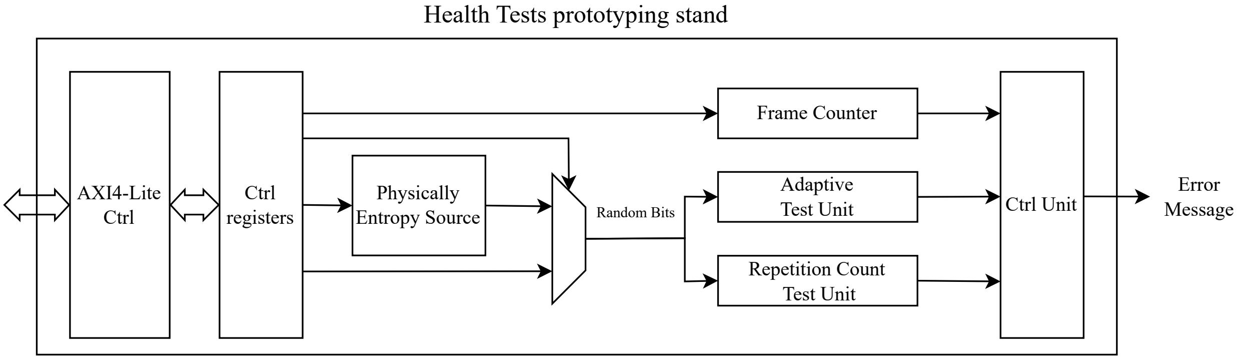

Figure 2 – Structure of Health Tests fast prototyping stand