FAST PROTOTYPING OF RECONFIGUABLE TRUE RANDOM NUMBER GENERATION IP-CORE

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

This work is devoted of the structuren of a reconfigurable IP-core for rapid prototyping of true random number sources based on Xilinx FPGAs. The developed IP-core allows you to configure TRNG at the design stage. In the proposed IP-core, developers can easily change the structure of the Entropy Source unit, Conditioning units, post-processors, performance tests, DRBG, component access interfaces.

Introduction

There are two types of random number generators: pseudo-random and true random. A pseudorandom number generator is an algorithm that simulates a random number.Predicted sequences can be generated by the pseudo-random number generator in software implementations, but it cannot be used as an entropy source for cryptographic methods. A true random number generator uses physical processes (eg. thermodynamic noise, mechanical noise, quantum process noise) to generate random numbers that cannot be predicted. These generators are more expensive and more difficult to use, but they produce more cryptographically secure random numbers.

I. NIST Standards for the Construction of Random Number Generators

NIST Special Publications (SP) 800-90 series describe methods and approaches for constructing random number generators for cryptographic and non-cryptographic purposes. SP 800-90A [1] defines several characteristics of a Deterministic Random Bit Generator (DRBG) based on cryptographic algorithms, SP 800-90B[2] contains recommendations for the development and testing of entropy sources, SP 800-90C [3] – identify Random Bit Generator (RBG) implementation designs that incorporate DRBG mechanisms as specified in SP 800-90A and use an entropy source as specified in SP 800-90B.

According to NIST SP 800-90C, true random number generators can be of three types:

1. RBG1: The entropy source and DRBG are implemented in different blocks and are connected to each other using a secure channel.
2. RBG2: Entropy source, random bit post-processing block and DRBG are within the same safety boundary.
3. RBG3 (XOR): The design contains one or more verified entropy sources and DRBGs whose the output is XORed to produce random numbers with full entropy.

Despite the different ways of constructing generators, they all have a common structure (fig. 1), consisting of a physical source of entropy, health tests of the source, a conditioning unit and DRBG.

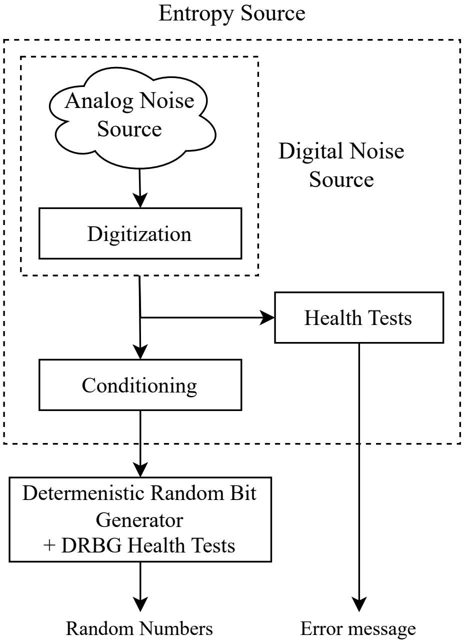

Figure 1 – NIST Random Bit Generator Structure

II. Development a Reconfigurable Random Number Generator

Accelerate the process of prototyping and researching sources of true random numbers, an approach was proposed to develop a reconfigurable generator that allows replacing blocks of the physical source of entropy, conditioning unit, DRBG, changing the nature of the connections between them (both in accordance with NIST SP 800-90C [3], and in other methods). The general structure of the developed IP-core of such a reconfigurable generator is depicted in figure 2, blocks circled in a dotted line – support reconfiguration at the design stage (before synthesis).The developed generator, as in NIST SP 800-90C [3], consists of the following main parts: entropy source, conditioner, Healt Tests Unit, DRBG, but there are also other blocks, such as – hardware FIFO for storing and speeding up access to random numbers, interface controller blocks and registers programmatically accessible to the host controller. The developed number generator can be integrated into a system on a chip, such as an FPGA or ASIC, and provide host-controller (processor) access to the source of random numbers using various interfaces. The interface is configured at the design stage using the `define` directives of the SystemVerilog hardware description language and currently the following interfaces are supported: AXI4-Lite, Naive Interface (addr, data, we, re), UART, SPI, and others can also be added.

The main goal in the development of TRNG is to make the right choice of the physical source of entropy and to ensure the reliability of random number generation using post-processing methods of data from this source. Usually, the construction of ring generators is used as a source of entropy [4], linear feedback registers (LFSR) are used as a Conditioner, and NIST AES256/AES512 algorithms are used as DRBG.

III. Conclusion

An IP-core of a hardware accelerator based on Xilinx FPGA was developed to conduct experimental studies of cryptographic primitives, in particular, physically unclonable functions as sources of entropy, post-processing blocks of random data and deterministic random number generators (DRBG), which underlie the hardware implementation of the generator true random numbers according to NIST standards. The oscillation frequency of ring generators strongly and linearly depends on the temperature [5], which makes it difficult to use them as sources of entropy, reduces reliability and resistance to attacks on TRNG. The developed IP-core makes it possible to introduce various entropy source structures into the TRNG structure, which makes it possible to expand the study area and conduct research on other physical sources, such as static memory (SRAM).

Bibliography

1. NIST Special Publication, NIST SP 800-90A 3pd, Recommendation for Random Bit Generator (RBG) Constructions – NIST,September 2022. [Electronic resource] – Mode of access: `https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf`. – Date of access: 15.10.2023
2. NIST Special Publication, NIST SP 800-90B 3pd, Recommendation for Random Bit Generator (RBG) Constructions – NIST,September 2022. [Electronic resource] – Mode of access: `https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf`. – Date of access: 15.10.2023
3. NIST Special Publication, NIST SP 800-90C 3pd, Recommendation for Random Bit Generator (RBG) Constructions – NIST,September 2022. [Electronic resource] – Mode of access: `https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90C.3pd.pdf`. – Date of access: 15.10.2023.
4. Physically unclonable functions based on a controlled ring oscillator, Ivaniuk.A, Yarmolik.V
5. Temperature Compensation in CMOS Ring Oscillator, Dingyufei Zhang, Xiaohua Wei, Department of Electrical Engineering, Linköping University, 2022 [Electronic resource] – Mode of access: `https://liu.diva-portal.org/smash/get/diva2:1662148/FULLTEXT01.pdf`. – Date of access: 15.10.2023.

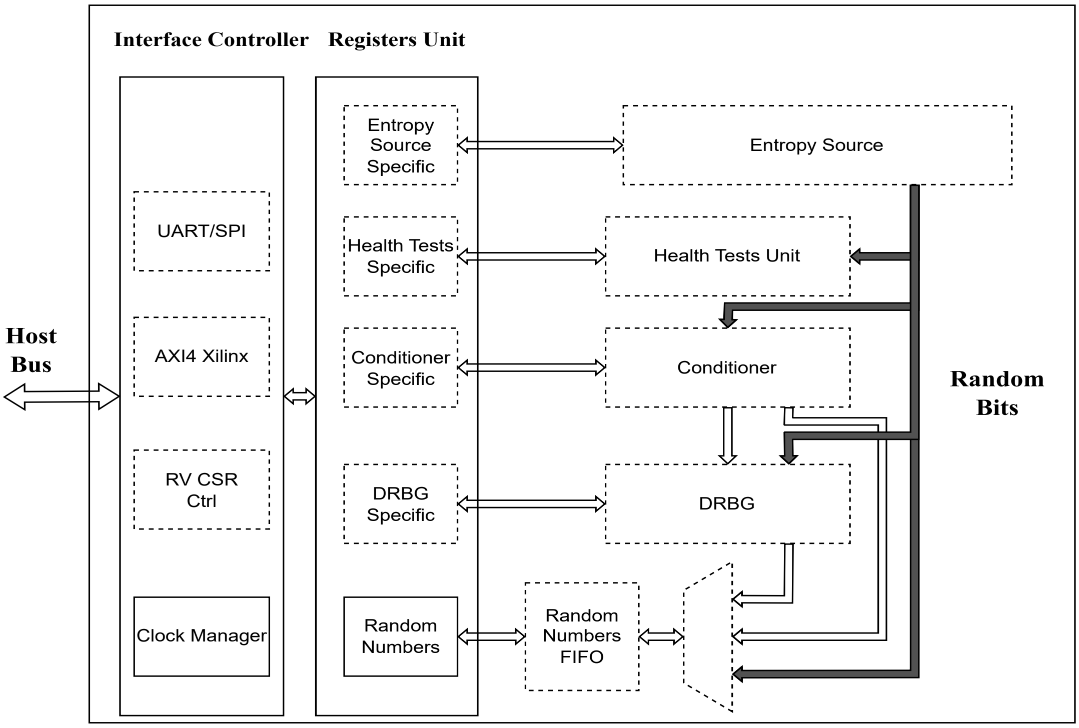

Figure 2 – Block diagram of the IP-core the reconfigurable true random number generator