Physical Unclonable Functions as Entropy Source to Build True Random Number Generator

S.S. Zalivaka, e-mail: zalivako@bsuir.by
A.A. Ivaniuk, e-mail: ivaniuk@bsuir.by
Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus

True random number sequences are widely used in many areas: cryptography, modeling, game industry, decision support systems, random sampling, art and etc [1].

In general case TRNG consists of three components: entropy source, compressing scheme and true random number register.

Basic hypothesis of this research work is that the Physical Unclonable Functions (PUF) can be high quality, unclonable, not reproducible, unpredictable entropy source with low hardware costs.

Physical unclonable functions

Physical unclonable function – function, that embodied in a physical structure, which is easy to estimate, but it is hard to describe, simulate or reproduce. Initially, the idea of using PUF belongs to R. Pappu [2]. One of the most widely used PUF definitions today was proposed by P. Tuils [3]. PUF by Tuils is physical system (device), which has inherent property – unclonability (nonrepeatability) of some its functions, properties, characteristics and parameters.

PUF is described by pairs of input and corresponding output values of parameters (signals). Such pair consists of input physical parameter (challenge) and output parameter (response) and is called challenge-response pair (CRP). In simplest case PUF can be considered as function, which converts the challenges C_i to responses R_i:

$$R_i = PUF\ (C_i) \quad (1)$$

PUF has two important properties: practically impossible to create a physical copy of PUF; it is impossible to create precise mathematical model of PUF that means to compute the response, if exact parameters of the challenge and other challenge-response pairs are given. This problem is connected with huge computational difficulties because physical interaction is too hard.

These properties together are called unclonability.

PUF based TRNG circuit implementation

All implemented generators have the same structure, which shown on Fig. 1.

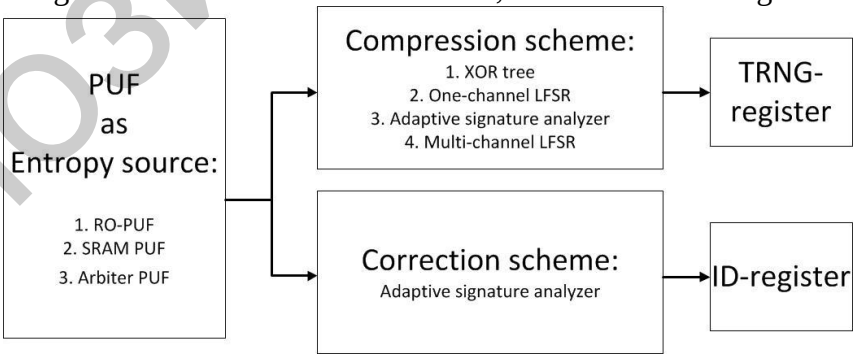

Fig. 1.Common TRNG structure.

As shown on Fig. 1 PUF may be the source of entropy and the source of stability.

There are three implementation of PUF based TRNG:

1) Modified Ring Oscillator PUF (RO-PUF) as entropy source, XOR tree and one-channel Linear Feedback Shift Register (LFSR) as compression scheme [4];

The ring oscillator PUF technology was used as the basis of the circuital implementation of the random number generator. The hardware circuit of the RO-PUF can be implemented with sequentially connected$2n + 1$ inverters with a negative feedback. The number of inverters should be odd. It provides the formation of the output signal in the form of a meander. Its frequency is determined by the signal propagation delay through a feedback circuit.

All RO-PUF elements together generate a bit sequence. After that sequence are compressed by n-input XOR-gate (XOR tree) and LFSR.

2) Combined PUF (Static Random Access Memory (SRAM) PUF when challenge = 1 and RO-PUF when challenge = 0) as entropy source, adaptive signature analyzer as compressing scheme [5];

The circuit basis is combined PUF, which can be implemented on the two inverters and multiplexer. Depending on the control signal *challenge* circuit can operate in two modes: RO-PUF (*challenge* = 0) and SRAM-PUF (*challenge* = 1).

In the SRAM-PUF mode every system start PUF emulates the memory cell behavior, which «holds» bits of information. At the same time memory cell can constantly take a logical zero (one), or to change its value from run to run.

Adaptive signature analyzer [6] was used for compressing PUF generated sequence true random number sequence.

3) Arbiter PUF as entropy source, multichannel LFSR as compressing scheme (see Fig. 3) [7];

Arbiter PUF can be implemented using a single pulse generator, the output pulse is applied to the component, which consists $2n$ multiplexers. Selecting signal C_i ($0 \le i \le n-1$) is applied to the input of each pair of multiplexers. The result of the two «chains» of multiplexers is applied to the input of D-Flip-Flop, which is an «arbiter». «Arbiter» defines, which of the signals came first. Depending on the «arbiter» decision PUF result bit can be different.

Multichannel LFSR compress several arbiter PUFs result to the true random number.

Arbiter PUF and SRAM-PUF can be used for digital device identification with adaptive signature analyzer correction scheme.

TRNG sequences testing

All generated sequences are tested on two identical FPGA Nexis-2 Spartan 3E-500 FG320 with statistical toolkit Statistica ®, statistical tests packages NIST and Diehard.

Statistical tests are passed by all data packages (1000 selections of 100000 bits).

By the statistical tests result sequence is unclonable, not reproducible, unpredictable. TRNG is simple to implement and has low hardware costs.

Mentioned types of PUF also have possibility to solve digital device identification problem with the same circuit.

References

1. Chairmaine, K. Random number generators: An evolution and comparison of Random.org and some Commonly used Generators, Management Science and Information Systems Studies. Project Report, April 2005.

2. Pappu, R. Physical One-Way Functions // Science. – 2002. – Vol. 297.p. 2026–2030.

3. Tuyls, P. Security with Noisy Data // London: Springer. – 2007. – 339 p.

4. Zalivaka, S.S., Ivaniuk, A. A The use of physical unclonable functions for true random number generation // Automation control and computer science. – 2013. – №3.-p.61-72.

5. Zalivaka, S.S., Ivaniuk, A. A Combined Physical unclonable function circuit implementation for true random number generation // Doklady BGUIR. – 2013. – №7 (77).- p.34-72, (in Russian).

6. Ivaniuk, A.A., Yarmolik, V.N. Testable digital devices design / A.A. Ivaniuk, V. N. Yarmolik. – Minsk: Bestprint, 2006. – 296 p.

7. Zalivaka, S.S., Ivaniuk, A.A. True random number generation with arbiter physical unclonable function // Informational Technologies and Systems (ITS'2013): Proc. of Int. conf., BSUIR, Minsk, Republic of Belarus, 23 Oct. 2013 / edit. : L.U. Shilin [et al.]. – Minsk : BSUIR, 2013. – P. 204–205, (in Russian).