Paweł KUBCZAK, Łukasz MATUSZEWSKI, Mieczysław JESSA, Szymon ŁOZA
POZNAN UNIVERSITY OF TECHNOLOGY, FACULTY OF ELECTRONICS AND TELECOMMUNICATIONS
3 Polanka St., 61-131 Poznań

Digital random bit generators implemented in FPGAs offered by various manufacturers

Abstract

In cryptography, we require that a random sequence should have excellent statistical properties as well as non-deterministic character. Combining multiple independent sources of randomness using the modulo two operation, significantly improves the statistical properties of the generated sequences and also affects the accumulation of true randomness generated in the oscillator sources. This is a very promising method of producing random sequences. In this paper, we compare the implementations of the RO-based combined random generator in various FPGAs technologies offered by various manufactures (Xilinx, Altera, Lattice). In this research, we used a NIST 800-22 statistical test suite to assess the statistical properties. The results show that the method of producing strings with a combined generator is the method stable in terms of technology. The results are similar for implementation in all FPGA used in the experiment. So, the proposed generator can be implemented in various programmable structures together with other components of a cryptographic system.

Keywords: true random number generator, ring oscillator, cryptography, field programmable gate array.

1. Introduction

Most of modern cryptographic systems are digital devices. Therefore, it is expected that random bit generators will also be digital structures, integrated with the whole system. The simplest example of a digital random number generator is a ring oscillator (RO) whose output is sampled with a periodic signal with significantly lower frequency. A source of randomness is jitter available at the RO output. Generators using a physical source of randomness are called True Random Number Generators (TRNGs) in the literature. A TRNG using a single entropy source has no good statistical properties and the output sequence is often affected with a deterministic factor. To provide good statistical properties, we combine TRNGs using ROs with the XOR operation [1-5]. In this paper, we will prove that an RO-based combined TRNG is technology independent.

2. Combined TRNG

The scheme of a combined TRNG is shown in Figure 1. The N bit streams produced by sampling ROs are combined in several steps by XOR gates [6-9]. The number of streams combined in a single step is adjusted by synthesis tools provided by manufacturers.

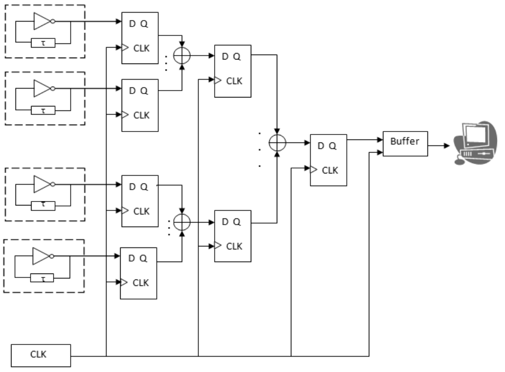

Fig. 1. A combined TRNG

Bits are gathered in a buffer and sent to a personal computer (PC) via a FTDI device and a USB 2.0. No post-processing is performed in the PC. In a single ring oscillator, τ is a delay element. For most technologies it can be a single latch, but for Lattice, we have to replace it by two inverters, because there is no latch in a single LUT construction and artificially created latch gives too large delay. Synthesis, placement and the rest of operations are performed automatically. We only must add synthesis 'keep' attribute to prevent removing elements from combinational loops. The buffer size has to be variable because in variable amount of inner memory is available in devices. For the NIST 800-22 statistical test suite, we gather thousand sequences of length one million bits each. The procedure of collecting bits was as follows: the data generated by a combined TRNG were first pushed into the buffer, then the data were sent from the buffer to a PC, and after buffer flush the procedure was repeated till we archived a desired amount of data.

3. Ring oscillators implemented in various FPGAs

A big FPGA market is divided by manufacturers in an irregular way, as we can see in Figure 2. Two biggest producers Xilinx and Altera have almost 90% of the total revenue. We need to mention about two more producers that have 10% of market: Lattice with 6% share and Microsemi (known also as Actel) with 4% share. The rest have less than 1% of participation.

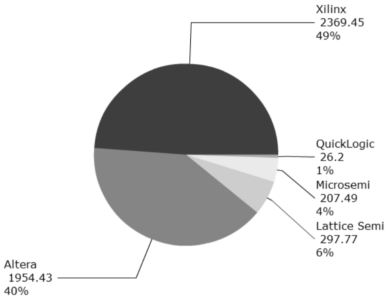

Fig. 2. FPGA Market Share by 2010 revenue in millions of USD[10]

For tests, we chose a representable set of devices from various manufactures that reflected participation in the market. In our collection there were low-cost series such as Spartan, Cyclone and ECP3 and high-end series such as Virtex and Stratix. The devices were made in different technologies from 90 nm up to 40 nm. Data on an aggregate basis are shown in Table 1.

Tab. 1. Comparison of different FPGAs technologies

Manufacturer	Device	Technology	LUT inputs
Xilinx	Spartan 3A	90 nm	4
	Spartan 6	45 nm	6
	Virtex4	90 nm	4
	Virtex 5	65 nm	6
Altera	Cyclone 2	90 nm	4
	Cyclone 4	60 nm	4
	Stratix 4	40 nm	8
Lattice	ECP3	65 nm	4

The tested FPGAs had variable constructions of logic cells, variable number of total logic cells, different size of internal memory size, different number of pins, different power consumption and thermal noise level and different clock generation resources [10-17].

For all the devices, we used the same main clock speed which was equal to 100 MHz. In Xilinx and Altera devices we achieved this by multiplying by two in PLL (Phase Locked Loop) built into evaluation boards with a 50 MHz oscillator. For Lattice, we connected directly 100 MHz quartz located on the evaluation board.

We used various software environments. To compile and program Xilinx devices, we used ISE Design Suite 14.6. For Altera devices it was Quartus II 14.1 (13.0 for Cyclone2) and Diamond 3.5 for Lattice.

A single RO consists of an inverter and a latch in Xilinx and Altera devices and of three inverters in a Lattice device, because there is no latch in a single logic cell construction and artificially created latch gives too large delay.

In Figures 3-7 there are shown the samples of different architectures of basic logic cells. The main difference is the number of inputs in Look Up Table (LUT).

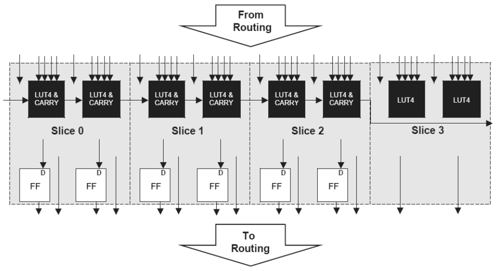

Fig. 3. PFU (programmable functional unit) from Lattice [13]

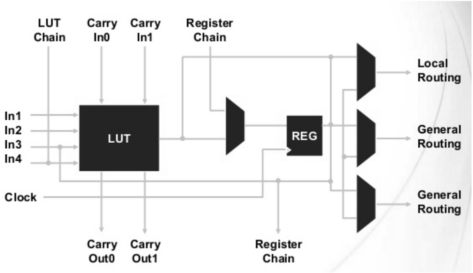

Fig. 4. Cyclone 2 logic element [15]

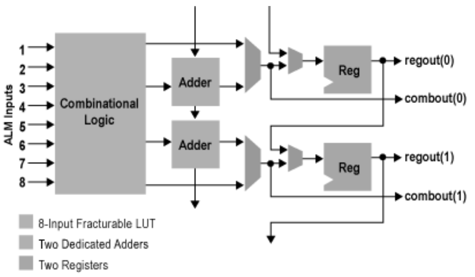

Fig. 5. ALM in Stratix 4 [16]

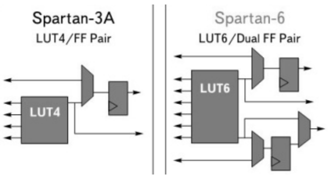

Fig. 6. LUT-flipflop in Spartan series [11]

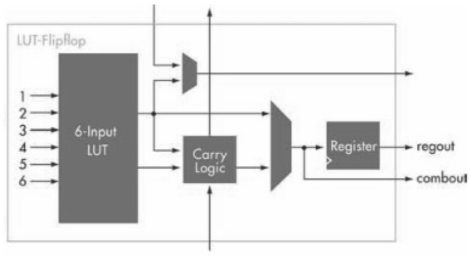

Fig. 7. LUT-flipflop in Virtex 5[17]

4. The statistical properties of bit sequences produced by TRNG using ROs

The NIST 800-22 statistical test suite was used in our work [18]. It consists of 15 basic statistical tests:

- The Frequency (Monobit) Test - The focus of the test is the proportion of zeroes and ones for the entire sequence,
- Frequency Test within a Block - The focus of the test is the proportion of ones within M-bit blocks,
- The Runs Test - The focus of this test is the total number of runs in the sequence, where a run is an uninterrupted sequence of identical bits,
- Tests for the Longest-Run-of-Ones in a Block - The aim of the test is the longest run of ones within M-bit blocks,
- The Binary Matrix Rank Test - The focus of the test is the rank of disjoint sub-matrices of the entire sequence,
- The Discrete Fourier Transform (Spectral) Test - The focus of this test is the peak heights in the Discrete Fourier Transform of the sequence,
- The Non-overlapping Template Matching Test - The focus of this test is the number of occurrences of pre-specified target strings,
- The Overlapping Template Matching Test - The focus of this test is the number of occurrences of pre-specified target strings,
- Maurer's "Universal Statistical" Test - The focus of this test is the number of bits between matching patterns,
- The Linear Complexity Test - The focus of this test is the length of a linear feedback shift register,
- The Serial Test - The focus of this test is the frequency of all possible overlapping *m*-bit patterns across the entire sequence,
- The Approximate Entropy Test - The purpose of the test is to compare the frequency of overlapping blocks of two consecutive/adjacent lengths (*m* and *m*+1) against the expected result for a random sequence,
- The Cumulative Sums (Cusums) Test - The focus of this test is the maximal excursion (from zero) of the random walk defined by the cumulative sum of adjusted (–1, +1) digits in the sequence,
- The Random Excursions Test - The focus of this test is the number of cycles having exactly *K* visits in a cumulative sum random walk,
- The Random Excursions Variant Test - The focus of this test is the total number of times that a particular state is visited (i.e., occurs) in a cumulative sum random walk.

When a random sequence passed all of those tests, we accepted that sequence as random. In Table 2 we summarized the NIST 800-22 test results for the circuits considered in a real experiment. The standard set of parameters proposed by NIST in v. 2.1.1 was used. The significance level was $\beta = 0.01$. The minimum passing value for the standard set of parameters was approximately 0.9805. The minimum P_T value was 0.0001. If any of P_T or proportion *R* from a single test failed, we assumed that the whole test suite for that device and specified number of ROs failed. For ten ROs no device passed the statistical tests. When we increased the number of rings to fifteen or more, the combined TRNGs passed all the statistical tests for all the devices and technologies.

Tab. 2. NIST 800-22 test results

Device	Number *N* of used ROs			
	10	15	20	30
Spartan 3A	**fail**	pass	pass	pass
Spartan 6	**fail**	pass	pass	pass
Virtex 4	**fail**	pass	pass	pass
Virtex 5	**fail**	pass	pass	pass
Cyclone 2	**fail**	pass	pass	pass
Cyclone4	**fail**	pass	pass	pass
Stratix 4	**fail**	pass	pass	pass
ECP3	**fail**	pass	pass	pass

We expect that it should also be true for combined RO-based TRNGs implemented in application specific integrated circuits (ASICs). The boundary conditions for *N* for producing sequences with arbitrary small correlation between the adjacent bits can be found in [5].

5. Conclusions

The use of an RO-based combined TRNG as a source of randomness is a great solution, because it can be implemented in various devices provided by many manufacturers. The technological process as well as power consumption and thermal noises associated with it do not influence the quality of the produced sequences. Even a different construction of a single logic cell in an FPGA does not change the statistical properties of the produced digits for a sufficiently large *N*. In a ring oscillator (RO), we can use any logic gate as a delay element but the frequency of oscillations must be significantly faster than that of the sampling clock. The most important factor is the number *N* of the used RO-based source generators. If we use too few oscillators, the generated sequences will fail the NIST 800-22 statistical test suite.

The goal of further research is to increase the robustness of an RO-based combined TRNG to an injection attack and to assess the amount of true randomness present at the output with the restart mechanism.

The presented work has been funded by the Polish Ministry of Science and Higher Education within the status activity task 08/83/DSPB/4707 in 2015.

6. References

[1] Sunar B., Martin W. J., and Stinson D. R.: A provably secure true random number generator with built-in tolerance to active attacks. IEEE Trans., Comput., vol. 56, pp. 109-119, Jan. 2007.

[2] Wold K. and Petrović S.: Security properties of oscillator rings in true random number generators. In Proc. of 15th Inter-national Symposium on Components, Circuits, Devices and Sys-tems, pp. 145-150, 2012.

[3] Valtchanov B., Aubert A., Bernard F., and Fischer V.: Modeling and observing the jitter in ring oscillators implement-ed in FPGAs. In Proc. of IEEE Workshop on Design and Diag-nostics of Electronic Circuits and Systems, DDECS'08, pp. 1-6, 2008.

[4] Güler Ü., Ergün S., and Dündar G.: A digital IC random number generator with logic gates only. Proc. of 17th IEEE International Conference on Electronics, Circuits, and Systems (ICECS), Dec. 2010, pp. 239-242.

[5] Jessa M.: On the Quality of Random Sequences Produced with a Combined Random Bit Generator. IEEE Transactions on Computers*,* Vol. 64, No. 3, March 2015, pp. 791-804.

[6] Jessa M. and Matuszewski L.: Producing random bits with delay-line-based ring oscillators. Int. Journal of Electronics and Telecommunications, vol. 59, No. 1, pp. 41-50, 2013.

[7] Wold K. and Tan C. H.: Analysis and enhancement of random number generator in FPGA based on oscillator rings. Int. J. of Reconfiugurable Computing, vol. 2009, pp. 1-8, 2009.

[8] Jessa M. and Jaworski M.: Randomness of a combined RBG based on the ring oscillator sampling method. Proc. of International Conference on Signals and Electronic Systems, ICSES'10, pp. 323-326, 2010.

[9] Markettos A. T. and Moore S. M.: The frequency injection attack on ring-oscillator-based true random number generators. In Proc. Workshop Cryptograph. Hardware Embed. Syst. CHES'2009, Sept., 2009, LNCS 5747, pp. 317-331.

[10] http://www.fpgadeveloper.com/2011/07/list-and-comparison-of-fpga-companies.html

[11] www.xilinx.com

[12] www.altera.com

[13] www.latticesemi.com

[14] LatticeECP3EAFamilyDataSheet.pdf

[15] Cyclone II Device Handbook, Volume 1

[16] https://www.altera.com/products/fpga/features/stxiv-alm-logic-structure.html

[17] Stratix III FPGAs vs. Xilinx Virtex-5 Devices:Architecture and Performance Comparison, Altera Corporation.

[18] Rukhin A., Soto J., Nechvatal J., Smid M., Barker E., Leigh S., Levenson M., Vangel M., Banks D., Heckert A., Dray J., Vo S.: A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST special publication 800-22, Revised: April 2010, Available at: http://csrc.nist.gov/rng/.

Received: 07.04.2015 Paper reviewed Accepted: 02.06.2015

Paweł KUBCZAK, MSc, eng.

He received the M.S. degree from Poznan University of Technology in 2013. He continues studies at Faculty of Electronics and Telecommunications and prepares the Ph.D. thesis. His research interest include: digital measurement systems, time interval error measurement, randomness in digital logic, microcontrollers, and Field Programmable Gate Arrays.

e-mail: szymon.piotr.loza@gmail.com

Łukasz MATUSZEWSKI, MSc, eng.

He received the M.S. degree from Poznan University of technology in 2010. Now he prepares his Ph.D. thesis. He works in the Chair of Telecommunication Systems and Optoelectronics of Poznan University of Technology as teaching assistant. His research interest include randomness in digital logic, reconfigurable systems and Field Programmable Gate Arrays.

e-mail: lukasz.matuszewski@et.put.poznan.pl

Mieczysław JESSA, DSc, eng.

He works in the Chair of Telecommunication Systems and Optoelectronics at Poznan University of Technology. Initially, his research interest included phase-locked loops and network synchronization. In the years 1995-1997 he was an expert of the Polish Ministry of Communications. His current research concerns the mathematical models of randomness and pseudo-randomness and the applications of the chaos phenomenon. He is the author or co-author of over one hundred journal and conference papers and fifteen patents.

e-mail: mjessa@et.put.poznan.pl

Szymon ŁOZA, MSc, eng.

Graduate of Poznan University of Technology. He gained Bachelor of Engineering degree in specialization of Computer and Information Systems Security/Information Assurance within Computer Science studies at the Faculty of Electrical Engineering. He graduated master studies also in Computer Science at the Faculty of Computer Science, specializing in Embedded System and Mobile Devices. Currently a PhD student at the Faculty of Electronics and Telecommunications. Area of his interests are systems security/information assurance.

e-mail: szymon.piotr.loza@gmail.com