

Oct 27th, 4:15 PM - 6:00 PM

Study of the Power Consumption of Pseudo Random Bit Generator Circuits Implemented on FPGA

Galia Marinova

Technical University-Sofia, gim@tu-sofia.bg

Follow this and additional works at: <https://knowledgecenter.ubt-uni.net/conference>



Part of the [Computer Engineering Commons](#), and the [Computer Sciences Commons](#)

Recommended Citation

Marinova, Galia, "Study of the Power Consumption of Pseudo Random Bit Generator Circuits Implemented on FPGA" (2017). *UBT International Conference*. 84.

<https://knowledgecenter.ubt-uni.net/conference/2017/all-events/84>

This Event is brought to you for free and open access by the Publication and Journals at UBT Knowledge Center. It has been accepted for inclusion in UBT International Conference by an authorized administrator of UBT Knowledge Center. For more information, please contact knowledge.center@ubt-uni.net.

Study of the Power Consumption of Pseudo Random Bit Generator Circuits Implemented on FPGA

Galia Marinova¹

¹Technical University-Sofia, Faculty of Telecommunications
8, Boulevard „KlimentOhridski“, Sofia, Bulgaria
gim@tu-sofia.bg

Abstract. This paper presents a power consumption estimation study for a set of PRBG circuits in the aim to add power consumption constraints at the design stage for such circuits and to help optimal design selection with minimal power consumption for a given application. The PRBG circuits are implemented on XILINX FPGA devices and they are simulated with the Power analyzer option of VIVADO tool. The power consumption of 8 PRBG circuits implemented on a same FPGA device is estimated – 6 of the circuits are LFSR or Galois and the other two are Kasami and Gold. The influence of the LFSR length on the power consumption is considered both at synthesis and implementation stages. On the other hand 2 different VHDL descriptions of a circuit are compared, to consider the influence of the code. The approach proposed can be useful for other classes of communication circuits.

Keywords: PRBG, FPGA, VHDL, Power consumption

Introduction

Pseudo Random Bit Generator (PRBG) circuits, being very widely used for security, compressive sensing and diverse other applications in telecommunications, are studied in different aspects in the laboratory of Computer-aided Design in Telecommunications in Technical University-Sofia. Some results of this study are published in [1] where tests for randomness from the National Institute of Standards and Technology (NIST) suite [5] are applied on commonly used PRBGs. Other aspects of the PRBG circuits study are their power consumption in the aim of green communications as noticed in [2],[3] and low power consuming devices for Internet of Things (IoT). A recent research, described in [4] has confirmed the strong influence of VHDL codes of a circuit design from a given specification and it's illustrated for a 4-bit comparator circuit.

The basic structure for hardware realization of PRBG is the Linear Feedback Serial Register (LFSR). The number of D flip-flops N in the register defines the maximal length of the pseudo-random bits generated 2^N-1 and the taps passing through XOR or NXOR gates form the feedback and determine the concrete suit for a given initial state called seed. Combinations from 2 or 3 LFSRs form more complicated circuits as Kasami and Gold, which for correctly selected polynomials, show better randomness of the bits generated than the simple LFSR circuits. One of the most widely used random bit and number generator algorithm - the Mersenne Twister, implemented in MATLAB, is also based on LFSR at the first step, the second step being tempering. The concern for low power design and green communications, as noticed in [2],[3] motivated the research described in the current paper on power consumption of PRBG circuits on FPGA. Some results on power consumption of PRBG circuits on FPGA are presented in [6], but the concrete FPGA device used is not specified and it limits the possibilities for comparison. As illustrated in [4] the concrete FPGA device is one of the factors

that influence the power consumption of the design. Other factor of influence illustrated in [4] is the type of the VHDL code – structural or behavioral. The study described further covers 2 elements: first 8 PRBG circuits with structural VHDL description, implemented on the same FPGA device, are estimated for power consumption and then 2 VHDL description of a given PRBG circuit are compared for power consumption. The results obtained for elaborated and synthesized design schematics, numbers of nets and cells generated, power consumption at synthesis and implementation stage are analyzed.

Study of the power consumption of PRBG circuits with structural VHDL descriptions

The study covers 8 PRBG circuits described in VHDL, based on LFSRs with different length, as well as Kasami and Gold circuits. The circuits studied are:

- LFSR 8 bits, TAP(0,2,3,4) – circuit described in [6],[7];
- Galois, 8 bits, TAP(4,5,6) – circuit described and studied for randomness in [1];
- LFSR, 9 bits, TAP(4,0) – circuit used in Rohde&SchwarzVector Signal Generator SMIQ03B [9], described and studied for randomness in [1];
- LFSR, 10 bits, TAP(3,0);
- LFSR, 16 bits, TAP(2,0)-circuit used in Rohde&SchwarzVector Signal Generator SMIQ03B [9], described and studied for randomness in [1];
- LFSR, 21 bits, TAP(5,3,2,0) - circuit used in Rohde&SchwarzVector Signal Generator SMIQ03B [9], described and studied for randomness in [1];
- Kasami, TAP(0,7), TAP(0,1), TAP(0,2), m=011, k=011 – circuit described in [2] and presented on Fig. 1;
- Gold, TAP(0,7), TAP(0,2,7,8) – circuit presented on Fig. 2.

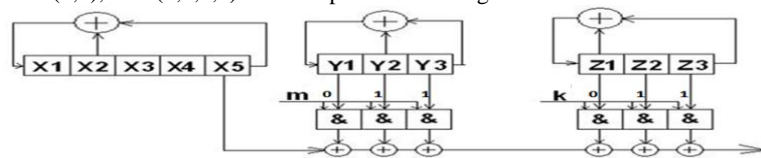


Fig.1. Kasami PRBG circuit

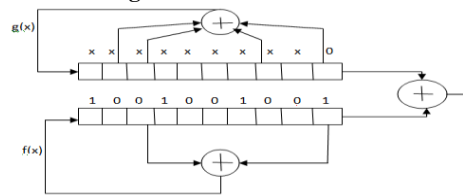


Fig. 2. 10 bit Gold PRBG circuit

The polynomials for the Gold circuit studied are:

$$f(x) = x^{10} + x^3 + 1 . \quad (1)$$

$$g(x) = x^{10} + x^8 + x^3 + x^2 + 1 , \quad (2)$$

The length of the PRBG sequence for each circuit is presented in Table 1.

Table 1.Length of the PRBG sequence for the studies LFSR, Kasami and Gold circuits

N ^o	Pseudo-random bit generator circuit On-chip power Synthesized/Implemented	Length of the PRBG sequence
1.	LFSR 8 bits, TAP(0,2,3,4)	255
2.	Galois, 8 bits, TAP(4,5,6)	255
3.	LSFR, 9 bits, TAP(4,0)	511
4.	LFSR, 10 bits, TAP(3,0)	1023
5.	LFSR, 16 bits, TAP(2,0)	65535
6.	LFSR, 21 bits, TAP(5,3,2,0)	2097152
7.	Kasami, TAP(0,7), TAP(0,1), TAP(0,2), m=011, k=011	1023
8.	Gold, TAP(0,7), TAP(0,2,7,8)	1023

All 8 circuits are first designed based on structural descriptions in VHDL, using D flip-flops and NXORs as components. All 8 circuits are implemented on the same FPGA XCZ020clg484-1 on Zedboard development system. Design and simulations are performed in VIVADO 2014 tool (XILINX).

The steps of the study in Vivado 2014 are:

- Timing simulation based on the VHDL structural description of the circuit;
- Generation of elaborated design schematic and estimation of the number of nets and cells;
- Generation of synthesized design schematic and estimation of the number of nets and cells;
- Power estimation of the synthesized design;
- Power estimation of the implemented design.

Elaborated design schematics and estimation of the number of nets and cells of the elaborated and synthesized designs for the 8 circuits from Table 1 are presented in Table 2.

Results for on-chip power consumption of the synthesized and implemented designs of the 8 circuits are presented in Table 3.

As shown on Fig. 3 for the 6 LFSR – based circuits there is slight increase of the power consumption estimated at the synthesis stage starting from 154 W for 8 bit circuits to 164 W for 21 bit circuit and almost no influence on the power consumption estimation at the implementation stage which stays constant 0.137 W from 8 to 16 bits and increases with 1mW to 0.138 W for 21 bit LSFR.

Table 2.Elaborated design schematics of PRBG circuits in Vivado 2014

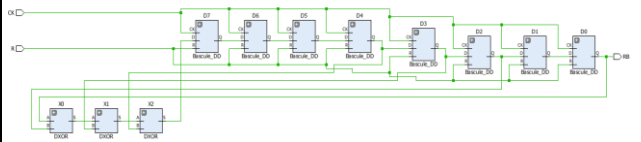
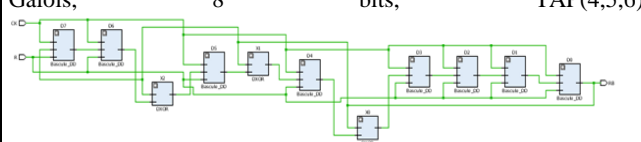
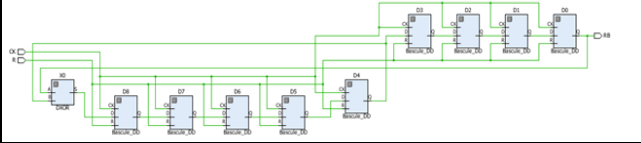
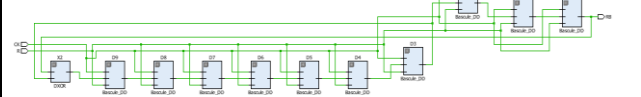
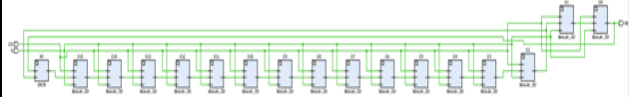
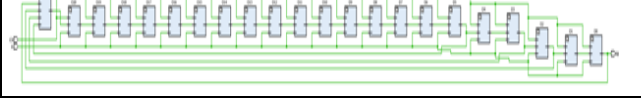
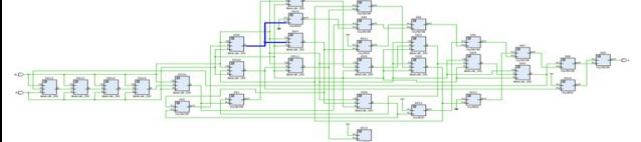
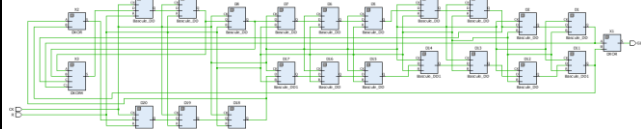
№	Pseudo-random bit generator circuit Elaborated design in Vivado 2014.4	Cells, Nets Synthesized Implemented
1.	<p>LFSR 8 bits, TAP(0,2,3,4)</p> 	11 Cells, 13 Nets 12 Cells, 16 Nets
2.	<p>Galois, 8 bits, TAP(4,5,6)</p> 	11 Cells, 13 Nets 12 Cells, 18 Nets
3.	<p>LSFR, 9 bits, TAP(4,0)</p> 	10 Cells, 12 Nets 12 Cells, 16 Nets
4.	<p>LFSR, 10 bits, TAP(3,0)</p> 	11 Cells, 13 Nets 12 Cells, 15 Nets
5.	<p>LFSR, 16 bits, TAP(2,0)</p> 	17 Cells, 19 Nets 20 Cells, 24 Nets
6.	<p>LFSR, 21 bits, TAP(5,3,2,0)</p> 	22 Cells, 24 Nets 25 Cells, 29 Nets
7.	<p>Kasami, TAP(0,7), TAP(0,1), TAP(0,2), m=011, k=011</p> 	31 Cells, 34 Nets 20 Cells, 26 Nets
8.	<p>Gold, TAP(0,7), TAP(0,2,7,8)</p> 	23 Cells, 25 Nets 24 Cells, 29 Nets

Table 3.Power consumption of PRBG circuits at synthesis and implementation stage

№	Pseudo-random bit generator circuit On-chip power Synthesized/Implemented	Synthesized Implemented
1.	<p>LFSR 8 bits, TAP(0,2,3,4)</p> <p>Synthesized: Dynamic: 0.034 W, Signals: 0.021 W, Logic: 0.006 W, I/O: 0.008 W, Device Static: 0.120 W</p> <p>Implemented: Dynamic: 0.017 W, Signals: 0.007 W, Logic: 0.006 W, I/O: 0.005 W, Device Static: 0.120 W</p>	0.154 W 0.137W
2.	<p>Galois, 8 bits, TAP(4,5,6)</p> <p>Synthesized: Dynamic: 0.034 W, Signals: 0.021 W, Logic: 0.006 W, I/O: 0.007 W, Device Static: 0.120 W</p> <p>Implemented: Dynamic: 0.017 W, Signals: 0.007 W, Logic: 0.006 W, I/O: 0.004 W, Device Static: 0.120 W</p>	0.154 W 0.137W
3.	<p>LSFR, 9 bits, TAP(4,0)</p> <p>Synthesized: Dynamic: 0.033 W, Signals: 0.021 W, Logic: 0.006 W, I/O: 0.007 W, Device Static: 0.120 W</p> <p>Implemented: Dynamic: 0.017 W, Signals: 0.007 W, Logic: 0.006 W, I/O: 0.004 W, Device Static: 0.120 W</p>	0.154 W 0.137W
4.	<p>LFSR, 10 bits, TAP(3,0)</p> <p>Synthesized: Dynamic: 0.036 W, Signals: 0.023 W, Logic: 0.006 W, I/O: 0.007 W, Device Static: 0.120 W</p> <p>Implemented: Dynamic: 0.017 W, Signals: 0.007 W, Logic: 0.006 W, I/O: 0.004 W, Device Static: 0.120 W</p>	0.157W 0.137W
5.	<p>LFSR, 16 bits, TAP(2,0)</p> <p>Synthesized: Dynamic: 0.040 W, Signals: 0.027 W, Logic: 0.006 W, I/O: 0.007 W, Device Static: 0.120 W</p> <p>Implemented: Dynamic: 0.017 W, Signals: 0.007 W, Logic: 0.006 W, I/O: 0.004 W, Device Static: 0.120 W</p>	0.160W 0.137W
6.	<p>LFSR, 21 bits, TAP(5,3,2,0)</p> <p>Synthesized: Dynamic: 0.043 W, Signals: 0.030 W, Logic: 0.006 W, I/O: 0.008 W, Device Static: 0.120 W</p> <p>Implemented: Dynamic: 0.018 W, Signals: 0.007 W, Logic: 0.006 W, I/O: 0.005 W, Device Static: 0.120 W</p>	0.164W 0.138W
7.	<p>Kasami, TAP(0,7), TAP(0,1), TAP(0,2), m=011, k=011</p> <p>Synthesized: Dynamic: 0.457 W, Signals: 0.042 W, Logic: 0.011 W, I/O: 0.404 W, Device Static: 0.122 W</p> <p>Implemented: Dynamic: 0.428 W, Signals: 0.017 W, Logic: 0.010 W, I/O: 0.401 W, Device Static: 0.121 W</p>	0.579W 0.55W
8.	<p>Gold, TAP(0,7), TAP(0,2,7,8)</p>	0.309W 0.282W

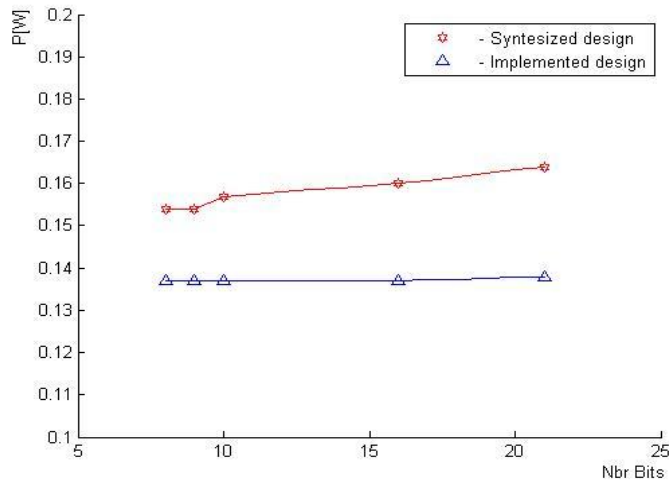
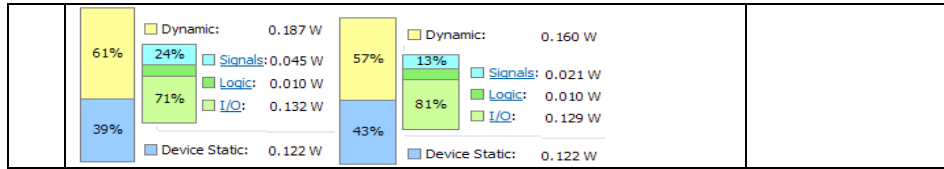


Fig. 3. Power consumption of LFSR with different width – 8, 10, 16, 21 bits for synthesized and implemented designs

The power consumption of the Gold circuit grows to 0.309W at synthesis stage and 0.282 W at implementation stage. The power consumption estimation for Kasami circuit shows the highest values from all studied circuits 0.579 W at synthesis stage and 0.550W at the implementation stage.

The decrease of the estimate at the implementation stage is due to more realistic calculation at that stage compared to worst case based estimation at the synthesis stage. The realistic correction concerns the dynamic power estimate which decreases twice at implementation stage for the 6 LFSR circuits estimated, while static power estimation stays constant. Therefore the percentage of dynamic and static power at implementation stage varies from the one at synthesis stage. The variance in power consumption estimation for the circuits of Kasami and Gold circuits concerns also the dynamic part, thus determining different percentage shares of static and dynamic powers estimates.

The predominance of power consumption for Signals in dynamic power is observed for the 6 LFSR circuits and the predominance of power consumption in I/O is observed for Kasami and Gold circuit. The power consumption in logic varies few in all 8 circuits – from 6mW for the 6 LFSR circuits to 10 mW for Kasami and Gold circuit.

The comparison of the structural elements of the different circuits from Figures 1 and 2 and the elaborated designs from Table 2 show that the increasing number of D flip-flops has little influence on the power consumption, but Kasami circuit which has also a higher number of XOR gates, has a considerable (3 times) increase of the power consumption. Power consumption of XOR circuits and means for its reduction are studied in several references as [9].

Study of the influence of different VHDL descriptions of a PRBG circuit on its power consumption

As pointed in [4] the VHDL description of a circuit for a given specification influences considerably the power consumption of the design when implemented on FPGA. In [4] the illustration is given for comparator circuits. Here a similar experience is realized for 2 different VHDL descriptions of the circuit LFSR 10 bits, TAP(3,0). The first VHDL code with structural description is:

```

library ieee;
use ieee.std_logic_1164.all;
entity LFSR10 is
    port(R, CK:in bit; RB:out bit);
end LFSR8;
architecture archLFSR8 of LFSR8 is

    signal int:bit_vector(9 downto 0);
    signal int1:bit;
    component Bascule_DD
        port(R, CK:in bit;D:in bit;Q:out bit);
    end component;
    component DXOR
        port(A,B:in bit;S:out bit);
    end component;
begin
    D9:Bascule_DD port map(R=>R,CK=>CK,D=>int1,Q=>int(9));
    D8:Bascule_DD port map(R=>R,CK=>CK,D=>int(9),Q=>int(8));
    D7:Bascule_DD port map(R=>R,CK=>CK,D=>int(8),Q=>int(7));
    D6:Bascule_DD port map(R=>R,CK=>CK, D=>int(7),Q=>int(6));
    D5:Bascule_DD port map(R=>R,CK=>CK,D=>int(6),Q=>int(5));
    D4:Bascule_DD port map(R=>R,CK=>CK,D=>int(5),Q=>int(4));
    D3:Bascule_DD port map(R=>R,CK=>CK,D=>int(4),Q=>int(3));
    D2:Bascule_DD port map(R=>R,CK=>CK,D=>int(3),Q=>int(2));
    D1:Bascule_DD port map(R=>R,CK=>CK,D=>int(2),Q=>int(1));
    D0:Bascule_DD port map(R=>R,CK=>CK,D=>int(1),Q=>int(0));
    X0:DXOR port map(A=>int(0),B=>int(3),S=>int1);
    RB <= int(0);
end archLFSR10;

```

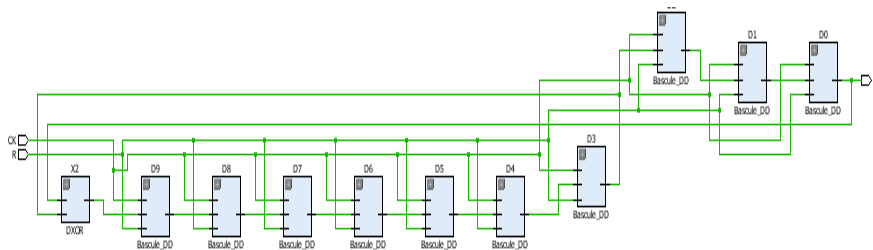


Fig 4. Elaborated design from the VHDL structural description of 10 bit LFSR TAP(3,0)

For this description the elaborated design is shown on Fig. 4 and the on-chip power estimations, the numbers of cells and nets are as follows:

- At the synthesis stage: 0.157 W, 11 Cells, 13 Nets;
- At the implementation stage: 0.137W, 12 Cells, 15 Nets.

Figure 5 shows the power reports at synthesis and implementation stage for the VHDL structural description of the 10 bit LSFR TAP(3,0).

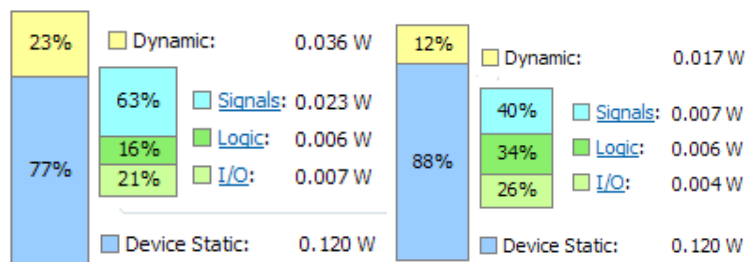


Fig. 5. Power consumption estimation at synthesis and implementation stage of the LFSR 10 bits TAP (3,0) PRBG circuit from Fig. 4

The second VHDL code using the command *reg* is:

```

library IEEE;
use IEEE.STD_LOGIC_1164.ALL;
entity lfsr is
    Port ( clk : in STD_LOGIC;
          rst : in STD_LOGIC;
          q_out : out STD_LOGIC);
end lfsr;
architecture Behavioral of lfsr is
    signal reg:std_logic_vector (9 downto 0);
    signal input_bit:std_logic;
begin
    process(rst,clk)
        begin
            if rst='1' then
                reg<="1010101010";
            elsif clk'event and clk='1' then
                reg<=(reg(8 downto 0)&input_bit);
            end if;
        end process;
    input_bit<=reg(9) xor reg(6);
    q_out<=reg(9);
end Behavioral;

```

Figure 6 shows the power reports at synthesis and implementation stage for the VHDL description with the command *reg* of the 10 bit LSFR TAP(3,0).

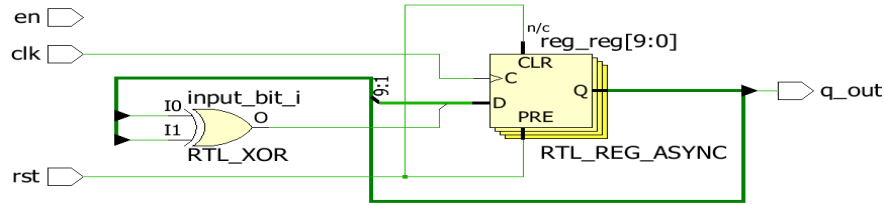


Fig. 6. Elaborated design from the VHDL description of 10 bit LFSR TAP(3,0) using the instruction *reg*

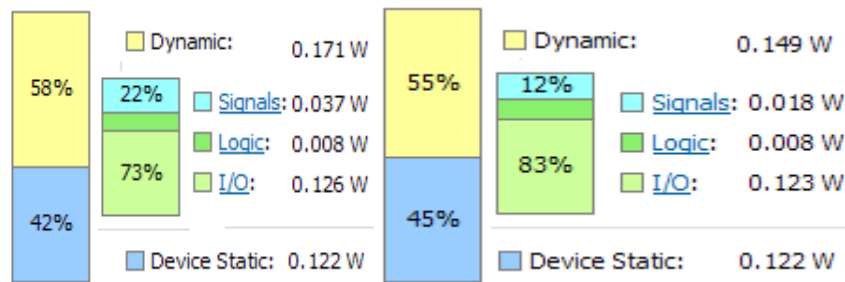


Fig. 7. Power consumption estimation at synthesis and implementation stage of the LFSR 10 bits TAP (3,0) PRBG circuit from Fig. 6

For this description the elaborated design is shown on Fig. 4 and the on-chip power estimations, the numbers of cells and nets are as follows:

- At the synthesis stage: 0.293W, 11 Cells, 13 Nets;
- At the implementation stage: 0.27W, 15 Cells, 18 Nets.

The VHDL description using the command *reg* turns to increase the power consumption of the LFSR circuit almost twice both at synthesis and at implementation stage. As noted previously there is variation in the dynamic power estimation and more precisely at power for Signals and I/O, which changes the percentage images as well.

Conclusion

The study of LFSR random bit generator circuits with structural VHDL descriptions shows very slight or missing variance of the power consumption from the length of the LFSR. More complicated circuits as Kasami and Gold show a bigger power consumption, growing to 3 times for the on-chip power estimation of Kasami circuit. As Kasami and Gold circuits are proven to be with better randomness than LFSR circuits (failing some of the NIST criteria, see [1]) and these 2 circuits have randomness performance comparable to the one of the most popular Mersenne Twister circuit (algorithm used in MATLAB), the use of Gold circuit proves to be optimal not only in terms of randomness but in terms of consumption. Results for power consumption of some of the LFSR circuits studied in this paper are given in [6] and they confirm the slight dependence of power consumption from the number of bits. They show lower values compared to the results obtained in the current study because of the implementation on a different and unspecified circuit, included in previous version of XILINX tool ISE.

The results in the paper illustrate the strong influence of the VHDL code description of the PRBG FPGA-based design on its power consumption. The methodology steps of the study realized and described in the paper can be used for studying and optimizing other classes of digital circuits for low power consumption.

References

1. Marinova G., Tchobanova Z.: Simulation, Measurement and Test Environment for Pseudo Random Number Generator Circuits, Proc. of 20th IMEKO TC4 Int. Symp., Benevento, Italy, September 15-17 (2014), 833-838
2. Marinova, G., Tchobanova Z.: Circuit Design for Green Communications – Methods, Tools and Examples, Proc. of 5th UBT Int. Conf. for Computer Science and Communication Engineering, Durres, Albania, October, 28-30, 2016, published (2017), 27-37
3. Tchobanova Z., Marinova G.: Telecommunication Systems for Green Economy – a Survey, J. Electrotechnika&Electronika E+E, V.1.2 (2017), 10-16
4. Marinova G., Tchobanova Z.: Study of the Factors Influencing Power Consumption of FPGA-based designs, Electronics'2017, National Science and Technological Center, Sofia, Bulgaria (2017), in press
5. Rukhin A. et al.: Revised: April 2010 L.E. Bassham III, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications”, NIST Special Publication 800-22 revision 1a Natl. Inst. Stand. Technol. Spec. Publ. 800-22rev1a, 1 (2010)
6. Goankar S.: Design of 8 bit, 16 bit and 32 bit LFSR for PN Sequence Generation using VHDL, Int. J. of Technical Research and Applications, e-ISSN: 2320-8163, www.ijtra.com, Special Issue 31 (2015), 305-308
7. Panda A.K., Rajput P., Shukla Bh.: FPGA Implementation of 8, 16 and 32 Bit LFSR with Maximal Length Feedback Polynomial using VHDL, IEEE Int. Conf. on Communication Systems and Network Technologies, India, (2012), 769-775
8. Vector Signal Generator SMIQ03B, Operating manual, Vol.1 and 2, Rohde&Schwarz, Germany
9. Ye Y., Roy K., Drechsler R.: Power Consumption in XOR-Based Circuits, IEEE Asia and South Pacific Design Automation Conf. ASP-DAC'99, Hong Kong, (1999), 299-302.