Mirosław PUCZKO
POLITECHNIKA BIAŁOSTOCKA, WYDZIAŁ INFORMATYKI,
ul. Wiejska 45a, 15-351 Białystok

TPG and SA with low power consumption

M.Sc. eng. Mirosław PUCZKO

Works on low power Buil-In Self-Testing. Main research concentrate on reduction power consumption in Test Pattern Generators and Signature Analyzers which are used in BIST. Additional work is exploring power reduction methods on cryptographic key generation and two-pattern testing.

e-mail: miroslaw.puczko@gmail.com

Abstract

In this paper new solutions for reducing a switching activity of BIST environment for the scan-organized BIST architectures are presented. Several approaches of low power BIST have been proposed. In [1], the author presents a test scheduling approach that takes into consideration the power consumption. For general BIST structure a new test pattern generator is proposed in [2]. There is a set of solutions to eliminate useless pseudo random patterns during the test mode [3-5]. The paper is organized as follows. In Section 2 the power consumption issue and weighted switching activity modeling are investigated. Section 3 presents switching activity of basic logic structures. In Section 4 a new technique is proposed. Section 5 shows the multi-input modulo 2 adder with low power consumption. In Section 6 modified structures of TPG and SA are presented. Section 7 shows two-pattern testing and Section 8 cryptographic key generation with low power consumption. Sections 9-11 include hardware verification of the presented solutions. Section 12 is the summary.

Keywords: TPG, SA, M–sequence, Geffe generator, BIST, low power, test-per-clock, two-pattern testing.

Projektowanie generatorów testów (TPG) oraz analizatorów sygnatur (SA) o obniżonym poborze mocy

Streszczenie

Pobór mocy w systemach cyfrowych może znacząco wzrosnąć podczas procesu testowania. Niniejsza publikacja opisuje metodę, dzięki której może zostać zmniejszone zużycie energii w układach cyfrowych podczas testowania BIST (ang. *Built-In Self-Testing*). Niniejsze rozwiązanie zostało opracowane w oparciu o standardową strukturę rejestru przesuwającego z liniowym sprzężeniem zwrotnym LFSR(ang. Linear Feedback Shift Register). Weryfikacja sprzętowa pokazuje, iż pobór mocy został zmniejszony o około 50% w porównaniu ze strukturą klasyczną. Zaproponowane rozwiązanie zweryfikowano sprzętowo w generatorze testów TPG (ang. *Test Pattern Generator*), analizatorze sygnatur SA (ang. *Signature Analyzer*), generatorze par wektorów testowych oraz zmodyfikowanym generatorze Geffe'go. Zawartość artykułu jest następująca. W części 2. opisano podstawowe definicje związane z poborem mocy w BIST. W części 3. przedstawiono sposób obliczania aktywności przełączeń podstawowych struktur logicznych. W części 4. pokazano wpływ sposobu projektowania układu na jego aktywność przełączeń. Część 5. zawiera metodę projektowania wielowejściowego sumatora modulo 2 o minimalnej aktywności przełączeń. Zmniejszenie poboru mocy w generatorach testów i analizatorach sygnatur wykorzystywanych w BIST zostało zaprezentowane w części 6., natomiast obniżenie poboru mocy podczas testowania układów cyfrowych z wykorzystaniem par wektorów testowych w części 7. Część 8. to obniżenie poboru mocy podczas testowania układów cyfrowych z wykorzystaniem par wektorów testowych. Rozdziały 9–11 zawierają weryfikację sprzętową zaprezentowanych metod i algorytmów. Podsumowanie zawiera część 12.

Słowa kluczwe: TPG, SA, M–sekwencja, generator Geffe, BIST, niski pobór mocy.

1. Introduction

Power consumption in digital CMOS circuits depends directly on frequency and physical parameters of the primary gates. In [1] it has been shown that power consumption during testing mode is higher than during normal working mode. That is why any new solution for power reducing during the test mode is the matter of great interest for practice. At the same time the adequate power consumption metric is an open issue due to existing approaches allowing getting just an approximate value of real energy consumption, rather than worse case (maximal) estimation.

Several approaches of low power BIST have been proposed. In [2], the author presents a test scheduling approach that takes into consideration the power consumption. For general BIST structure a new test pattern generator is proposed [3] to reduce the circuit inputs activity without affecting test efficiency, thus reducing power consumption. There is a set of solutions to eliminate useless pseudo random patterns during the test mode [4] to keep the same fault coverage at acceptable test length as the result of the lower level of power consumption.

The most spread and the best known are scan design techniques. They assume that during testing mode all memory elements (flip-flops and latches) in sequential circuits are connected into one or more shift registers or scan paths. LFSR is the most popular device for generation pseudo-random test sequences. Also a structure of LFSR can be modified to accept an internal input in order to work as a polynomial divider (called Signature Analyzer - SA). That is why the sufficient amount of energy is consumed during the shifting mode, for the bit stream generation, output response compaction and bit stream shifting into the scan. In [5] it has been shown that BIST hardware may consume up to 70% of total energy during testing mode.

This paper presents a new solution for decreasing BIST switching activity for scan-based architecture. This method can also be used in low power Geffe generator and two-pattern testing.

The paper is organized as follows. In Section 2 the power consumption issue and weighted switching activity modeling are investigated. Section 3 presents switching activity of basic logic structures. In Section 4 there is proposed a new technique for more precise estimation of power consumption for arbitrary digital circuits based on the propagation of the switching along the chain of the gates. Section 5 shows the multi-input modulo 2 adder with low power consumption. In Section 6 the modified structures of TPG and SA are presented. Section 7 shows two-pattern testing and Section 8 cryptographic key generation with low power consumption. Sections 9-11 include hardware verification of the presented solutions. Section 12 is the summary.

2. Power model

Power dissipation in CMOS circuits can be classified into static and dynamic. As it has been shown in [6] dynamic power is the dominant source of power consumption, which is charging and discharging of the load capacitance during output switching. Energy used during one switching in node *j* is given by (1) [7].

$$E(1)_j = \frac{1}{2} \cdot C_j \cdot V_{dd}^2 \tag{1}$$

where: C_j –output capacity, V_{dd} –power supply. Nodes connected to more than one gate have higher load capacitance. For these nodes output capacity C_j is calculated from expression (2).

$$C_j = s_j \cdot C_0 \tag{2}$$

where : s_j – the fan-out of the node j, C_0 – load capacitance of standard logic element.

Substituting formula (2) to (1) and considering the number of cycles in j–node (f_j) one obtains the expression for calculation energy E_j in node j (3).

$$E_j = \frac{1}{2} \cdot s_j \cdot f_j \cdot C_0 \cdot V_{dd}^2 \tag{3}$$

Expression $s_j \cdot f_j$ is named switching activity on node j and is the metric of switching activity in this node. Because $s_j \cdot f_j$ is the only changing value in expression (3) calculation of energy use can be summed up in the calculation of (4):

$$SA_j = s_j \cdot f_j \tag{4}$$

Switching activity during one clock pulse (WSA_{CLK}) can be calculated from expression (5) and is named Weighted Switching Activity.

$$WSA_{CLK} = \sum_j s_j \cdot f_j \tag{5}$$

This metric will be used for calculation power in BIST.

3. Switching activity of logical structures

Switching activity of logical structures, in classical approach, is calculated on the gate level [8] based on signal probabilities in the nodes. The method for this is presented in [9] for non-delayed circuits. For delayed circuits in [10-11] there is presented the author's method for calculation of switching activity. It is based on calculation of the sum of multiplied switching activity of each input x_i, labeled in expression (6) as SA_{x_i}, and propagation probability of switching in the input x_i to output, marked in expression (6) as $P_{pr}(x_i)$. For *n*–input gate expression for calculation of switching activity (SA_{mj}) is presented in (6):

$$SA_{mj} = \sum_{i=1}^{n} SA_{x_i} \cdot P_{pr}(x_i) \tag{6}$$

By using probability propagation of switching in the input x_i to output it was possible to calculate the maximum switching activity.

4. Layout design and its switching activity

Using the method developed in [10-11] there was examined the impact of circuit design on the switching activity. Using 5-input circuit there were built its different variants for different logic gates and calculate its switching activity SA_w and maximal switching activity during one clock pulse $(\max(WSA_{CLK}))$.

As it is shown in Tab.1, the way of designing circuit has a significant impact on the switching activity, thus reducing the power consumption. Bold italics indicate the maximum switching activity during one clock cycle.

Tab. 1. Switching activity for 5-input circuit
Tab. 1. Aktywność przełączeń dla 5-cio wejściowego układu

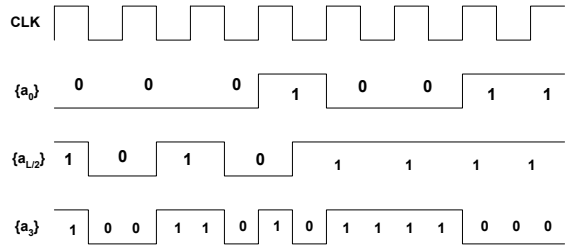
Variant	*F*=AND	
	SA_w	$\max(WSA_{CLK})$
1.	0,7714	1,0742
2.	0,9277	1,1875
3.	1,0292	***1,4140***
Variant	*F*=OR	
	SA_w	$\max(WSA_{CLK})$
1.	0,7714	1,0742
2.	0,9277	1,1875
3.	1,0292	***1,4140***
Variant	*F*=XOR	
	SA_w	$\max(WSA_{CLK})$
1.	2	***7***
2.	2	6,5
3.	2	6

5. Design method of multi-input adder modulo 2 with a minimum switching activity

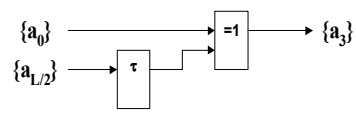
As it was shown in Section 4 the switching activity is different depending on the realisation variant of a multi-input circuit [10]. Using the optimal solution (minimal power consumption) presented in [11], the method of designing the multi-input adder modulo 2 with a minimal switching activity is presented. The additional result obtained during research was getting factor *k*, which means how many times (maximally) the switching activity could increase for realisation on 2-input XOR Gates.

6. Decreasing power consumption in TPG and SA using in BIST

In order to decrease the power consumption in a test pattern generator and a signature analyzer in [12] there was used decimation of M-sequence, example of which for the primitive polynomial $f(x)=1+x^3+x^5$ is shown in Fig.1. There are adopted the following signs: $\{a_0\}$–characteristic shift of M–sequence, $\{a_3\}$– the received M-sequence.



a) timing diagrams
a) diagramy czasowe



b) doubling frequency circuit
b) układ podwajający częstotliwość

Fig. 1. M–sequence generation with the double frequency
Rys. 1. Generowanie M–sekwencji o podwójnej częstotliwości

To generate double frequency M-sequence, there are needed two M-sequences in which the second one is the copy of the first one shifted equally on the half of its period. To make this conception, there is needed a delay element, whose delay equals $\tau = \frac{T}{2}$, where T is period of M-sequence. The block diagram of the presented solution is shown in Fig. 1,b [13]. The mathematical description of this solution is presented in [14].

7. Low power two-pattern testing

In order to ensure the high reliability of digital systems, they should be subjected to such a test which can detect delay faults and stuck-open faults [15].

It has been proven that by using the modified structure of the test pattern generator it is possible to generate the pairs of test vectors with the low weighted switching activity and thus with the low power consumption. Given the structure of the standard test generator, the primitive polynomials with the minimum number of non-zero coefficients (the minimum number of XOR gates) provide the lowest power consumption. The modified structure of the generator allows getting lower power consumption for one new bit. Calculations for the primitive polynomials up to 30th degree show that the efficiency can be over 80%. In contrast to the classical structure of the test generator, in the modified structure the weighted activity depends only to a small extent on the number of non-zero coefficients of the primitive polynomial while generating more than one new bit to a synchronization cycle [16-18].

8. Reducing power consumption of a cryptographic key generators

This section describes the use of a modified LFSR structure in Geffe's generator and show the results of calculations of WSA [19-21].

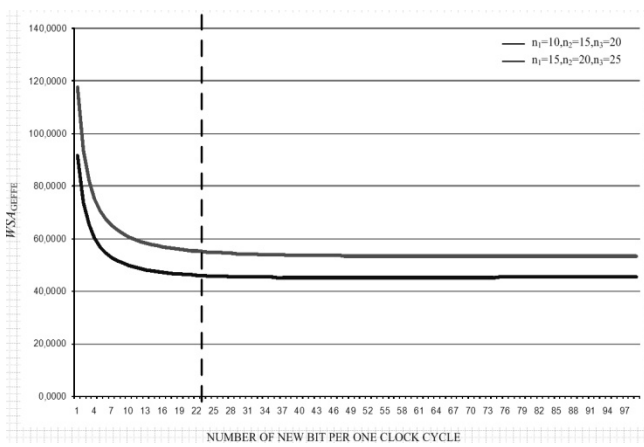


Fig. 2. WSA reduction for Geffe generator for primitive polynomials of degree n_1=10, n_2=15, n_3=20; n_1=15, n_2=20, n_3=25

Rys. 2. Zmniejszenie WSA dla generatora Geffe'go dla wielomianów pierwotnych stopni n_1=10, n_2=15, n_3=20; n_1=15, n_2=20, n_3=25

It can be concluded that the more new bits are generated during one clock cycle, the lower weighted switching activity is (Fig. 2). This relationship refers to the number of new bits fewer or equal to 22. After crossing this value the switching activity remained more or less stable.

9. Hardware verification of the presented solutions for TPG and SA

This section presents software (in VHDL language) and hardware (on the programmable board XSA-100) verification of methods concerning BIST. To achieve this goal, XILINX® Webpack ISE in v. 9.2i was used. Because there is no integrated simulator in this package the ModelSim XE III 6.4b was used. Power was measured by XILINX® XPOWER 9.2i v. J.36.

To verify the results of theoretical plate, there was used the programmable board XSA-100 from XESS ® (Fig. 3), which contained 100,000 gates.

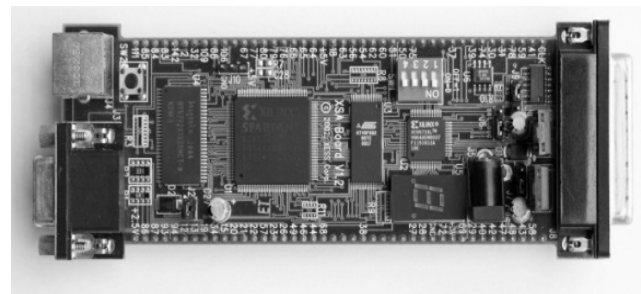


Fig. 3. XSA-100 programmable board

Rys. 3. Płyta programowalna XSA-100

Algorithms used in publications [10-14, 19-21] were coded in VHDL language and then programmed at selected board components. The aim was to verify the theoretical results and the possibility of their hardware implementation.

To confirm the proposed methods and algorithms of publications [10-14] and [16-21], there was used the main board (XSA-100) component - XC2S100 system (Fig. 4).

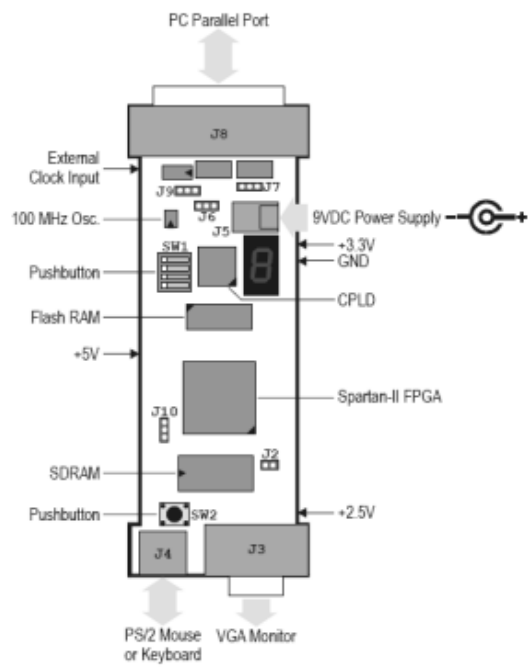


Fig. 4. XSA-100 components

Rys. 4. Komponenty płyty XSA-100

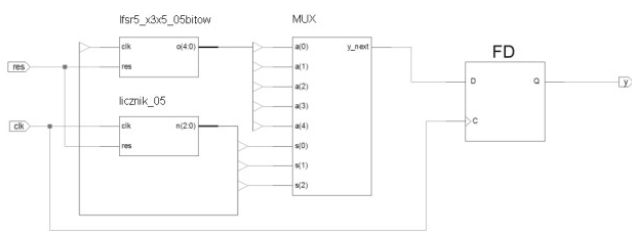
The information provided in Section 6 that in order to reduce the power consumption in the modified structure of the generator and signature analyzer it is necessary to generate more than one new bit in one clock cycle. Therefore written in VHDL designs for all polynomials 5 and 10 degree to the number of new bits from 1 to 40. An example of one such project, which generates 5 new bits, using the primitive polynomial $f(x)=1+x^3+x^5$, is shown in Fig. 5.

```
entity uklad_lfsr5_x3x5_05bitow is
generic ( n : natural :=4;
          i : natural :=2);
    Port ( clk : in  STD_LOGIC;
           res : in  STD_LOGIC;
           y : out  STD_LOGIC);
end uklad_lfsr5_x3x5_05bitow;

architecture Behavioral of uklad_lfsr5_x3x5_05bitow is
signal y_next: std_logic;
signal a : std_logic_vector(n downto 0);
signal s :  std_logic_vector(2 downto 0);

component lfsr5_x3x5_05bitow is
Port (
                clk                 :         in
          std_logic;
                res                 :         in
          std_logic;
                o                   :         out
          std_logic_vector(4 downto 0));
end component;

component licznik_05 is
Port (
                clk                 :         in
          std_logic;
                res                 :         in
          std_logic;
                n : out  STD_LOGIC_VECTOR (2 downto 0)
                );
end component;

begin
ukl_lfsr5_x3x5_05bitow: lfsr5_x3x5_05bitow port map (s(2),res,a);
ukl_licznik_05: licznik_05 port map (clk,res,s);

process(a,s)
begin
case s is
          when "000" => y_next<=a(0);
          when "001" => y_next<=a(1);
          when "010" => y_next<=a(2);
          when "011" => y_next<=a(3);
          when others => y_next<=a(4);
end case;
end process;

process (clk)
begin
if clk'event and clk='1' then
y<=y_next;
end if;
end process;

end Behavioral;
```

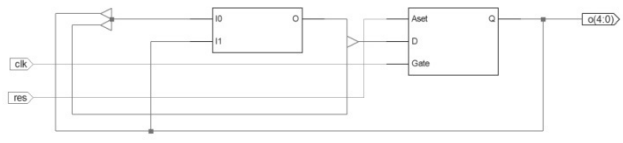
Fig. 5. Main program for 5 new bits generation for primitive polynomial $f(x)=1+x^3+x^5$
Rys. 5. Główny program, którego wynikiem jest wygenerowanie 5 nowych bitów dla wielomianu pierwotnego $f(x)=1+x^3+x^5$

Then, using Xilinx® Webpack ISE, there was carried out the synthesis of low power outlined in the section three, and there was measured the power consumption of the FPGA Spartan-II XC2S100 in the program XILINX ® XPOWER.

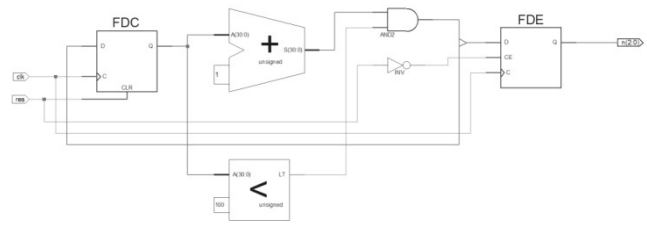
For verification of the design patterns there were used RTL schemas, giving views of scheme systems at an early design stage (Fig. 6).



a) RTL scheme
a) schemat RTL



b) RTL scheme of component *lfsr5_x3x5_05bitow*
b) schemat RTL komponentu *lfsr5_x3x5_05bitow*



c) RTL scheme of component *licznik_05*
c) schemat RTL komponentu *licznik_05*

Fig. 6. RTL schemes
Rys. 6. Schematy RTL

Once satisfied, on the basis of patterns of RTL that the system will work as expected, that will generate more than one new bit in one clock cycle, there was measured the power consumption of all primitive polynomials of 5 and 10 degree.

Figs. 7 and 8 show the results of power measurements for all polynomials of 5 and 10 degree, respectively. The power was at its highest frequency XSA-100 board of 100 MHz and working time 4000 ns.

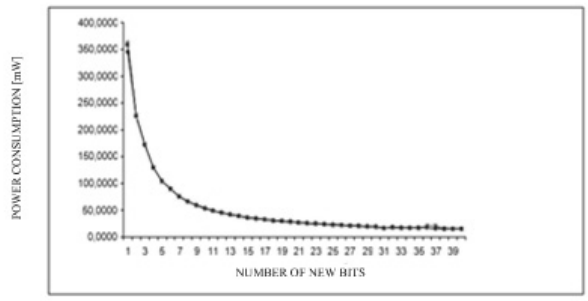


Fig. 7. Power consumption for primitive polynomials of 5th degree for number of new bits 1-40
Rys. 7. Pobór mocy wielomianów pierwotnych 5-go stopnia dla liczby nowych bitów 1-40

As seen from Figs. 7 and 8, implementation of the methods and algorithms described in publications [10-14] allows for lower power in BIST both TPG and SA.

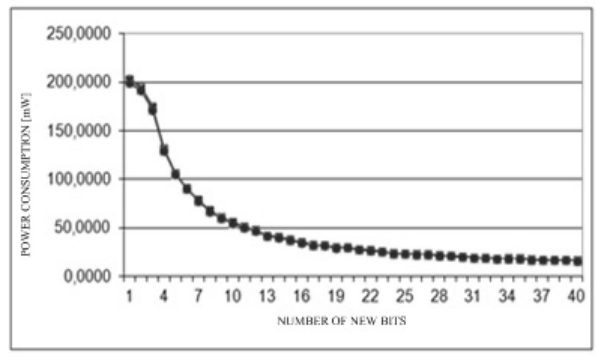
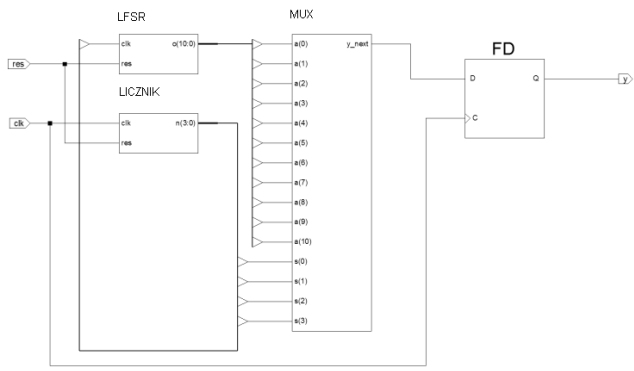


Fig. 8. Power consumption for primitive polynomials of 10th degree for number of new bits 1-40
Rys. 8. Pobór mocy wielomianów pierwotnych 10-go stopnia dla liczby nowych bitów 1-40

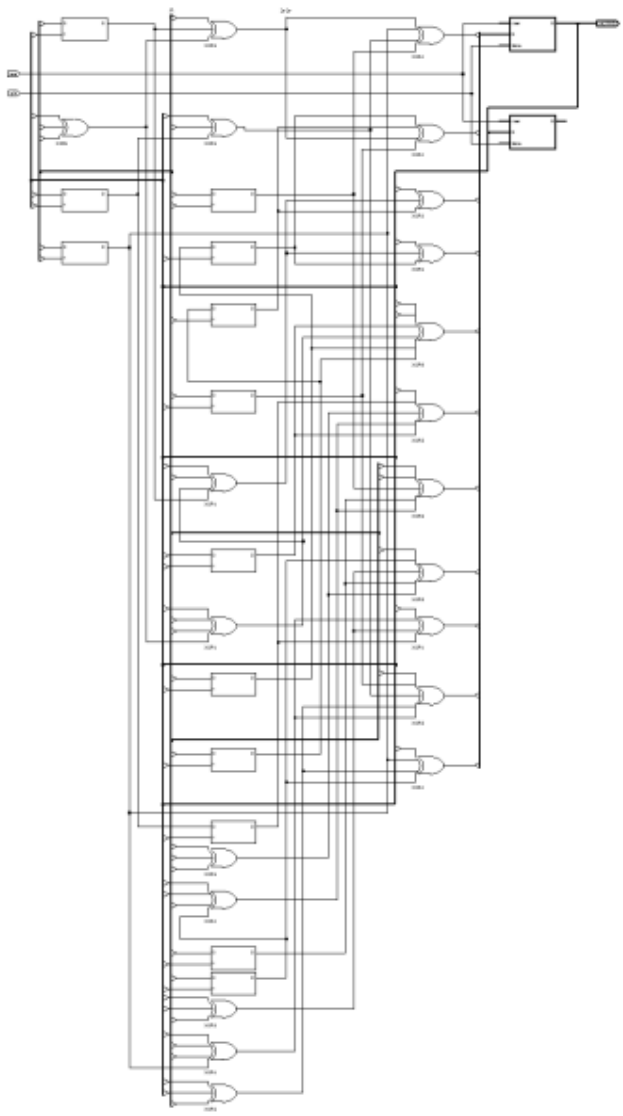
10. Hardware verification of the presented solutions for two-pattern testing

The results of theoretical calculations of the power contained in Section 7 were simulated.

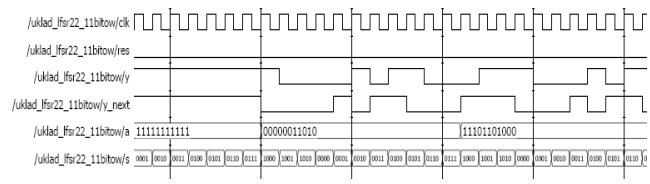
For each of the used primitive polynomials of 20, 22, 24, 26, 28, 30 degree there was generated the number of new bits equal a half of the degree. In Fig.9 there is presented a) circuit RTL scheme for primitive polynomial $f(x)=1+x^6+x^8+x^9+x^{10}+x^{11}+x^{12}+x^{14}+x^{15}+x^{16}+x^{17}+x^{18}+x^{19}+x^{21}+x^2$, b) modified LFSR RTL scheme, c) timing diagram, d) power consumption in XPOWER.



a) circuit RTL scheme
a) schemat RTL



b) modified LFSR RTL scheme
b) schemat RTL zmodyfikowanej struktury LFSR'a



c) timing diagram
c) diagram czasowy

```
--------------------------------------------------------------------
Release 9.2i - XPower SoftwareVersion:J.36

Power summary:                              I(mA)     P(mW)
--------------------------------------------------------------------
Total estimated power consumption:                      620
                                             ---
                          Vccint 2.50V:      221       552
                          Vcco33 3.30V:       21        68
                                             ---
                               Clocks:        19        48
                               Inputs:        20        49
                                Logic:       147       369
                              Outputs:
                                 Vcco33       19        61
                              Signals:        32        81
                                             ---
                 Quiescent Vccint  2.50V:      2         5
                 Quiescent Vcco33  3.30V:      2         7

Thermal summary:
--------------------------------------------------------------------
   Estimated junction temperature:                      44C
                       Ambient temp:  25C
                          Case temp:  41C
                    Theta J-A range:  31 -  32C/W
```

d) power consumption in XPOWER
d) pobór mocy w programie XPOWER

Fig. 9. Power calculation scheme for primitive polynomial $f(x)=1+x^6+x^8+x^9+x^{10}+x^{11}+x^{12}+x^{14}+x^{15}+x^{16}+x^{17}+x^{18}+x^{19}+x^{21}+x^{22}$
Rys. 9. Pobór mocy dla wielomianu pierwotnego $f(x)=1+x^6+x^8+x^9+x^{10}+x^{11}+x^{12}+x^{14}+x^{15}+x^{16}+x^{17}+x^{18}+x^{19}+x^{21}+x^{22}$

As seen from the obtained results, the power consumption does not depend on the selected primitive polynomial. It is true that the minimum number of ones in the primitive polynomial, power consumption is the lowest, but the difference is not large (about 18%). It can be seen that the higher the degree of the primitive polynomial and the number of the generated new bits the difference between the power consumption of the polynomials with the minimum and maximum number of ones in the primitive polynomial (for the 20-degree and 10 new bits the difference between the energy consumption of the polynomial with 2 non-zero coefficients and 16 is 4.6 mW, and for the polynomial 30-degree for a 4 and 24 non-zero coefficients amounts to 9.14 mW).

11. Hardware verification of the presented solutions for cryptographic key generator

To verify theoretical calculation presented in publications [19-21], the modified Geffe generator was designed. In Fig.10 there is an example of XPOWER measurement for the Geffe's generator using degree LFSR's: $LFSR_1$=20, $LFSR_2$=21, $LFSR_3$=22 and primitive polynomials $f(x)=1+x^{17}+x^{20}$, $f(x)=1+x^{19}+x^{21}$, $f(x)=1+x^{21}+x^{22}$ number of new bits equals from 1 to 40.

As seen from Fig. 11, with increase in the number of new bits per clock cycle, the power consumption decreases. The largest decrease occurs in the first 10 bits, and 20 bits, and for the next new bits the difference in the power consumption is low.

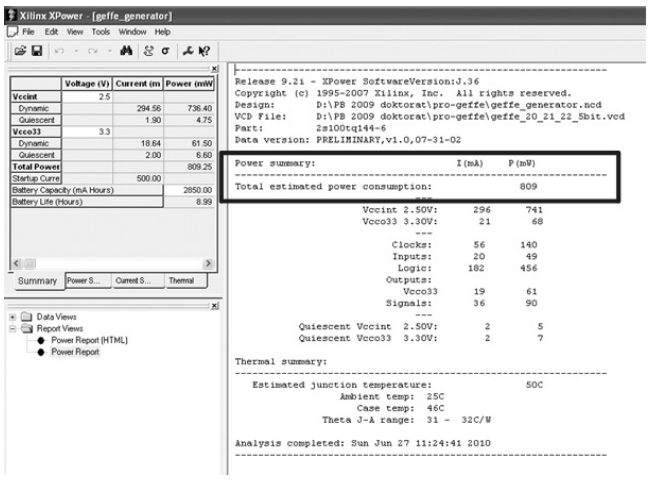


Fig. 10. XPOWER screen capture for Geffe generator for primitive polynomial $LFSR_1$=20, $LFSR_2$=21, $LFSR_3$=22

Rys. 10. Zrzut ekranu z programu XPOWER generatora Geffe'go dla wielomianów pierwotnych $LFSR_1$=20, $LFSR_2$=21, $LFSR_3$=22

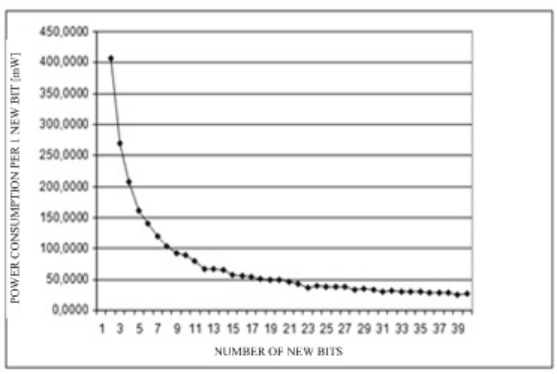


Fig. 11. Power consumption for modified Geffe generator with primitive polynomials: $f(x)=1+x^{17}+x^{20}$, $f(x)=1+x^{19}+x^{21}$, $f(x)=1+x^{21}+x^{22}$

Rys. 11. Pobór mocy dla zmodyfikowanej struktury generatora Geffe'go dla wielomianów pierwotnych $f(x)=1+x^{17}+x^{20}$, $f(x)=1+x^{19}+x^{21}$, $f(x)=1+x^{21}+x^{22}$

12. Summary

The methods and algorithms presented in [10-21] analyze the problem of considerable power consumption by test pattern generators and signature analyzers in BIST. The paper presents currently used methods and techniques for the design of test pattern generators and signature analyzers which allow minimizing the power consumption. The method of designing a multi-input adder modulo 2, built of 2-input XOR gates, used in TPG and SA is presented. The methods of fast generation on M-sequence, using a delay element and the adder modulo 2 is proposed. This method could also be used in two-pattern testing design and Geffe generator.

A set of the developed methods and algorithms, simulation and hardware verification confirm that their use leads to lower power consumption in BIST.

13. References

[1] Zorian Y.: A Distributed BIST Control Scheme for Complex VLSI Dissipation, Proc. Proc.11th IEEE VLSI Test Symposium, 1993, pp. 4-9.

[2] Wang S., Gupta S.: DS-LFSR: A new BIST TPG for low Heat Dissipation, Proc. of IEEE International Test Conference (ITC'97), November 1997, pp. 848-857.

[3] Corno F., Rebaudengo M., Sonza Reorda M., Violante M.: A new BIST Arhitecture for Low Power Circuits, IEEE European Test Workshop (ETW'99), 1999,pp.160-164.

[4] Girard P., Guiller L., Landrault C., Pravossoudo-vitch S.: A Test Vector Inhibiting Technique for Low Energy BIST Design, Proc. 17th IEEE VLSI Test Symposium, 1999, pp.407-412.

[5] Gerstendorfer S., Wunderlish H.J.: Minimized Power Consumption for Scan-Based BIST, Proc. of IEEE Int. Test Conf., 1999. pp. 77-83.

[6] Cirit M.A.: Estimating Dynamic Power Consumption of CMOS Circuits, ACM/IEEE International Conference on CAD, November 1987, pp.534-537.

[7] Gary P. Yeap: Practical Low Power Digital VLSI Design, Kluwer Academic Publisher, 1998.

[8] Zhou H.: Optimal Low Power XOR Gate Decomposition, Design Automation Conference: 37th International Conference, Danvers, USA, 5–9 June 2000, ACM, pp. 104–107.

[9] Brzozowski I., Bratek P., Dziurdzia P., Kos A.: New concept of low power digital circuits design, 7th International Conference Mixdes Design of Integrated Circuits and Systems, MIXDES'2000, 2000, pp. 181-184.

[10] Puczko M., Yarmolik V.N.: Projektowanie samotestujących się układów o niskim poborze mocy, IV Ogólnopolskie Warsztaty Doktoranckie: OWD'2002, Istebna, 2002, pp. 93-98.

[11] Yarmolik V.N., Puczko M.: Power consumption evaluation for built-in self-test circuitry, Advanced computer systems: ACS'2002: 9th International Conference, Międzyzdroje, 2002, pp. 209-215.

[12] Puczko M., Murashko I.: Techniki zmniejszania poboru mocy wykorzystywane podczas wbudowanego samotestowania, Pomiary, Automatyka, Kontrola, 2006, R.51, No. 6, pp. 56-58.

[13] Puczko M., Murashko I., Yarmolik V.N.: Zmniejszanie poboru mocy w samotestujących układach cyfrowych, Pomiary, Automatyka, Kontrola, 2007, R.53, No. 7, pp. 3-5.

[14] Puczko M., Yarmolik V.N.: Projektowanie generatorów testów o niskim poborze mocy, VII Krajowa konferencja Naukowa: Reprogramowalne układy cyfrowe, Szczecin, 2004, pp. 283-290.

[15] Chowdhury S., Barkatullah J.S.: Estimation of maximum currents in MOS IC logic circuits, IEEE Transactions on Computer-Aided Design, 1990, Vol. 9, No. 6, pp. 642-654.

[16] Puczko M., Yarmolik V.N.: Low power design for two-pattern test sequence generator based on LFSR, Computer Information Systems and Applications Vol.1, 2004, pp. 246-253.

[17] Puczko M., Yarmolik V.N.: Two-pattern test generation with low power consumption based on LFSR, Information processing and security systems, Springer-Verlag, 2005, pp. 159-166.

[18] Puczko M.: Symulacja poboru mocy podczas testowania układów cyfrowych z wykorzystaniem par wektorów testowych, XI Warsztaty Naukowe PTSK: Symulacja w badaniach i rozwoju, 2005, pp. 251-258.

[19] Puczko M., Yarmolik V.N.: Designing cryptographic key generators with low power consumption, 3rd IEEE International Workshop on Electronic Design, Test and Applications : DELTA'2006, pp. 418-421.

[20] Puczko M., Yarmolik V.N.: Stream cipher keys generation with low power consumption based on LFSR, In: Biometrics, computer security systems and artificial intelligence applications, Springer Verlag, 2006, pp. 165-173.

[21] Puczko M., Yarmolik V.N.: Stream cipher keys generation with low power consumption based on LFSR, In: Image analysis, computer graphics, security systems and artificial intelligence applications, WSFiZ, Białystok, 2005, pp. 269-275.

otrzymano / received: 03.07.2013
przyjęto do druku / accepted: 02.09.2013 *artykuł recenzowany / revised paper*