Testing an SCA hardened combinational standard cell - preliminary considerations

Milena Stanojlović, Vančo Litovski and Predrag Petković

Abstract - This paper describes testing of the NSDDL AND cell, being part of NSDDL (No Short-circuit current Dynamic Differential Logic) side-channel-attack-resistant library. The simulation results illustrate a vulnerability of AND logic cell in the presence of a defect. Fault dictionary will be created based on repetitive simulation preformed on the circuit level description of the AND cell with faults inserted one by one. Only short-circuit faults will be considered. The cells are designed in CMOS TSMC035 technology using Mentor Graphics design tools.

Keywords - crypto-system, SCA, testing, defect.

I. Introduction

The significance of information encrypted within running messages provokes adversaries to try to disclose their contents. Any illegal attempt to access encrypted content is treated as an attack on the cryptographic system. A common way for unauthorized disclosure of encrypted information relays on attempts for finding combinations that allow encryption key detection. Complex cryptographic algorithms are designed to discourage the attacker, or to impede the breaking the key by searching for all possible combinations in real time. Additional information about the behaviour of an electronic crypto-system can significantly reduce the number of combinations needed to explore a cipher [1]. Collecting such information is known as the Side Channel Attack - SCA. The most popular methods for SCA relay on monitoring of dynamics consumption at the electronic crypto-system. The most effective are SPA (Simple Power Analysis), DPA (Differential Power Analysis) and EMA (Electromagnetic Analysis) [2, 3].

The supply current (I_{DD}) is a very important additional source of information about the behaviour of cryptographic systems. An abrupt change of I_{DD} in a CMOS digital circuit occurs only during transition between logic states. When changing from 0 to 1, the output capacitances are charged to V_{DD} through the PMOS network. As the state changes from 1 to 0, capacitances are discharge to ground. In addition, during transition some short-circuit current flows when PMOS and NMOS transistors are in on-state simultaneously. Attackers are able to provide stimulus data, but cannot access the points in which they could register the response. The only source of information about the behavior of a circuit is activity expressed through the change of the supply current. Obviously, the information of circuit consumption is correlated with the circuit activity. In the struggle against these attacks different cryptographic methods are used as hardware solutions.

We chose the NSDDL (No Short-circuit current Dynamic Differential Logic) [4] as a cryptographic method in hardware for data protection. The method is based on a modification TDPL (Three-Phase Dual-Rail Pre-Charge Logic) approach which introduces a third phase of work, during which all the capacitors in the circuit are empty [5]. An important novelty in NSDDL method is its immunity on unbalanced load of the true and false outputs. In addition, the method requires only one new cell that is combined with standard logic cells.

To our knowledge the subject of test sequence synthesis and generally, testing of NSDDL based circuits was not considered in the literature and in that sense these proceedings are kind of pioneering work. Namely, the NSDDL method being based on (anti-) symmetry of two circuits named TRUE and FALSE (as will be explained later on in this paper) is by nature susceptible to faults that disturb the symmetry. From that point of view testing such circuits, or better to say, test signal synthesis should be a relatively straightforward task. It is the goal of this paper to propose a procedure for test signal synthesis and to give the first answers as to how easy the testability of this kind of circuits is. This is to be considered as a continuation of our research in testing of NSDDL circuit since in [6] fault simulation of a sequential circuit was performed.

For demonstration of the procedure we usually implement in such situations [7], in this paper, we will consider testing of one of the simplest NSDDL cells - the AND circuit. In fact, after insertion of short-circuit defects in the fault free circuit, the output signal and the proper NSD value (calculated using supply current) for each defect for certain combinations of input signals will be monitored by simulation. Namely, besides examining the logic function of the circuit, it is also very important to compare the supply currents of the faulty and fault free circuits. When defect is present in the circuit, it is very likely that it will be mapped in to change of mentioned supply current

Milena Stanojlović is with with ICAT, Vojvode Mišića 58/2, 18000 Niš, and also with LEDA laboratory Faculty of Electronic Engineering, University of Niš, Aleksandra Medvedeva 14, Serbia E-mail: (milena@venus.elfak.ni.ac.rs)

Vančo Litovski and Predrag Petković are with Department of Electronics, Faculty of Electronic Engineering, University of Niš, Aleksandra Medvedeva 14, 18000 Niš, Serbia
E-mail: (vanco.litovski@elfak.ni.ac.rs)
E-mail: (predrag.petkovic@elfak.ni.ac.rs)

[6]. The number of simulations will depend on the number of defects which are tested.

Simulation results were obtained using *ELDO* simulator of *Mentor Graphics Design Architect* environment. To get the proper circuit parameters for simulation, layout design was performed first and post-layout parameter extraction took place. To draw the layout *IC studio Mentor Graphics tools* was used.

The subsequent section reviews the core of NSDDL method. The third section explores design methodology and SCA resistivity of AND NSDDL cell. The simulation results for AND logic cell, in the presence of a defect, is described in the fourth section. Fault dictionary is created in order to allow for verification of the input signal for testing purposes.

II. NSDDL METHOD

Cells resistant to SCA are based on the idea that each combination of input signals results in the same power consumption. This is possible when every logic cell has a counterpart that will react complementary. Therefore every functional cell has two outputs denoted as *true* and *false*. The hardware is doubled, but the effect of masking the true function of the cell is gained.

NSDDL method is based on the three phase clocking. The first phase named *pre-charge* is aimed to drive all outputs (true and false) of all logic cells to go to high logic level. In the second phase, known as *evaluation* phase true output takes desired value and false output takes the complementary value. The third phase is named *discharged* because all outputs go to the low logic level.

The advantage of this method compared to other popular solutions, like WDDL [8], is its immunity to imbalance loads at true and false output. This is achieved by using a dynamic NOR circuit (DNOR) which minimizes the impact of short-circuit currents in the CMOS circuit. It is integral part of the control logic and NSDDL cells. Figure 1 illustrates the circuitry of DNOR cell.

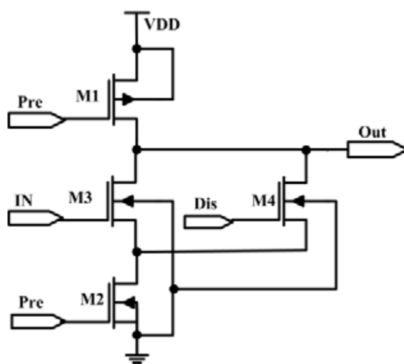

Fig. 1 DNOR circuit

Fig. 2 illustrates waveforms of control signals. During the pre-charge phase signals PRE=0 and DIS=0, transistor M1 is *on*, while the other transistors are *off*. The output goes to logic 1, regardless of the input signal IN. The *evaluation* phase begins when signal PRE=1 And DIS=0. Then M1 and M4 turn off, M2 is *on*, and the input signal IN controls the state of the transistor M3. If the signal IN=0, M3 is *off*, so that the output remains at logical 1. If IN=1, M3 and M2 are *on* and output switches to 0. It is obvious that the output becomes an inverting function of the input signal. Discharging phase occurs when PRE=1 and DIS=1. Therefore M3 is *off* and M4 is *on* and output goes to low logic level regardless to input signal.

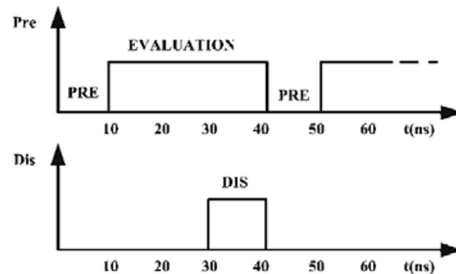

Fig. 2 Time waveforms of control signals for DNOR cell

III. NSDDL AND/NAND/OR/NOR CELL

This section recalls to the results obtained for NSDDL AND/NAND/OR/NOR cells [9-10]. All functions are implemented using usual logic circuits with negative logic (NAND and NOR) which can be easily implemented in CMOS technology. Using de Morgan rules it is easy to see that simple permutation of input signals (*A, notA, B, notB*) provides four different logic functions with the same hardware. Therefore this structure is named NSDDL AND/NAND/OR/NOR SCA resistant cell.

DNOR circuit represents basic element for all SCA resistant cells in NSDDL technique. Prime role of this circuit is to decrease short-circuit current in CMOS circuit Moreover, it provides inverting function when transforming from standard to NSDDL logic.

Block diagram of NSDDL OR, SCA resistant cells are presented in Figure 3. According to the fact that NSDDL OR and NOR cells explore mutually complementary function, it is obvious that they can be realized using the same hardware. The only difference makes the meaning of the true and the false output.

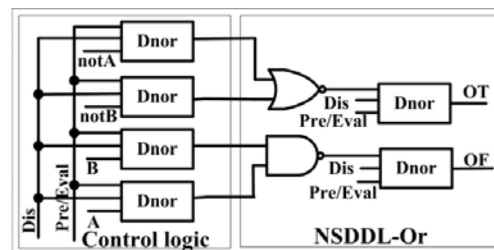

Fig. 3. Block scheme of NSDDL OR SCA resistance cell

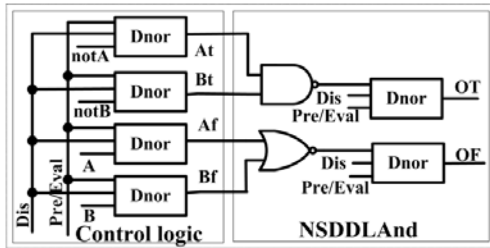

Fig. 4. Block scheme of NSDDL OR SCA resistance cell

Figure 4 illustrate NSDDL AND and NAND cells. NAND function occurs when the true and the false output replace their positions, under the same conditions.

In order to estimate SCA resistance we consider the energies needed for output state transition during different combinations of input signals. As reference we use standard AND, NAND, OR and NOR cells and compare behavior of standard and NSDDL cell. For standard cells one can expect strong correlation between energy required for particular transition and combination of input signals. In particular any neutral event requires minimal energy while rise transition at the output needs more current to charge the output capacitance. NSDDL cells are designed with intention to mask cell operation regarding I_{DD}. Therefore they should provide minimal correlation between stimulus signals and I_{DD}. Table I systematizes results of comparison.

TABLE I
CHARACTERISTICS COMPARISON OF CLASSIC AND NSDDL CELLS

1	2	3	4	5	6	7
A	**B**	**E_{ANDc} [pJ]**	**E_{NANDc} [pJ]**	**E_{ORc} [pJ]**	**E_{NORc} [pJ]**	**E_{NSDDL} [pJ]**
0	↑	0.05	0.05	-0.49	-0.46	-2.80
0	↓	-0.05	-0.05	-0.674	-0.47	-2.77
↑	**0**	0.05	0.05	-0.50	-0.50	-2.77
↓	**0**	-0.05	-0.05	-0.76	-0.55	-2.74
↑	↑	-0.72	-0.69	-0.44	-0.43	-2.75
↓	**1**	-0.86	-0.65	-0.05	-0.05	-2.82
↑	**1**	-0.65	-0.62	0.05	0.05	-2.77
1	↓	-0.93	-0.73	-0.007	-0.007	-2.79
1	↑	-0.69	-0.66	0.007	0.007	-2.74
↓	↓	-0.97	-0.76	-0.71	-0.52	-2.76
E_{av} [J]		-0.48	-0.41	-0.36	-0.30	-2.77
δE [%]		210.2	196.98	222.05	202.67	2.81
σ [fJ]		405.4	337.7	310.3	243.1	24.31
***NSD*[%]**		83.91	82.23	85.64	82.59	0.87

Columns 1 and 2 indicate input combinations. Symbols "↑" and "↓" denote the rise and fall transition, respectively. Columns 3, 4, 5 and 6 present results obtained for standard AND, NAND, OR and NOR cells, respectively, while column 7 refers to NSDDL cell.

Energy consumption is expressed as integral in time of instantaneous power ($I_{DD} \cdot V_{DD}$) during one cycle of input signal change. For AND, NAND, OR and NOR this cycle lasts as all three operational phases needed for NSDDL cell. In order to get better insight into the behavior of every cell we derived from the simulation results the following parameters:

- average energy (E_{av})
- relative difference in respect to E_{av} (δ)
- standard deviation (σ)
- normalized standard deviation in respect to E_{av} (*NSD*).

As a measure of SCA resistance we consider normalized standard deviation. This parameter indicates that AND/NAND/OR/NOR NSDDL cell is immune to SCA using DPA.

Figure 5 illustrates layout of SCA resistant AND/NAND/OR/NOR cell. Layout of NSDDL cells that perform particular logic function AND, NAND, OR and NOR cells differs only regarding the order of input and output ports which form desired functions. By rule of symmetry, true and false parts of the circuit are mirrored.

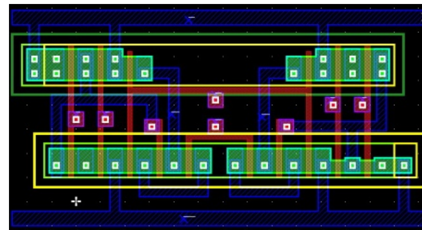

Fig. 5 Layout of SCA resistant NSDDL AND/NAND/OR/NOR cell

IV. TESTING OF NSDDL AND CELL

To create a fault dictionary one is supposed to define the set of defects that are to be tested first. After that, the defect should be inserted into the circuit, one at a time, in order to analyze the effect of defect propagation. Two categories of defects are sought: catastrophic, that includes shorts and opens, and soft faults where the delay faults belong. Here only one sub-category will be considered the shorts between the transistor terminals. To get the response of the faulty circuit, namely to get the fault-effect, one has to perform electrical simulation of the faulty circuit. Of course, a test signal is to be established beforehand that is supposed to be capable to expose the fault-effect if it is present into the response(s) of the faulty circuit.

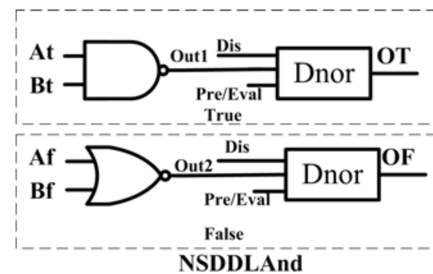

Fig.6.Block diagram of NSDDL AND cell

True and *False* blocks are emphasized with dashed rectangles in Figure 6 and their outputs are denoted as *OT* and *OF*, respectively. Observing this figure, one can see that these blocks have complementary structure where *OT* depends on *At* and *Bt*, while *OF* is function of *Af* and *Bf*. Figure 7.a shows an SCA unprotected NAND cell as a generic block while Figure 7.b shows the schematic (taken from the TSMC035u library [11]) with marked defects.

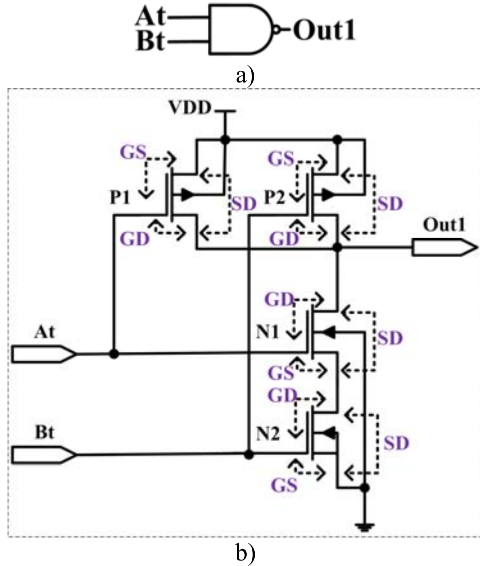

Fig. 7. Standard NAND cell a) generic representation b) standard CMOS realization with marked defects

TABLE II
COVERAGE OF DEFECTS FOR TRUE SUB CIRCUITS

Type of defects	Signal values											NSD_{NSDDL} AND
At	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**1**	**1**	**0**	**0**	**0**	**NA**
Bt	**1**	**0**	**0**	**0**	**1**	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**NA**
Fault free OT	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0.87**
P_1_F_{GD}	↓	0	0	0	0	↓	0	0	0	0	0	0	31.64
P_1_F_{GS}	1	0	0	0	1	1	1	0	1	0	0	0	54.11
P_1_F_{SD}	0	0	0	0	0	0	0	0	0	0	0	0	53.64
P_2_F_{GD}	0	0	↓	0	0	0	0	↓	0	0	0	0	29.54
P_2_F_{GS}	0	0	1	0	1	0	1	1	1	0	0	0	54.11
P_2_F_{SD}	0	0	0	0	0	0	0	0	0	0	0	0	53.64
N_1_ F_{GD}	↓	0	0	0	0	↓	0	0	0	0	0	0	31.67
N_1_ F_{GS}	0	0	0	0	0	0	0	0	0	0	0	0	0.48
N_1_ F_{SD}	↓	0	0	0	1	↓	1	0	1	0	0	0	151.0
N_2_ F_{GD}	0	0	0	0	0	0	0	0	0	0	0	0	37.28
N_2_ F_{GS}	0	0	0	0	0	0	0	0	0	0	0	0	0.50
N_2_ F_{SD}	0	0	↓	0	1	0	1	↓	1	0	0	0	151.2

The same analogy is applied for NOR cell, which is presented to Figures 8.a and 8.b (schematic also taken from the TSMC035u library) with marked defects. Transistors are denoted with P_i_F_{xy} or N_j_F_{xy}, where P and N represent type of the transistor. Counters marked as *i*=1-4, and *j*=1-4, represents index of PMOS and NMOS transistor, respectively. F_{xy} denotes a short-circuit between the *x* and *y* terminal of the proper transistor. Therefore *xy* can take values from the set {GD, GS, SD}, where GD stands for gate-drain, GS for gate-source, and SD source-drain.

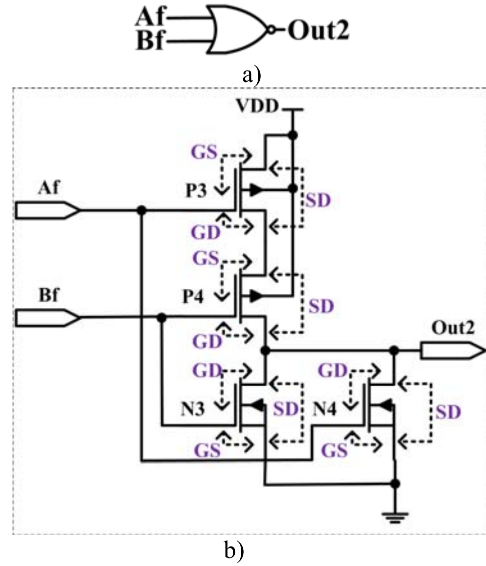

Fig. 8. Standard NOR cell a) generic representation b) standard CMOS realization with marked defects

TABLE III
COVERAGE OF DEFECTS FOR FALSE SUB CIRCUITS

Type of defects	Signal values											NSD_{NSDDL} AND
Af	**1**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**1**	**1**	**1**	**NA**
Bf	**0**	**1**	**1**	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**1**	**1**	**NA**
Fault free OF	**1**	**1**	**1**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**1**	**1**	**0.87**
P_3_F_{GD}	1	1	1	1	1	1	1	1	1	1	1	1	42.99
P_3_F_{GS}	1	1	1	1	1	1	1	1	1	1	1	1	54.38
P_3_F_{SD}	0	1	1	1	0	0	0	1	0	1	1	1	145.25
P_4_F_{GD}	1	1	0	1	1	1	1	0	1	1	1	1	22.77
P_4_F_{GS}	1	1	1	1	1	1	1	1	1	1	1	1	57.39
P_4_F_{SD}	1	1	0	1	0	1	0	0	0	1	1	1	145.06
N_3_ F_{GD}	1	1	0	1	1	1	1	0	1	1	1	1	22.77
N_3_ F_{GS}	1	1	0	1	0	1	0	0	0	1	1	1	0.44
N_3_ F_{SD}	1	1	1	1	1	1	1	1	1	1	1	1	52.86
N_4_ F_{GD}	0	1	1	1	↓	0	↓	1	↓	1	1	1	24.18
N_4_ F_{GS}	0	1	1	1	0	0	0	1	0	1	1	1	0.44
N_4_ F_{SD}	1	1	1	1	1	1	1	1	1	1	1	1	52.86

Effect of every defect is firstly observed with respect to a logic function of the circuit. When logic function is

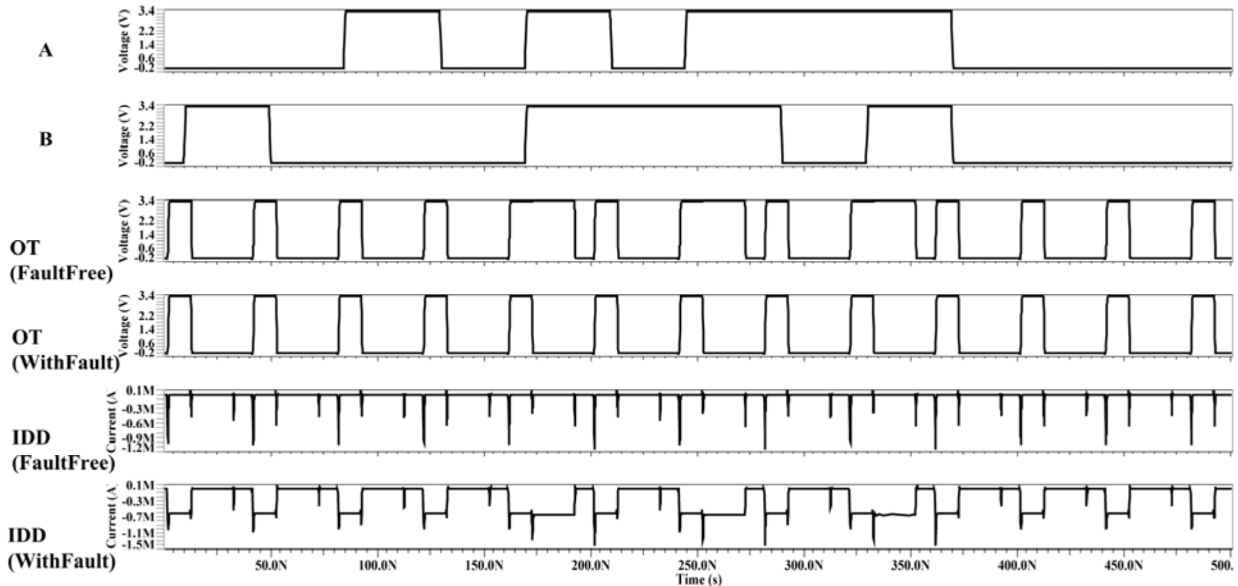

Figure 19. Responses of the TRUE circuit in its fault-free and faulty version (fault P2SD)

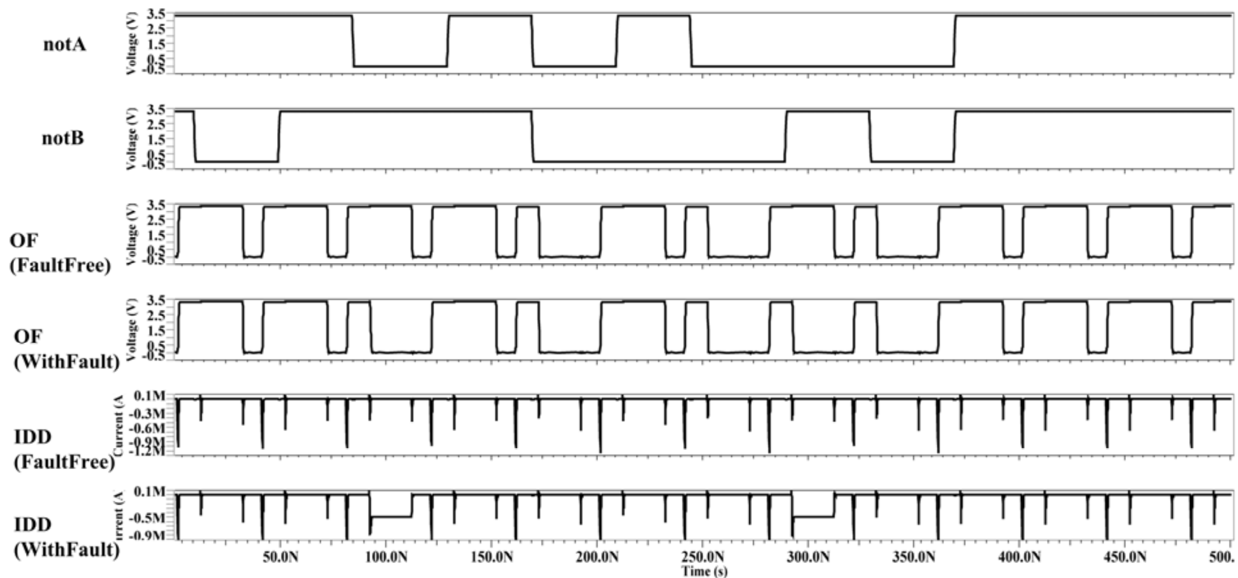

Figure 10. Responses of the FALSE circuit in its fault-free and faulty version (fault P4SD)

violated it can be considered that defect is detected. Table II give results for *True* sub-circuit while Table III for *False* sub circuit. The symbol "↓" denotes the fall-transition. Observing results given in tables II and III one can see that all defects in the circuit were detected in this way. Since operation of the circuit is very specific, logic function is observed during *EVALUATION* phase for fault free and faulty circuits under the same input conditions.

To illustrate, Figure 9. and Figure 10 depict the waveforms of the important signals in the TRUE and FALSAE circuit respectively, in the fault free and a faulty case (as indicated). These kinds of figures were created for every row in Table II and Table III.

Testing based on the supply current is an excellent supplement to the testing of logic functions of a circuit. As discussed above, *NSD* parameter directly depends on the I_{DD} and for that reason, this parameter is used as a second indicator. It can be seen form Table II and Table III that both criteria indicated the presence of a defect in a circuit for any simulated case. This means that defect coverage is 100% by the test signal given in the first two rows of the tables. This confirms that rough destruction (catastrophic

fault presence) of the NSDDL's circuit symmetry has apparent influence to its response. That is important for testing but also for evaluating its main function. Namely, in the presence of a fault the circuit is not so effective in data protection.

V. CONCLUSION

The NSDDL method design method for side channel attack hardening of digital electronic circuits is characterized by the implementation of duplicated hardware that provides true and false output. The false output has the same function as inverted true output. The basic idea is to mask the correlation between the supply current and the activity of the cell. This is possible to obtain if input signals are doubled.

For testing this cell two criteria were adopted: logic function verification, and IDDQ testing performed by calculating the *NSD* parameter. Twenty four simulations were performed in order to make the appropriate fault dictionary for defects of short-circuit type. After completing the test synthesis procedure for a simple AND gate one may conclude that expected results were obtained. Namely, both criteria give excellent coverage of defects. All twenty four defects were detected in either case. In fact the symmetry being violated by insertion of a fault, the fault effect is immediately visible at the output.

This conclusion, however, is still valid for simple circuits as the AND NSDDL is. It is our intention in future to perform in-depth analysis of detectability and observability of the catastrophic faults (including open-faults) in much more complex combinational NSDDL circuit.

ACKNOWLEDGEMENT

This work was supported by The Serbian Ministry of education and science within the project TR 32004.

REFERENCES

[1] Koc, Cetin Kaya (Ed.) *Cryptographic Engineering*, Springer, 2009.
[2] Petković P., Stanojlović M. and Litovski V. "*Design of side-channel-attack resistive criptographic ASICS*", Forum BISEC 2010, Zbornik radova druge konferencija o bezbednosti informacionih sistema, Beograd, Srbija, Maj 2010, pp 22-27.
[3] Stanojlović M. and Petković P., *"Hardware based strategies against side-channel-attack implemented in WDDL",* Electronics, Vol. 14, No. 1, Banja Luka, June, 2010, pp. 117-122
[4] J. Quan and G. Bai, "*A new method to reduce the side-channel leakage caused by unbalanced capacitances of differential interconnections in dualrail logic styles*", 2009 Sixth International Conference on Information Technology: New Generations, DOI 10.1109/ITNG. 2009.185, pp. 58-63.
[5] M. Bucci, L. Giancane, R. Luzzi, A. Trifiletti: *"Three-Phase Dual-Rail Pre-Charge Logic"*. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 232–241. Springer, Heidelberg (2006).
[6] Stanojlović, M. and Litovski, V., "*Simulation of defects in sequential NSDDL Master/Slave D flip flop circuit*", Proceedings of Small Systems Simulation Symposium 2012, Niš, Serbia, 12th-14th February 2012
[7] Milovanović, D. B., and Litovski, V. M., "*Fault models of CMOS Circuits*", Microelectrinics Reliability, Vol. 34, No. 5, pp. 883-896, 1994
[8] Danger, J.-L. Guilley, S. Bhasin, S. Nassar, M., *"Overview of Dual Rail with Precharge Logic Styles to Thwart Implementation-Level Attacks on Hardware Cryptoprocessors",* Proc. of International Conference on Signals, Circuits and Systems SCS'2009, Djerba, Tunisia, November 5-8 2009, pp. 1-8
[9] Stanojlović, M., Petković, P.: „*An ASIC cryptoosystem resistant to side channel attacks based on standard cells*", VIII Simposium on Industrial Electronics INDEL 2010, Banja Luka, Bosnia and Herzegovina, 4-6 November, 2010, pp. 110-114, ISBN 978-99955-46-03-8, In Serbian
[10] Petković, P., Stanojlović, M.: „*Hardware protection from side channel attacks based on masking the consumption information"*, Zbornik LV konferencije ETRAN, Banja Vrućica, Teslić, B&H, 2011, ISBN 978-86-80509-66-2.
[11] ASIC Design Kit, http://www.mentor.com/company/higher_ed/ic-asic