Faults Simulations in XOR/XNOR Cell Resistant to Side Channel Attacks

Milena Stanojlović Mirković
Innovation Centre of Advanced Technologies
ICAT
Niš, Serbia
milena.stanojlovic@icnt.rs

Vančo Litovski, Predrag Petković and Dragiša Milovanović
Faculty of Electronic Engineering, University of Niš
Niš, Serbia
{vanco,predrag,gilem}@elfak.ni.ac.rs

Abstract—**This paper describes simulation results of testing the No Short-circuit current Dynamic Differential Logic (NSDDL) XOR/XNOR cell which consist of two NSDDL AND cells and one NSDDL OR cell. The goal is to consider the impact of individual defects in such complex circuit. Fault dictionary will be created based on repetitive simulations preformed for defects inserted one by one. For a short circuit defects detection logical function and supply current will be exploited. All cells are designed in CMOS TSMC035 technology using Mentor Graphics design tools.**

Keywords- cell; defects; short circuits; testing.

I. INTRODUCTION

The dynamics consumption tracking of an electronic crypto-system, can provide more information about the system behavior and to make cracking the key easier. The most effective methods for attack on the crypto-system are Simple Power Analysis (SPA), Differential Power Analysis (DPA) and Electromagnetic Analysis (EMA) [1]. All of them relay on tracking the crypto-system activity by monitoring the changes in power consumption. Practically this means that measurements of biasing current will provide the additional information about circuit behavior. Therefore one talks about this current as a source of leaked information or as a Side Channel. 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. Collecting such information is known as the Side Channel Attack - SCA[2, 3].

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 NSDDL cells - the XOR/XNOR 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.

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.

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.

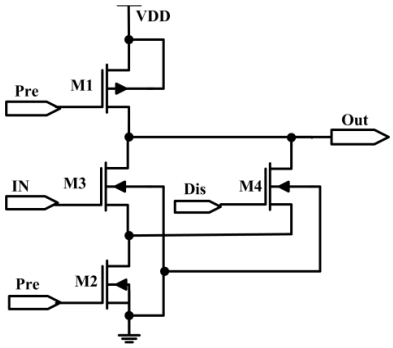

Figure 1. DNOR circuit

Figure 2 illustrates waveforms of control signals. During the pre-charge phase signals PRE=0 and DIS=0, transistorM1 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.

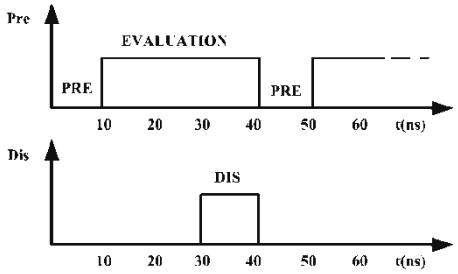

Figure 2. Time waveforms of control signals for DNOR cell

III. NSDDL XOR/XNOR CELL

Figure 3 illustrates block diagram of XOR/XNOR, SCA resistant cell. This cell consist of three cells, two NSDDL AND and one OR [9-10]. As all other NSDDL cells it has true and false inputs and output. It is clear that the same structure provides the XOR function at the true output (OT) and XNOR function at the false output (OF). Therefore it is referred to as NSDDL XOR/XNOR cell. NSDDL AND and NSDDL OR 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.

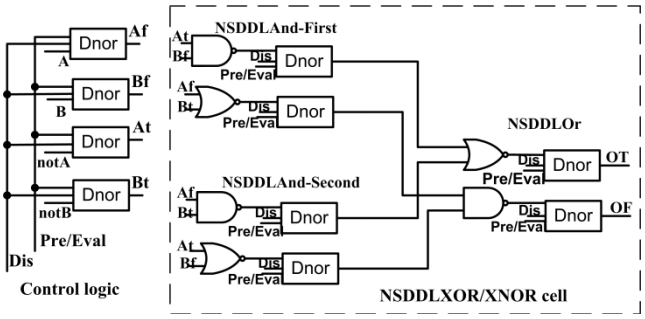

Figure 3. Block diagram of NSDDL XOR/XNOR SCA resistance cell

It is important to note that all functions are implemented using native logic circuits with negative logic (NAND i NOR) which can be easily implemented in CMOS technology. DNOR circuit represents basic element for all SCA resistant cells in NSDDL technique. It provides inverting function when transforming from standard to NSDDL logic.

Figure 4 shows layout of SCA resistant NSDDL XOR/XNOR cell. Layout of XOR and XNOR cells differs only in respect to the order of output ports which form desired functions.

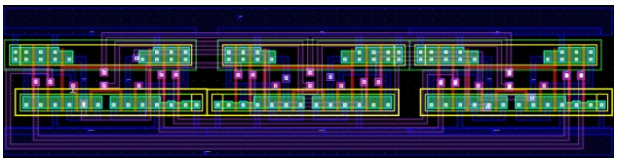

Figure 4. Layout of SCA resistant XOR/XNOR cell

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}.

Energy consumption is expressed as integral in time of power ($I_{DD} \cdot V_{DD}$) during one cycle of input signal change. For standard XOR and XNOR this cycle lasts as all three operational phases needed for NSDDL cell.

As a measure of SCA resistance we consider normalized standard deviation *NSD* according to (1).

$$NSD = 100 \cdot \frac{\sigma}{E_{avg}} \quad (1)$$

For each combination of input signals, energy is calculated. E_{avg} denotes average energy and is caluculated as the average value of energy for all input combinations. All energies for all input combinations calculated are further used to calculate the standard deviation, σ. Table I summarizes results of the comparison. Columns 1 and 2 indicate input combinations. Symbols "↑" and "↓" denote the rise and fall transition, respectively. Columns 3 and 4 present results obtained for standard XOR and XNOR cells, respectively, while column 5 refers to NSDDL cell.

TABLE I. CHARACTERISTICS COMPARISON OF CLASSIC AND NSDDL CELLS

1	2	3	4	5
A	**B**	**E_{XOR}[pJ]**	**E_{XNOR}[pJ]**	**E_{NSDDL}[pJ]**
0	↑	-0.35	-0.48	-6.38
0	↓	-0.51	-0.30	-6.21
↑	0	-0.34	-0.47	-6.22
↓	0	-0.48	-0.33	-6.22
↑	↑	-0.28	-0.05	-6.27
↓	1	-0.35	-0.47	-6.16
↑	1	-0.48	-0.31	-6.27
1	↓	-0.34	-0.47	-6.19
1	↑	-0.52	-0.32	-6.21
↓	↓	-0.27	-0.05	-6.23
E_{max} [pJ]		-0.27	-0.05	-6.16
E_{min} [pJ]		-0.52	-0.48	-6.38
E_{av} [pJ]		-0.39	-0.33	-6.24
δE [%]		63.64	131.76	3.53
σ [fJ]		91.77	154.18	56.58
NSD[%]		23.51	47.43	0.91

The simulation results for NSDDL XOR/XNOR logic cell, in the presence of a defect, are described in the next section.

IV. TESTING OF NSDDL XOR/XNOR 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 stimulation 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.

True and *False* blocks are emphasized with dashed rectangles in Figure 5 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 6.a shows an SCA unprotected NAND cell as a generic block while Figure 6.b shows the schematic (taken from the TSMC035u library [11]) with marked defects. The same analogy is applied for NOR cell, which is presented to Figures 7.a and 7.b.

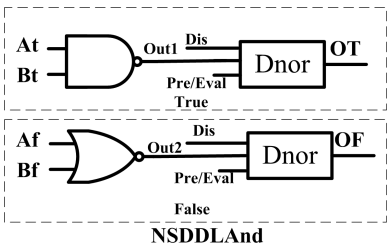

Figure 5. Block diagram of NSDDL AND cell

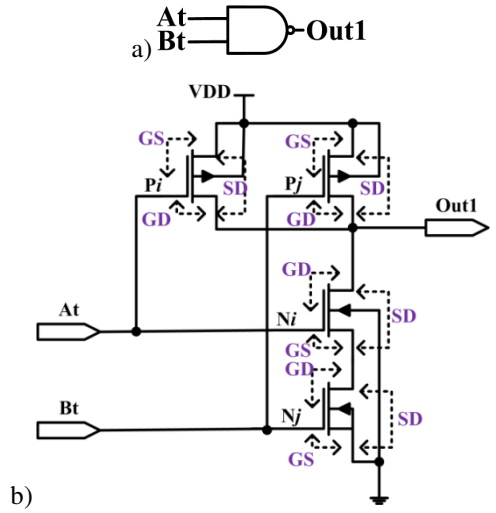

Figure 6. Standard NAND cell a) generic representation b) standard CMOS realization with marked defects

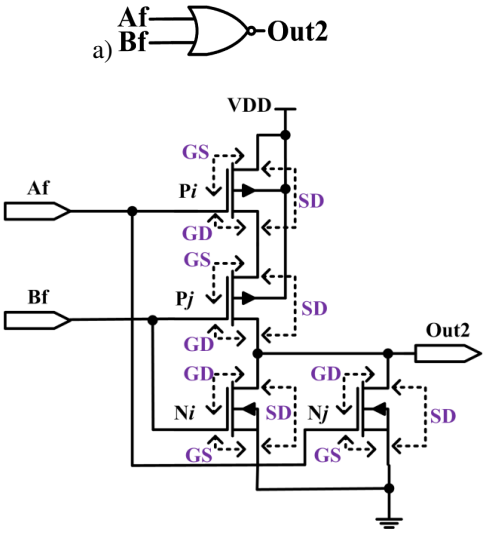

Figure 7. Standard NOR cell a) generic representation b) standard CMOS realization with marked defects

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* and *j* represents index of PMOS and NMOS transistor, respectively. These counters take next values: *i*=1-4, and *j*=1-4 for NSDDL AND-First cell, *i*=5-8, and *j*=5-8 for NSDDL AND-Second cell and *i*=9-12, and *j*=9-12 for NSDDL OR cell. F_{xy} denotes a short-circuit fault (hence F) 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.

Effect of every defect is firstly observed with respect to a logic function of the circuit. When logic function is violated it can be considered that defect is detected. Results summarized in Tables II, III and IV provides detail information about coverage of the defects for NSDDL XOR/XNOR cell in presence of short-circuit faults in NSDDL AND-First, AND-Second and OR cell, respectively. The symbol "↓" denotes the fall-transition.

TABLE II. COVERAGE OF DEFECTS FOR NSDDL XOR/XNOR CELL IN PRESENCE OF SHORT-CIRCUIT DEFECTS IN NSDDL AND-FIRST CELL

		Signal values of NSDDL XOR/XNOR cell												NSD
Fault free circuit														
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**
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**
OT		**1**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0.91**
OF		**0**	**1**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**1**	**1**	**1**	
Value of OT and OF signals in presence of short-circuit defects in TRUE NSDDL AND-First sub-circuits														
P_1_F_{GD}	**OT**	1	0	0	0	0	1	0	0	0	0	0	0	34.64
	OF	1	1	0	1	1	1	1	0	1	1	1	1	
P_1_F_{GS}	**OT**	1	1	1	1	0	1	0	1	0	1	1	0	53.61
	OF	1	1	0	1	1	1	1	0	1	1	1	1	
P_1_F_{SD}	**OT**	1	0	0	0	0	1	0	0	0	0	0	0	47.69
	OF	**0**	**1**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**1**	**1**	**1**	
P_2_F_{GD}	**OT**	1	0	0	0	0	1	0	0	0	0	0	0	32.61
	OF	1	1	0	1	1	1	1	0	1	1	1	1	
P_2_F_{GS}	**OT**	1	0	1	0	1	1	1	1	1	0	0	0	60.34
	OF	1	1	0	1	1	1	1	0	1	1	1	1	
P_2_F_{SD}	**OT**	1	0	0	0	0	1	0	0	0	0	0	0	47.69
	OF	**0**	**1**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**1**	**1**	**1**	
N_1_ F_{GD}	**OT**	1	0	0	0	0	1	0	0	0	0	0	0	34.64
	OF	1	1	0	1	1	1	1	0	1	1	1	1	
N_1_ F_{GS}	**OT**	1	0	0	0	0	1	0	0	0	0	0	0	2.43
	OF	0	1	0	1	0	0	0	0	0	1	1	1	
N_1_ F_{SD}	**OT**	1	↓	1	↓	0	1	0	1	0	↓	↓	↓	115.82
	OF	**0**	**1**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**1**	**1**	**1**	
N_2_ F_{GD}	**OT**	1	0	0	0	0	1	0	0	0	0	0	0	33.79
	OF	0	0	0	0	1	0	1	0	1	0	0	0	
N_2_ F_{GS}	**OT**	1	0	0	0	0	1	0	0	0	0	0	0	2.51
	OF	0	0	0	0	1	0	1	0	1	0	0	0	
N_2_ F_{SD}	**OT**	1	0	1	0	↓	1	↓	1	↓	0	0	0	111.22
	OF	**0**	**1**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**1**	**1**	**1**	
Value of OT and OF signals in presence of short-circuit defects in FALSE NSDDL AND-First sub-circuits														
P_3_F_{GD}	**OT**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	37.76
	OF	0	1	1	1	1	0	1	1	1	1	1	1	
P_3_F_{GS}	**OT**	1	0	1	0	1	1	1	1	1	0	0	0	52.99
	OF	0	1	1	1	1	0	1	1	1	1	1	1	
P_3_F_{SD}	**OT**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	110.29
	OF	0	0	0	0	1	0	1	0	1	0	0	0	
P_4_F_{GD}	**OT**	0	0	1	0	0	0	0	1	0	0	0	0	17.32
	OF	0	1	1	1	0	0	0	1	0	1	1	1	
P_4_F_{GS}	**OT**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	34.12
	OF	0	1	1	1	0	0	0	1	0	1	1	1	
P_4_F_{SD}	**OT**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	104.12
	OF	0	1	0	1	0	0	0	0	1	1	1	1	
N_3_ F_{GD}	**OT**	0	0	1	0	0	0	0	1	0	0	0	0	17.32
	OF	0	1	1	1	0	0	0	1	0	1	1	1	
N_3_ F_{GS}	**OT**	1	0	1	0	0	1	0	1	0	0	0	0	2.41
	OF	0	1	0	1	0	0	0	0	0	1	1	1	
N_3_ F_{SD}	**OT**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	39.02
	OF	0	1	1	1	1	0	1	1	1	1	1	1	
N_4_ F_{GD}	**OT**	0	0	1	0	0	0	0	1	0	0	0	0	18.77
	OF	0	0	1	0	1	0	1	1	1	0	0	0	
N_4_ F_{GS}	**OT**	0	0	1	0	1	0	1	1	1	0	0	0	2.55
	OF	0	0	0	0	1	0	1	0	1	0	0	0	
N_4_ F_{SD}	**OT**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	39.02
	OF	0	1	1	1	1	0	1	1	1	1	1	1	

TABLE III. COVERAGE OF DEFECTS FOR NSDDL XOR/XNOR CELL IN PRESENCE OF SHORT-CIRCUIT DEFECTS IN NSDDL AND-SECOND CELL

		Signal values of NSDDL XOR/XNOR cell												NSD
Fault free circuit														
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**
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**
OT		**1**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0.91**
OF		**0**	**1**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**1**	**1**	**1**	
Value of OT and OF signals in presence of short-circuit defects in TRUE NSDDL AND–Second sub-circuits														
P_5_F_{GD}	**OT**	0	0	1	0	0	0	0	1	0	0	0	0	34.04
	OF	0	1	1	1	1	0	1	1	1	1	1	1	
P_5_F_{GS}	**OT**	1	0	1	0	1	1	1	1	1	0	0	0	52.99
	OF	0	1	1	1	1	0	1	1	1	1	1	1	
P_5_F_{SD}	**OT**	0	0	1	0	0	0	0	1	0	0	0	0	49.68
	OF	**0**	**1**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**1**	**1**	**1**	
P_6_F_{GD}	**OT**	0	0	1	0	0	0	0	1	0	0	0	0	32.77
	OF	0	1	1	1	1	0	1	1	1	1	1	1	
P_6_F_{GS}	**OT**	1	1	1	1	1	1	1	1	1	0	0	0	53.52
	OF	0	1	1	1	1	0	1	0	1	1	1	1	
P_6_F_{SD}	**OT**	0	0	1	0	0	0	0	1	0	0	0	0	49.68
	OF	**0**	**1**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**1**	**1**	**1**	
N_5_ F_{GD}	**OT**	0	0	1	0	0	0	0	1	0	0	0	0	34.04
	OF	0	1	1	1	1	0	1	1	1	1	1	1	
N_5_ F_{GS}	**OT**	0	0	1	0	0	0	0	1	0	0	0	0	2.55
	OF	0	0	0	0	1	0	1	0	1	0	0	0	
N_5_ F_{SD}	**OT**	1	0	1	0	↓	1	↓	1	↓	0	0	0	23.16
	OF	**0**	**1**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**1**	**1**	**1**	
N_6_ F_{GD}	**OT**	0	0	1	0	0	0	0	1	0	0	0	0	36.68
	OF	0	1	0	1	0	0	0	0	0	1	1	1	
N_6_ F_{GS}	**OT**	0	0	1	0	0	0	0	1	0	0	0	0	2.41
	OF	0	1	0	1	0	0	0	0	0	1	1	1	
N_6_ F_{SD}	**OT**	1	↓	1	↓	0	1	0	1	0	↓	↓	↓	115.72
	OF	**0**	**1**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**1**	**1**	**1**	
Value of OT and OF signals in presence of short-circuit defects in FALSE NSDDL AND–Second sub-circuits														
P_7_F_{GD}	**OT**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	29.68
	OF	1	1	0	1	1	1	1	0	1	1	1	1	
P_7_F_{GS}	**OT**	1	1	1	1	1	1	1	1	1	0	0	0	53.61
	OF	1	1	0	1	1	1	1	0	1	1	1	1	
P_7_F_{SD}	**OT**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	105.32
	OF	0	1	0	1	0	0	0	0	0	1	1	1	
P_8_F_{GD}	**OT**	1	0	0	0	0	1	0	0	0	0	0	0	18.73
	OF	1	0	0	0	1	1	1	0	1	0	0	0	
P_8_F_{GS}	**OT**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	49.73
	OF	1	1	0	1	1	1	1	0	1	1	1	1	
P_8_F_{SD}	**OT**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	109.25
	OF	0	0	0	0	1	0	1	0	1	0	0	0	
N_7_ F_{GD}	**OT**	1	0	0	0	0	1	0	0	0	0	0	0	16.83
	OF	1	0	0	0	1	1	1	0	1	0	0	0	
N_7_ F_{GS}	**OT**	1	0	0	0	0	1	0	0	0	0	0	0	2.51
	OF	0	0	0	0	1	0	1	0	1	0	0	0	
N_7_ F_{SD}	**OT**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	38.21
	OF	1	1	0	1	1	1	1	0	1	1	1	1	
N_8_ F_{GD}	**OT**	1	0	0	0	0	1	0	0	0	0	0	0	19.18
	OF	1	1	0	1	0	1	0	0	0	1	1	1	
N_8_ F_{GS}	**OT**	1	0	1	0	0	1	0	1	0	0	0	0	2.44
	OF	0	1	0	0	0	0	0	0	0	1	1	1	
N_8_ F_{SD}	**OT**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	38.21
	OF	1	1	0	1	1	1	1	0	1	1	1	1	

TABLE IV. COVERAGE OF DEFECTS FOR NSDDL XOR/XNOR CELL IN PRESENCE OF SHORT-CIRCUIT DEFECTS IN NSDDL OR CELL

		Signal values of NSDDL XOR/XNOR cell												NSD
Fault free circuit														
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**
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**
OT		**1**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0.91**
OF		**0**	**1**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**1**	**1**	**1**	
Value of OT and OF signals in presence of short-circuit defects in TRUE NSDDL OR sub-circuits														
$P_9\_F_{GD}$	**OT**	1	1	1	1	1	1	1	1	1	1	1	1	14.65
	OF	0	1	0	1	1	0	1	0	1	1	1	1	
$P_9\_F_{GS}$	**OT**	1	1	1	1	1	1	1	1	1	1	1	1	36.16
	OF	0	1	0	1	1	0	1	0	1	1	1	1	
$P_9\_F_{SD}$	**OT**	1	0	0	0	0	1	0	0	0	0	0	0	0.24
	OF	0	1	0	1	1	0	1	0	1	1	1	1	
$P_{10}\_F_{GD}$	**OT**	0	1	1	1	1	0	1	1	1	1	1	1	0.28
	OF	0	1	1	1	1	0	1	1	1	1	1	1	
$P_{10}\_F_{GS}$	**OT**	1	1	1	1	1	1	1	1	1	1	1	1	35.35
	OF	0	1	0	1	1	0	1	0	1	1	1	1	
$P_{10}\_F_{SD}$	**OT**	0	0	1	0	0	0	0	1	0	0	0	0	19.27
	OF	0	1	0	1	1	0	1	0	1	1	1	1	
$N_9\_F_{GD}$	**OT**	0	1	1	1	1	0	1	1	1	1	1	1	14.65
	OF	0	1	1	1	1	0	1	1	1	1	1	1	
$N_9\_F_{GS}$	**OT**	0	0	1	0	0	0	0	1	0	0	0	0	2.51
	OF	0	1	0	1	1	0	1	0	1	1	1	1	
$N_9\_F_{SD}$	**OT**	1	1	1	1	1	1	1	1	1	1	1	1	130.19
	OF	0	1	0	1	1	0	1	0	1	1	1	1	
$N_{10}\ F_{GD}$	**OT**	1	1	0	1	1	1	1	0	1	1	1	1	25.16
	OF	0	1	0	1	1	0	1	0	1	1	1	1	
$N_{10}\ F_{GS}$	**OT**	1	0	0	0	0	1	0	0	0	0	0	0	2.43
	OF	0	1	0	1	1	0	1	0	1	1	1	1	
$N_{10}\ F_{SD}$	**OT**	1	1	1	1	1	1	1	1	1	1	1	1	6.25
	OF	0	1	0	1	1	0	1	0	1	1	1	1	
Value of OT and OF signals in presence of short-circuit defects in FALSE NSDDL OR sub-circuits														
$P_{11}\_F_{GD}$	**OT**	1	0	1	0	0	1	0	1	0	0	0	0	16.41
	OF	0	0	0	0	0	0	0	0	0	0	0	0	
$P_{11}\_F_{GS}$	**OT**	1	0	1	0	0	1	0	1	0	0	0	0	23.02
	OF	0	1	1	1	1	0	1	1	1	1	1	1	
$P_{11}\_F_{SD}$	**OT**	1	0	1	0	0	1	0	1	0	0	0	0	19.58
	OF	0	0	0	0	0	0	0	0	0	0	0	0	
$P_{12}\_F_{GD}$	**OT**	1	0	1	0	0	1	0	1	0	0	0	0	15.31
	OF	0	0	0	0	0	0	0	0	0	0	0	0	
$P_{12}\_F_{GS}$	**OT**	1	0	1	0	0	1	0	1	0	0	0	0	35.95
	OF	1	1	0	1	1	1	1	0	1	1	1	1	
$P_{12}\_F_{SD}$	**OT**	1	0	1	0	0	1	0	1	0	0	0	0	27.05
	OF	0	0	0	0	0	0	0	0	0	0	0	0	
$N_{11}\ F_{GD}$	**OT**	1	0	1	0	0	1	0	1	0	0	0	0	15.31
	OF	0	0	0	0	0	0	0	0	0	0	0	0	
$N_{11}\ F_{GS}$	**OT**	1	0	1	0	0	1	0	1	0	0	0	0	2.51
	OF	0	0	0	0	0	0	0	0	0	0	0	0	
$N_{11}\ F_{SD}$	**OT**	1	0	1	0`	0	1	0	1	0	0	0	0	8.51
	OF	0	1	↓	1	1	0	1	↓	1	1	1	1	
$N_{12}\ F_{GD}$	**OT**	1	0	1	0`	0	1	0	1	0	0	0	0	16.56
	OF	0	0	0	0	0	0	0	0	0	0	0	0	
$N_{12}\ F_{GS}$	**OT**	1	0	1	0	0	1	0	1	0	0	0	0	2.54
	OF	0	0	0	0	0	0	0	0	0	0	0	0	
$N_{12}\ F_{SD}$	**OT**	1	0	1	0	0	1	0	1	0	0	0	0	33.78
	OF	↓	1	0	1	1	↓	1	0	1	1	1	1	

Observing results given in Tables II and III one can see that defects, in the TRUE sub-circuit, can be mapped to both outputs, OT and OF. The same applies for FALSE sub-circuit. Defects which do not affect both outputs OT or OF are marked with a bold. This is the case with NSDDL OR cell. These results are given in Table IV. Here, e.g. if the defect is in TRUE sub-circuits, its effect will be demonstrated only at OT output. Similarly, effect of the defect in the FALSE sub-circuit will be visible only at OF output. 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.

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

In this paper, we showed how individual defects in lower level circuits (OR, AND) affect behaviour of cells at higher level (XOR/NXOR). For testing NSDDL XOR/XNOR cell two criteria were examined: logic function verification and IDDQ testing performed by calculating the *NSD* parameter. Seventy two 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 XOR/XNOR gate one may conclude that expected results were obtained. Namely, both criteria give excellent coverage of defects. All seventy two 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. It is important to mention that the individual defects inserted in the input NSDDL-And circuits of the NSDDL XOR/XNOR cell can be demonstrated on both outputs. This is not the case for defects in output NSDD-OR circuitry where effect of the defect is visible only at the one of the outputs (true or false). The number of defects visible on both outputs for is twenty eight.

ACKNOWLEDGMENT

This research was funded by The Ministry of Education, Science and Technological Development of Republic of Serbia under contract No. TR32004.

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