Resistance of XOR/XNOR NSDDL cell to Side Channel Attack

Milena Stanojlović and Predrag Petković

Abstract - Complex cryptographic algorithms guard the content of data from unauthorized persons. The security level depends directly on the coding complexity. The complicated algorithm prevents, or impedes the searching for possible combinations that breaks the code in real time. However the attackers use additional information about the behavior of an electronic crypto-system to reduce the number of combinations needed to explore the key. Collecting such information is referred to as Side Channel Attack - SCA. This paper describes simulation results that illustrate resistance of XOR/NXOR logic cell designed by NSDDL method to SCA. The cells are designed in CMOS TSMC035 technology using Mentor Graphics design tools.

Keywords - crypto-system, SCA.

I. Introduction

The importance of data being transferred through open or semi-closed communication networks provokes unauthorized users to discover their contents. Any unauthorized attempt to access to encrypted content is treated as an attack to the cryptographic system. A common way to prevent unauthorized attack is to increase number of combinations needed to detect the cryptographic key. However it is proven that additional information about cryptosystem behavior reduces required number of combinations [1]. Any attempt for illegal data collection about system behavior that does not rely on direct data reading is known as Side Channel Attack (SCA). The most popular methods for SCA relay on monitoring of dynamics consumption at electronic crypto-system. The most effective are SPA (Simple Power Analysis), DPA (Differential Power Analysis) and EMA (Electromagnetic Analysis) [2, 3].

The waveform of the supply current (IDD) hides very useful additional information about the behavior of cryptographic systems. An abrupt change of current IDD in a CMOS digital circuit occurs only during transition of the logical state. When changing from 0 to 1, output capacitances are charged to the VDD through PMOS network. As the state changes from 1 to 0, capacitances are discharge to ground. In addition within the transition some short-circuit current flows when PMOS and NMOS transistors are on 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.

During this research, authors were gained significant experience at a physical level implementation of data protection from SCA into LEDA Laboratory of Electronics, University of Nis. The research team is developing library of CMOS cells that are resistant to DPA attacks. Resistance is measured by the degree of masking and it is larger if the correlation between IDD and circuit behavior is diminished. The focus of our interest is NSDDL (No Short-circuit current Dynamic Differential Logic) method [5, 6].

We have already developed a restricted set of simple cells resistive to SCA [7, 8]. The aim of this paper is to present SCA resistivity of a more complex cell that is composed of already developed. To illustrate types of cells required for implementation of the RSA public key cryptosystem we refer to [4]. The squaring with serial squarer block requires NOT, AND, delay element and full adder. As we already have designed NOT, AND and D-flip-flop, the next step is to design XOR that would be a building block for the full adder. This paper reports the resistance to SCA of the new cell.

Simulation results were obtained using *ELDO* simulator of *Mentor Graphics Design Architect* environment. To draw the layout was used *IC studio Mentor Graphics tools*, while the DRC (*Design Rule Check*), LVS (*Layout Versus Schematics*) and PEX (*Parasitic Extraction*) perform by using *Calibre*. The technology chosen for the design is TSMC035.

The subsequent section reviews the core of NSDDL method. The third section explores design methodology and SCA resistivity of AND/NAND/OR/NOR NSDDL cell. This cell is a building block for XOR/XNOR NSDDL cell that is described in the forth section.

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 the counterpart that will react complementary. Therefore every 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 go to high logic

Milena Stanojlović and Predrag Petković are with the Department of Electronics, Faculty of Electronic Engineering, University of Niš, Aleksandra Medvedeva 14, 18000 Niš, Serbia,
E-mail: milena@venus.elfak.ni.ac.rs,
predrag.petkovic@elfak.ni.ac.rs.

level. In the second phase, known as *evaluation* phase true outputs 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 [3] 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 the integral part of the control logic and NSDDL cells. Figure 1 illustrates circuitry of DNOR cell.

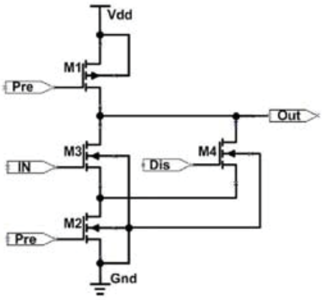

Fig. 1. DNOR circuit

Figure 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 turns 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 achieves 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.

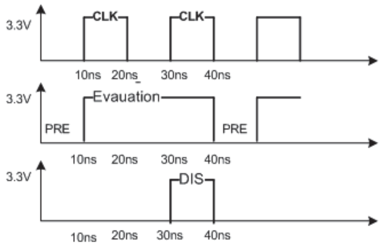

Fig. 2. Time waveforms of control signals for DNOR cell

III. Resistance to Side Channel Attacks of AND/NAND/OR/NOR NSDDL cell

This section recalls to the results obtained for AND/NAND and OR/NOR NSDDL cells [8] that will be used in the design of XOR/NXOR NSDDL cell.

Block diagram of NAND/AND and NOR/OR NSDDL, SCA resistant cells are presented in Figures 3 and 4, respectively. According to the fact that these 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.

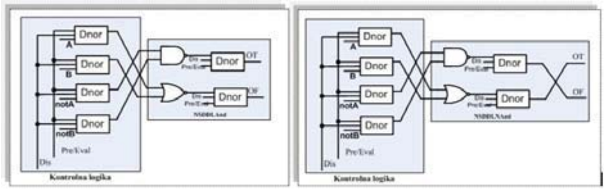

Fig. 3. Block scheme of NSDDL AND and NAND SCA resistance cell

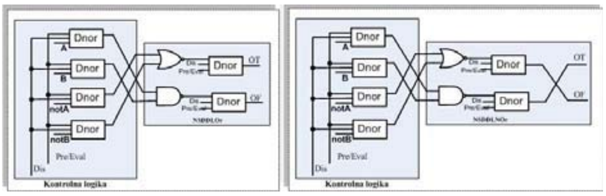

Fig. 4. Block scheme of NSDDL OR and NOR SCA resistance cell

Figures 3 and 4 illustrate that both cells need mutually complement input signals A/notA and B/notB. 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 AND/NAND/OR/NOR SCA resistant 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. 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.

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.

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.

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_{max} [pJ]		0.05	0.05	0.05	0.05	-2.74
E_{min} [pJ]		-0.97	-0.76	-0.76	-0.55	-2.82
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

Energy consumption is expressed as integral in time of 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 behavior of every cell we derived from the simulation results the following parameters:

- maximum energy (E_{max}),
- minimum energy (E_{min})
- 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.

For standard logic cells this parameter reaches 85%. Obviously this indicates strong correlation between energy (practically the current, because V_{DD}=const) and input signal transition. However, NSDDL cell has NSD <1%. This is sufficient to conclude that AND/NAND/OR/NOR NSDDL cell is immune to SCA using DPA.

Figure 5 illustrates layout of SCA resistant AND/NAND/OR/NOR2 cell. Layout of NSDDL cells that perform particular logic function AND2, NAND2, OR2 and NOR2 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.

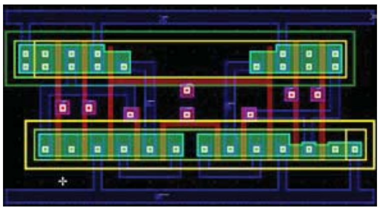

Fig. 5. Layout of SCA resistant AND/NAND/OR/NOR2 cell

IV. RESISTANCE TO SIDE CHANNEL ATTACKS OF XOR/XNOR NSDDL CELL

Figure 6 illustrates block diagram of XOR/XNOR, SCA resistant cell. 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 XOR/XNOR NSDDL cell.

Comparing Figures 3 and 4 with Fig. 6 one easily concludes that it is composed of three AND/NAND/OR/NOR2 cells described above.

Therefore it is interesting to track how the property defined as resistance to SCA is being transferred from lower hierarchical design level to the higher. Aiming that goal we performed similar set of simulation as for AND/NAND/OR/NOR2 NSDDL cell.

Referent cells were standard XOR and standard XNOR cell. They are compared for energy consumption with XOR/XNOR NSDDL cell.

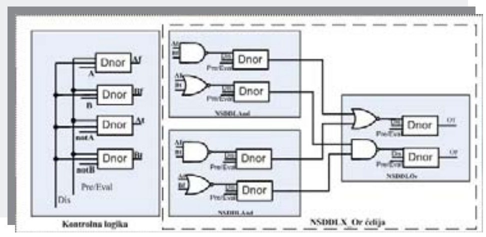

Fig. 6. Block diagram of NSDDL XOR SCA resistance cell

Table II summarizes results of the comparison. NSD parameter that was less than 1% (0.87%) for AND/NAND/OR/NOR2 NSDDL cell remained almost the same. Although slightly increased to 0.91%, it is still less than 1% that qualifies this cell as resistant to SCA. Actually NSD has increased for 4.6% in respect to AND/NAND/OR/NOR2 NSDDL cell. The total improvement of the resistivity to SCA in comparison with standard cells overcomes 2500% for XOR and 5000% for XNOR cell.

Figure 7 shows layout of SCA resistant XOR/XNOR NSDDL cell. Layout of XOR and XNOR cells differs only in respect to the order of input and output ports which form desired functions.

The layout complies with all rules for symmetry of true

TABLE II
CHARACTERISTICS COMPARISON OF CLASSIC AND NSDDL CELLS

1	2	3	4	5
A	B	E_{XORc}[pJ]	E_{XNORc}[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

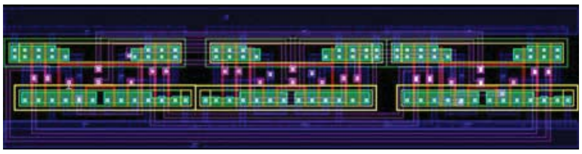

Fig. 7. Layout of SCA resistant XOR/XNOR cell

and false parts in order to suppress unequal consumption in complementary parts of the cell.

V. CONCLUSION

This paper presents simulation results that prove resistance of XOR/XNOR cell designed by NSDDL method to side channel attack. NSDDL method characterizes 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 Three-phase clock signal guarantee that all outputs will start from the high level during the pre-charging and that will take low level during the third phase. The cell operates the desired logic function in the middle phase. Then the true output takes the desired output state and, simultaneously the false output has opposite transition. Due to duplicated hardware the same cell is able to generate both XOR and XNOR functions and consequently named XOR/XNOR NSDDL cell. This cell is composed of three simple NSDDL cells that perform AND/NAND /OR/NOR function. The resistance to SCA was monitored through energies required for output transition under different combination of input signal. The cell is resistive if all changes require the same energy.

Therefore as a measure for a cell resistance to SCA we considered standard deviation normalized to the average energy (NSD). The resistance of AND/NAND/OR/NOR NSDDL cell is less than 1% (0.87%). When implemented into XOR/XNOR NSDDL cell the resistivity decreased for less than 5% relatively to AND/NAND/OR/NOR NSDDL but still remained less than 1% (0.91%). This proves that NSDDL cells transfer their resistivity to SCA into the complex circuit where they are build-in.

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] P. M. Petković, M. Stanojlović, V. B. Litovski "*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] M. Stanojlović, P. Petković, *"Hardware based strategies against side-channel-attack implemented in WDDL"*, Electronics, Vol. 14, No. 1, Banja Luka, June, 2010, pp. 117-122

[4] 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

[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] 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.

[7] Stanojlović, M., Petković, P.: *Otpornost na bočne napade ASIC kripto sistema zasnovanog na standardnim ćelijama*, 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

[8] Petković, P., Stanojlović, M.: *Hardverska zaštita od napada na kripto-sistem zasnovana na primeni ćelija koje maskiraju informaciju o potrošnji*, Zbornik LV konferencije ETRAN, Banja Vrućica, Bosna i Hercegovina, ISBN 978-86-80509-66-2.