Design and Simulation of Multiplexer Cell Resistant to Side Channel Attacks

Milena Stanojlović
Innovation Center
University of Belgrade, School of Electrical Engineering
Belgrade, Serbia
milena@venus.elfak.ni.ac.rs

Predrag Petković
Department of Electronics, LEDA laboratory
University of Nis, Faculty of Electronic Engineering Nis
Nis, Serbia
predrag.petkovic@elfak.ni.ac.rs

Abstract — **This paper discusses a part of hardware implementation of a complex cryptographic algorithms. A common way for data protection relies on the complexity of coding algorithm. It is expected that it will decrease the possibility of finding the combinations that breaks the encryption key in real-time. The attackers often use additional information about the behavior of an electronic cryptosystem in order 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 top down design of MUX2x1 cell that explores high immunity to SCA. Simulation results confirm resistance of MUX2x1 based on NSDDL method to SCA. The cell is designed in CMOS TSMC035 technology using Mentor Graphics design tools.**

Keywords-* *CMOS, cryptography, SCA, cell, NSDDL.

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 the 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 are based on monitoring of dynamics consumption at electronic cryptosystem. The most effective are Simple Power Analysis (SPA), Differential Power Analysis (DPA) and Electromagnetic Analysis (EMA) [2, 3].

The supply current (IDD) waveform hides very useful additional information about behavior of a cryptographic system. An abrupt change of current IDD in a CMOS digital circuit occurs only during transition of the logical state. During logic change from 0 to 1, output capacitances are charging to VDD through PMOS network. As the state changes from 1 to 0, capacitances are discharging to ground. In addition within the transition some short-circuit current flows when PMOS and NMOS transistors are turned 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 of data protection implementation. The research team is developing library of CMOS cells 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 [4-7].

Simulation results were obtained using *ELDO* simulator from *Mentor Graphics Design Architect* environment. The complete cell design was accomplished on *Mentor Graphics* design platform in TSMC035 technology. The subsequent section reviews the core of NSDDL method. The third section explores design methodology and SCA resistivity of MUX2x1 NSDDL cell together with simulation results.

II. NSDDL METHOD

The key idea in designing cells resistant to SCA is to eliminate correlation between power consumption and logic state change. Practically it means to force a logic cell to retain the same power consumption regardless combination of input signals. One of the straightforward techniques is to duplicate hardware by insertion of a complementary counterpart cell. Consequently the cell will have transition in both directions simultaneously at two output ports denoted as *true* and *false*. The hardware is doubled, but the effect of masking the true function of the cell is gained. Moreover, in order to mask neutral logic changes every change at inputs must provoke changes at outputs.

NSDDL method is based on the three phase clocking. The first phase named *pre-charge* is aimed to drive all outputs (true and false) to high logic 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 (*Wave Dynamic Differential Logic*) [8] is its immunity to imbalanced 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. DNOR is the integral part of the control logic and NSDDL cells. This method uses negative logic because DNOR cell acts as an inverter. Fig. 1 illustrates circuitry of DNOR cell.

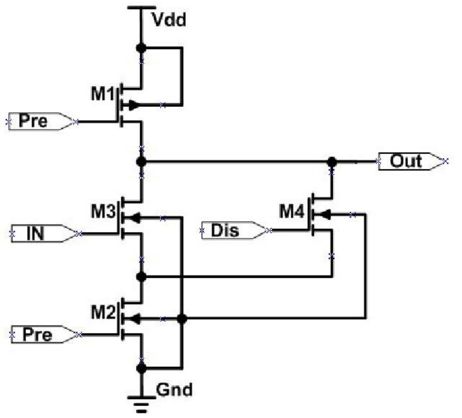

Figure 1. DNOR circuit

Figure 2 illustrates waveforms of control signals. When signals PRE=0 and DIS=0 the *pre-charge* phase occurs: transistor M1 is *on*, while the other transistors are *off*. The output goes high, 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 high. 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.

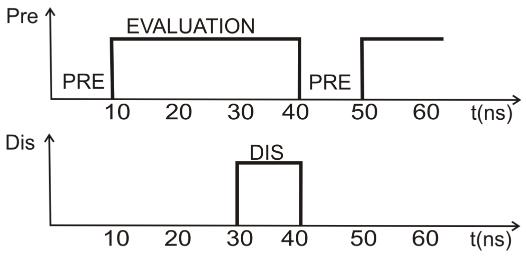

Figure 2. Time waveforms of control signals for DNOR cell

III. MUX2x1 NSDDL CELL

This section presents a design of a new NSDDL multiplexer cell that will be referred to as MUX2x1 NSDDL. The design is based on a standard MUX2x1 cell with inverted function and DNOR cell. As DNOR cell operates as an inverter, it is a natural to use standard cells with negative logic.

Block diagram of MUX2x1 NSDDL cell is presented in figure 3. True and false blocks are emphasized with dashed rectangles. Observing this figure one can see that these blocks have the same structure. It consists of two DNOR cells and one MUX2x1. The number of input and output signals in these blocks is the same but input signals are sorted differently. Therefore, A and B input signals must be permuted in one of those (true and false) blocks. Table I present the truth table for NSDDL MUX2X1. Output signal of multiplexer with inverted function is marked with OIM. OEVAL presents output signals of encrypted cell in evaluation phase separately for true and false output. *Sel* has function to switch between appropriate input signals. In the False block, inputs A and B exchange their positions because true and false output signals in evaluation phase must be complementary. That is seen in Table I.

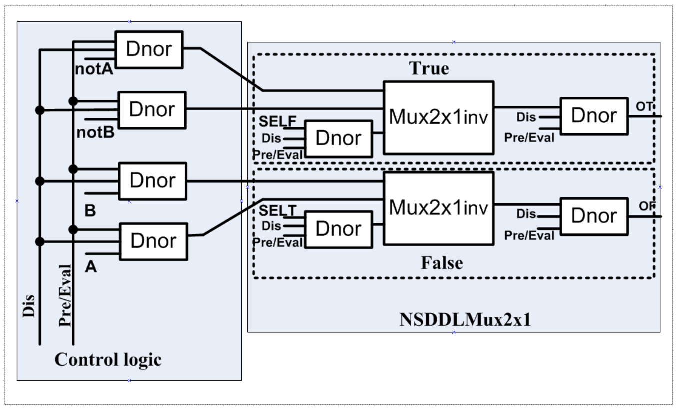

Figure 3. Block scheme of MUX2x1 NSDDL cell

TABLE I. TRUTH TABLE FOR NSDDL MUX2X1

NSDDL Mux2x1							
True				***False***			
A/B	***Sel***	***OIM***	***OEVAL***	***B/A***	***Sel***	***OIM***	***OEVAL***
0/0	0	1	0 (A)	1/1	1	0	1 (A)
0/1	0	1	0 (A)	0/1	1	0	1 (A)
0/0	1	1	0 (B)	1/0	0	0	1 (B)
1/1	1	0	1 (B)	0/0	0	1	0 (B)

Comparison between standard and NSDDL Mux2x1 cell demonstrates the validity of the proposed design.

Waveforms in figure 4 present in top down direction: excitation voltages A and B (1st and 2nd), Discharge and Pre-charge control signals (3rd and 4th), selection signal (5th), I_{DD} and output voltage of NSDDL cell (6th and 7th), and I_{DD} and output voltage for standard MUX2x1cell (8th and 9th).

Comparing IDD waveforms for NSDDL and standard cell one can see very clear difference. The information about output states, for standard MUX2x1, becomes recognizable and accessible by observing IDD current. In contrary, supply current of MUX2x1 NSDDL have regular pattern independent on output logic states. Consequently it is immune on side channel attack.

To quantify resistivity to SCA we have adopted a measure based on computed integral of consumed power in time (energy) according to (1).

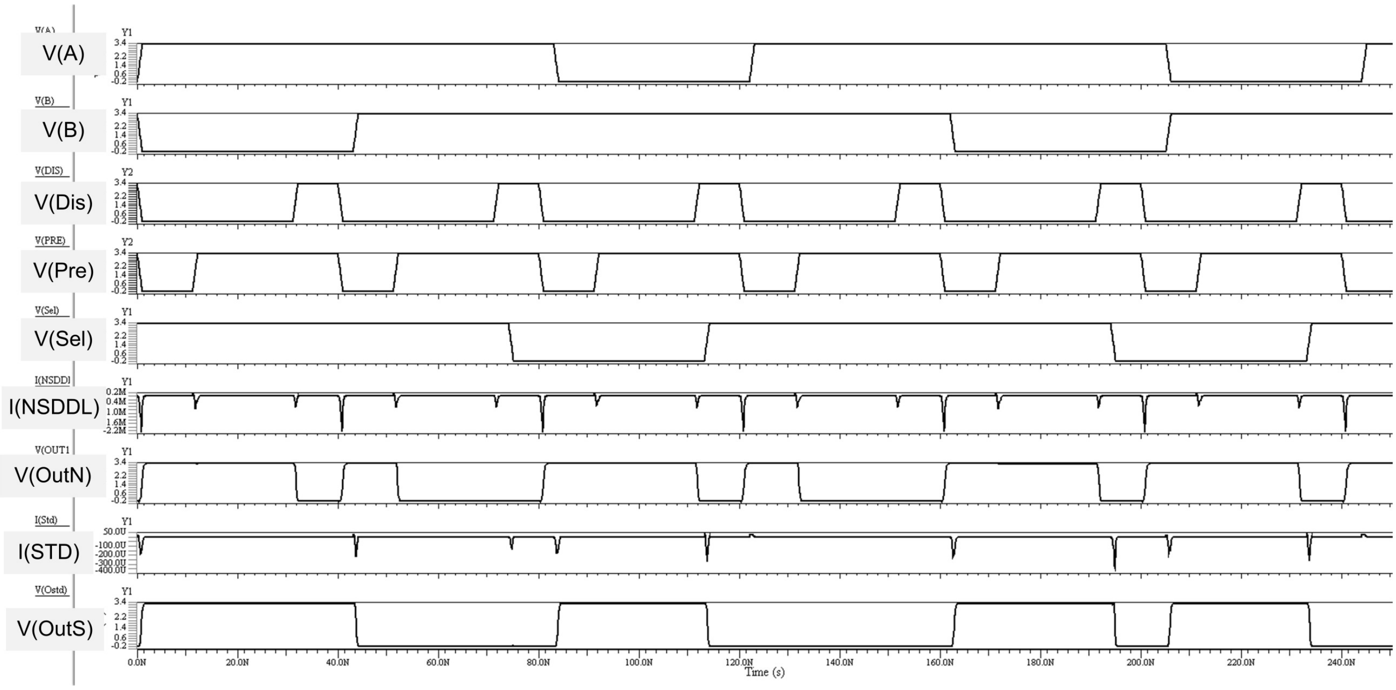

Figure 4. Waveforms of characteristic signals in NSDDL and standard MUX2x1 cell

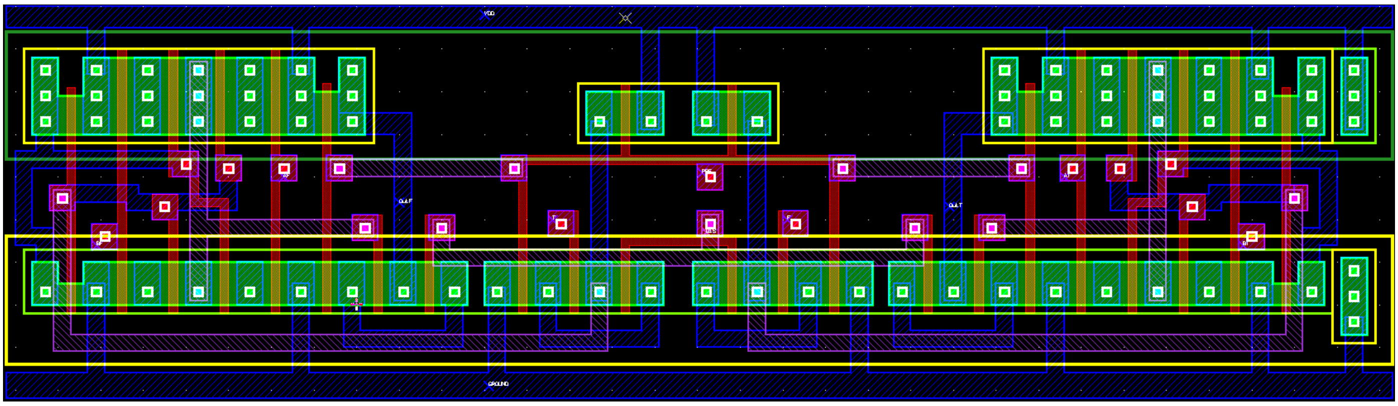

Figure 5. Layout of SCA resistant MUX2x1 cell

$$E = V_{DD}\int_{0}^{T} i_{DD}(t)\cdot dt \qquad (1)$$

Energy consumption is observed during one cycle of input signal change. For MUX2x1 NSDDL this cycle lasts for all three operational phases. In order to get better insight into behavior of both cells we derived the following parameters from the simulation results:

1. maximum energy (E_{max}),
2. minimum energy (E_{min})
3. average energy (E_{av})
4. relative difference in respect to E_{av} (δ)
5. standard deviation (σ)
6. Normalized Standard Deviation (NSD) in respect to E_{av}.

Table II summarizes results of comparison. Columns 1 and 2 indicate input combinations. Symbols "↑" and "↓" denote the rise and fall transition, respectively. The third column present results obtained for standard MUX2x1 cell while the 4th column refers to MUX2x1 NSDDL cell.

As a measure of SCA resistance we considered normalized standard deviation. For standard logic cells this parameter reaches 71%. Practically it means that consumed energy needed for particular signal change (depending on input signal combinations) will differ up to 71% in respect to average. Obviously this indicates strong correlation between energy and input signal transition. However, NSDDL cell has NSD nearly

1%. This is sufficient to conclude that MUX2x1 NSDDL cell is immune to SCA using DPA.

The total improvement of the resistivity to SCA in comparison with standard multiplexer cell is about sixty times in favor to MUX2x1 NSDDL cell. This can be easily verified by observing *NSD* parameter value in Table II for these two cells.

Figure 5 illustrates layout of SCA resistant MUX2x1 cell. Layout of True and False blocks differs only in respect to the ordering of input ports which form desired functions. The layout complies with all rules for symmetry of true and false parts in order to suppress unequal consumption in complementary parts of the cell.

TABLE II. CHARACTERISTICS COMPARISON OF STANDARD AND NDDDL MUX2X1 CELL

A	B	E_{STD} [J]	E_{NSDDL} [J]
1	↑	-2.57E-13	-5.03E-12
↓	1	-5.40E-13	-5.18E-12
↑	1	-2.55E-13	-5.17E-12
1	↓	-4.02E-13	-5.01E-12
↓	↑	-7.66E-13	-5.10E-12
↑	1	-2.54E-13	-5.16E-12
1	1	3.37E-16	-5.05E-12
↓	↓	-6.12E-13	-5.15E-12
↑	↑	-2.50E-13	-5.15E-12
1	1	3.66E-16	-5.05E-12
E_{max} [J]		3.66E-16	-5.01E-12
E_{min} [J]		-7.66E-13	-5.18E-12
E_{av} [J]		-3.33E-13	-5.11E-12
δE [%]		-100.05	-3.29
σ [J]		2.37E-13	6.12E-14
NSD[%]		-71.00	-1.19

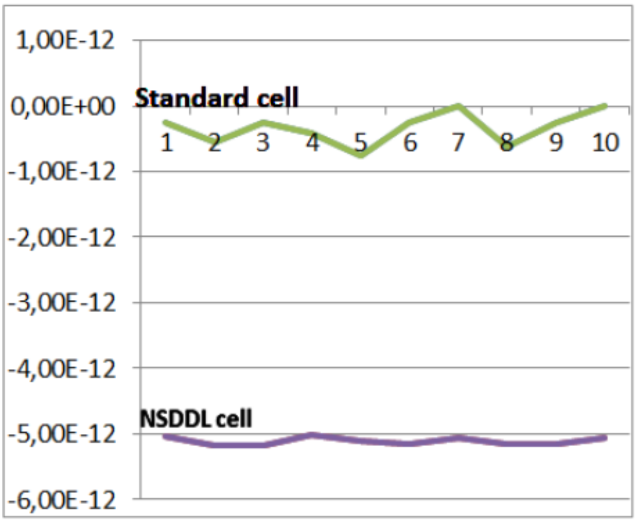

Figure 6. Energy consumption during ten cycles of input signal change for both cells

Figure 6 shows profile of energy consumption during ten cycles of input signal change for both cells. Standard MUX2x1 cell characterize lower average energy and considerable dispersion of values corresponding to particular input signal combinations. Oppositely, the energy profile of MUX2x1 NSDDL cell shows no deviation and is very uniform.

IV. CONCLUSION

This paper presents simulation results that prove resistance of MUX2x1 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. Two additional three-phase control signals guarantee that all outputs will start from the high level during the pre-charging and that will take low level during the discharging phase. Between these changes the cell operates in desired logic mode. Then the true output takes the preferred output state while the false output performs opposite transition. This structure consists of two same blocks. One block contains two DNOR cells and one MUX2x1. The number of input and output signals in these blocks is the same but input signals are sorted complementary. 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 MUX2x1 NSDDL cell is approximately 1.19% in comparison to 71% that explores standard MUX2x1 cell in the same technology.

ACKNOWLEDGMENT

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, Z Proc. of II Conference about security of information systems,, Belgrade, Serbia, May 2010, pp 22-27.

[3] Danger, J., Guilley L., Bhasin S., Nassar S., " 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

[4] Bucci M, Giancane L, Luzzi R, Trifiletti A: *"Three- Phase Dual-Rail Pre-Charge Logic"*. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 232–241. Springer, Heidelberg (2006).

[5] Quan J. and Bai G, "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.

[6] Stanojlović, M., Petković, P. „*Asic cryptosystem based on standard cells resistant to SCA*", VIII Symposium on Industrial Electronics INDEL

2010, Banja Luka, Bosnia and Herzegovina, 4-6 November, 2010, pp. 110-114, ISBN 978-99955-46-03-8

[7] Petković, P., Stanojlović, M.: *"Hardvare protection against attacks on cryptosystem based on the implementation of cells that masked information about consumption*“, Proc. of LV Conference ETRAN, Banja Vrućica, Bosnia and Herzegovina, ISBN 978-86-80509-66-2

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