Library of Combinational Logic Cells Resistant to Side Channel Attacks

Milena Stanojlović Mirković, Miljana Milić, Dejan Mirković and Vančo Litovski

Abstract – This paper presents an overview of research in the field of hardware cryptography. An effort was made to develop the library of CMOS cells that are resistant to Side Channel Attack. The No Short-circuit current Dynamic Differential Logic method is implemented. Characteristics of encrypted cells are compared with the standard, (not encrypted), cells under various operational conditions in order to prove the SCA resistance. Designed encrypted cells represent the basis of developing more complex crypto system and increase its overall security.

Keywords – CMOS, IC design, SCA, Cryptography, NSDDL method.

I. Introduction

The content of an encrypted data in digital systems is protected by utilizing specific algorithms which should harden obstruct the decrypting. The protection is usually based on application of complex keys which require hacker to apply a large number of combinations in order to break them. The longer time it takes for trying of each bits combination, the protection is better. However, time for key breaking may be significantly reduced if, besides logical states, other characteristics of the signal are observed. Usually, analysis of power consumption i.e. power supply current time profile are used for this purpose. Every unauthorized collecting of such information about crypto system behaviour is referred to as Side Channel Attack (SCA) [1-2].

The main source of information about the behaviour of a circuit is the circuit activity expressed through the change of the supply current. Observing changes in the supply current (I_{DD}) and correlating them with known input vector can be used as valuable information for breaking the coding key. Physical background for this approach lies in the fact that an abrupt change of the I_{DD} in a CMOS digital circuit occurs only during transition of a logic state. For example, during the 0-to-1 transition of the signal an additional charge is needed to load capacitances. Besides, some "short-circuit" current flows when PMOS and NMOS transistors are turned on simultaneously. During this transition, I_{DD} changes produce electromagnetic field variations which the attackers may detect using special probes.

Milena Stanojlović Mirković, Miljana Milić, Dejan Mirković and Vančo Litovski are with the University of Niš, Faculty of Electronic Engineering, Aleksandra Medvedeva 14, 18000 Niš, Serbia, E-mail: stanojlovim@gmail.com, milana.milic@elfak.ni.ac.rs, dejan.mirkovic@elfak.ni.ac.rs vanco.litovski@elfak.ni.ac.rs.

The encrypted library of CMOS cells, that are resistant to SCA attacks, is developed in LEDA Laboratory at the Faculty of Electronic engineering, University of Nis. The key achievement in this study is the development of the part of this library which applies only to combinational logic.

The SCA resistance is measured by the degree of the information hiddenness and it is larger if the correlation between the I_{DD} and the circuit behaviour is suppressed. For the design of encrypted cells, the No Short circuit current Dynamic Differential Logic method is adopted [3].

This paper is organized as follows: the section II presents the basics of the NSDDL method; the section III presents the design methodology of combinational encrypted cells; while in the section IV considers the difference between power supply currents (I_{DD}) for standard and encrypted cells. The final section summarizes key contributions of this research.

II. NSDDL method

The encrypted cells' functioning exploits the idea that each combination of input signals results in the same power consumption. This can be realized 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 hiding the true function of the cell is achieved.

The NSDDL method requires three different operation phases. During the first, precharge, phase both outputs (true and false) of all logic cells are driven to high logic level. In the second phase, known as the evaluation phase, the desired value is set at the true output and the complementary value is established at the false output. The third phase is named discharged because all outputs achieve low logic level. These phases are illustrated in Fig. 1.

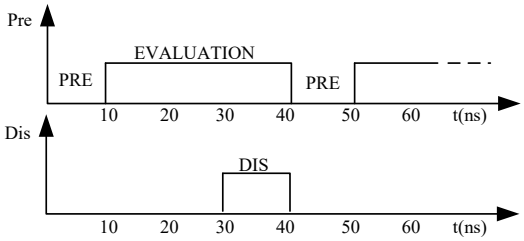


Fig. 1 Waveforms of control signals for the Dnor cell

The advantage of this method compared to other popular solutions, like WDDL [4-5], is its immunity to imbalance loads at true and false outputs. This is achieved by using a dynamic NOR circuit (DNOR) which minimizes the impact of short circuit currents in the CMOS circuit. It is an integral part of the control logic and NSDDL cells. Figure 2 illustrates this circuitry.

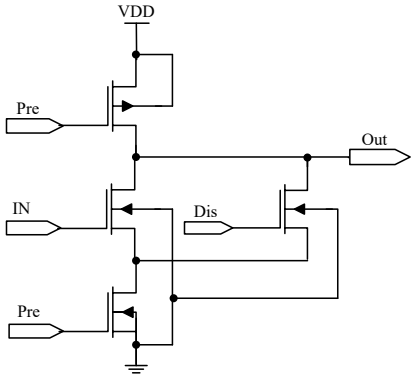


Fig. 2. Dnor cell

III. NSDDL CELLS - COMBINATIONAL LOGIC

All logic cells resistant to SCA are designed in CMOS technology TSMC 0.35um. The idea of the NSDDL methodology requires that the responses of each input signal combination consume the same power. This is possible with the doubled hardware that contains a cell with the complementary properties. Therefore, any input combination will imply the transitions on both true and false outputs.

A. Designing an inverter / buffer cell (INV / BUFF)

Due to the complementary design an inverter (INV) cell will behave as a buffer (BUFF) at the false output[6-7]. However, the simplicity of the logic function requires a different design approach comparing to the general NSDDL concept. Obviously, complementary signals A and notA are required at true and false inputs At the output of the cell two signals denoted with OT (Output True) and OF (Output False) are generated. The signal OT represents the true output signal (inverted A signal), while OF represents the false one, as depicted in Fig. 3.

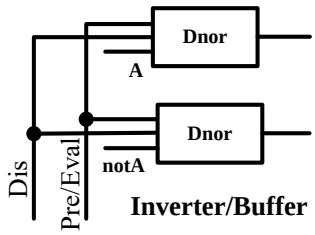
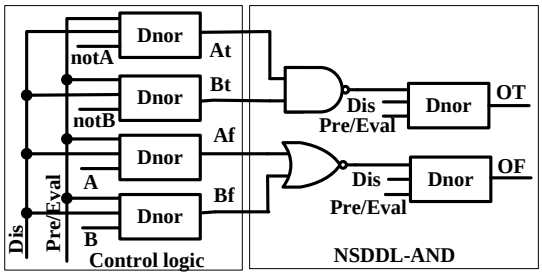


Fig. 3. Block diagram of the NSDDL INV/BUFF cell

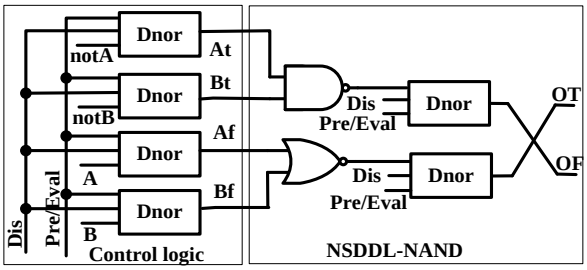
In the case of a BUFF cell, OT and OF signals, meaning, are swapped. At the same time this cell represents a part of the logic that controls others NSDDL cells. This practically means that the inverting function in the NSDDL logic is obtained with crisscrossing of true and false outputs.

B. Design of two - input AND/NAND/OR/NOR cell

Consider mutually complementary NAND and NOR cells, as a part of a SCA resistant structure. Block schemes of AND/NAND and OR/NOR NSDDL, SCA resistant cells are presented in figures 4 and 5, respectively [8].

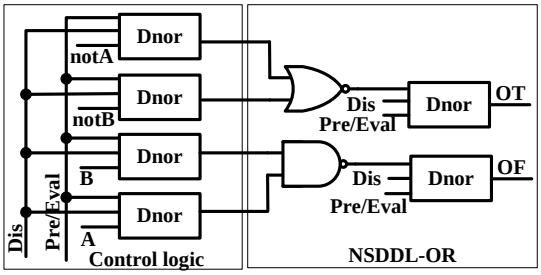


a)

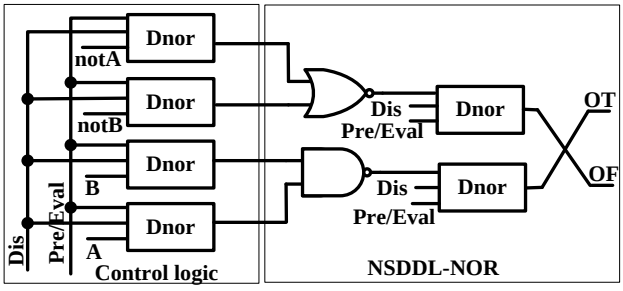


b)

Fig. 4. Block diagrams of a) NSDDL AND cell; b) NSDDL NAND cell



a)



b)

Fig. 5. Block diagrams of a) NSDDL OR cell; b) NSDDL NOR cell

Besides, from figures 4 and 5 can be seen that cells are excited with mutually complement input signals A and notA i.e. B and notB. Using de Morgan rules it can be shown that with simple input signal (A, notA, B, notB).

It is obvious that the same hardware structure implement AND, NAND, OR and NOR functions. That is why this structure is referred to as the AND/NAND/ OR/NOR SCA resistant cell. It is important to notice that all functions are implemented using negative logic circuits with negative logic (NAND and NOR) which can be easily implemented using CMOS technology.

The DNOR circuit represents the basic element for all SCA resistant cells within the NSDDL technique. It provides inverting function when transforming from standard to the NSDDL logic.

C. Design of the XOR/XNOR cell

This cell consist of two NSDDL AND cells and one NSDDL OR cell. The block diagram of the XOR/XNOR SCA resistant cell is presented on Fig. 6.

The control logic generates the input signals for this cell. Since that the input (true and false) signals, are complementary, the same structure provides both functions: the XOR function at the true output (OT) and XNOR function at the false output (OF).

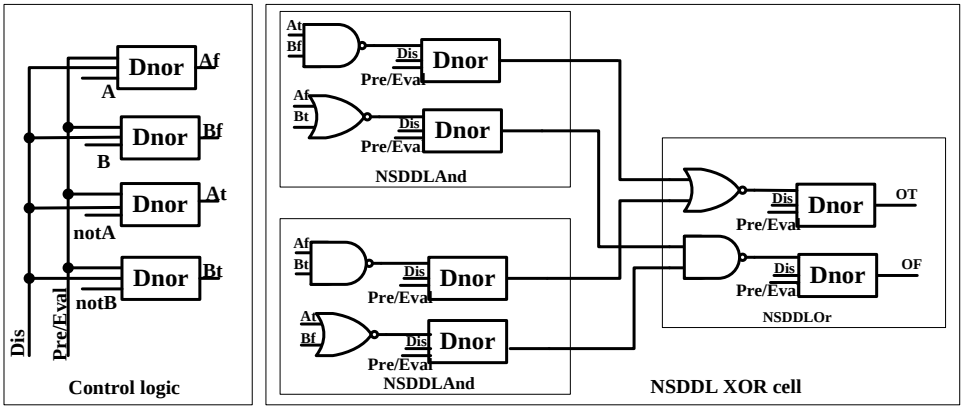


Fig. 6. Block scheme of NSDDL XOR SCA resistance cell

IV. RESULTS

This section will present comparative results of the simulations for standard and encrypted cells. For standard cells one can expect strong correlation between energy required for the particular transition and the 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 hide the cell's operation regarding I_{DD}. Therefore, they should provide a minimal correlation between the stimulus signals and the I_{DD} value. To quantify the resistivity to SCA we have adopted a measure based on the calculated integral of the consumed power over time (energy) [11-12].

$$E = V_{DD} \cdot \int_0^T i_{DD}(t) \cdot dt, \tag{1}$$

In order to provide better insight into the behavior of every cell from the simulation results we have derived the following parameters: standard deviation (σ) normalized standard deviation in respect to average energy (E_{avg}) *(NSD)*. As a measure of the SCA resistance we have considered normalized standard deviation according to (2).

As for the INV and BUFF cells, only two transitions of input signal are possible. Therefore, it makes no sense to statistically process only two data values. That is why only relative average energy consumption difference is observed, and it is denoted with δE in Table I. One can notice that the uniformity of the cell's energy consumption is increased. This means that the presented cell has the significant SCA resistance. Also, when the δE parameter is observed, there is a 98.9 times increase in the SCA resistivity.

$$NSD = 100 \cdot \frac{\sigma}{E_{avg}} [\%]. \tag{2}$$

TABLE I RESULTS OF STANDARD AND NSDDL INVERTER CELLS

A	notA	$E_{standard}$ [J]	E_{NSDDL} [J]
↑	↓	2.48136E-13	1.32838E-12
↓	↑	2.21651E-13	1.3299E-12
E_{avg} [J]		2.34894-13	1.3291E-12
δE [%]		11.275	0.114

Results obtained for standard AND, NAND, OR and

NOR, and NSDDL AND/NAND/OR/NOR cells are compared and presented in Table II. Also, the same table contain results for standard XOR and XNOR cells and the NSDDL XOR/XNOR cell.

It is interesting to track how the property defined as resistance to the SCA is being transferred from lower to higher hierarchical design level. With this in mind, we have performed a similar set of simulations for NSDDL XOR/XNOR as for the NSDDL AND/NAND/OR/NOR cell.

TABLE II RESULTS OF STANDARD AND NSDDL CELLS

	E_{avg} [J]	δE [%]	σ [fJ]	NSD [%]
AND	4.83E-13	210.15	405.4	83.91
NAND	4.11E-13	196.98	337.7	82.23
OR	3.62E-13	222.05	310.3	85.64
NOR	2.94E-13	202.67	243.1	82.59
NSDDL AND/NAND/OR/NOR	2.77E-12	2.81	24.31	0.87
XOR	3.90E-13	63.64	91.77	23.51
XNOR	3.25E-13	131.76	154.18	47.43
NSDDL XOR/XNOR	6.24E-12	3.53	56.58	0.907

Dynamic energy consumption, as mentioned before, is expressed through the integral of the I_{DD} over time during one cycle of the input signal change. This cycle is the same for standard cells as for NSDDL cells, in all three operational phases. As before, relative, average consumed energy difference, standard deviation and normalized standard deviation are taken as measures of the SCA resistance. Parameters are denoted with *δE,* σ and *NSD*, and are given in columns one, two and three, respectively.

The *NSD* parameter that is less than 1% (0.87%) for the AND/NAND/OR/NOR2 NSDDL cell remained almost the same. Although slightly increased to the value of 0.91%, it is still less than 1%, which qualifies this cell as the SCA resistant one. Actually, the *NSD* has increased for 4.6% in respect to the AND/NAND/OR/NOR NSDDL cell. The total improvement of the resistivity to SCA in comparison with standard cells overcomes 2500% for the XOR and 5000% for the XNOR cell.

Figures 7 and 8 show trends of the energy consumption for:

- the four unprotected standard cells (AND, NAND, OR, NOR) and encrypted NSDDL AND/NAND/OR/NOR cell (Fig.7)
- two unprotected standard cells (XOR and XNOR) and the encrypted NSDDL XOR/ XNOR cell (Fig. 8)

The input signal combinations are given in the horizontal axis labels, A and B, where the symbols "↑" and "↓" denote rising and falling transitions, respectively. The ordinate label denotes obtained energy levels for those cells.

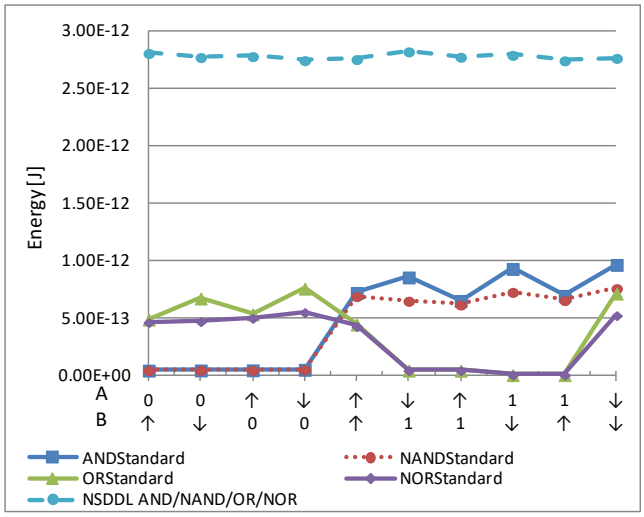


Fig. 7. Energy consumption during ten cycles of input signals change for the unprotected standard cells and the encrypted NSDDL AND/NAND/OR/NOR cell

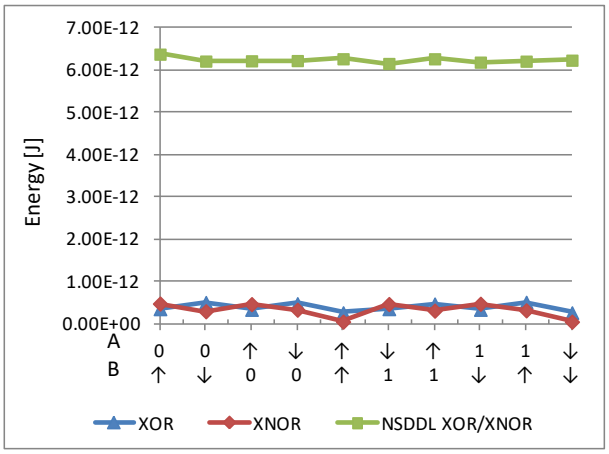


Fig. 8. Energy consumption during ten cycles of input signals change for the unprotected standard cells and the encrypted NSDDL XOR/XNOR cell

V. CONCLUSION

This paper presents the part of library logic cells resistant to side channel attacks (combinational logic) designed by the rules of the NSDDL method. This method is characterized by the duplicated implementation of hardware that generates true and false outputs. The false output has the same function as the 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 with doubled input signals Three-phase clock signal guarantees that all outputs will start from the high logic level during the pre-charging phase, and will end with

the low logic level during the third phase. The cell performs the desired logic function in the second operating phase. Then the true output takes the desired output state and, while, simultaneously the false output changes with the opposite transition. The energies required for output transition under different combination of input signal were considered as a measure of the SCA resistance. The cell is resistant if all changes at its outputs require the same energy. As a measure of a cell SCA resistance we have considered the normalized standard deviation (NSD). All designed cells have showed a good resistivity to SCA when this parameter is observed.

ACKNOWLEDGEMENT

This work was partially funded by Serbian Ministry of Education, Science and Technological Development under contract No. TR32004.

REFERENCES

[1] Lomné, A. Dehaboui, P. Maurine, L. Torres, M. Robert, "Side Channel Attack"', in B. Badrignans, J. L. Danger, V. Fischer, G. Gogniat, L. Torres, "*Security Trends for FPGA*", Springer Netherlands 2011, pp. 47-72

[2] Stanojlovic M., Petkovic P., " Strategies against side-channel-attack" in *Proceedings of the Small Systems Simulation Symposium*, Niš, Serbia, pp. 86–89, 2010.

[3] Quan J., Bai G., "A new method to reduce the side-channel leakage caused by unbalanced capacitances of differential interconnections in dual rail logic styles", *Sixth International Conference on Information Technology*: New Generations, pp. 58-6, 2009.

[4] Tiri K., Verbauwhede I., "Place and Route for Secure Standard Cell Design", CARDIS'04, pp. 143-158, 2004.

[5] Velegalati R., "Securing Light Weight Cryptographic Implementations on FPGAs Using Dual Rail with Pre-Charge Logic", PhD Thesis, George Mason University, Fairfax, VA, 2009.

[6] Stanojlović M**.**, Milovanović, D. "Simulacija defekata osnovnog kola kontrolne logike NSDDL metoda", *Zbornik LV konferencije ETRAN,* Banja Vrućica, Bosna i Hercegovina, 06.06.-09.06., EL 4.5, 2011.

[7] Stanojlović M., "D flip-flop ćelija otporna na bočne napade analizom struje napajanja", *Zbornik LVII konferencije ETRAN*, Zlatibor, 03.06.-06.06., EL3.3, 2013.

[8] Stanojlović M**.**, Litovski V., Petković P., "Testiranje standardne AND ćelije otporne na bočne napade", *Zbornik LVIII konferencije ETRAN*, Vrnjačka Banja, 02.06.-05.06., EL2.5, 2014.

[9] Stanojlović Mirković M**.**, Litovski, V., Petković P., Milovanović, D., "Faults Simulations in XOR/XNOR Cell Resistant to Side Channel Attacks", *X Simposium on Industrial Electronics INDEL*, Banja Luka (Bosnia and Herzegovina), pp. 83-88, 6-8th November, 2014.

[10] Stanojlović M., Petković P., "Resistance of XOR/XNOR NSDDL Cell to Side Channel Attack", *Proceedings of Small Systems Simulation Symposium*, Niš, Serbia, 12.02.-14.02., pp. 141-144, 2012.

[11] Monteiro C., Takahashi Y., Sekine T., "Charge-sharing symmetric adiabatic logic in countermeasure against power analysis attacks at cell level", *Microelectronics Journal, Elsevier*, vol. 44, no. 6, pp. 496-503, 2013. doi.org/10.1016/j.mejo.2013.04.003

[12] Wang P., Zhang Y., Zhang X., "Design of two-phase SABL flip-flop for resistant DPA attacks", *Chinese Journal of Electronics*, vol. 22, no.4, pp.833-837, 2013.