FACTA UNIVERSITATIS
Series: **Automatic Control and Robotics** Vol. 18, Nº 3, 2019, pp. 141 - 152
https://doi.org/10.22190/FUACR1903141S

EVALUATION OF RESISTANCE TO SCA FOR DIFFERENT ARCHITECTURES OF ENCRYPTED CELL

UDC (621.3.049.77)

Milena Stanojlović Mirković, Miljana Milić, Dejan Mirković

University of Niš, Faculty of Electronic Engineering, Department of Electronics, Niš, Republic of Serbia

Abstract. *This paper deals with a top down design of an example multiplexer cell that exhibits high immunity to Side Channel Attack (SCA). Four different solutions of the encrypted multiplexer cell are revised, and the best design adopted. The post-layout simulations prove resistance of the multiplexer logic cell to the SCA. Since the physical layout structure and the functionality of this kind of design is based on symmetry, concerns were expressed as to what will be the effectiveness of the method under real production conditions. To get a proper answer to that, the adequacy of the chosen design for the multiplexer cell, which uses the "No Short-circuit Current Dynamic Differential Logic" (NSDDL) method, is confirmed by observing a Normalized Standard Deviation (NSD).*

Key words: *CMOS integrated circuits, encrypted cell, layout, electrical and post-layout simulation, SCA*

1. INTRODUCTION

By following the trends in the IC technology one can conclude that cryptography takes the leading research challenge because of the high importance of data security. Starting from the credit cards, coded alarm systems to all types of cipher-protected data transfer, it is necessary to protect the code keys from the misuse [1-2]. Even the protected systems can be attacked. Any unauthorized collecting of information about cryptosystem behavior is referred to as Side Channel Attack (SCA) [3-5]. The dominant mechanism for SCA is based on observing the dynamics consumption of electronic encrypted system. The key source of information about the behavior of a circuit is the circuit's activity. This information is usually impressed in the power supply current, I_{DD}. Therefore, one of the

Received December 03, 2019
Corresponding author: Milena Stanojlović Mirković
University of Niš, Faculty of Electronic Engineering, Department of Electronics, Aleksandra Medvedeva 14, Niš, Republic of Serbia
E-mail: milena.sm@elfak.ni.ac.rs

most powerful methods for analyzing this current is the Differential Power Analysis (DPA) which belongs to the group of SCA attacks [6-7]. Observing changes in the supply current and correlating them with a known input vector can be used as valuable information for breaking the coding key. The physical background for this approach comes from the fact that significant current drawn from the power supply, I_{DD}, in a CMOS digital circuit flows only during the transition of a logic state. Moreover, I_{DD} changes produce electromagnetic field variations which the attackers may catch using special probes. Therefore, the circuits' immunity to SCA - i.e. SCA resistance, is determined by the ability to mask the correlation between I_{DD} and stimulated, input, code sequence.

The focus of this research is the implementation of countermeasures, at the transistor level design. In particular, the protection against SCA should be built-in in every custom design of digital cell. The cryptographic method chosen for the design of these cells is known as the No Short-circuit current Dynamic Differential Logic (NSDDL) method [8]. Our goal here is to characterize a two-to-one multiplexer (MUX2x1) cell designed with a good SCA resistance using as little hardware as possible. This cell is a part of a standard cell library that is developed as a base for the synthesis of cryptographic systems. We consider it as a suitable representative since it is complex enough to expose the main weaknesses of the NSDDL method.

This paper is organized as follows: the second section presents the basics of the NSDDL method, while the third section describes the design of an encrypted multiplexer cell. The fourth section considers results obtained with the post-layout simulation. It includes comparisons, as well. The final section summarizes the overall contribution of this research.

2. CONCEPT OF THE SCA PROTECTION AND AN OVERVIEW OF THE NSDDL METHOD

Each rising edge of a digital signal requires additional charge to be added from the power supply line to the output capacitance. On the other hand, the load discharges during the falling edge. The amount of the charge increment is proportional to the number of capacitors being charged as well as - the circuit activity.

The attacker is usually armed with probes that sense the I_{DD} change. He tracks the I_{DD} for the known input signals (tried password). Accordingly, anyone who has elementary knowledge of digital electronic circuits may conclude about the transitions occurring inside an IC. Therefore, digital signal tracking supported by monitoring of the I_{DD} becomes a powerful tool for eavesdropping the activities within a digital circuit.

Hence, the concept of protection against SCA is based on hiding the correlation between changes of the logic states and the waveform of power consumption. According to the level where the protection is applied, protection concepts can be classified as: architectural, gate and transistor levels [9]. The focus of this research is the third class of protection.

The last-mentioned way represents the class of methods known as Dual-rail with Pre-charge Logic (DPL) method [10]. With this methodology all the signals in the circuit are duplicated by introducing their complements in order to have their true and false

representatives. Therefore, each combination of input signals applied to the inputs of SCA resistant cells manifests with the same power consumption. This is possible when every logic cell has the counterpart that will act complementary. For that reason, every cell needs to have two outputs, denoted as true and false. Consequently, the cell will have transitions in both directions simultaneously at two output ports. The obtained hardware is doubled but the increased complexity enables the cell to hide its true function. Moreover, in order to mask neutral logic changes, every change at inputs must provoke changes at outputs.

According to this methodology all logic in the circuit operates in Precharge and Evaluation phases to ensure exactly one switching event per cycle.

One of the DPL representatives is the Wave Dynamic Differential Logic (WDDL) method [11-12]. The drawback of this method is the requirement for balanced loads at true and false outputs. Therefore, very careful matching is required at the layout level to diminish this problem. An alternative method, known as the Current Mode Logic (CML) [13], is also sensitive to mismatching. Accordingly, other techniques have been proposed in the literature to avoid this obstacle.

The following section describes the one known as the No Short-circuit current Dynamic Differential Logic (NSDDL). The most important property of this method is the duplication of the hardware, as in the case of the DPL method. The most important aspect of the NSDDL method is that it operates in three phases synchronized with the clock signal, as in the TDPL methodology (Three-Phase Dual-Rail Pre-Charge Logic) [5, 14].

The task of the Precharge phase is providing the high logic level at all (true and false) outputs. The Evaluation phase is the second phase, where the true outputs take real values while the false outputs take the complementary levels. The next phase is called the Discharge phase where all outputs reach a low logic level. For the implementation of all three phases the Dynamic nor (Dnor) circuit is used. Fig. 1 presents the schematic of one Dnor circuit. It is used both in the control logic and in all encrypted NSDDL logic cells. Table 1 describes the logic function of the Dnor cell.

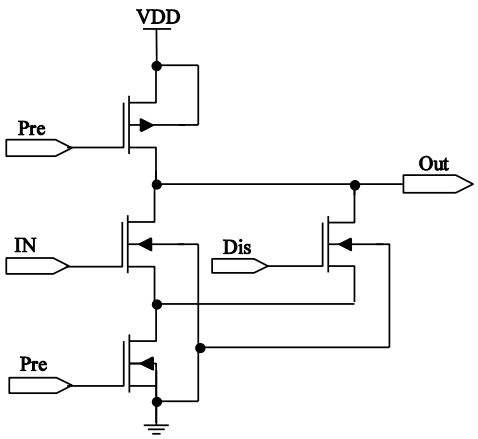

Fig. 1 Schematic of Dnor cell

Table 1 Logic function of Dnor cell

	Signals			
Phases	Pre	Dis	In	Out
Precharge	0	0	0/1	1
Evaluation	1	0	0/1	1/0
Discharge	1	1	0/1	0

3. EVOLUTION OF THE DESIGN FOR THE ENCRYPTED MULTIPLEXER CELL

The goal is to create an encrypted cell that gives high degree of protection against the SCA. The search for the best design required a development of several different architectures. The essential requirement is that the logic function of the circuit remains the same as for the unprotected cell. Fig. 2.a presents a symbol of a standard MUX2x1 cell. The value of the *SEL* signal determines which of the input signals (*A* or *B*) will be forwarded to the output. The Fig. 2.b shows the schematic of this multiplexer as is in the TSMC035u library [15].

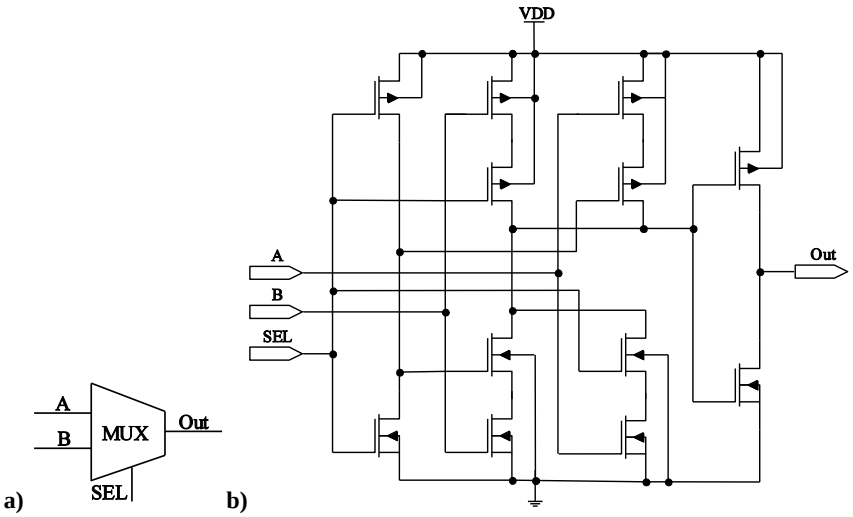

Fig. 2 Multiplexer MUX2x1 cell a) generic representation b) standard CMOS realization

In the NSDDL methodology all input and output signals are controlled using the Dnor cells**.** Since the Dnor cell has an inverting function, all designs use a multiplexer cell with the inverted function. Those two structures are the base for the design of the encrypted MUX2x1 cell in accordance with the NSDDL method. Figs. 3a and 3b present the symbol and schematic of a standard MUX2x1 cell with inverted function, respectively. The schematic is taken from the same library. One can see that only the output inverter is removed when comparing with the MUX cell in Fig. 2.b.

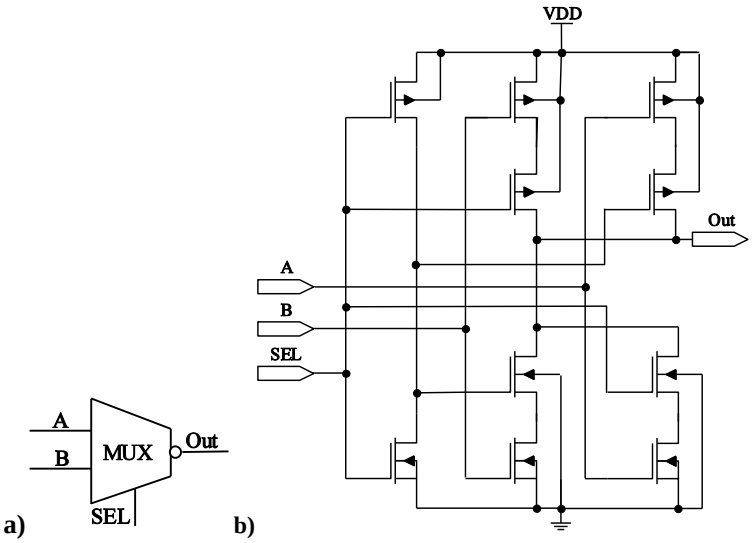

Fig. 3 Multiplexer MUX2x1 cell with an inverted function a) generic representation b) standard CMOS realization

The realization of all four NSDDL architectures will be described within this section. The complete cells design was accomplished using the Mentor Graphics design platform in a TSMC035 technology. All layouts of true and false sub-blocks are drawn symmetrically following the proper rules. In this way unequal power consumption in the complementary parts of the cell was suppressed [16].

3.1. Architecture I

In the first architecture, true and false input signals are introduced as in Fig. 4 as notA, notB, and B, A respectively.

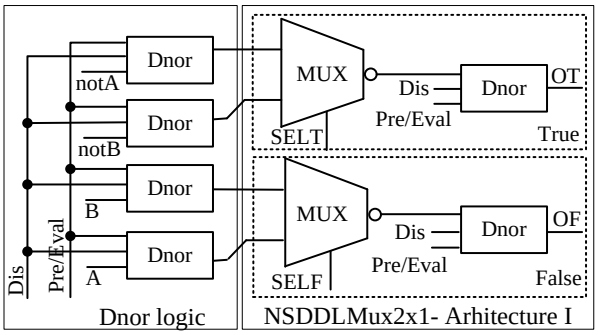

Fig. 4 Conceptual diagram of the MUX2x1 cell - Architecture I

Also, the sub-blocks are denoted as true and false and their outputs as OT and OF. These sub-blocks have the same structure but OT depends on notA and notB signals, while OF is a function of B and A. The signals *SELT* and *SELF* are directly connected to the multiplexers as *SELT=SEL, SELF=NOT (SEL)*. Fig. 5 gives the layout of the Architecture I.

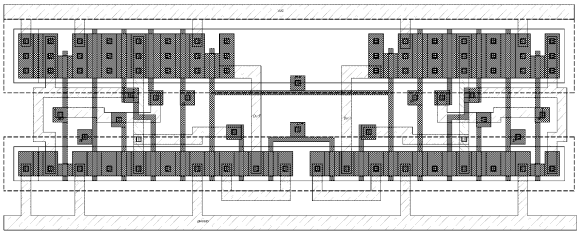

Fig. 5 Layout of Architecture I

3.2. Architecture II

In the second architecture (Architecture II) only one *SEL* signal controlled by a Dnor cell is used. This means that both sub-blocks use the same *SEL* signal. The arrangement of input signals is different in comparison to the first architecture. This can be seen from the block diagram of the Architecture II in Fig. 6. The layout is given in Fig. 7.

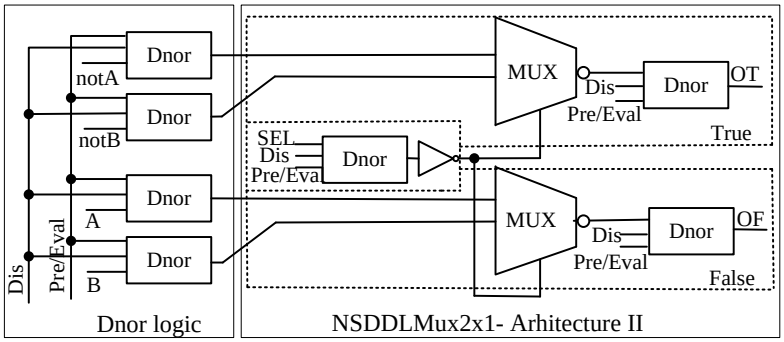

Fig. 6 Conceptual diagram of the MUX2x1 cell - Architecture II

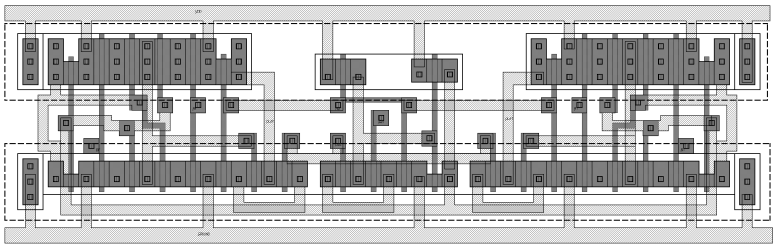

Fig. 7 Layout of Architecture II

As already mentioned, the true and false blocks are controlled with a single SEL signal that does not have its complementary pair. The aim of this modification is to investigate the additional reduction in the number of internal signals without losing the circuit's main purpose and protection ability. With this layout the complementary SEL signal was avoided, cell area was minimally increased, while the functionality of the circuit retained.

3.3. Architecture III

The third architecture (Architecture III) considers *SEL* signals as any other inputs (which are included through Dnor). The *SEL* blocks must be reversed in comparison to the Architecture I, because the Dnor cell works as an inverter. Block diagram and layout of the third NSDDL MUX2x1 architecture (Architecture III) is presented in Figs. 8 and 9, respectively.

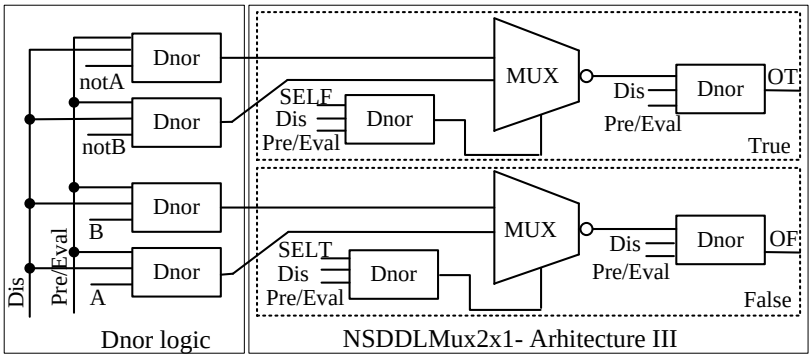

Fig. 8 Conceptual diagram of the MUX2x1 cell - Architecture III

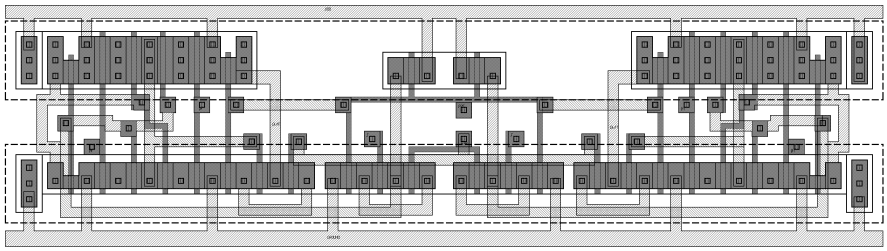

Fig. 9 Layout of Architecture III

3.4. Architecture IV

The fourth Architecture (Architecture IV) is based on a modification of the standard cell. Namely, the standard MUX2x1 cell can be customized to fit the NSDDL with reduced complexity. Figs. 10a and 10b give the symbol (generic representation) and schematic of modified MUX2x1 cell with the inverted function, respectively. When comparing Figs. 3b and 10b it can be noticed that one inverter is omitted.

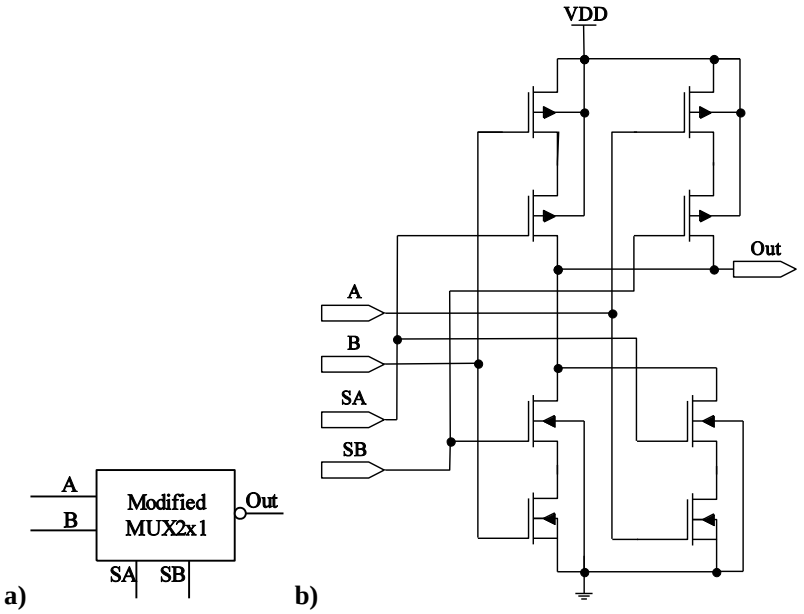

Fig. 10 Modified MUX2x1 with inverted function a) generic representation b) modified CMOS realization

Actually, the Dnor circuit, used for the *SEL* signal, provides the omitted inverting function. In addition, it is necessary to connect the input signals as depicted on the block diagram in Fig. 11.

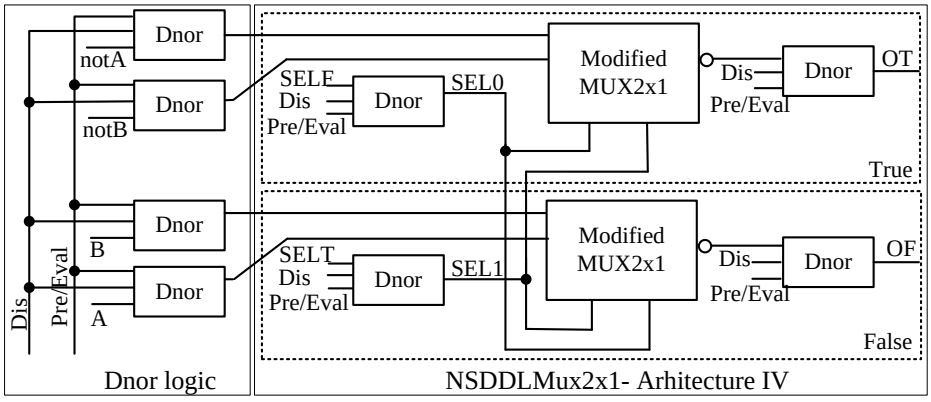

Fig. 11 Conceptual diagram of the MUX2x1 cell - Architecture IV

Since, the *SEL* signals for true and false blocks are complementary the proposed arrangement of input signals is possible. The introduced innovation simplifies the hardware. The reduction of the number of transistors in multiplexer cell prevents buffering of the *SEL*

signal and the total propagation time of the cell, as well. In this way the SCA resistivity is increased, as will be elaborated in the next section. The Layout of Architecture IV is given in Fig. 12.

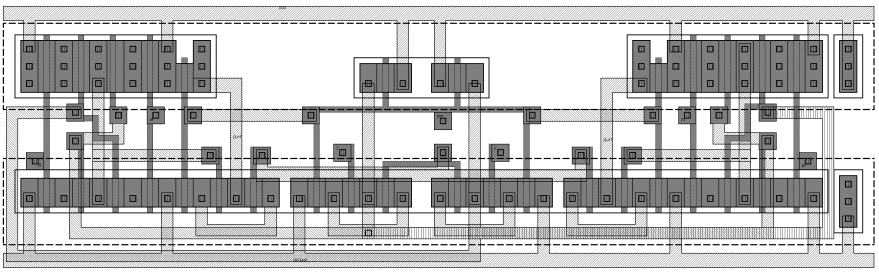

Fig. 12 Layout of Architecture IV

Table 2 gives comparative results of the layout areas for the unprotected standard MUX cell and for other four analysed architectures of the encrypted cell. The third row gives the normalized area for all cells. All cells are normalized with the area of the unprotected standard cell.

Table 2 Comparative results of layout areas

	Standard cell	Architecture			
		I	II	III	IV
Area [μm^2]	288	861.12	1119.72	1232.8	1115
Normalized area	1	2.99	3.88	4.28	3.87

4. RESULTS

The adopted criteria for the evaluation of designs' specifications are: area of the layout, energy consumption and the SCA resistivity. The unprotected standard cell presents the reference case for the assessment of the protection degree for the encrypted cells. The normalized standard deviation (NSD) is adopted as a quantitative measure of the SCA resistivity for the encrypted cells designed at the transistor level [13-14, 17-18].

The electrical and post-layout simulations were performed using Mentor Graphics® ELDO Spice. Obtained results were processed through the MATLAB® script.

The estimation of the energy consumption is based on the computation of the integral of the power consumed over time (energy) according to (1) [5, 19].

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

One cycle (T) is defined as a time needed for the execution of three operational phases: Precharge, Evaluation and Discharge. The energy consumption is observed during this

cycle when the input signals of standard MUX2x1 change. Each input signal combination results with one power profile (waveform). Based on the obtained power profile, the energy - *Ei*, is calculated. Here, index i =1, 2,..., N is the i-th input combination, while N represents the number of input combinations. Therefore, *E*i represents one element in the statistical assembly.

Fig. 13 shows trends of the energy consumption for the unprotected standard cell and all four presented architectures. The input signal combinations are given in horizontal axis labels, A and B, where the symbols "↑" and "↓" denote the rise and fall transition, respectively. The ordinate label shows energy levels for the standard MUX2x1 cell and for all other architectures.

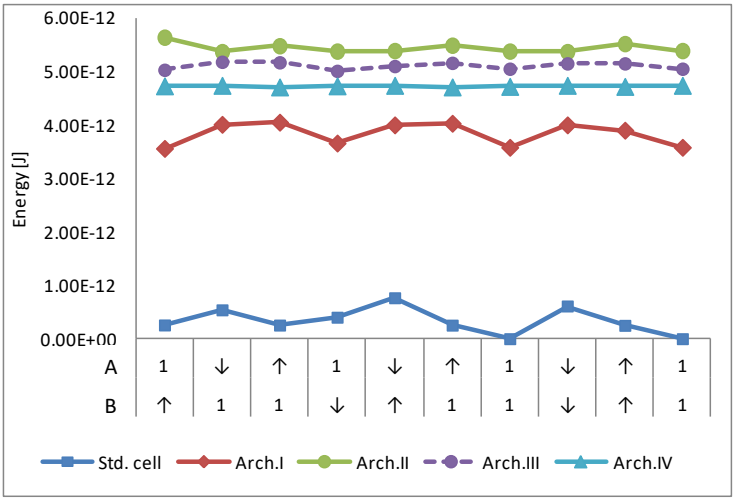

Fig. 13 Energy consumption during ten cycles of input signals change for the unprotected standard cell and for all four presented architectures.

The Maximal and minimal values for the energy and the standard deviation are denoted with *Emax*, *Emin* and σ respectively. *NSD* is expressed as a perceptual ratio of the standard deviation and the mean energy value, according to (2). Table 3 gives these values for the unprotected standard cell and for all four presented architectures.

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

For the standard logic cell, the *NSD* reaches 71%. It practically indicates the strong correlation between energy and input signal transitions. However, the NSDDL cell has the NSD value of nearly 5% for Architecture I, 1.69% for Architecture II, 1.2% for Architecture III and excellent 0.27% for Architecture IV. It should be emphasized that the published results for one-bit full adder; designed using the TPDyCML method [13] in terms of *NSD* achieved 0.35%. Obviously, Architecture IV exhibits very good resistance to SCA.

Table 3 Evaluation of results for the unprotected standard cell and for all four presented architectures

	Standard cell	Architecture			
		I	II	III	IV
Emax[J]	7.66E-13	4.05E-12	5.64E-12	5.18E-12	4.74E-12
Emin[J]	-3.66E-16	3.56E-12	5.37 E-12	5.01E-12	4.71E-12
Eavg[J]	3.33E-13	3.84E-12	5.46E-12	5.11E-12	4.73E-12
σ [J]	2.37E-13	2.03E-13	9.23E-14	6.13E-14	1.26E-14
NSD[%]	71.00	5.29	1.69	1.2	0.27

Further, in comparison with the results achieved for the combinational logic cells, given in [20 - 21], where the NSD values are close to 1%, the Architecture IV represents a significantly improved solution in hardware SCA protection.

5 Conclusion

In this paper we have presented improvement in designing the architectures of the encrypted multiplexer cell. Four different architectures have been compared with the unprotected Mux2x1 cell, and also with each other.

The advantages of the first architecture are: simplicity and the smallest area. The second architecture increased circuit complexity by introducing one Dnor cell for the controlling signal. This improved the SCA resistance by a factor of 3.13, while decreasing NSD to 1.69%.

In the third architecture two Dnor cells are introduced for controlling of *SEL* signals, which contributed to better symmetry of the circuit. In this way the NSD is reduced to 1.2. The improvement in SCA immunity is about 1.4 times with regard to the previous (Architecture II) NSD value.

In the fourth architecture the modification within the standard MUX2x1 cell has been applied (that is a part of NSDDL MUX2x1). It has diminished the complexity for exactly one inverter. This innovation has decreased the previous design in size and gave 4.4 times better SCA immunity, as well. The NSD here was only 0.27%. Finally, in comparison to the unprotected multiplexer cell the total improvement is about 263 times.

The Architecture III offers better SCA resistance with the area similar to the Architecture II (1.1 times larger area). Architectures II and IV have occupied almost the same areas but the NSD of Architecture IV is about 6.26 times smaller.

The benefit is not only in the increased resistance to SCA but also in the total power consumption. Depending on the required security level and areas, one can use less expensive solutions, as Architecture I, II or III have demonstrated.

Acknowledgement: *This research was funded by The Ministry of Education, Science and Technological Development of Republic of Serbia under the Grant TR32004.*

REFERENCES

[1] V. Borović, S. Borović, V. Drąsutė, D. Rančić, “Secure organ transplant information system”, Facta Universitatis, Series: Automatic Control and Robotics, vol. 17, no. 1, pp. 1-12, 2018.

[2] E. Dubrova, “Energy-Efficient cryptographic primitives”, Facta Universitatis, Series: Electronics and Energetics, vol. 31, no. 2, pp. 157-167, 2018.

[3] S. Hong, Special Issue on “Side Channel Attacks”, Applied Sciences, vol. 9, no. 9, pp. 1-6, 2019. doi.org/10.3390/app9091881

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

[5] C. Monteiro, Y. Takahashi, T. Sekine, “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

[6] P. Kocher, J. Jaffe, B. Jun, “Differential power analysis”, Advances in Cryptology (CRYPTO'99), California, USA, pp. 388-406, 1999.

[7] K. Tiri, I. Verbauwhede, “A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation", *Design, Automation and Test in Europe Conference* (DATE 2004), pp. 246-251, 2004.

[8] J. Quan, G. Bai, “A new method to reduce the side-channel leakage caused by unbalanced capacitances of diferential interconnections in dual rail logic styles”, Sixth International Conference on Information Technology: New Generations, pp. 58-63, 2009.

[9] H. Marzouqi, M. Al-Qutayri and K. Salah, Review of gate-level differential power analysis and fault analysis countermeasures, in IET Information Security, vol. 8, no. 1, pp. 51-66, 2014. doi: 10.1049/ietifs.2012.0319

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

[11] M. Stanojlovic, P. Petkovic, “Hardware based strategies against side-channel-attack implemented in WDDL” Electronics, vol. 14, no. 1, pp. 117-122, 2010.

[12] E. Amouri, H. Mehrez, Z. Marrakchi, “Impact of Dual Placement and Routing on WDDL Netlist Security in FPGA”, International Journal of Reconfigurable Computing, vol. 2013, ID. 802436, pp. 24, 2013. http://dx.doi.org/10.1155/2013/802436

[13] H. Kim,, V. Rozic, I. Verbauwhede, “Three Phase Dynamic Current Mode Logic A More Secure DyCML” to Achieve a More Balanced Power Consumption’, *13th International Workshop*, WISA 2012, Jeju Island, Korea, pp. 68-81, 2012.

[14] M. Bucci, L. Giancane, R. Luzzi, A. Trifiletti, “Three-Phase Dual-Rail Pre-charge Logic”. In: L. Goubin and M. Matsui, Cryptographic Hardware and Embedded Systems - CHES 2006 (Springer, Berlin, Heidelberg 2006), pp. 232-241, 2006. doi.org/10.1007/11894063_19

[15] Mentor Graphics, ASIC Design Kit, 2007.

[16] X. Linfu, E. F. Young, H. Xiaoyong, K. P. Pun, “Practical placement and routing techniques for analog circuit designs”, *in Proceedings of the International Conference on Computer-Aided Design*, San Jose, California, pp. 675-679, 2010.

[17] T. Wenyi, J. Song and W. Yuan, “Dual-Voltage Single-Rail Dynamic DPA-Resistant Logic Based on Charge Sharing Mechanism”, Chinese Journal of Electronics, vol. 26, no. 6, pp. 899-904. 2017.

[18] F. Mace, F.-X. Standaert, I. Hassoune, J.-D. Legat, J.-J. Quisquater, “A dynamic current mode logic to counteract power analysis attacks”, *in Proceedings of DCIS*, pp.186-191, 2004.

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

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

[21] M**.** Stanojlović Mirković, V. Litovski, P. Petković, D. Milovanović, “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, 2014.