11th International Conference on Electrical, Electronics and Computer Engineering (IcETRAN), Nis, 3-6 June 2024

Design and Simulations of cryptography block using the custom Library of Cells Resistant to Side Channel Attacks

1st Milena Stanojlović Mirković
Department of Electronics
University of Niš,
Faculty of Electronic Engineering
Niš, Serbia
milena.stanojlovic.mirkovic@elfak.ni.ac.rs & ORCID 0000-0002-0935-6922

2nd Miljana Milić
Department of Electronics
University of Niš,
Faculty of Electronic Engineering
Niš, Serbia
miljana.milic@elfak.ni.ac.rs & ORCID 0000-0001-7037-7709

3rd Dejan Mirković
Department of Electronics
University of Niš,
Faculty of Electronic Engineering
Niš, Serbia
dejan.mirkovic@elfak.ni.ac.rs & ORCID 0000-0001-5877-1404

***Abstract*— This paper describes the construction of a complex cryptographic block using a No Short-circuit current Dynamic Differential Logic (NSDDL) methodology. The simulation results show the validity of cryptographic shift register design which is developed using NSDDL D flip flop cells. All cryptography cells are designed in CMOS TSMC035 technology using Mentor Graphics tools.**

Keywords—Cryptography, NSDDL Method, SCA, CMOS, IC design.

I. Introduction

In digital systems encrypted data are provided through the implementation of specific algorithms, designed to prevent and impede decryption attempts. This protection primarily relies on the utilization of complex keys, which requires a large number of combinations in order to break. The protection is better, if it takes more time for trying of each combination of bits. Potential circuit vulnerabilities may arise from considering other characteristics of the circuit, leading to a reduction in decryption time. The information such as the power supply current-time profile, are used for this purpose. Any unauthorized collecting of information about the behavior of a cryptographic system is named as a Side Channel Attack (SCA) [1-2].

The primary source of information about circuit behavior resides in monitoring the circuit activity, typically manifested by variations in the supply current (I_{DD}). Analyzing of variations in I_{DD} and linking them to specific input vectors holds significant potential for deciphering cryptographic keys. 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 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. 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 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 behavior is suppressed. For the design of encrypted cells, 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; section III presents the design methodology and applications of NSDDL D flip flop encrypted cell. The sub-section B shows a cryptographic shift register design by applying the mentioned NSDDL D flip flop cells. Section IV gives and compares simulation results for standard D flip flop cell, encrypted NSDDL D flip flop cell and encrypted two-bit shift register. The final section summarizes key contributions of this research.

II. Cryptography NSDDL method

The NSDDL method works in 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.

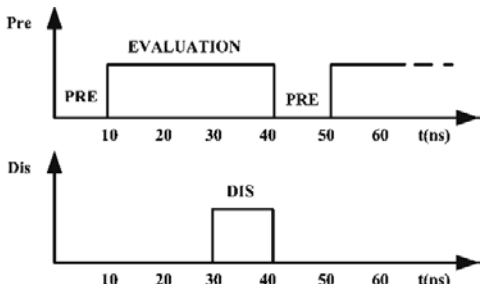

Fig. 1. Waveforms of control signals for the Dnor cell

The advantage of this method compared to other popular solutions, like WDDL [4-6], 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. Table I describes the logic function of the Dnor cell while Fig. 2 illustrates this circuitry.

The encrypted cells' functioning exploits the idea that each combination of input signals results in the same power consumption [7]. 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. This

hardware is doubled, but the effect of hiding the true function of the cell is achieved.

TABLE I. LOGICAL FUNCTION OF THE DNOR

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

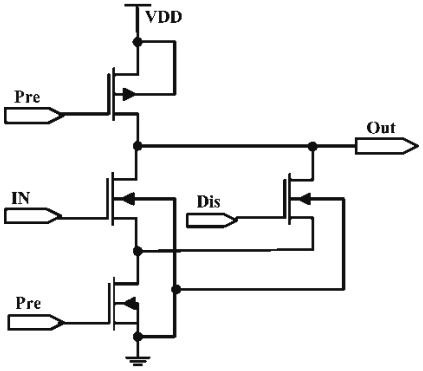

Fig. 2. Dnor cell

III. DESIGN AND APPLICATION OF NSDDL CELLS

The goal here is to create an encrypted cell that gives high degree of protection against the SCA. The essential requirement is that the logic function of the circuit remains the same as for the unprotected cell [8].

A. Designing of NSDDL D flip flop

This sub-section presents custom designed NSDDL D flip flop cell which provides remarkably good SCA resistance. This is achieved by hiding the correlation between power supply current and logic states of the circuit. For this purpose the NSDDL method was implemented. Characteristics of the cell are compared with standard, not encrypted, DFF cell under various operational conditions in order to prove SCA resistance. Designed encrypted cell will be the part of complex system providing overall system's data security.

Block scheme of NSDDL D flip flop SCA resistant cells are presented in Fig. 3. According to the fact that NSDDL D flip flop cell consists of two semi-partitions who have mutually complementary functions it is obvious that they can be realized using the same hardware. True and False blocks are emphasized with dashed Rectangles. The only difference between two the same semi-partitions is in the true and the false inputs and therefore also the outputs signals. Dnor circuit represents basic and important 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

The states of the output signals of sequential circuits in the evaluation phase in addition to the input signals also depend on the clock signal. It is very important to determine when will it appear in the relationship to Pre and Dis signals. Fig. 4 shows the mutual relationship of these signals according to the recommendation of the author of this method. The execution time represents the time necessary for the Precharge, Evaluation and Discharge phases to occur.

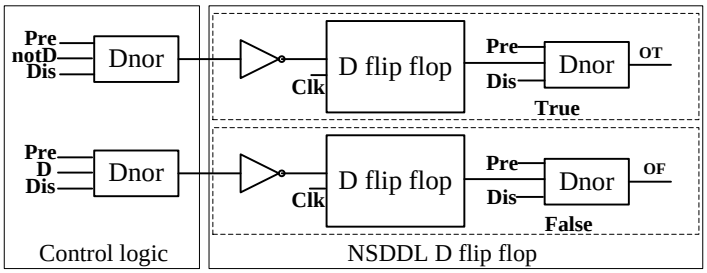

Fig. 3. Block diagram of NSDDL D Flip Flop cell

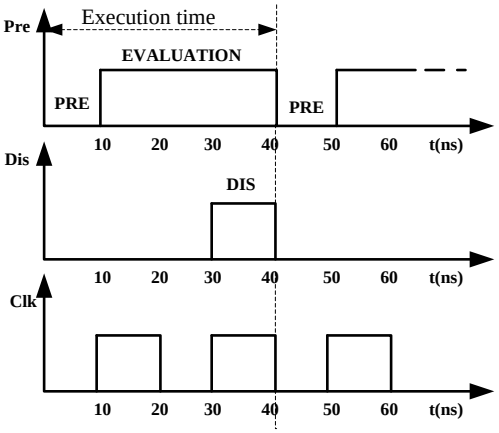

Fig. 4. Timing diagram of the clock signal in relation to the Pre and Dis signals

B. Cryptographic two-bit shift register

This section confirms the validity of cryptographic shift register design which is developed using NSDDL D flip flop cells from custom Library of Cells Resistant to SCA. It is known that shift register are implemented using a cascade connection between flip flops, where the output signal of one represents the input of the next flip flop [9]. The same idea applies to the encrypted shift register using encrypted D flip flops.

Block diagram of cryptographic two-bit shift register are presented in Fig. 5. It can be seen that this block consists of two NSDDL D flip flop cells with the same semi-partitions. Fig.6 confirms the shift register function by tracing the waveforms of the True sub-circuit. Bearing in mind the fact that the true and false sub-circuits are of symmetrical structure with complementary signals at the input, it is enough to consider the waveforms of one sub-circuit. The signal V(CryptoD) presents an encrypted signal of V(D). Following the input signal CryptoD, it can be seen its shifting by passing through the first and second NSDDL flip flops.

Signals V(OUT-D1) and V(OUT-D2) are outputs of first and second NSDDL flip flops, respectively. This shows that the logic function of the circuit is satisfied. The supply current I_{DD} the presented in Fig.6 $I(V_{DD})$ is the total current of the encrypted shift register circuit.

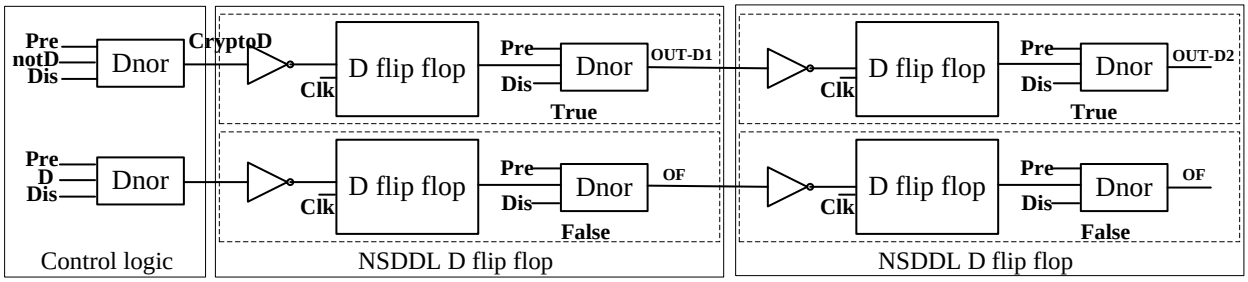

Fig. 5. Block diagram of NSDDL cryptographic two-bit shift register

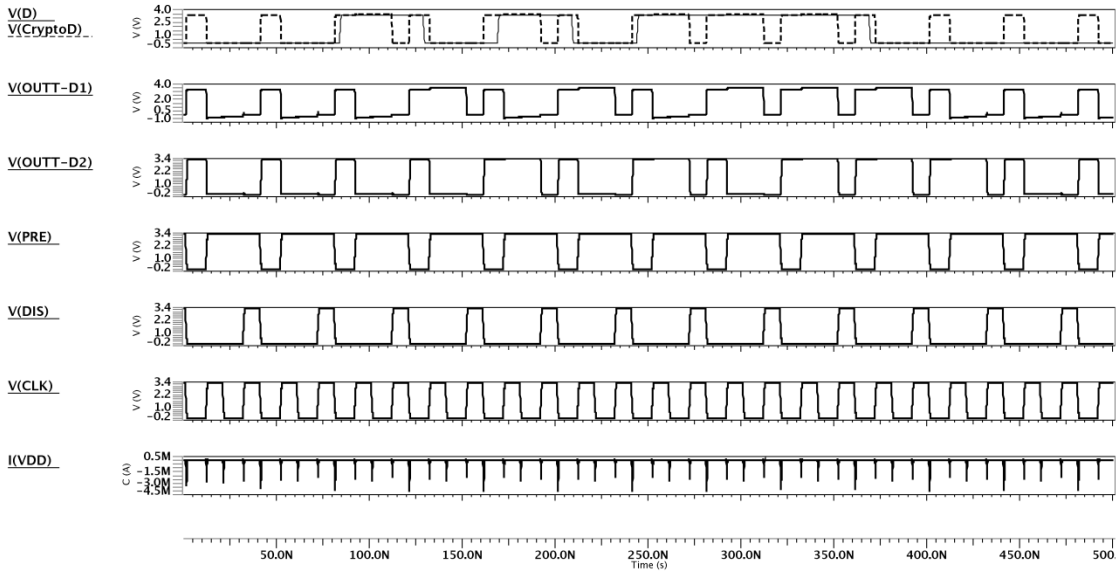

Fig. 6. Time waveforms of signals for NSDDL cryptographic two-bit shift register (true semi-partition)

.

IV. Simulations Results

The simulations results obtained for observed cells were performed using Mentor Graphics® ELDO Spice [10].

In order to estimate the SCA resistance we consider the energies needed for output state transition during different combinations of input signals. To quantify resistivity to SCA we have adopted a measure based on computed integral of consumed power in time (energy), as in [11-12]:

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

For NSDDL structures, this cycle (T) is defined as a time needed for the execution of three operational phases: Precharge, Evaluation and Discharge. In order to get better insight into behavior of every cell we derived the following parameters from the simulation results:

- Mean energy value E_{av}
- Standard deviation (σ)
- Normalized Standard Deviation in respect to E_{av} (*NSD*).

NSD is expressed as a perceptual ratio of the standard deviation and the mean energy value, as in [13]:

$$NSD = 100 \cdot \frac{\sigma}{Eav} \qquad (2)$$

Fig. 7 shows trends of the energy consumption for the unprotected standard cell, encrypted D flip flop cell and two-bit shift register. The input signal combinations are given in horizontal axis labels, denoted with D.

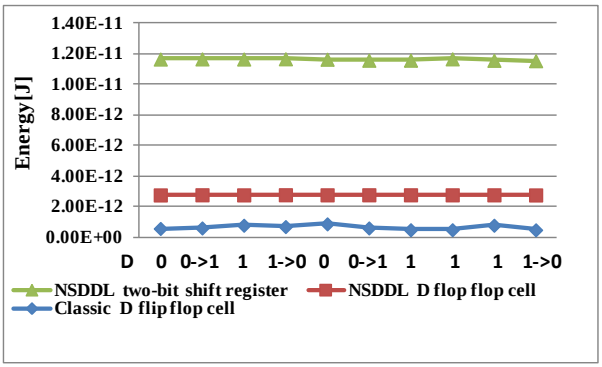

Fig. 7. Energy consumption during ten cycles of input signals change for the unprotected standard cell, encrypted D flip flop cell and two-bit shift register

As a reference we have used a standard D flip flop cell and compared the behavior of a 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 hide cell operation regarding I_{DD}. Therefore they should provide minimal correlation between stimulus signals and I_{DD}. Table II systematizes results of comparison.

TABLE II. CHARACTERISTICS COMPARISON OF CLASSIC AND NSDDL CELLS

	Classic D flip flop cell	**NSDDL D flop flop cell**	**NSDDL shift register**
E_{av} [J]	6.307e-13	2.768e-12	1.16E-11
σ [J]	1.326e-13	4.021e-15	4.602E-14
NSD[%]	21.031	0.145	0.395

As a measure of SCA resistance we consider normalized standard deviation. For standard logic cells this parameter reaches 21%. This obviously indicates strong correlation between energy (i.e. the current, because V_{DD} = const) and input signal transition. Further, in comparison with the results achieved for the combinational logic cells, given in [14], where the NSD values are close to 1%, the results for sequential circuits represents a significantly improved solution in hardware SCA protection. This is sufficient to conclude that NSDDL D flip flop cell gives an excellent resistivity to SCA using DPA countermeasures because the *NSD* value is 0.145%. For the encrypted shift register this parameter reaches 0.395%. It exhibits very good resistance to SCA, as well. It's clear that the *NSD* parameter gradually increases with the complexity of circuits.

V. CONCLUSION

In this paper we have presented standard encrypted cell in designing the bigger encrypted block, exactly the two-bit shift register. This block confirmed the functionality of the NSDDL method in realization of complex sequential circuits. The *NSD* parameter proves that NSDDL cells transfer their resistivity to SCA into the complex circuit where they are build-in.

Two encrypted structures have been compared with the unprotected cell, and also with each other. Results of NSDDL D flip flop are obtained from post-layout simulation, while results for standard D flip flop and encrypted shift register used from the schematic simulations. 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

In future work, we will try improving or repeating the value of NSD parameter for the shift register using post layout simulation results. Symmetry in layout design contributes more to the increased resistivity of the SCA than in obtained results from schematic simulations.

ACKNOWLEDGMENT

This work has been supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia.

REFERENCES

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

[2] K. C. Kaya (Ed.) Cryptographic Engineering, Springer, 2009

[3] Quan J. and 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 Genera*tions, 2009, pp. 58-63

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

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

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

[7] J.-L. Danger, S. Guilley, S. Bhasin, M. Nassar, "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

[8] M. Stanojlović Mirković, M. Milić, and D. Mirković, "Evaluatio of resistance to SCA for different architectures of encrypted cell", Facta Universitatis, Series: Automatic Control and Robotics, 18(3), pp.141-152. doi.org/10.22190/FUACR1903141S

[9] T. Ndjountche (2016). Shift Register. In Digital Electronics 2, T. Ndjountche (Ed.). doi.org/10.1002/9781119329756.ch3

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

[11] 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.

[12] C. Monteiro, Y. Takahashi, T. Sekine, "Chargesharing 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

[13] M. Stanojlović Mirković, M. Milić, D. Mirković and V. Litovski, "Hardware Reduction and Statistical Verification of Cryptographic Standard Cell Resistant to SCA", Journal of Circuits, Systems and Computers, 2019, doi.org/10.1142/S0218126620501315

[14] M. Stanojlovic and P. Petkovic, "Resistance of XOR/XNOR NSDDL cell to side channel attack", Proc. Small System Simulation Symp. (Nis, Serbia, 2012), pp. 141–144