Simulation of defects in sequential NSDDL Master/Slave D flip flop circuit

Milena Stanojlović and Vančo Litovski

Abstract - Testing of the NSDDL Master/Slave D flip flop (MSDFF) that represents a sequential cell, being part of NSDDL (No Short-circuit current Dynamic Differential Logic) side-channel-attack-resistant library, will be presented in this paper. Fault dictionary will be created based on repetitive simulation preformed on the circuit level description of the flip-flop with faults inserted one by one. Only open-circuit and short-circuit will be considered.

Keywords – Testing, sequential logic, encryption, open circuits, short circuits.

I. INTRODUCTION

The misuse of data is increasingly common. It became necessary to develop new methods, both in software and in hardware, in order to protect data. The domain of this paper is the use of cryptographic methods in ASIC hardware, based on applying standard cell design. The cryptographic algorithm in hardware protects the information leaks out of the device trough so called "side channel". Attacks are based on analyses of the leaked data are known as side channel attacks (SCA) [1]. Important information, such as secret keys, can be obtained by observing the power consumption, the electromagnetic radiation, the timing information etc.

After a long study of different cryptographic methods in hardware, for data protection, we chose one that meets the set criteria. This is the so-called NSDDL logic [2] (*No Short-circuit current Dynamic Differential Logic*). The method is based on a modification TDPL (Three-Phase Dual-Rail Pre-Charge Logic) approach [3] which introduces a third phase of work, during which all the capacitors in the circuit are empty. An important novelty in NSDDL method is immunity on unbalanced load true and false output. In addition, the method requires only one a new cell that is combined with standard logic cells.

Further in this paper, special attention will be devoted to testing NSDDL Master/Slave D flip flop circuit. For intentional introduction of defects, shorts and opens, in fault free circuit, output signal and supply current for each defect for certain combinations of input signals will be monitored. A number of simulations will depend on number of defects which are tested. The authors decided for this way of testing because of establishing the test sequence. Therefore with given sequence success of the test is determined. As Coverage of defects with given sequence is better, testing is more successful. With this, it can be shown that one test cover more defects which significantly speeds up process of testing. Besides examining logic function of the circuit, it is also very important to compare supply currents of faulty and fault free circuits. When defect is present in the circuit, it is very possible that it will be mapped in to change of mentioned supply current [4].

Milena Stanojlović is with The Innovation Center, School of Electrical Engineering, University of Belgrade, Bul. Kralja Aleksandra 73, 11120 Belgrade, Serbia, E-mail: milena@venus.elfak.ni.ac.rs

Vančo Litovski is with the Faculty of Electronic Engineering, University of Niš, Aleksandra Medvedeva 14, 18000 Niš, Serbia., E-mail: vanco@elfak.ni.ac.rs.

II. CELL TESTING

A. NSDDL Master/Slave D flip flop circuit

Block schemes of NSDDL Master/Slave D flip flop (MS DFF) cell is presented on figures 1. This structure is composed of two identical standard MS DFFs, invertors and Dnor circuits. Each of MS DFFs inputs are connected to appropriate output of Dnor circuit in crisscross manner. Outputs of MS DFFs are connected to the Dnor circuit as well, but this time over inverting logic gate.

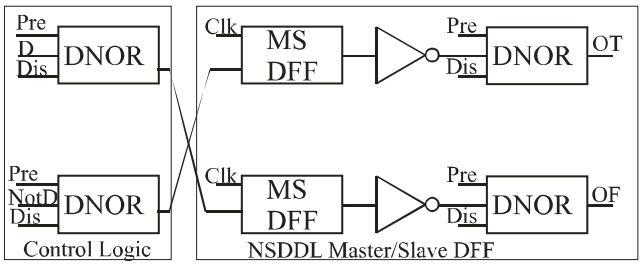

Fig. 1. Block scheme of SCA resistant NSDDL MS DFF cell

B. Testing of Master/Slave D flip flop circuit

Since a number of transistors in MSDFF is big, so marking defects for each transistor on MSDFF schematic is irrational. In order to perform simulations a number of defects which are to be simulated have to be determined. After that defect is inserted in the circuit and appropriate observing point is adopted. This point should provide visibility of the defect's effect [5, 6]. Since circuit contains eighty-eight transistors, five hundred and eight defects of mentioned type can occur. As can be seen from Figure 1

symmetric circuit structure in respect for true and false output is considered. This enables to half the total number of defects. Taking the previous in to account there are still forty four transistors to examine. Therefore the simulation of defects for each transistor for its self is a very tedious but unavoidable work. For all allowable combinations of input signals two hundred and sixty four simulations for faulty and one for fault free circuit are performed. For each transistor six defects are examined where each defect is introduced one after another. Transistors are denoted with *Pi_KSxy/Prex*, or *Nj_KSxy/Prex*, where P and N represent type of the transistor. Counters marked as *i*=0,1...,20, and *j*=0,1...,22 represents index of pMOS and nMOS transistor, respectively. With *KSxy* short circuit is denoted while xy determines between transistor connections these shorts occurs. Therefore xy can take values from set {GD, GS, DS} where GD stands for gate-drain, GS for gate-source and DS drain-source. Similar is valid for Prex as well. In this case Prex represent open circuit of connection denoted with x. Here x is from set {G, D, S} where G, D and S represents gate, drain and source transistor terminals, respectively.

The goal is to perform exhaustive test regardless this kind of test is very demanding and tedious.

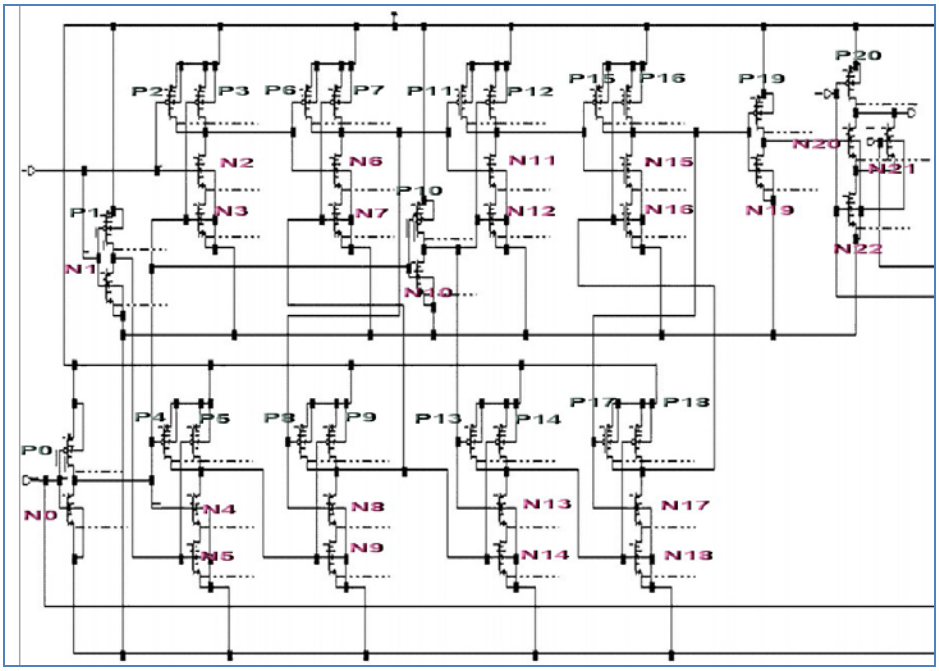

Fig. 2 NSDDL MSDFF, half circuit schematic with denoted transistors

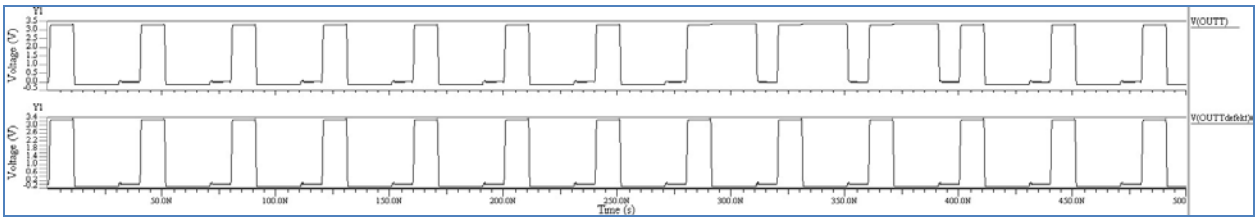

Fig. 3 Time waveforms of output voltage fault free and faulty circuit with defect P4_PreS

This is primarily reflected on time needed for simulations, processing and systematization of obtained results which makes this kind of testing very time consuming.

On Figure 1 block scheme of NSDDL MSDFF is shown which consist of is eighty eight transistors. Respecting symmetry, only half of the circuit is observed so figure 2 illustrates half regarding true output.

Erect of every defect is firstly observed with a respect to a logic function of the circuit. When logic function is violated in can be considered that defect is detected. An important number of defects in the circuit were detected in this way. From two hundred and sixty four defects, two hundred and thirty two defects were detected by only observing output signal. Figure 3 illustrates one such case for inserted defect of open circuit at source of pMOS trans-

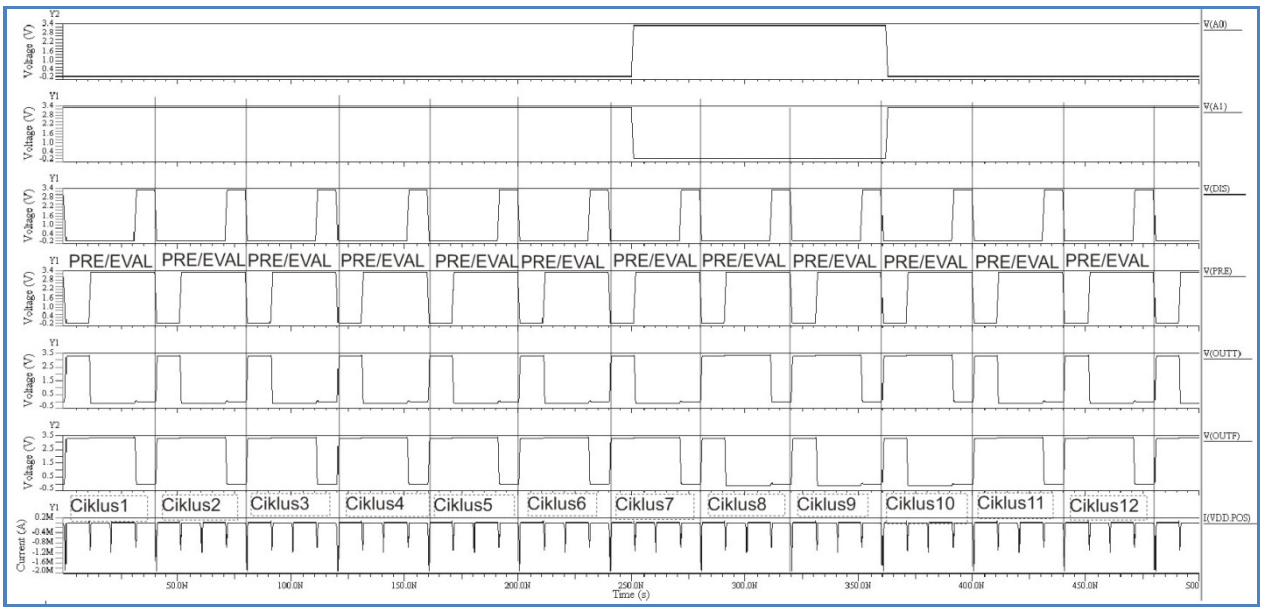

Fig. 4. Time waveforms of inputs, outputs and *idd* of fault free NSDDL MSDFF circuit

istor with index four (*P4_PreS*).

First waveform represents response of fault free circuit, while second represents response for faulty one. It can be clearly seen that these two responses are different which automatically implies defect detectability. Response of the circuit can be different depending on the type of a defect that is inserted in to it. Hence, at the output of the circuit distorted or fixed value (logic zero or one) signal can occur which is enough for detecting the presence of the defect since logic function is violated.

It can be noted that with this kind of testing good results are archived because large number of defects are detected in a quite easy way. For defects that do not violate logic function, additional analysis of *idd* is required. Namely, autocorrelation function of *idd* for fault free and correlation function between *idd*s for fault free and faulty circuit are compared.

Autocorrelation function of *idd* for fault free circuit is defined with (1) while correlation function between *idd*s for fault free and faulty circuits is defined with (2).

$$R_{iddidd}(\tau) = \frac{1}{T}\int_0^T i_{dd}(t)\cdot i_{dd}(\tau + t)\cdot dt \qquad (1)$$

$$R_{iddi^L dd}(\tau) = \frac{1}{T}\int_0^T i_{dd}(t)\cdot i_{dd}^L(\tau + t)\cdot dt \qquad (2)$$

Practically, root mean square (RMS) values of these functions are compared in order to detect defect. Table I gives results for thirty two defects which were not detectable with logic simulations.

For this reason it was necessary to introduce a new method for defect detection. According to results given in the third column of Table I, where relation between $R^{L}_{idd\ idd}{}^{L}$ and $R_{idd\ idd}$ is expressed in percentages, influence of the defects on *idd* can be seen. It can also be concluded that this approach provide detection of nine of thirty two undetected defects (colored rows in Table I). Remaining twenty there defects stay unrevealed.

Observing results given in Table I one can see that deviation of RMS value of correlation function from RMS value of autocorrelation function is mostly very small (few percent). Therefore it is not safe to adopt vary low threshold for defect detection. Since first significant deviation occurred for *N_11KS_DS* defect (≈ 22%), it was meaningful to adopt 20% deviation for threshold of defect detection in this case.

Besides previously discussed method for defect detection, time integral of the *idd* can be used in this purpose as well.

Since operation of the circuit is very specific, time integral of *idd* is calculated during PRE and EVALUATION phases separately for all combinations of input signals. Therefore, time integral of *idd* for fault free and faulty circuits are compared under same input conditions. Time interval occupied with PRE and EVALUATION phases represents one cycle. Practically, no this interval time integration of *idd* is performed. On figure 4 these intervals are marked as cycles.

Every deviation in value of the integral for each cycle is expressed in percentage and given in Table II. Value of this integral for faulty circuit is compared with fault free one in every cycle. With this method eleven of remaining twenty three defects are detected.

TABLE I
DETECTION OF DEFECTS BASED ON CORRELATIONS OF CURRENTS FAULT FREE AND FAULTY CIRCUITS

Type of defect on the transistor	**RMS_R*iddidd* $[A^2]$**	**$(RMS_{ispravno}-RMS_{Loše})/RMS_{ispravno}*100$**
Ispravno kolo	8.45E-6	
P_0KS_GS	8.06E-2	953586.10%
P_2PrekD	8.59E-6	1.59%
P_2PrekS	8.62E-6	2.03%
P_3prekD	8.27E-6	-2.13%
P_3prekS	8.26E-6	-2.28%
P_5PrekD	8.87E-6	4.91%
P_5PrekS	8.96E-6	6.05%
P_7PrekD	8.51E-6	0.72%
P_7PrekS	8.55E-6	1.10%
P_8PrekD	8.44E-6	-0.16%
P_8PrekS	8.47E-6	0.28%
P_11PrekD	8.63E-6	2.12%
P_11PrekS	8.51E-6	0.68%
P_11PrekG	1.19E-5	41.11%
P_12PrekD	8.23E-6	-2.65%
P_12PrekS	8.16E-6	-3.47%
P_13PrekD	8.29E-6	-1.86%
P_13PrekS	8.33E-6	-1.42%
P_14PrekD	8.41E-6	-0.52%
P_14PrekS	8.51E-6	0.66%
P_14PrekG	1.05E-5	24.36%
P_16PrekD	8.44E-6	-0.10%
P_16PrekS	8.50E-6	0.58%
P_17PrekD	8.40E-6	-0.60%
P_17PrekS	8.46E-6	0.06%
P_20KS_GS	4.32E-2	510526.44%
N_2KS_DS	1.19E-5	40.27%
N_3KS_GD	1.48E-5	75.17%
N_3KS_DS	8.67E-6	2.56%
N_11KS_DS	1.03E-5	21.97%
N_13KS_DS	1.09E-5	29.23%
N_14KS_DS	1.26E-5	48.91%

Therefore, number of undetected defects is reduced to only twelve. Comparing this number with total number of defects (two hundred and sixty four) one can conclude that defect coverage is quite good using these test methods.

Remaining twelve defects do not significant influence on *idd* so they can hardly be detected this way. These defects are: *P7_PrekD, P7_PrekS, P8_PrekD, P8_PrekS, P13_PrekS, P14_PrekS, P14_PrekD, P16_PrekS, P16_PrekD, P17_PrekS and P17_PrekD.*

It can be concluded that combination of three test methods, i.e. logic function violation, comparison of autocorrelation and correlation functions and comparison of time integral of *idd* for fault free and faulty circuits gives solid defect coverage.

This means that for safe testing a different methods and techniques should be combined.

From two hundred and sixty four defects two hundred and fifty two were detected. Since this is result for only a half of circuit, total defect coverage is five hundred and four from five hundred and twenty eight which is nearly 96%. It can be said that the testing was successful.

TABLE II
COVERED DEFECTS

	N2_ KSDS	**P10_ PrekD**	**P11_ PrekS**	**P11_ PrekD**	**P12_ PrekS**	**P1_ PrekS**	**P1_ PrekD**	**P2_ PrekS**	**P2_ PrekD**	**P4_ PrekS**	**P4_ PrekD**
1	6.94%	18.38%	-8.40%	5.71%	-67.49%	-5.81%	30.16%	6.30%	-0.10%	84.54%	81.70%
2	0.77%	18.35%	0.17%	-0.22%	31.21%	0.83%	24.14%	0.18%	-0.07%	81.20%	64.43%
3	0.87%	18.34%	0.16%	-0.45%	130.6%	0.82%	24.09%	0.13%	-0.09%	81.27%	64.40%
4	0.88%	18.34%	0.16%	-0.15%	230.1%	0.82%	24.10%	0.24%	-0.08%	81.73%	64.41%
5	0.88%	18.34%	0.16%	-0.37%	329.5%	0.82%	24.10%	0.09%	-0.08%	81.87%	64.41%
6	0.88%	18.34%	0.16%	-0.37%	429.0%	0.82%	24.10%	0.17%	-0.08%	80.77%	64.41%
7	239.60 %	0.13%	-3.51%	-3.07%	528.0%	6.49%	-1.80%	-4.86%	-4.91%	91.98%	76.74%
8	240.06 %	-0.15%	-5.45%	-4.55%	629.1%	6.12%	-1.48%	-4.87%	-4.82%	11.82%	0.65%
9	239.70 %	-0.22%	-5.52%	-4.65%	728.2%	6.23%	-1.59%	-4.98%	-4.89%	11.83%	0.38%
10	1.27%	18.51%	-1.75%	-1.83%	829.1%	0.90%	24.45%	0.13%	0.11%	11.11%	-0.46%
11	0.79%	18.35%	0.17%	-0.10%	928.0%	0.83%	23.97%	0.13%	-0.07%	80.79%	64.55%
12	0.87%	18.33%	0.15%	-0.22%	1027.%	0.82%	24.13%	0.17%	-0.09%	81.71%	64.40%

III. CONCLUSION

This paper presents some of the techniques for testing applied on encrypted NSDDL MSDFF cell. First basic operation of unit under test was explained. Two proper methods for testing this sequential logic are adopted, namely logic function violation and testing based on power supply current. From last method two techniques are chosen to be applied on the circuit, i.e. comparison of autocorrelation and correlation functions and comparison of time integral of *idd* for fault free and faulty circuits. These techniques were briefly commented and explained. A number of simulations were performed in order to make appropriate fault dictionary for defects of short/open circuit type. Obtained results are presented and commented as well.

ACKNOWLEDGEMENT

This research was partially funded by The Ministry of Education and Science of Republic of Serbia under contract No. TR32004

REFERENCES

[1] Petković, P. M., Stanojlović, M., and Litovski, V. B. “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.

[2] Quan J., and Bai, G., "A new method to reduce the sidechannel leakage caused by unbalanced capacitances of differential interconnections in dual-rail logic styles", 2009 Sixth International Conference on Information Technology: New Generations, DOI 10.1109/ITNG.2009.185, pp. 58-63

[3] Bucci, M., Giancane, L., Luzzi, R., and 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)

[4] Litovski, V., “Projektovanje elektronskih kola”, ISBN 86-7369-015-3, DGIP Nova Jugoslavija, Vranje, 2000.

[5] Litovski, V., Osnovi testiranja elektronskih kola, ISBN 978-86-85195- 71-6, Elektronski fakultet, Niš, 2009.

[6] Milovanović, D., and Litovski, V., “Fault Models of CMOS Circuits”, Microelectronics and Reliability, 1994, Vol.34, No. 5, pp. 883-896.