Testing and fault tolerance of secured circuits

G. Ait Abdelmalek, R. Ziani, and M. Laghrouche

***Abstract*—** In this paper we studied the secured circuit's testing and fault tolerance under resistive open defects. However, this work focused on the analysis of the impact of resistive-open defects on the electrical behavior of two categories of secured circuits implemented in Wave Dynamic Differential Logic (WDDL) and in Quasi Delay Insensitive (QDI). The quality of this analysis is verified by SPICE simulations. It is shown that the detection of defect depends on the open resistance value. The some results are given for the defect detection and the fault tolerance conditions.

***Keywords*—** asynchronous circuits, C-element, fault models resistive open fault, Secured circuits.

I. Introduction

TESTING component and integrated systems is a fundamental step that must ensure their proper functioning. Many works have concerned the implementation of different methodologies for testing integrated circuits [1]-[9]. To test effectively the integrated circuits, it is imperative to define fault models in adequacy with the actual defects of current nanoscale CMOS and future technologies. The majority of the resistive open fault models [10]-[12] and the resistive bridging fault models [13]-16] are used to describe resistive shorts and resistive open fault between logical nodes. Modeling defects of the traditional CMOS technologies received a particular attention during the last year's including largely submicron technologies (until 45 nm). But very few works were carried out to model this type of defect for circuits using CMOS technology like secured circuits. In the secured circuits which require security and long communication links, it is important to consider the interconnect testing and their reliability. Indeed, they are a class of physical attacks in which the observation of the current consumption, the electromagnetic radiation, the timing information, allows obtaining important information, such as secret keys. Consequently, the security of cryptographic implementations relies not only on the algorithm quality but also on the countermeasures to thwart attacks aiming to disclosing the secrets. There are several types of protection and some will be discussed in this paper. We focus especially on WDDL and QDI countermeasures for the secure circuit design that was evaluated in terms of fault tolerance and reliability on two examples. More recently, we have demonstrated that the secure circuits can be tested with fault models similar to those used for standard CMOS circuits [16]. Fick et al. proposed fault-tolerant routing algorithms under the permanent faults for specific applications, such as NoCs [17]. Lehtonen et al. [18] implemented error detection and retransmission methods in asynchronous communication link for tackling intermittent and permanent faults. Lehtonen and Almukharizim have focused on the permanent interconnect fault in the asynchronous circuits [18], [19]. Verdel and Makris proposed a duplication method [20]. They compared the outputs of the duplicated circuits within a specified time window to detect transient and permanent faults. However, the authors found that the duplicated circuit cannot be operated correctly under the permanent faults. In [8], [9], we have evaluated the fault tolerance and reliability of TMR under stuck-at fault. We showed that if only one module is faulty, then the two others will be dominant. Therefore, the fault will be masked and the TMR produces the correct output, the TMR can be operated with the presence of a single permanent fault. But these approaches are limited to specific applications, such as standard CMOS integrated circuits. However, Almukharizim and Sinanoglu proposed Triple Modular Redundancy (TMR) method for asynchronous circuits [19]. They also showed that the TMR -based circuit can function under a single permanent fault.

This paper evaluates the robustness of the TMR -based AND WDDL and the TMR -based AND QDI gates by injecting open faults at the transistor level in the two of three gates which generate the same outputs. In order to detect the resistive open fault and therefore to know whether the TMR is fault tolerant or not, we analyzed the impact of the open defect on the electrical behavior of this type of structures. Since the voltage level at the output V_{out} in the resistive open-fault condition is above or lower than the threshold voltage, the gate in the input port can recognize the interconnect fault by comparing V_{out} with a threshold voltage whose amount determines whether the interconnect fault is an open fault or not. As a result, the fault detection can be realized based on the proposed output voltage monitoring.

The paper is organized as follows. The first step presents the TMR -based AND WDDL and the TMR -based AND QDI gates implementation, and shows when and how these latter are fault tolerant or not. The simulated results of the

G. Ait Abdelmalek is with the Department of Electronics, Mouloud Mammeri University, Tizi-ouzou, Algeria (corresponding author: +21326218642; e-mail: ghania_79@ yahoo.fr).

R. Ziani. is with the Department of Electronics, Mouloud Mammeri University, Tizi-Ouzou. Algeria. He is the head of the Department of Electronics (e-mail: ziani_r@yahoo.fr).

M. Laghrouche is with the Electronics Department, University of Mouloud Mammeri, Tizi-ouzou, Algeria. He is the vice dean of the Electrical Engineering and computer Institute (e-mail: larouche_67@yahoo.fr).

electrical analysis of these two TMR structures and thus the resistive open fault detection based on the proposed method are presented by the second step. And finally we will conclude our work.

II. COUNTERMEASURES AGAINST SCAS”SIDE-CHANNELS ATTACKS”

The countermeasures in hardware protect the information leaks out of the device through so called, "side-channel attacks" (SCA). They are a class of physical attacks in which the observation of the current consumption, the electromagnetic radiation, the timing information, allows obtaining important information, such as secret keys. Fault injections are another menacing attack type targeting specific interconnect lines in order to change their value. There are several types of protection [21]-[29], and some will be discussed in this paper. We focus especially on WDDL and QDI countermeasures for the secure circuit design that was evaluated in terms of fault tolerance and reliability on two examples.

III. TAILORED METHOD FOR TESTING AND FAULT TOLERANCE

The concept of fault tolerant technique is to allow the circuit to continue functioning even in the presence of faults. There are several fault tolerant structures [30], [31] which are classified according to the resources of redundancy which they use: material, information, time, software or hybrid. These structures have been designed to tolerate transient or temporary faults but they can also tolerate manufacturing defects. They all use the concept of redundancy of which the principle is to use material resources to correct the faults. In our work, we have chosen to use the Triple Modular Redundancy (TMR). The TMR is a well-known fault tolerant technique for avoiding errors in integrated circuits. As presented in Fig. 1, the TMR scheme uses three identical logic blocks performing the same task in tandem with corresponding outputs being compared through majority voters. The voter chooses the outputs of the fault-free modules that which masks the defectives modules.

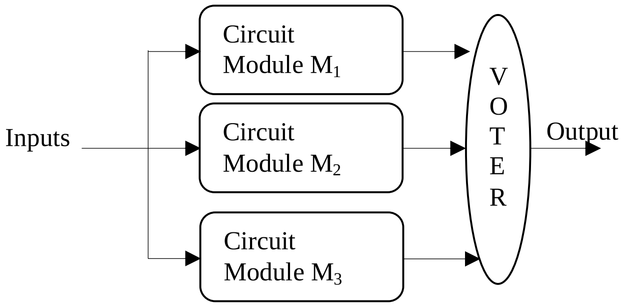
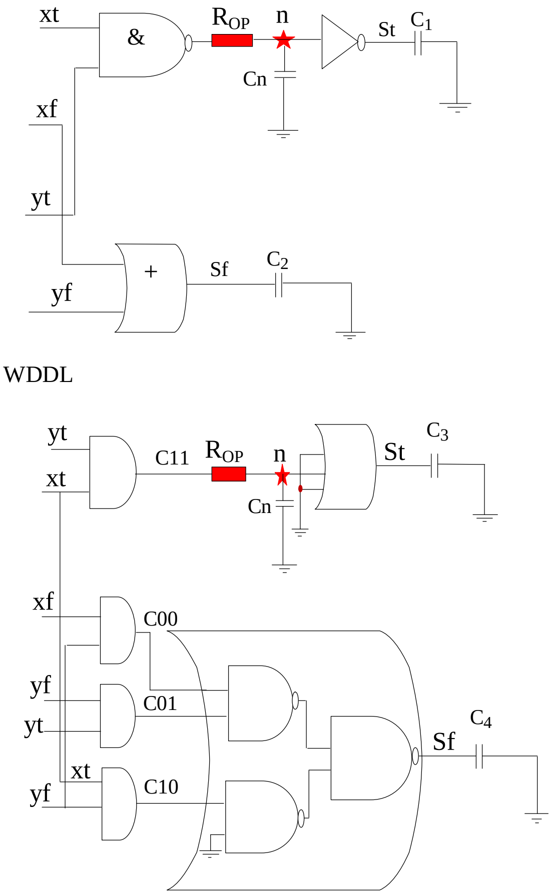


Fig. 1 TMR structure

The voter is a combinatorial structure whose number is equal to the number of the modules outputs [31]. As an example, if the modules have three outputs, i.e., $S_{1,1}$, $S_{1,2}$, $S_{1,3}$ are the first module outputs, $S_{2,1}$ $S_{2,2}$, $S_{2,3}$ the second module outputs and $S_{3,1}$, $S_{3,2}$, $S_{3,3}$ the third module outputs. $S_{x,\ 1}$outputs are voted together as well as the $S_{x,\ 2}$ and $S_{x,\ 3}$ outputs. The function performed by each voter is: $S_i = S_{1,\ i} .S_{2,\ i} + S_{1,\ i}. S_{3,i} + S_{2,\ i}. S_{3,\ i}$.

In this section, we develop a TMR fault tolerance method adapted to reliability test issues in WDDL and QDI gates. This method will enable high resistive open fault coverage for relatively low costs compared to others methods. It is clear that such a defect modify the dynamic behavior of the circuit, so it can be detected by a dynamic voltage test strategy (delay testing). The open circuit fault is shown in Figure 2 by injecting the resistance R_{OP}. The open resistance value R_{OP} is a variable parameter of the defect completely unpredictable [10].



a. AND WDDL

b. AND QDI

Fig. 2 Resistive open injection

To analyze the impact of the resistive open fault on the dynamic behavior of TMR -based AND WDDL and TMR - AND QDI, we follow the above procedure shown in Figure3. Firstly, we use the AND WDDL and the AND QDI gates, as illustrated by Fig. 2(a) and 2(b), and we transform them into TMR structure, i.e., TMR -based AND WDDL and TMR-based AND QDI for which we inject the open fault between the interconnect lines of the module 2 and 3 (Fig. 3), and finally we make several simulations based on SPICE and a 45 nm CMOS cell library with 1.1 V power supply and with different values of resistance to compare the resulting behavior against the fault-free module1 behavior and characterize its effects.

The fault tolerance principle is described in Section 4. The dynamic behavior and the results obtained on the collection of the fault tolerance range are described in Section 5.

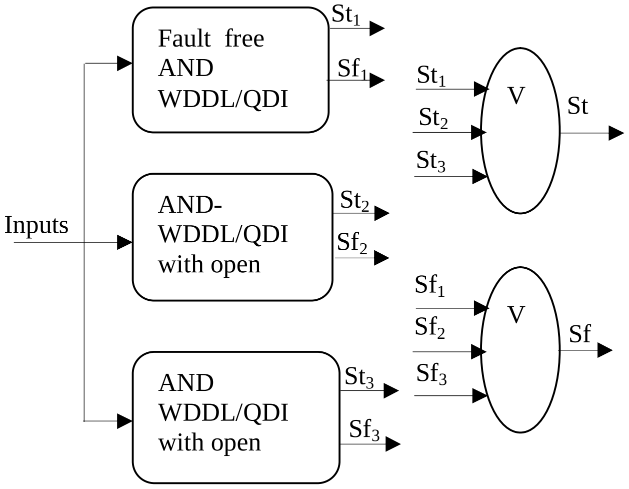


Fig. 3 Resistive open injection in TMR.

IV. FAULT TOLERANCE PRINCIPLE

When the defects are correlated they occur by an error at the same time, and cause the decrease of the circuit reliability. To known when and how these circuits are able to tolerate manufacturing defects, we must distinguish two cases [31]:

- The defects are present in the modules of the TMR "Redundant part";
- The defects are present in the voter "non-redundant part".

To study the tolerance to manufacturing defects affecting the modules in TMR, we distinguish several cases given by [31-32]: (i) One or more open defects affect only one module, (ii) two open defects affect two different modules and (iii) more than two open defects affecting several different modules.

Let us consider for our work that the voter is fault free and that both faults affect two different modules. If two defects (d_1, d_2) are present in two different modules, then they can be tolerated or not according to their effects, that is to say:

- They are tolerated if none test vector applied at the input cannot propagate two errors up to two common outputs of modules,
- They are not tolerated if two errors are propagated until two common outputs of modules.

V. FAULT DETECTION AND FAULT TOLERANCE RESULTS

Before the fault injection, it is necessary to characterize the dynamic response of the two fault-free TMR structures (without the injection of R_{OP} resistance). Figure 4 shows the transient response of these gates. The initial state is given by the test vector V_0 = [xt, yt, xf, yf] = [0011] and the final state by the test vector V_1 = [0100]. The input yt switches from 0 to VDD and the inputs xf and yf switch from VDD to 0, creating thus the transition. We note that the evolution of the general shapes, as presented in Fig. 4.a and 4.b are quite similar.

It is important to note that we have considered a cycle time of about Tcl = 0.1ns in TMR –based AND WDDL, and Tcl = 0.2ns in TMR –based AND QDI). Thus from this simulation we can define the following propagation times [33]:

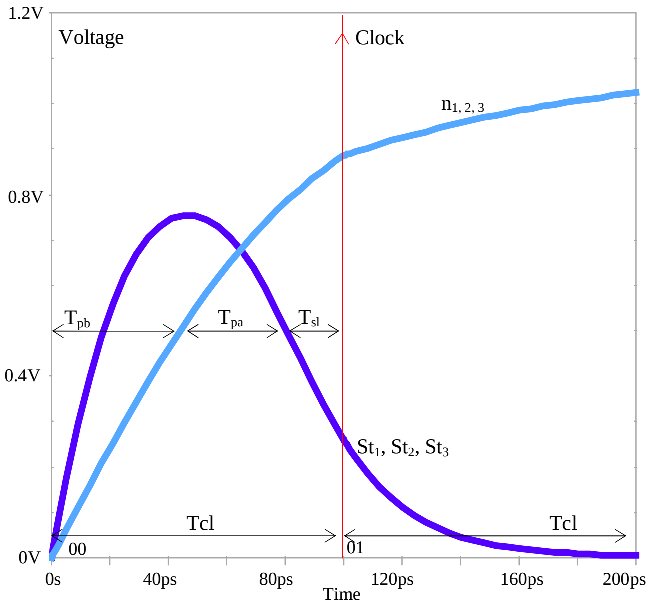
- T_{pb}, the propagation time before the defect,
- T_{pa}, the propagation time after the defect,
- T_{op}, the delay induced by default,
- T_{sl}, the slack time of path yt to St which depends on the three previous parameters and T_{cl}).

It is seen from Figure 4 that the rising edge of the input xt reached the defect at time T_{pb}= 46.7 ps for TMR –based AND WDDL and at time T_{pb} = 166.5 ps for TMR –based AND QDI. This time is equal to the sum of the different gate propagation delays (T_{di}) situated before node n.

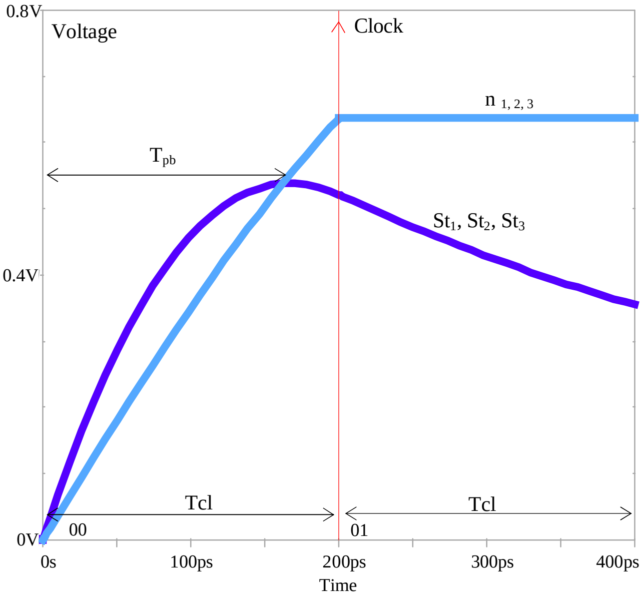
It is very important to note that each gate propagation delay depends on: the resistance R_n of the line n, the size of the transistors used (w_i^n, L_i^n, w_i^p, L_i^P) and the node capacitance C_n. For TMR –based AND WDDL, the defect spreads to the outputs $(St)_{1, 2, 3}$ of the gates in a period of time T_{pa} = 19.73ps, which depends on the existing gates propagation delays after the node n.

Then the outputs $(St)_{1, 2, 3}$ stay stable for a period of time T_{sl} = 33.721 ps before being safeguarded, assuming a certain shift register [34]. By cons, in TMR –based AND QD the slack time T_{sl} and is not defined and therefore it is the same for T_{pa}, because the outputs $(St)_{1, 2, 3}$ never reaches the threshold voltage. Generally the following relationship links the different propagation times [33]:

$$T_{cl} = T_{Pb} + T_{Pa} + T_{Sl} \ldots\ldots.. (1)$$



a. TMR –based AND WDDL



a. TMR –based AND QDI

Fig. 4 Defect free dynamic behavior ($R_{OP} = 0\Omega$)

After injecting the resistive open faults at the level of the module 2 and 3 (Fig. 3**)**, we will observe and analyze their electrical behavior to highlight the fault detection and the fault tolerance conditions. It is important to note that the resistive open will have the same consequences on the more complex secured circuits and therefore the conclusions that can be drawn from this study can be extended and applied to complex and fault tolerant secured circuits.

Figure 5 represents the SPICE simulation of the two TMR with two test vectors. In Fig. 5a and 5b, we choose a rather small fault resistance: R_{op} = 2kΩ for TMR -based AND WDDL and R_{op}= 4kΩ for TMR -based AND QDI. The initial state is given by the test vector V0 = [xt yt] = [00], and the transition is created by applying the vector V1 = [01]. It is clear that the presence of the open circuit slows the signal. An additional delay T_{op} = 16.213 ps for (AND WDDL) $_{2,3}$ and T_{op} = 7.494 ps for (AND QDI) $_{2,3}$ is observed. However, this delay remains smaller than the slack time T_{sl} = 16.812 ps for (AND WDDL) $_{2,3}$ and T_{sl} = 15.805 ps for (AND QDI) $_{2,3}$. The output St is interpreted normally and still insensitive to the presence of a defect. A correct value is latched into the scan register and the circuit operates correctly. In other words, the fault is masked and the two TMR are fault tolerant.

$$T_{pb} + T_{op} + T_{pa} < T_{cl} \text{ .... (2)}$$

Considering this simulation, we can say that an open circuit with a small fault resistance cannot be detected and thus can be tolerated by the structure TMR.

If we consider now a higher fault resistance, R_{op} = 5.329 kΩ for the TMR -based AND WDDL and R_{op} = 5.713 kΩ for the TMR -based AND QDI, as illustrated in Fig 6.a and 6.b, we find that the additional delay T_{op} is larger than or equal to the slack time. The output voltage St has not dropped below the threshold value of 0.55V when the clock edge occurs; we obtain 1 logic value instead 0 logic. An incorrect output value is captured in the shift register and open circuit fault can be detected:

- T_{pb}+ T_{OP} + T_{pa} ≥T_{cl} for (AND WDDL) $_{2,3}$……(3)
- T_{pb}+ T_{OP} + T_{pa} ≥ T_{cl} for (AND QDI) $_{2,3}$………(4)

This means that a resistive open can be detected by a two test vectors {V0, V1} if and only if the resistive value of the defect R_{op} is larger than a certain critical value R_C. We associate to an open circuit fault the detection interval DI associated to the vectors V0 and V1 defined by:

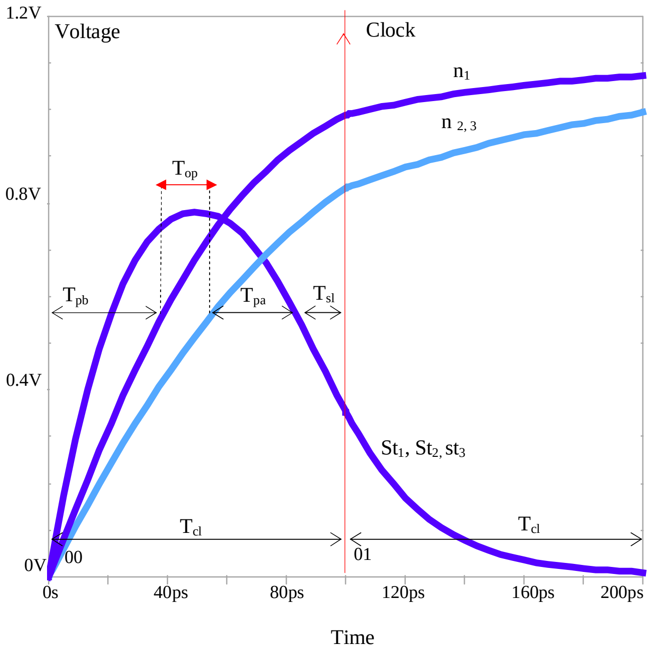
$$DI^{\{V_0,V_1\}} = [R_c^{\{V_0,V_1\}}, \infty[$$

DI = [R_C, ∞ [= [5.325 kΩ, ∞ [, for TMR -AND WDDL.... (5)

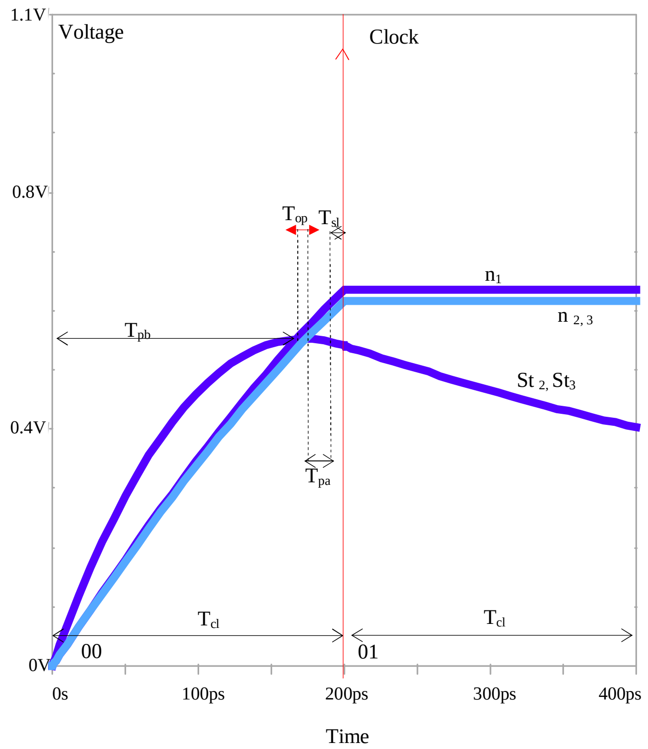
DI = [R_C, ∞ [= [5.713kΩ, ∞ [, for TMR -AND QDI…… (6)

We note that there is a slight difference between the two latter two due to the fact that the TMR -based AND QDI gate is more robust than the TMR -based AND WDDL gate. However, it is important to note that this value is associated to the pair of test vector {T0, T1} and another vector test may detect even smaller resistances and therefore a wider detection interval.

In summary, for R_{OP} ∈ [5.325 kΩ, ∞ [in AND WDDL and for R_{OP} ∈ [5.713 kΩ, ∞ [in AND QDI, the TMR -based AND WDDL and the TMR -based AND QDI cannot function correctly in the presence of two resistive open faults. Otherwise, the two faults will not be masked and the voter produces the faulty output St, the two TMR structures are not fault tolerant and hence not reliable. However, for R_{OP} ∈ [0, 5.325 kΩ [and for R_{OP} ∈ [0, 5.713 kΩ [, the TMR -based AND WDDL and the TMR -based AND QDI operate correctly with the presence of the two permanent faults. In other word, the two resistive open faults will be masked and the voter produces the correct output St, the TMR -based AND WDDL and the TMR -based AND QDI, are fault tolerant and thus reliable.

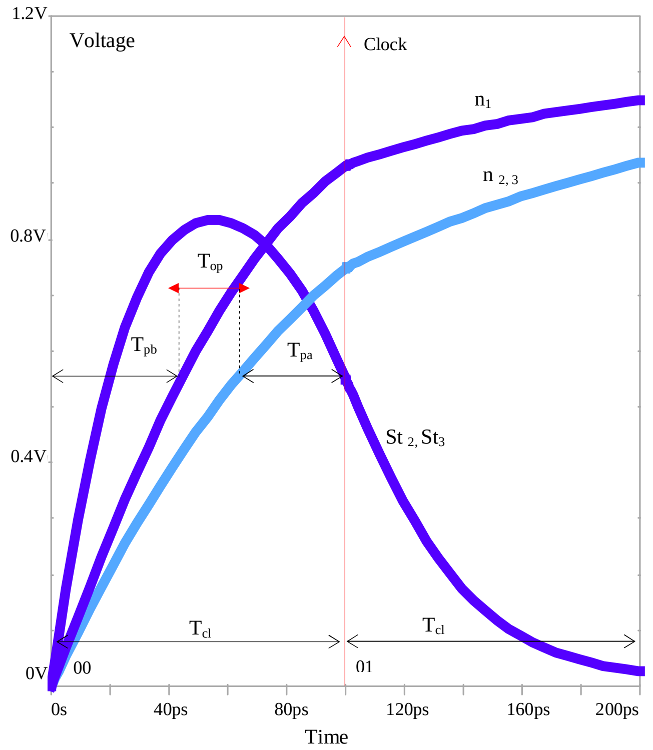


a. TMR –based AND WDDL with small resistance R_{op}=2 kΩ

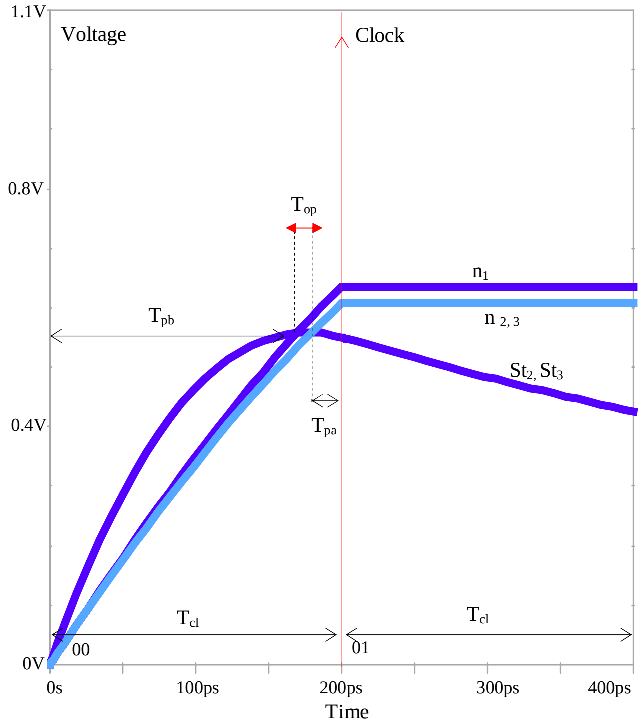


b. TMR –based AND QDI with R_{op}=4 kΩ

Fig. 5 Dynamic behavior of small fault resistance R_{OP}



a. TMR -based AND WDDL with high resistance R_{OP} = 5.329 kΩ



b. TMR –based AND QDI with high resistance ROP = 5.713 kΩ

Fig. 6 Dynamic behavior of high fault resistance R_{OP}

VI. Conclusion

This paper analyzes the resistive open fault impact on the dynamic behavior of TMR -based AND WDDL and TMR -based AND QDI. It is shown that the dynamic characterization encourage the use of delay based testing techniques, in order to improve the weak opens detection in TMR -based secure circuits. On the other hand, we have shown that depending on the open resistance value there are two operating intervals of fault tolerant secured circuits. In other word, it is showed that there is a critical resistance at which the fault is detected and the TMR is not fault tolerant and thus not reliable. Future works will consider analyzing the effect of resistive open in QDI circuits while taking into account the communications protocols performed by request-acknowledge based handshaking.

References

[1] A. Latoui, F. Djahli , "An Optical BILBO for On-Line Testing of Embedded Systems ", IEEE design & test of computers , Vol. PP, N°: 99, March 2013, pp. 1-12.

[2] S. Schulz, J. W. Rozenblit, K.J. Buchenrieder, "Multilevel Testing for Design Verification of Embedded Systems", IEEE design and test of computer, pp.60-69, 2002.

[3] J. Wen-Ben, H. Der-Chen and S.R. Das, "An Efficient BIST Method for Non-Traditional Faults of Embedded Memory Arrays", IEEE Transactions on Instrumentation and Measurement, Vol. 52, NO. 5, October 2003

[4] H.D. Thacker, O.O. Ogunsola, , A.V. Muler, , J.D. Meindl, , "Wafer Testing of Optoelectonic–Gigascale CMOS Integrated Circuits",

IEEE Journal of Selected Topics in Quantum Electronics, VOL. 17, NO. 3, pp. 659-670, 2011.

[5] G. Papa, A.T.T. Garbolino, " Optimal On-Line Built-In Self-Test Structure for System-Reliability Improvement", *IEEE Congress on Evolutionary Computation (CEC)*, pp. 222-229, 2011.

[6] H. Al-Asaad, , “Efficient Techniques for Reducing Error Latency in On-line Periodic Built-in Self-Test”, IEEE Instrumentation & Measurement Magazine, pp. 28-32, 2010.

[7] M. Grosso, M.S. Reorda, M. Portela-Garcia, M. Garcia-Valderas, C. Lopez-Ongil, L. Entrena, " An On-line Fault Detection Technique Based on Embedded Debug Features”, IEEE 16th International On-Line Testing Symposium (IOLTS),pp. 167-172, 2010.

[8] G. Ait Abdelmalek, R. Ziani, M. Laghrouche, Fault injection for verifying testability of fault tolerant structures at the Verilog level, IEEE XPLORE, Proceedings of The 24th International Conference of Microelectronics ICM 2012, December 17-20, 2012, Algiers

[9] G. Ait Abdelmalek, R. Ziani and M. Laghrouche, Study and modeling of defects in integrated circuits for their reliability analysis, IEEE XPLORE, Proceedings of The 24th International Conference of Microelectronics ICM 2012, December 17-20, 2012, Algiers.

[10] R. Rodriguez-Montanes, P. Volf and J. Pineda de Gyvez, “Resistance characterization for weak open defects”, IEEE Design & Test of Computers , Vol. 19, n°5, pp. 18-26, 2002.

[11] D. Arumi, R.Rodriguez-Montanes, J. Figueras, “Defective Behaviors of Resistive Opens in Interconnect Lines”, IEEE European Test Symposium, pp. 28-33, 2005.

[12] Z. Li, X. Lu, W. Qiu, W. Shi, and D. M. H. Walker, “A circuit level fault model for resistive opens and bridges,” VLSI Test Symposium, pp. 379–384, 2003.

[13] H. Hao and E.J. McCluskey, “Resistive shorts within CMOS gates”, International Test Conference, pp. 292–301, 1991.

[14] D. Shaw, D. Al-Khalili, and C. Rozon, “Accurate CMOS bridge fault modeling with neural network-based VHDL saboteurs”, International Conference on Computer Aided Design, pp. 531–536, 2001.

[15] Z. Li, X. Lu, W. Qiu, W.Shi, and D.M.H. Walker, “A Circuit Level Fault Model for Resistive Bridges”, ACM Transactions on Design Automation of Electronic Systems, Vol. 8, No. 4, October 2003.

[16] G. Ait Abdelmalek, R. Ziani, Study and Impact Analysis of Resistive Bridge within Deep Submicron Secured CMOS Circuits, IEEE XPLORE, Proceedings of The 9th International Design and Test Symposium IDT 2014, December 16-18, 2014, Algiers.

[17] D. Fick, A. DeOrio, G. Chen, V. Bertacco, D. Sylvester and D. Blaauw, "A Highly Resilient Routing Algorithm for Fault Tolerant NoCs," Proc.Design, Automation and Test in Europe 2009, pp.21-26, 2009.

[18] T. Lehtonen, P. Liljeberg and J. Plosila, "Online Reconfigurable Self-Timed Links for Fault Tolerant NoC," VLSI Design, vol. 2007, Article ID 94676, 2007.

[19] S. Almukharizim and O. Sinanoglu, "A Hazard-Free Majority Voter for TMR-Based Fault Tolerance in Asynchronous Circuits," Proc. Design and Test Workshop 2007, pp. 93-98, 2007.

[20] T. Verdel and Y. Makris, "Duplication-Based Concurrent Error Detection in Asynchronous Circuits:Shortcomings and Remedies," Proc. IEEE Int. Symp. Defect and Fault Tolerance in VLSI Systems 2002. pp.345-353, 2002.

[21] K. Tiri, M. Akmal, and I. Verbauwhede, “A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards,” Proc. European Solid-State Circuits Conf. (ESSCIRC ’02), pp. 403-406, Sept. 2002.

[22] J.M. Rabaey, A. Chandrakasan, and B. Nikolic, Digital Integrated Circuits. Prentice Hall, ISBN-10: 0130909963, 2003.

[23] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, “Three-Phase Dual-Rail Pre-Charge Logic,” Proc. Eighth Int’l Workshop Cryptographic Hardware and Embedded Systems (CHES ’06), pp. 232-241, 2006.

[24] S. Guilley, P. Hoogvorst, Y. Mathieu, R. Pacalet, and J. Provost, “CMOS Structures Suitable for Secured Hardware,” Proc. Design, Automation, and Test in Europe Conf. (DATE ’04), pp. 1414-1415, Feb. 2004.

[25] S. Guilley, F. Flament, R. Pacalet, P. Hoogvorst, and Y. Mathieu, “Secured CAD Back-End Flow for Power-Analysis Resistant Cryptoprocessors,” Design and Test of Computers, vol. 24, no. 6, pp.546- 555, Nov./Dec. 2007

[26] S. Guilley, F. Flament, R. Pacalet, P. Hoogvorst, and Y. Mathieu, “Security Evaluation of a Secured Quasi-Delay Insensitive Library,” Proc. Conf. Design of Circuits and Integrated Systems (DCIS ’08), DCIS, full text in HAL, http://hal.archives-ouvertes.fr/hal-00283405/en/, pp. 1-7, Nov. 2008.

[27] M.W. Allam and M.I. Elmasry, “Dynamic Current Mode Logic (DyCML), a New Low-Power/High-Performance Logic Family,” Proc. IEEE Custom Integrated Circuits Conf. (CICC ’00), pp. 421-424, 2000, doi:10.1109/CICC.2000.852699.

[28] F. Mace, F. X. Standaert, J.J. Quisquater, and J. D. Legat, “A Design Methodology for Secured ICS Using Dynamic Current Mode Logic,” Proc. 15th Int’l Workshop Integrated Circuit and System Design, Power and Timing Modeling, Optimization and Simulation (PATMOS ’05), pp. 550-560, 2005.

[29] F. Regazzoni et al., A Simulation-Based Methodology for Evaluating DPA-Resistance of Cryptographic Functional Units with Application to CMOS and MCML Technologies, SAMOS IC, July 2007.

[30] J. Han and P. Jonker,“Toward hardware redundant, fault tolerant logic for Nanoeletronics”, IEEE Design & Test of computer, Vol.22,No.4, 2005.

[31] M. Hafezparast,“tolerant Fault hardware designs and to their reliability analysis”, thesis of doctorate, Brunel university of west London, 1990.

[32] L. Fang, M.S.Hsiao, “Bilateral Testing of Nano-scale Fault Tolerant Circuits”, Proc. of IEEE Defect and Fault Tolerance in VLSI Systems, pp.309-317, 2006.

[33] N. Houarche, ” Modélisation de défauts paramétriques en vue de tests statiques et dynamiques”, thèse de doctorat, Université Montpellier II, Octobre 2009.

[34] D. Arumi, R.Rodriguez-Montanes, J. Figueras, “Defective Behaviors of Resistive Opens in Interconnect Lines”, IEEE European Test Symposium, pp. 28-33, 2005.

Ghania Ait Abdelmalek is currently a PhD student in Electronics Department of Mouloud Mammeri University of Tizi-Ouzou (Algeria). She has received his engineering degree and Master's degree in electronics from the University of Mouloud Mammeri in 2005 and 2011 respectively. Her current research interest is reliability and hardware security.

Rezki Ziani received his engineering degree in electronics in 1978 From the Polytechnic School of Algiers. He obtained his Master's degree in automatic in 1983 and his PhD in automatic in 1986 from the University of Technology of Compiegne (France). He is currently Professor in Mouloud Mammeri University of Tizi-Ouzou (Algeria) and head of department’s electronic. He is the author of more papers. His area of research includes test and reliability.

Mourad Laghrouche is a Professor in Mouloud Mammeri University of Tizi-Ouzou (Algeria) and vice dean of the Electrical Engineering Institute of Mouloud Mammeri University. He has received his engineering degree, Master's degree and PhD in electronics from Mouloud Mammeri University of Tizi-Ouzou (Algeria) in 1990, 1995 and 2005 respectively. He is the author of more papers. His area of research includes test and reliability, sensors, measurements, instrumentation.