Study of the Resistive Bridging Impact on the Delay in QDI Countermeasures

G. AIT ABDELMALEK, R. ZIANI and M. LAGHROUCHE

Abstract**—**The present paper highlights the impact of the resistive bridging faults on the delay in secured CMOS 45 nm technology implemented in quasi delay insensitive (QDI) countermeasure. We have analyzed the static and the dynamic behavior of resistive bridges as a function of its unpredictable resistance. We showed that the defect detection depends upon both conditions i.e., the value of the bridging resistance and the vectors that have applied to the circuit entry. The delay estimation induced by the resistive bridging faults is observed and analyzed.

Keywords—asynchronous circuits, fault models, small delay faults, SecLib, testability.

I. Introduction

THE rapid development of technology in the area of the digital CMOS circuits results in an increase in the size of circuits, severe leakage, very large process variations, more process defects and several physical defects during the circuit manufacturing process that are not yet modeled or detected by traditional testing techniques [1, 2]. Short between circuit's nodes are the predominant type of manufacturing defect [3], and shorts between gate outputs or bridging faults account for 90% of shorts [4-5]. Short defects are represented by bridging faults. Simple bridging fault models ignore the resistance of the defect. Resistive bridging faults are modeling this aspect with a higher degree of accuracy. The bridge resistance Rbr is a random parameter not known in advance. This is because it cannot be known in advance which particle will cause the short defect corresponding to the bridge (parameters like its shape, conductivity, exact location on the die, evaporation behavior and electromigration can influence the resistance of the short defect). Hence, a resistive bridging faults simulator calculates for a given fault the range of resistances in which a given test pattern set detects the fault. This range is called analogue detectability interval or ADI [4]. An ADI [R1, R2] is introduced by Renovell et al. [4, 6-7] and it is defined for a given fault and a given test set. The short having the resistance Rbr is detected by the test set if and only if Rbr is within this interval R1≤ Rbr ≤ R2. This concept is applicable both to resistive bridging faults between two logical nodes and to resistive stuck-at faults [7]. The resistive bridge modeling for standard CMOS technologies has received a particular attention during the last years including largely submicron technologies (until 45nm). Several authors considered modeling [4, 7-8] and simulation [9-12] of this fault class. In contrast, there are only few publications dealing with resistive bridges modeling of circuits using conventional CMOS technology for specific application specially, in the security field (cryptographic circuits). Indeed, previous analysis of faulty in asynchronous circuits has been done using the stuck-at -0/stuck-at -1 fault model [13]. This work examines the effects of stuck-at faults in delay-insensitive, quasi-delay insensitive (QDI), and speed independent circuits, testing QDI circuits, using the stuck-at model, is thoroughly explored in [14]. This testing method classifies a fault as either inhibiting (preventing an action) or stimulating (causing an action), identifies faults that can't be observable by adding testing points. A technique to mask transient faults that occur in asynchronous, speed independent, interfaces is described in [15]. This technique employs the use an adjudicator to mask transient faults between a circuit and the environment. Recently, we have demonstrated that the secure circuits can be tested with fault models similar to those used for standard CMOS circuits [16]. The aim of this work is the fault modeling of the resistive defects in secured circuits, implemented in QDI countermeasures. We have taken into account the unknown value, the bridge resistance Rbr. The impact of the resistive bridge on the electrical dynamic behavior of QDI-AND induced by resistive bridging faults is analyzed by SPICE simulations. We have used the concept of ADI for detecting resistive bridging defect in the CMOS 45nm technology.

The study is structured as follows. Section 2 gives the general definitions around the QDI countermeasure. Section 3 shows the electrical properties for the detection of the resistive bridge considering a specific sequence of two test vectors. In section 4, the small-delay faults caused by the resistive bridge are analyzed and the section 5 concludes this paper.

II. Countermeasures against SCA “Side Channels Attacks”

Side Channels Attacks (SCAs) presents a serious threat to implementations of cryptographic hardware devices. They are a class of physical attacks in which an attacker can gain information by monitoring the power consumption, execution time, electromagnetic radiation, and other information leaked by the switching behavior of digital complementary metal-oxide semiconductor (CMOS) gates. For example, the execution times that depend on values of data and/or key show that they are doing. Simple timing or power attacks give visual information on the circuit. During the last years, many countermeasures have been proposed to protect cryptographic devices against SCA. The goal of the countermeasures is to balance each logic cell such that the instantaneous power consumption is equal for all processed logic values and transitions to ensure that it does not produce a data-dependent power signature which can be used in an attack. The gate-level granularity of the method allows easy application to many different designs and the distributed nature of the countermeasures makes it harder for an attacker to circumvent. One approach, called Dual-Rail Precharge Logic (DPL), appears to be one of the most promising techniques. The principle of hiding consists in consuming the same amount of power consumption regardless of data inputs. This is achieved by using differential logic (signals are encoded as two complementary wires), and pre-charging the differential signals in every clock cycle. It is also called Dual-Rail Precharge logic (DPL). Several implementations of secure dual rail cells have been proposed, specifically for ASICs, such as SABL [17], WDDL [18], MDPL [19] and the balanced quasi-delay insensitive (QDI) cell library, called SecLib" [20]. The Wave Dynamic Dual Rail Logic (WDDL) technique developed by K. Tiri [18] is the most popular DPL countermeasures. It is based on a standard cell fow, and it is the most suited for FPGA implementation. In WDDL design, the netlist is duplicated into a true and a false part. The components used are limited to positive logic to avoid glitches. Inverters are implemented by cross coupling complementary outputs. This allows the precharge wave propagation throughout the combinatorial gates. In addition the circuit is designed such that its activity is constant and independent of the input data. We focus in this section, an informal description of QDI countermeasure.

A. *Quasi Delay Insensitive*

Quasi delay-insensitive (QDI) circuits are asynchronous circuits that operate correctly regardless of gate and wires delays in the system. These circuits do not use any clocks [21, 22], and the function of the clock is replaced by handshaking signals on wires. The very nature of QDI circuits namely, that they are insensitive to gate delays which makes them well-suited for fault-tolerant design, because most delay faults do not cause the circuit to malfunction. The base of any circuit QDI is the Muller gate (otherwise called “C-element”). Fig. 1(a) shows the C-element symbol, Fig. 1(b) and Fig. 1(c) show the C-element in two possible versions “regular C-element” and “secured C-element”. A Muller C-element is a state holding gate used to synchronize events in an asynchronous circuit. Its transitory behavior is described by the SPICE simulation results shown in Fig. 1(d). Namely, when both inputs X and Y are low the output S should below. When both inputs are high, the output should be high. Finally, if the inputs are different, the output should retain its old state.

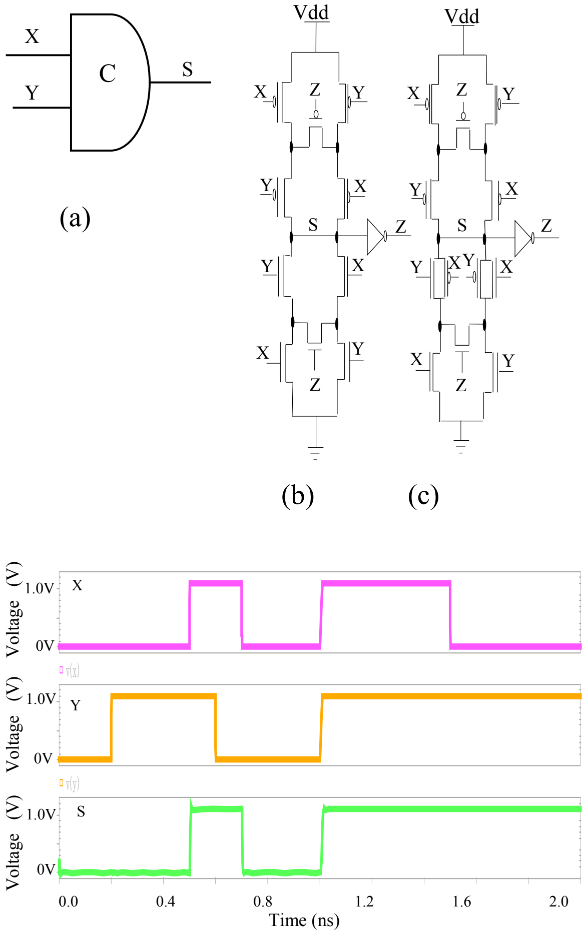
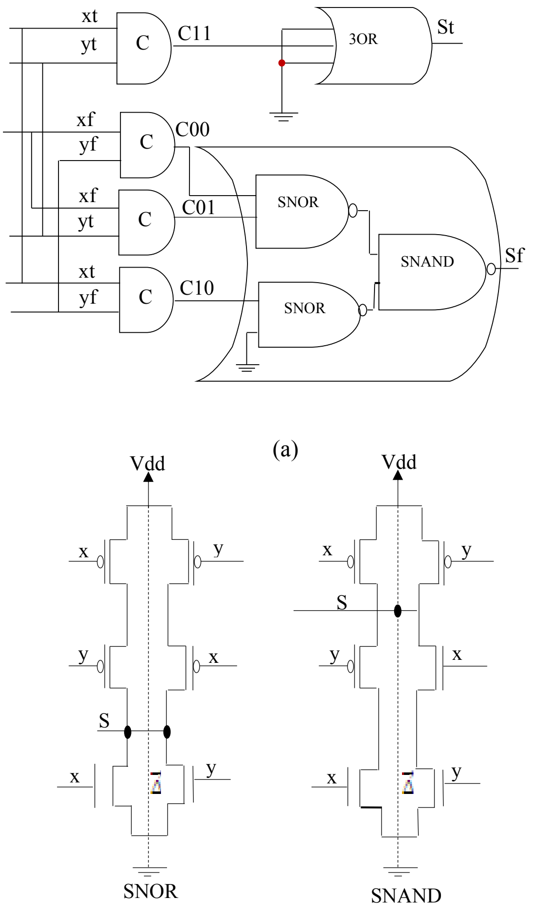


Fig. 1 (a) C-element symbol, (b) Regular C-element, (c) Secured C-element and (d) Simulation results

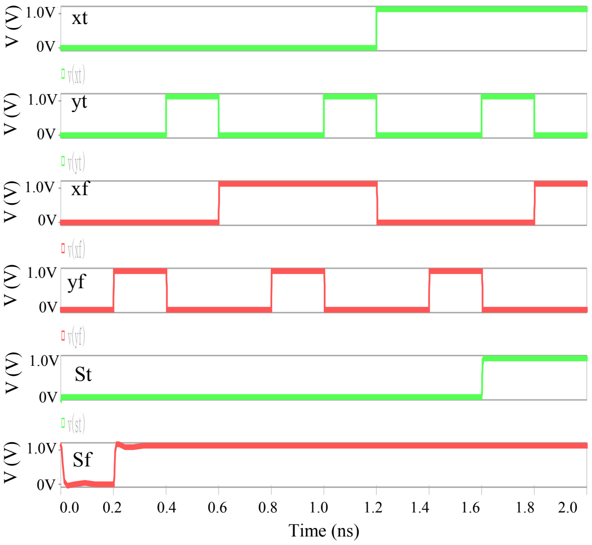
Asynchronous logic is a promising technology for building the chip-level interconnect of integrated systems. In fact, recent research suggests that asynchronous implementations have better resistance to fault injection than synchronous counterparts. They also have potential advantages in power consumption, modularity and compatibility which have attracted many researchers in recent years. Indeed, asynchronous designs also offer good resistance against DPA and many transient disruptions, thanks to their intrinsic properties that greatly increase their resistance to such attacks. In fact, in the QDI AND gate shown in Fig. 2(a), the encoding redundancy of dual -rail data (x, y) → (Coo, C_{01}, C_{10}, C_{11}) is well suited for an indiscernible processing. Indeed, it reduces the dependencies between the data and the current consumed. The dual rail encoding of data makes it more unlikely that data modification due to natural events will occur since a flip in a logical value requires the modification of two signals. The encoding redundancy of dual -rail data can be used for fine grained checking of data validity for detection of many transient disruptions that result in an invalid data token value (i.e. ‘11’).

Also, the balanced data paths offer the ability to precisely control the number of logical transitions in each calculation block. This helps to balance the paths data in order to maintain an independent consumer data on each path. For example, in QDI circuit, the designer can ensure the switching of a constant number of gates, regardless of the data. As shown in Fig. 2(a), the QDI AND gate is composed of four C-element gates and of two 3OR gate each consisting of two balanced NOR and a one balanced SNAND (called SNOR and SNAND, for Secured NOR and secured NAND) which have a perfectly symmetrical architecture as shown in Fig. 2 (b), keeping the same logical function of NOR and NAND gates of the standard cells library. The layout challenge consists in porting the symmetry from the schematic to the masks. Its SPICE simulation result is shown in Fig. 2 (c).



(a)

(b)



(c)

Fig. 2 Schematic of the (a) SecLib QDI secured AND gate, (b) its internal transistors 3OR architecture and (c) Its Spice simulation.

III. Influence of the Value of the Resistive Bridge

A. *Fault Model*

The most common model used for process faults is the stuck-at fault model [23]. The stuck-at model is attractive because it considers faults at the gate level, rather than the transistor level, which makes test pattern generation easy. However, the stuck-at fault model doesn’t model bridging faults, open fault or transistor level faults well. In this work, testing resistive bridges has been limited to analysis of interconnect with RC models. Capacitive coupling between interconnect has been lumped or altogether ignored. Inductive effects have been altogether ignored. To accurately model the behavior of bridging faults, we must determine the voltage at the bridged nodes for each vector that excites the bridging fault. Then, based on the logic threshold of the driven gates, we can determine whether the bridge is detectable at the driven gate output. We can also determine the maximum detectable resistance at the output of this gate, which gives us the detectable resistance interval.

B. *Fault Model Description*

In Fig. 3, the QDI AND is a faulty gate and it is affected by a resistive bridge. Indeed, there is a resistive bridge between conducting lines St and Sf. The resistive bridge is represented by the bridge resistance Rbr who’s the value a priori unknown of the defect since it depends on random parameters such as the topology or the material of the defect. In order to optimize and guarantee the detection of such a defect, its electrical behavior has to be analyzed as a function of this random parameter and optimal detection conditions must be derived. Thus, we assume that the thresholds of the two 3OR gates are the same (Th= Vdd/ 2= 0.55V). It is thus significant to be interested in the behavior of the circuit in the presence of defect of various sizes. However, the value of the resistance of shorted interconnect nodes is not the only factor to be taken into account. The impact of a resistive bridge is such as each node tries to impose its logical value on the other. However, if the two nodes are on the same logical level or the two transitions are in the same direction then the influence of the resistive bridge is transparent, the presence of the defect of resistive bridge does not disturb the operation of the circuit [24].

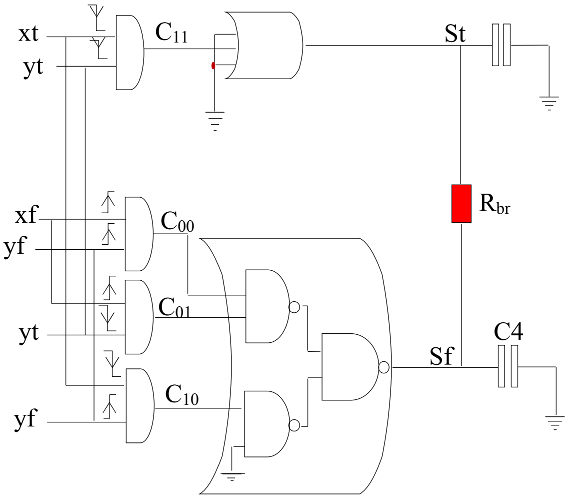
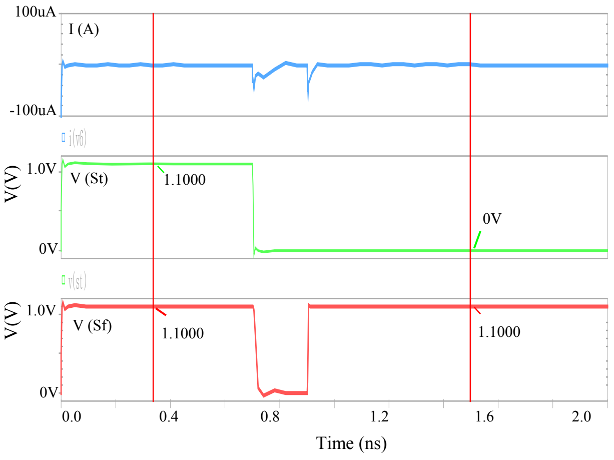


Fig. 3 Resistive bridge between conducting lines St and Sf of the QDI-AND.

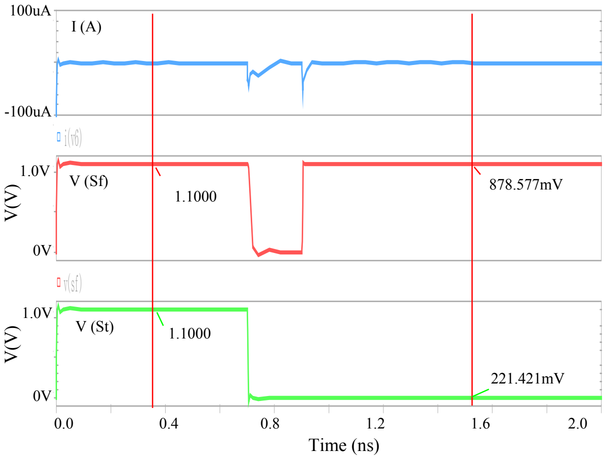
IV. SIMULATION AND RESULTS

A. *Critical Resistance Bridge Detection*

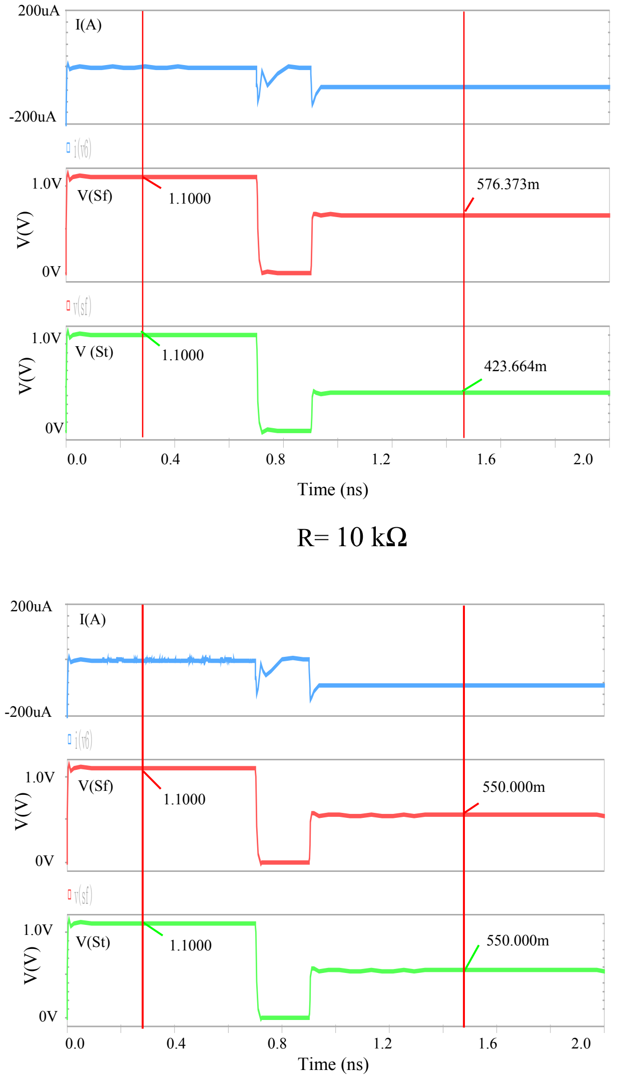
Define Let us first assume that the vectors {1, 1, 0, 0} and {0, 0, 1, 1} are applied successively to the input {xt, yt, xf, yf} of the secured AND gate shown in Fig.3. Now let us make vary Rbr resistance and we observe the electrical behavior of the QDI-AND for four discrete values of R_{br} resistance: 100 Ω, 10kΩ, 1000 kΩ and ∞. SPICE simulations were performed for 45nm CMOS technology, with nominal V_{DD} of 1.1 V. For these cases, simulation results are shown in Fig. 4. Initially, we observe on these four cases that the current consumed by QDI-AND is more significant with the reduction of the resistance value of the defect. The appearance of the peaks of consumption increase when the resistance of the defect decreases. This consumption appears especially at the time of the transition from a logical level to another. Also, in the range of resistance] 100 Ω, 10 kΩ], the circuit works correctly, but the current consumption becomes dependent of the data. In other word, the access to the current consumption allows possibly the detection of the sequence of the data. Thus, the circuit becomes less robust and unsecured against side channel attacks. Moreover, we notice that beyond a value of R_{br} = 100 Ω the transitory response of the output voltages V (St) and V (Sf) of the defected gate approach very clearly the fault free QDI AND behavior. On the other hand, when the resistance of the defect decreases, the transitions on the Sf node and St are in the opposite direction and are completely confused, in the same way a low level appears at output Sf instead of a high level, in other words these V (St) and V (Sf) voltages, according to Fig. 4, cannot to go beyond Vdd /2 = 0.55V; the presence of the resistive bridge produces here a logical error. In conclusion, more the resistance is small enough and more the defect is significant, it is thus possible to affirm that a resistive bridge of significant size can be detected if and only if the value of its resistance is lower or equal to 100 Ω. This maximum resistance is called Rc "critical resistance". We can thus associate to the faulty value 0/1 or 1/0 a resistance interval of [0, Rc] for which the value is indeed faulty. As Rc represents the maximum value of the resistive bridges for which the defect is detected. Thus, in our case the Detection Interval of the bridge resistive is [0, 100 Ω]. We will see in the following section that the static voltage test can also be extended to a dynamic voltage testing strategy (delay testing).



R= ∞



R= 1000 kΩ



R= 10 kΩ

R= 100 Ω

Fig. 4 Faulty secured QDI AND gate.

B. *Delay Fault Testing*

Logic voltage failures are static fault effects. Resistive bridging can also change the dynamic behavior of the circuit, for instance by increasing some propagation delays. We apply successively the vectors {1, 1, 0, 0} and {0, 0, 1, 1} to the input of the AND gates considered in the Fig. 3. Fig. 5 shows a small increase in the propagation delay due the 500 Ω bridging fault between nodes St and Sf in QDI-AND gate. The delay measured for the fault free gate is almost very small and it is of 13, 86 ps whereas that in the case of a QDI-AND affected by a resistive bridge of 500 Ω is of 64, 84 ps. We thus raise well a deceleration of about 50, 98 ps.

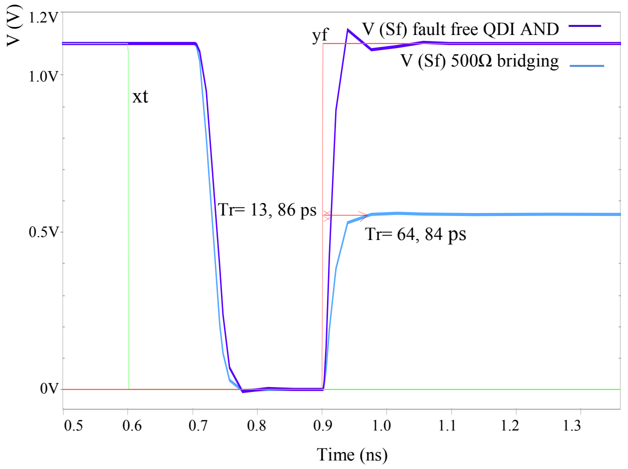


Fig. 5 Impact of the resistive bridge on the dynamic behavior of QDI- AND

Now, let us analyze the influence of the bridge resistance value R_{br}. Logically, the delay of a line affected by a resistive bridge decreases when the bridge resistance R_{br} increases. The resistances for shorted interconnect nodes are typically below 500 Ω, but measurements by [25] on process related defect monitoring wafers also report small percent-ages in the range of 500 Ω to 20 kΩ that vary from batch to batch. Measurements by [26] on four gate-to-source transistor shorts show values ranging from 800 Ω to 4.7 kΩ. Compared to the on-impedance of an MOS transistor, 500 Ω is low and 20 kΩ is high. To make sure that our fault evaluation is representative for the complete range of short resistance, we will model both a low-resistive value (of 300 Ω) and a high-resistive value (of 3 kΩ) for each short. Fig. 6 shows that for R_{br}= 300 Ω, the delay created on the Sf line inside the QDI-AND is of 54, 06 ps. Whereas for R_{br} = 3 kΩ, the delay is of 36, 15 ps. We can say that the delay measured on the level of the QDI- AND is more significant when the resistance value decreases. Also, the defect has less effect in proposed secured circuits than in CMOS standard circuits.

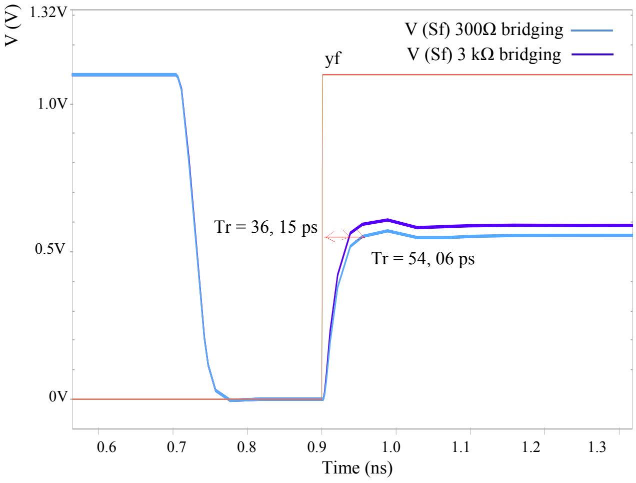


Fig. 6 Small delay faults according R_{br} resistance

V. Conclusion

This paper analyzes the impact of resistive bridging fault on the dynamic behavior of secured circuits. We have demonstrated the existence of the range of short resistance from which the power consumption becomes dependent data, so the behavior of the secured circuit is correct but it becomes unsecured. The results also showed the existence of a critical resistance at which the fault is detected. Considering delay fault testing induced by bridging faults in secured QDI AND gate, it is also shown that more the resistance is low and its influence is most important, i.e. the delay increases as the resistance value decreases. In other word, it is demonstrated that the delay measured follows the same low as it demonstrated by other works in the case of the standard CMOS circuits.

.

References

[1] International Technology Roadmap for Semiconductors, 2009 Edition, available at the following URL http://www.itrs.netLinks/2009 ITRS/Home2009.htm.

[2] C. Yu, G. Liu, L. Lai, “Diagnosis of Resistive-Open Defects using I DDT in Digital CMOS Circuits, *WSEAS Transactions on Circuits and Systems*, Volume 13, 2014, pp. 296-300.

[3] R. Rodriguez-Montanes, E. Bmls, and J. Figueras, “Bridging Defect Resistance Measurements in a CMOS Process,” Inr. Test Conf., 1992,pp. 892-899.

[4] M. Renovell, P. Huc, and Y. Bertrand, “The Concept of Resistance Interval: A New Parametric Model for Realistic Resistive Bridging Fault,” VLSf Test Symp., 1995, pp. 184-189.

[5] J. J. T. Sousa, F. M. Goncalves, and J. P. Teixeira, “IC Defects Based Testability Analysis,” In!. Test Conf., 1991, pp. 500-509.

[6] M. Renovell, P. Huc, and Y. Bertrand. CMOS bridge fault modeling. In VLSI Test Symp., pages 392–397, 1994.

[7] M. Renovell, F. Aza¨.s, and Y. Bertrand. Detection of defects using fault model oriented test sequences. Jour.of Electronic Testing: Theory and Applications, 14:13–22, 1999.

[8] I. Polian, P. Engelke, M. Renovell, and B. Becker. Modelling feedback bridging faults with non-zero resistance. In *European Test Workshop*, 2003.

[9] C. Lee and D. M. H.Walker. PROBE: A PPSFP simulator for resistive bridging faults. In *VLSI Test Symp.*, pages 105–110, 2000.

[10] V. Sar-Dessai and D.M.H. Walker. Accurate fault modeling and fault simulation of resistive bridges. In *Int. Symp. Defect and Fault Tolerance in VLSI Systems*, pages 102–107, 1998.

[11] V. Sar-Dessai and D.M.H. Walker. Resistive Bridge Fault Modeling, Simulation and Test Generation.In *Int’l Test Conf.*, pages 596–605, 1999.

[12] P. Engelke, I. Polian, M. Renovell, and B. Becker. Simulating resistive bridging and stuck-at faults. In *Int’l Test Conf.*, pages 1051–1059, 2003.

[13] H. Hulgaard, S. M. Burns, and G. Borriello. Testing asyn- chronous circuits: a survey. Integr. VLSI J., 19(3):111–131, 1995.

[14] P. J. Hazewindus. Testing Delay-Insensitive Circuits . PhD thesis, California Institute of Technology, Pasadena, Califor- nia, 1996.

[15] A. Yakovlev. Structural technique for fault-masking in asyn- chronous interfaces. In IEE Proceedings E - Computers and Digital Techniques, pages 81–91. IEEE Computer Society, 1993.

[16] G. Ait Abdelmalek, R. Ziani, Impact Analysis of Resistive Bridge within Deep Submicron Secured CMOS Circuits, *9th International Design and Test Symposium*, 2014, pp. 112- 117.

[17] 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.

[18] K. Tiri and I. Verbauwhede, “A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation,” Proc. Design, Automation, and Test in Europe Conf. (DATE ’04), pp. 246-251, Feb. 2004.

[19] T.Popp and S.Mangard, Masked Dual-Rail Pre-Charge Logic: DPA-Resistance without Routing Constraints , CHES 2005, pp. 172-186.

[20] M. NASSAR et al. BCDL: A High Speed Balanced DPL for FPGA with Global Precharge and no Early Evaluation. Proc. DATE 2010.

[21] S-Y.TAN, W-T. Huang, "A VHDL-Based Design Methodology for Asynchronous", *WSEAS Transactions on Circuits and Systems*, issue 5, Volume 9, 2010, pp. 315-324.

[22] J. Carlsson, K. Palmkvist, and L. Wanhammar, “Synchronous Design Flow for Globally Asynchronous Locally Synchronous Systems”, *Proceedings of the 10th WSEAS International Conference on CIRCUITS*, Vouliagmeni, Athens, Greece, July 10-12, 2006, pp. 64-69.

[23] M. L. Bushnell and V. D. Agrawal. Essentials of Electronic Testing for Digital, Memory and Mixed-Signal VLSI Circuits Kluwer Academic Publishers, 2000.

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

[25] R. Rodriguez-Montanes, E. M. J. G. Bruls, and J. Figueras, “Bridging defects resistance measurements in a CMOS process,” *in Proc. Int. Test Conf.,* 1992, pp.892-899.

[26] C. F. Hawkins and J.M. Soden, Electrical characteristics and testing considerations for gate oxide shorts in CMOS IC’s,” *in Proc. Int. Test Conf.*, 1985, pp. 544-555.

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 test 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 Faculty 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.