

Security and fault tolerance evaluation of TMR–QDI circuits

ISSN 1751-8709

Received on 14th August 2018

Revised 22nd December 2018

Accepted on 11th January 2019

E-First on 30th January 2019

doi: 10.1049/iet-ifs.2018.5439

www.ietdl.org

Ghania Ait Abdelmalek¹ ✉, Rezki Ziani¹, Rabah Mokdad²

¹Department of Electronics, Mouloud Mammeri University, Tizi Ouzou, Algeria

²Department of Physics, Mouloud Mammeri University, Tizi Ouzou, Algeria

✉ E-mail: ghania_79@yahoo.fr

Abstract: The authors report the results of a study on the impact of resistive bridging faults on triple modular redundancy (TMR)-based quasi-delay-insensitive (QDI) asynchronous countermeasures, which is used to provide a secure circuit against power analyses. They have carried out the present study on CADENCE using a resistive bridges fault model. They show that the resistive bridge faults can have serious impacts on the security of integrated circuits and it is possible to discover the secret data. Based on the bridges resistance value, there are three operating intervals of secure circuits, in which TMR-based QDI may or may not function correctly in the presence of two resistive bridge faults depending on the interval of the resistance value.

1 Introduction

The two most important types of implementation attacks against secure embedded systems are active fault attacks (FAs), and passive side-channel analysis (SCA). SCA observes the physical implementation of cryptography and uses implementation effects (time, power etc.) to find the secret key. The most powerful SCA, differential power analysis (DPA), enables the adversary to accumulate knowledge over many encryptions [1]. FA, on the other hand, deliberately injects faults into the cryptographic implementation, and analyses the erroneous outputs under the assumption of a specific fault model [2].

To achieve these FA, several techniques can be used in order to perturb the computation, i.e. attacks alterations in the operating environment, in the power supply [1] or in the clock signal [3]; additionally, illumination by laser or electromagnetic (EM) waves can also provide a precise and effective technique of injecting errors into the circuit [4]. DPA attacks, on the other hand, analyse how the power consumption at fixed moments of time depends on the input data. To weaken the relationship between processed data and power consumption several hardware countermeasures have been proposed in the literature at different logic levels; system level, gate level and transistor level countermeasures [5–7]. On the one hand, the asynchronous design presented by Sparso and Furber [8] is a solution to the problem of power consumption dependent data. The intrinsic properties of asynchronous circuits (double-rail coding and feedback loops) make them more attractive by increasing their resistance to attacks as faults injection and DPA. Double-rail coding is used to improve robustness, and feedback loops that should be able to tolerate delay faults are used to ensure time-independent synchronisation [9]. Besides, the spatial and temporal hardware redundancy becomes an essential design for faults tolerance in digital systems, especially in highly specialised fields such as security. Since the faulty behaviour can be processed as side-channel information, offering all the benefits of DPA including noise averaging and hypothesis testing by correlation.

Based on the faulty behaviour, several works proposed to exploit the fault-based attacks which use the intentionally injected faults to obtain some abnormal behaviour and to recover the secret data. The recent FAs, which were demonstrated to be very powerful, are fault sensitivity analysis (FSA) [10] and differential behaviour analysis (DBA) [11]. However, both FSA and DBA attacks require the attackers to have dedicated control of fault injection intensity, and a lot of times fault injections. Theoretically FSA and DBA only need to distinguish the abnormal behaviour of

the device and does not need the value of the faulty output [12]. The important to the attacker is under what conditions the fault appears. He observes the behaviour of the circuit in response to the fault injection process. The faulty behaviour can be the faulty output or the side-channel leakage when faults are injected, e.g. the timing information, the power consumption, the electro-magnetic radiation. Cryptographic applications are vulnerable to fault injection attacks. In this work, we propose a fault-based attack called fault behaviour analysis (FBA). The FBA attacks were presented for the first time by Li *et al.* [12]. Their work discusses only the faulty output, which is the most direct information available to the attacker. The novelty in the current work compared the one previously published in [12] is that the information about the input data can be retrieved not only from the output of the circuit at the presence of the fault but also by observing the current consumption. The faults injection is carried out on the simulation of the hardware TMR-quasi-delay-insensitive (QDI) countermeasure rather than on an algorithm implementation of the advanced encryption standard (AES). Also, compared to the FSA and DBA attacks, the FBA requires faulty output but does not require the strict control of the fault injection intensity.

Our main goal is to test an implementation where combined countermeasures against FBA have been embedded. To that purpose, we combine the TMR structure with QDI logic style (combined countermeasures). These two countermeasures are recognised as being the most effective against power analysis and fault injection attacks. In the following, we will study and evaluate the robustness and the security of the type of combined countermeasure. For our simulations, we have developed a TMR–QDI one of the AND gates. We have performed fault-injection simulations at the transistor level on an AND gate of TMR design to evaluate the effects of TMR bridging resistive defects on the robustness and the security of QDI circuits.

The paper is organised as follows. The first section describes the DPA principles, the QDI countermeasures and presents the implementation of the TMR-based AND QDI, and shows when and how this latter is fault tolerant or not. The second section presents our fault injection attack approach. The simulated results of the electrical analysis of the TMR-based AND QDI are presented by the last section. Also, finally, we provide concluding remarks about this work.

2 DPA and resistive bridges fault injection

The security applications such as cryptographic circuits contain confidential information; this is why they are subject to SCA and FAs. SCA attacks have been introduced by Kocher *et al.* in their seminal work describing simple power analysis (SPA) and DPA [13]. In SPA attack, an attacker uses the side channel information from one measurement directly to determine the secret data. Mangard [14] demonstrated that SPA attacks on the implementation of the AES key expansion reveal the secret key of AES software implementations on smart cards by exploiting the fact that the power consumption of most smart-card processors leaks information during the AES key expansion.

The side channel information can be a power consumption leakage which is the outcome result of changes in current-supply during logic state transitions. Each 0–1 change requires an additional charge to be passed from bias to the output capacitance. On the contrary, 1–0 change discharges load and no current flows from V_{DD} . It is this deterministic link between consumption and manipulated data that will exploit the DPA to the scale of a circuit. So this is sufficient to detect what is happening inside the secured circuit just by monitoring the power consumption. In DPA, many measurements are used in order to filter out the noise. While SPA exploits the relationship between the operations that are executed and the power leakage, DPA exploits the relationship between the processed data and the power leakage. Over the years, several SCA techniques have been reported in the literature for differential EM analysis attacks [4], timing attacks [3], probing attacks [15] etc.

On the other hand, FAs were first introduced by Boneh *et al.* on a microcontroller [16]. In FA, an adversary injects faults to disturb the normal execution of a cryptographic algorithm and then analyses the corresponding leakage behaviour to retrieve the secret data. FAs are a potent threat to secure circuits since they are easy to mount and require low cost equipment.

Recent works proposed to exploit SCA and FA together to develop more power attacks, they are called hybrid attacks. Biham and Shamir introduced the principle of differential fault analysis (DFA) [1]. In DFA, the adversary injects a random fault and compares faulty and fault-free outputs to recover the secret data. Li *et al.* proposed a new FSA [10]. The attacks monitor the sensitivity information of the design under faults injection to try and reveal information about the circuit. FSA shares similarities with side channel analysis (SCA) attacks and has been recently combined with zero value attacks [17] for greater accuracy. Skorobogatov [18] uses a laser beam to increase the power consumption of a micro-controller logic cell and exploits this phenomenon via power analysis. Class of FAs DBA as described in [11] combines safe error attack [19] and DPA. DBA is similar to DPA, it exploits both the behaviour of the circuit when a fault is injected as a side channel and DPA statistical approach.

In this study, we propose to associate the SPA attacks with the FA-based resistive bridges fault injection. FBA exploits the correlation between the faulty behaviour and the power consumption of a circuit and the processed data. We show that the power consumption is dependent on the faulty behaviour, and thus it can be used for the data recovery, just like other side-channel leakages.

3 QDI countermeasures

Asynchronous designs are considered as an alternative to conventional synchronous circuits. Indeed, the development of technology has led to an increase of the clock frequency and a broadening of the clock distribution network. This has introduced extra difficulties in delivering the global clock signal all over the chip with acceptable clock skews. For this reason, on the one hand, a fundamental solution to the problems caused by clocks lies with asynchronous or clock-less design strategies presented by Sparsø and Furber [8]. The absence of a clock helps greatly complicate the attack. As explained by Yu *et al.* [20], the presence of a clock signal in the synchronous circuits generates always a large power consumption peak at a fixed time after each clock edge. This makes power consumption waveform being periodic. Therefore, the attack is made much easier by using the clock as a time

reference, because it is simple to apply statistical analysis techniques on this type of power waveforms which are no longer periodic and thus to compute the average waveform. However, asynchronous circuits use many local handshake signals instead of one global clock signal. Activities in each sub-circuit depend solely on their local synchronisation signals and circuits operate independently. Therefore the power consumption waveform does not have a global time reference. The power consumption of each sub-circuit does not contribute to the total power consumption with a coherent relative synchronisation as it does in synchronous circuits. Thus, there may not be large peaks in the total power consumption waveform. Indeed, the power consumption of asynchronous circuits will be much smoother since it is the aggregation of many small peaks appearing at arbitrary times according to their handshake signals. The statistical analysis of these power consumption waveforms is consequently expected to be more difficult because it is hard to align them to calculate the average value and to subtract this from each waveform to get the difference.

On the other hand, at the circuit level, the dual-rail with precharge logic (DPL) [21] countermeasures have been proposed to decrease the correlation between the side channel leakage and the secret data. Several implementations of secure dual rail cells have been proposed, such as Sense-Amplifier Based Logic (SABL) [22], Wave-Dynamic-Differential Logic (WDDL) [5], Masked Dual-Rail Pre-charge Logic (MDPL) [6] and the balanced quasi-delay insensitive (QDI) cell library, called SecLib" [7]. The QDI asynchronous countermeasures [23] employing delay insensitive code for data representation and processing and a four-phase handshake protocol for data communication is considered to be robust and is construed to be a viable alternative to the synchronous design method [24]. This is because QDI circuits have several advantages [25] such as low power [26, 27], tolerance to noise and EM interference [28, 29], ability to withstand process, voltage and temperature variations [30], self-checking [31], resistant to side channel attacks in the case of secure applications [32, 33] etc.

Unlike synchronous circuits where the shape of the current (current peaks) depends on the previous states and data values, the aim of the QDI asynchronous circuits is to always have the same current profile regardless of the data computed. The dual-rail encoding is often used to obtain constant-power computations. The protocol of this logic consists of two phases: precharge and evaluation. The precharge phase allows starting new computations from a known electrical state. It thus prevents unexpected transitions between two computation steps. The dual-rail signalisation of the data is conveyed by two wires for each Boolean variable. In the precharge phase, all the wires are set to be the precharge value, which is often assumed to be 0. In the evaluation phase, each pair of wires is set back to the logic values as either (00→01 or 00→10). As a result, every evaluation consists in the transition of exactly one wire (00→01 or 00→10), and the other remains 0. Since the number of bit transitions is independent of the processed data, a QDI circuit is likely to consume a constant amount of power for each transition. Therefore, if the design is adequately balanced, each transition occurred is indiscernible by power analysis attacks.

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. Balanced QDI circuits enable constant-power and constant-timing computations. The design of each circuit involves two steps [34]. The first step consists in the synchronisation task which is realised by Muller C-element. The second step consists of the redirection of the value to the adequate output. Redundant logic (C_{00} , C_{01} , C_{10} , C_{11}) is added to balance the paths to the direct (S_d) and dual (S_f) output couple, resulting in the schematic given in Fig. 1. In AND QDI gate, the computation is realised for both the direct and its dual output with the same logic, namely a three-input OR gate, which provides protection against an attacker that would be capable of distinguishing the two halves side-channel signature.

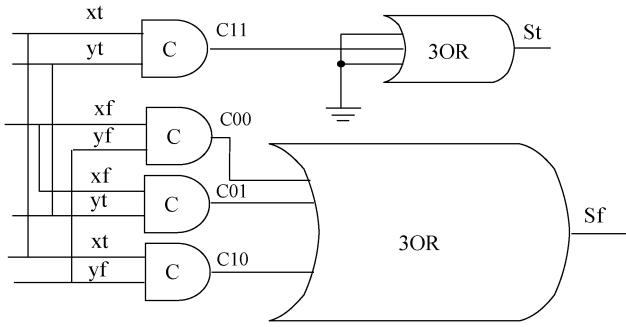


Fig. 1 AND QDI gate

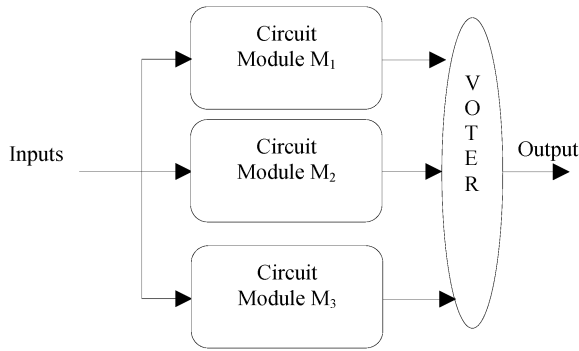


Fig. 2 TMR structure

Despite these important properties, it is necessary to evaluate the efficiency and robustness of asynchronous designs in the presence of permanent faults. Most researchers are studying the impact of permanent defects in traditional synchronous circuits [35, 36], but little attention has been given to asynchronous secure circuits.

In this study, we evaluate the security and the fault tolerance of the AND Gate QDI implementation against FBA attacks.

4 Spatial redundancy against FBA

As explained by Bar-El *et al.* [37] Lima *et al.* [38], the most popular countermeasure against fault injection consists of spatial or temporal redundancy. Clavier *et al.* [39] introduced a passive and active combined attack (PACA) on AES. The fault injection assumes a stuck-at model. It is shown that this attack can only break a first-order masking scheme of AES and for an AES implementation masked at order equal or >2 , this PACA is ineffective.

Thus, to our knowledge, no successful side-channel attack has been reported in the literature targeting a spatial or temporal redundancy countermeasure at order equal or >2 . One can then consider that a novel countermeasure which combines a high-order redundancy (>2) and QDI countermeasures is protected against both FA and SPA.

In this work, we focused on the triple modular redundancy (TMR) countermeasure with a majority voter. TMR architecture has been mostly considered for both study and practical applications [40, 41]. It is a fault tolerant structure where a module is repeated three times and a voter gathers all the outputs, giving as final output the majority output of the three modules. As long as no more than one of the modules fails, the output of the voter is the same as the outputs of the two other fault-free modules. The degree of fault tolerance is defined as the maximum number of faults that can be tolerated in a system [42]. Fig. 2 shows the TMR structure.

5 Defects and fault tolerance

Due to its simplicity, the stuck-at fault model is still widely used to represent permanent defects in the tests of digital circuits [43, 44]. In current circuits, however, instead of targeting only single faults, two or more faults must be taken into account. In addition,

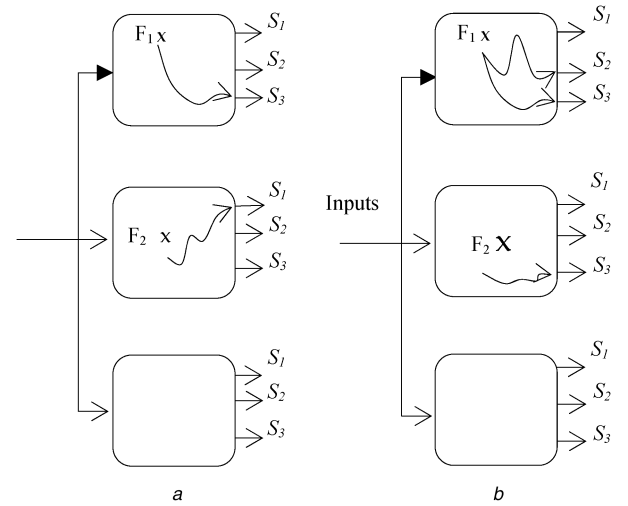


Fig. 3 Double bridging faults affecting two different modules (a) Tolerated, (b) Not tolerated

targeting all possible multiple faults may be infeasible. Thus, an efficient framework is needed to detect the defects.

In this paper, we propose to evaluate the impact of two resistive bridges defects on the fault tolerance and the security of the TMR AND QDI. To know when and how these circuits are able to tolerate resistive bridging faults, we assume the case when the voter is a fault-free circuit and when the defects are present in different modules.

In order to show the tolerance of the resistive bridging faults, we have used and adapted the case given by Fang and Hsiao [42] (when double stuck-at defects affect two different modules). In this work, we consider that two resistive bridge faults F_1 and F_2 affect two different modules of the TMR. They can be tolerated if there is no input test sequence to propagate two errors caused by the different faulty modules to common outputs in each module. However, they are not tolerated if two errors are propagated towards common outputs in each module. As shown in Fig. 3a, we assume that F_1 propagates towards S_3 in the first module, while F_2 propagates towards S_1 in the second module. By analysing the circuit, it can be observed that the third output S_3 of modules 2 and 3 will be dominant and therefore F_1 will be masked by the voter, and the first output S_1 of modules 1 and 3 will be dominant and F_2 will be masked. Thus the outputs of the TMR structure are correct and F_1 and F_2 are tolerated. However, in the case shown in Fig. 3b the output of the TMR structure is incorrect. If F_1 propagates towards S_2 and S_3 and F_2 propagate towards S_3 , the faults F_1 and F_2 cannot be masked because the third output S_3 of each of the modules (1 and 2) is faulty. Consequently, the voter receives two wrong values for S_3 and provides an error on the third output of the TMR. F_1 and F_2 are not tolerated.

6 Fault model

While the defect modelling of conventional complementary metal oxide semiconductor (CMOS) technologies is a relatively well-controlled domain, as evidenced by a fairly rich literature on this subject, there are many questions regarding CMOS-based circuit fault modelling for specific applications, such as cryptographic circuits. In [45], the authors have shown how resistive open faults injection onto TMR QDI circuits can cause local delay faults. Rahbaran and Steininger used the saboteurs to generate faults at gate level to compare the transient faults impact in an asynchronous processor and a synchronous one [9]. The fault tolerance of transient faults is discussed also by Zhang *et al.* [46] and Kuang *et al.* [47]. However, these works do not address the security and fault tolerance evaluation of TMR secure systems against resistive bridges defect, which are still the dominant defect for manufacturing process [48] and are more difficult to detect in a TMR structure due to the presence of redundancy [42]. The aim of our simulations is to evaluate the fault-tolerance and the security of

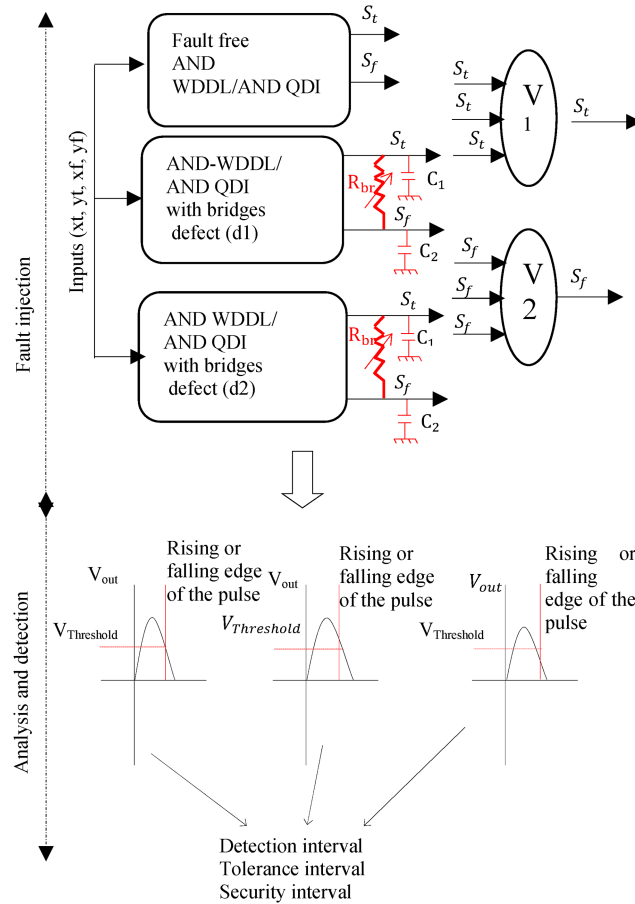


Fig. 4 Resistive bridging faults injection process

TMR secure circuits against resistive bridge faults injection based attacks.

A lot of work has focused on fault models of resistive bridge defects [35, 36] and throughout our simulations, we used the one proposed in [36], which describes the resistive bridge fault impact considering the static and dynamic behaviour of the circuit. The defect is modelled by a resistance R_{br} which is a random parameter. The fault resistive detection depends on the resistance value of the defect which causes a fault in the circuit. Consequently, we apply the following definition of detection in our simulations: given a resistive bridged-nodes voltages (V_1 , V_2) and related information of two driven gates ($G1$, $G2$), i.e. the threshold voltages (V_{G1}^{thres} , V_{G2}^{thres}), if $V_1 \geq V_{G1}^{thres}$ and $V_2 \geq V_{G2}^{thres}$, their logic values V_{G1} and V_{G2} are regarded as with logic-1. Otherwise, it is with logic-0 [36].

7 Fault injection attacks strategy

The new testing approach for security and fault tolerance evaluation presented in this study is a hybrid approach which is based on behaviour analysis of the combined countermeasure (i.e. TMR AND QDI countermeasures) against new combined attacks FBA (i.e. resistive bridges faults injection and SPA).

For the purpose of this study, our fault injection process presented in Fig. 4 requires lower restrictions in comparison with previous works and it is based on three steps. The first step consists of the choice of the asynchronous circuit (AND QDI gate is previously presented in [45] and has been used as an example to apply our testing method). Afterwards, a TMR architecture has been applied to this gate (i.e. TMR-based AND QDI), as presented in Fig. 4. Once the implementation of the TMR is done on SPICE, we recorded the results relating to the electrical behaviour of TMR architecture without defects. In the second step, we chose the default injection site. We are interested in the case where two resistive bridging faults (d1, d2) affect two different modules of the TMR, e.g. module 2 and module 3. For performing the fault injection simulations, the architecture of our approach is based on

adding a resistive bridges fault model to the output of the selected nodes of the TMR (Fig. 2). As shown in Fig. 4, the resistive bridge faults are injected between two nodes, which have different logic values, for instance, nodes S_t and S_f . The resistive bridge is represented by the bridge resistance R_{br} . Note that, these fault models allow injecting a lot of faults only by varying the resistance value of the defect. Being interested in injecting resistive bridge faults (R_{br}) in the TMR design, different resistance values can be chosen. In our simulations, we present only the most significant results of R_{br} 8 Ω , 100 Ω , 350 k Ω , and ∞ . It should be noted that only one simulation configuration is sufficient to inject a lot of faults. So, these injections and tests require a very short time. After we perform the faults injection, we optimise the input test sequences in order to detect the faults according to static analyses, and thereafter we analyse and record the electrical behaviour of the TMR in the presence of defects. In the last step, we compare the behaviour of TMR architecture (with and without defects) based on the threshold voltage of driven gates. For each resistance value, it is decided whether the analysed electrical behaviour is faulty or not, using the monitoring of their output voltage. Finally, the decisions relating to the different TMR architectures reveal the detection interval (DI), the security interval (SI) and the tolerance interval (TI).

8 Simulation results

The QDI style logic has equivalent routing for true and false paths and thus the coupling capacitance between interconnect lines with a bridges defect and the inductive effects have been neglected in our simulations. As the goal of the DPL logic style is to balance the power consumption of the logic gates, it is important to have equivalent routing for true and the complementary paths in order to avoid the inductive and coupling capacitance effects. As stated in [49, 50], the loading capacitance has three components which consist of (i) the intrinsic output capacitance, (ii) the interconnect capacitance and (iii) the intrinsic input capacitance of the load. The

Table 1 Test sequences

Sequence	Cycle	xytxfyf
S_0	initial state	1100
S_1	sequence 1	0100
S_2	sequence 2	0000
S_3	sequence 3	0011
S_4	sequence 4	1100

intrinsic input and output capacitances are controlled by the DPL logic, whereas the interconnect capacitance and the inductive effects should be controlled by the place and route process.

The TMR design has been tested by Spice simulation. TMR architecture is designed in a 45 nm CMOS technology and simulated by Cadence Spice with the supply voltage $V_{DD} = 1.1$ V. The fault injection is done at the transistor level. All transistors (N-type metal oxide semiconductor or P-type Metal Oxide Semiconductor) have a channel width of 95 nm and a channel length of 45 nm. The capacitors C_1 and C_2 are both set to 0.8 fF. The threshold voltage for each TMR gate is assumed to be equal to $V_{DD}/2$.

To analyse the impact of the resistive bridging faults on the security and the fault tolerance of the TMR design we generate a well-defined test sequence. The detection of the resistive bridge not only depends on the unpredictable resistance but also on the input sequences that have been applied to the circuit. The simulations in [36] suggest that adequate coverage of bridge defect require specific input sequences, i.e. the best input sequences are when In1 and In2 produce inverse transitions that are shifted in time. In1 and In2 are the inputs of the AND gate, independent of the design. For example, Table 1 gives the test sequence generated in order to detect the resistive bridging faults injected. The test sequence contains five inputs cycles [1100 0100, 0000, 0011, 1100]. The sequences $S_0 \rightarrow S_1 \rightarrow S_2 \rightarrow S_3$ have been generated to detect the resistive bridge between nodes S_t and S_f . S_4 has been generated to highlight the impact of the input sequence on the resistive bridge detection.

We realised the fault simulations in order to detect the maximum resistance value of the defect for which the output S_t and S_f values of the faulty TMR are opposite to the fault-free values. This detection is based on the observation of the appearance of faulty output values. This would allow us to associate the value of the resistance value of the defect and therefore this makes it possible to determine not only the TI of the TMR but also the SI.

The steps in our simulations are explained next. First, the simulation result of the electrical behaviour of the fault-free TMR is obtained. Then, the TMR with injected resistive bridging faults is performed while monitoring their output voltage S_t and S_f as well as their power consumption.

8.1 Fault-free behaviour results

In order to show the validity of our TMR design, Fig. 5 shows the simulation result of the electrical behaviour of the fault-free TMR AND QDI. In Fig. 5, xt, yt, xf and yf signals represent the input values of the TMR design of Fig. 4, $I(V)$ signal represents the power consumption of TMR design, while S_t and S_f signals represent the output values.

As shown in Fig. 5, it is demonstrated that based on a given inputs sequence [xt, yt, xf, yf] the fault-free TMR design operates correctly. The initial state is given by sequence $S_0 = [1, 1, 0, 0]$. The input xt switches to 0 in the sequence $S_1 = [0, 1, 0, 0]$ and so outputs S_t and S_f remain at 1. This can be explained by the fact that if the inputs of Muller C-element are different, the output should retain its previous state. Then input xt switches to 0 in the second sequence $S_2 = [0, 0, 0, 0]$, in this case, a voltage level of the output signals $V(S_t)$ and $V(S_f)$ becomes low when the transition is applied at the input xt. When inputs xf and yf switch from 0 to V_{DD} , i.e. $S_3 = [0, 0, 0, 0]$ and $S_4 = [0, 0, 1, 1]$, output S_f switch from 0 to V_{DD} ,

while S_t remains at 0. However, when inputs xf and yf switch from V_{DD} to 0 and inputs xt and yt switch from 0 to V_{DD} , i.e. $S_4 = [0, 0, 1, 1]$ and $S_5 = [1, 1, 0, 0]$, this transition propagates through the critical path and outputs S_t switch from 0 to V_{DD} and S_f still equal to 1.

In the case of fault-free TMR, the current consumption traces are independent of the inputs applied to the TMR AND QDI. The power consumption $I(V)$ of Fig. 5 demonstrates that the TMR QDI has exactly one charging event per cycle and charge a constant capacitance in that charging event. For both the events all the internal node capacitances and one of the balanced output nodes are discharged. In each event, the same amount of charge is needed to charge the same capacitances, and hence the same amount of current consumption is used. The power consumption variation does not give either information on the inputs or on the outputs because the peaks remain balanced. When only S_2 and S_3 switch from 0→1 a narrow glitch occurs. However, when (S_t, S_f) and (S_f, S_t) pass from 1→0, the peak current consumption is wide and this is explained by the voluntary shift between the signals xt and yt input of the nanosecond order. The inputs are not leaked through the power consumption and this TMR AND QDI is secure against power analysis.

8.2 Faulty TMR behaviour results

We consider the faulty TMR and that the voter is a fault-free circuit. As the bridge resistance R_{br} is an unknown parameter of the defects, we perform our Spice simulations with different resistance values to efficiently and accurately reflect the behaviours of the TMR designs in the presence of such defects. The following bridge resistance examples use different resistance values (∞ , 350 k Ω , 100 Ω , and 8 Ω). We apply the fault model to the TMR AND QDI. In the TMR asynchronous case, both signals S_t and S_f in modules 2 and 3 were bridged. The defect can be detected when the faulty node switches and becomes observable on the primary outputs. For this reason, the test sequence of Table 1 has been applied.

8.2.1 Simulation for a very high resistance, $R_{br} = \infty$ ($\gg 350$ k Ω):

As module #1 is supposed to be fault-free we only represent the chronograms of faulty modules 2 and 3. Fig. 6a shows that these voltage levels ($V(S_t)$, $V(S_f)$) and ($V(S_f)$, $V(S_t)$) are the same in both no fault and resistive bridge fault conditions. So, the faults propagated a correct logical value towards (S_t, S_f) and (S_f, S_t) on each gate. The voter V1 receives three correct values for S_t and the voter V2 receives three correct values for S_f . The outputs of the TMR design are therefore correct and the two resistive bridge faults are tolerated. The TMR operates correctly and the two defects are not detected. Fig. 6a shows also the current consumption traces $I(V)$ of the TMR. It can be seen that the current-consumption peaks or glitch are balanced and we cannot deduce the state of the transitions. So, the power consumption traces are independent of the applied data at the inputs of the TMR. Therefore, the security is maintained and TMR AND QDI is immune to power analysis attacks.

8.2.2 Simulation for high resistance, $R_{br} = 350$ k Ω :

Fig. 6b shows the experimental results of $R_{br} = 350$ k Ω . When decreasing R_{br} , ($V(S_t)$, $V(S_f)$) and ($V(S_f)$, $V(S_t)$), move in the opposite direction than $V(S_t)$ and $V(S_f)$ in fault-free TMR AND QDI, but

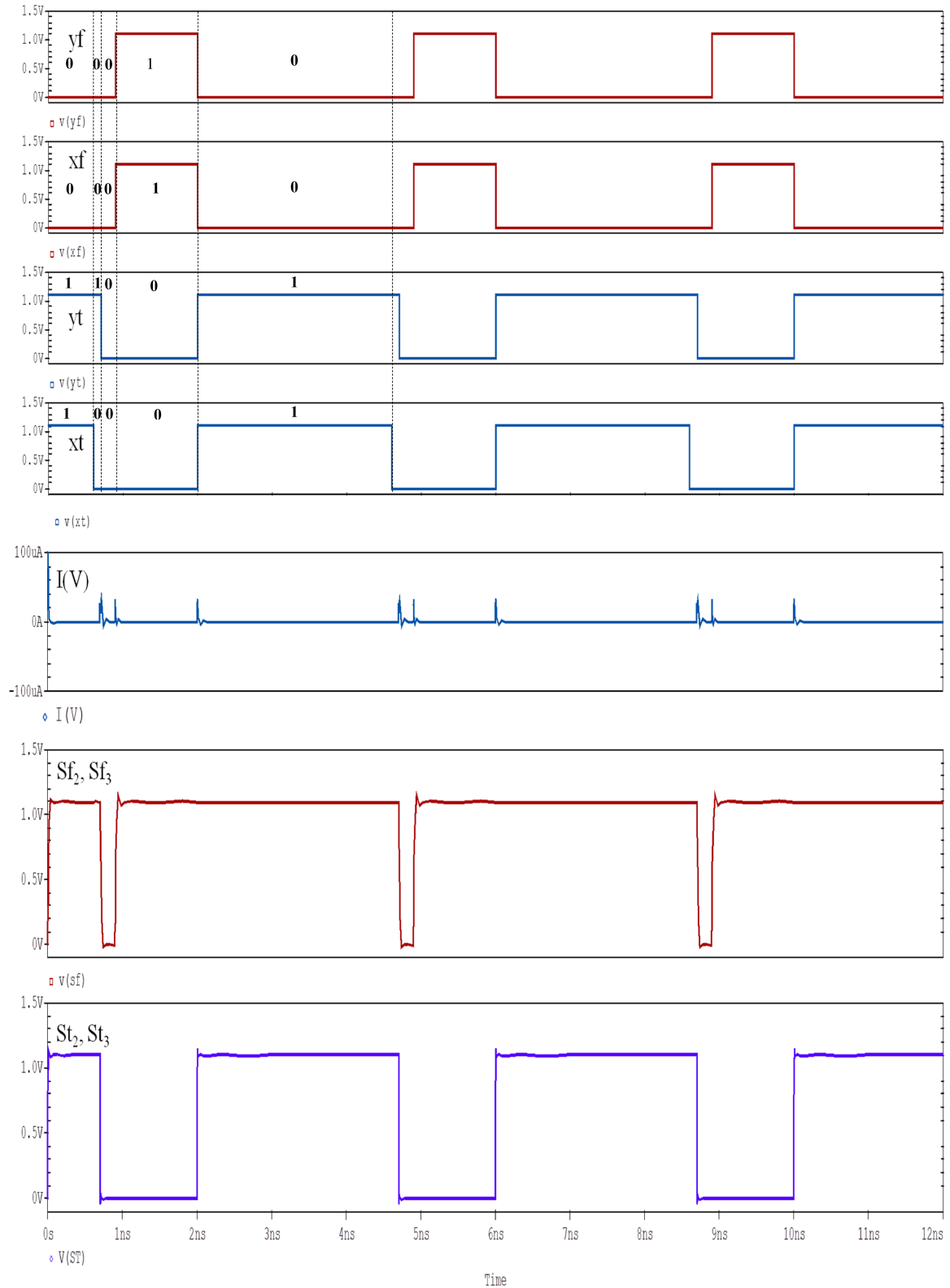


Fig. 5 Behaviour of the fault-free TMR AND QDI

they are, respectively, below and above the threshold voltage and they are still interpreted as the logical value of 0 rep. 1. So, the voltages $V(S_i)$ and $V(S_f)$ are the same in both no fault and resistive bridge fault conditions. The voter V1 receives three correct values for S_i and the voter V2 receives three correct values for S_f . The two resistive bridge faults are tolerated and the TMR operates correctly. The different voltage amplitudes are due to the impact of a resistive bridge is such that each of the faulty nodes tries to impose its logical value on the other; hence when the resistive bridge value R_{br} decrease, the balanced current consumption of the QDI circuit is distorted. It is the result of the charging and discharging of the

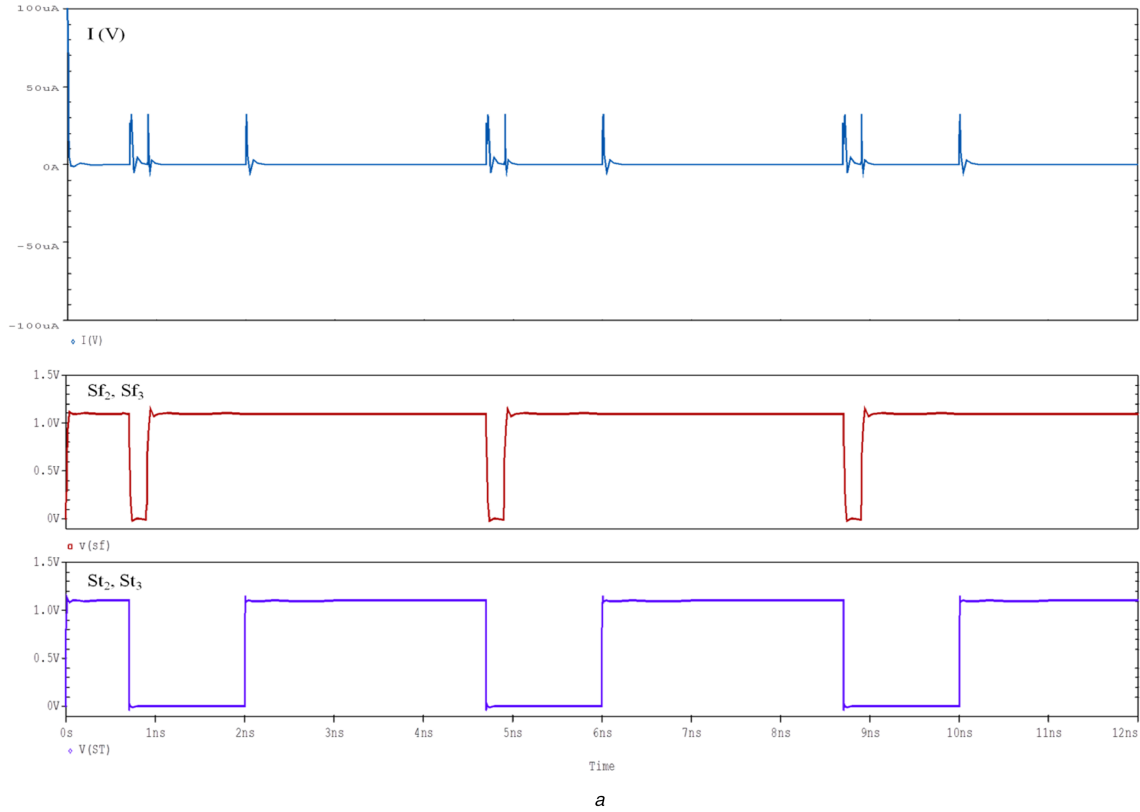
parasitic capacitances connected to the outputs of the QDI circuit. Variations in power consumption occur as the TMR performs different transitions, i.e. the current consumption peaks are unbalanced. When both outputs (Sf_2, Sf_3) and (St_2, St_3) switch from 1 to 0, a small peak appears in the current consumption traces, and when only Sf_2 and Sf_3 go high a highest and large peak occurs. However, when the outputs (St_2, St_3) and (Sf_2, Sf_3) switch at the same time from 0 to 1 there is no current consumption peak. Identifying the two kinds of peaks reveals the inputs data. The current consumption variation $I(V)$ gives information about the

states of inputs (Fig. 7). Consequently, the TMR AND QDI is unsecure against power analysis attacks.

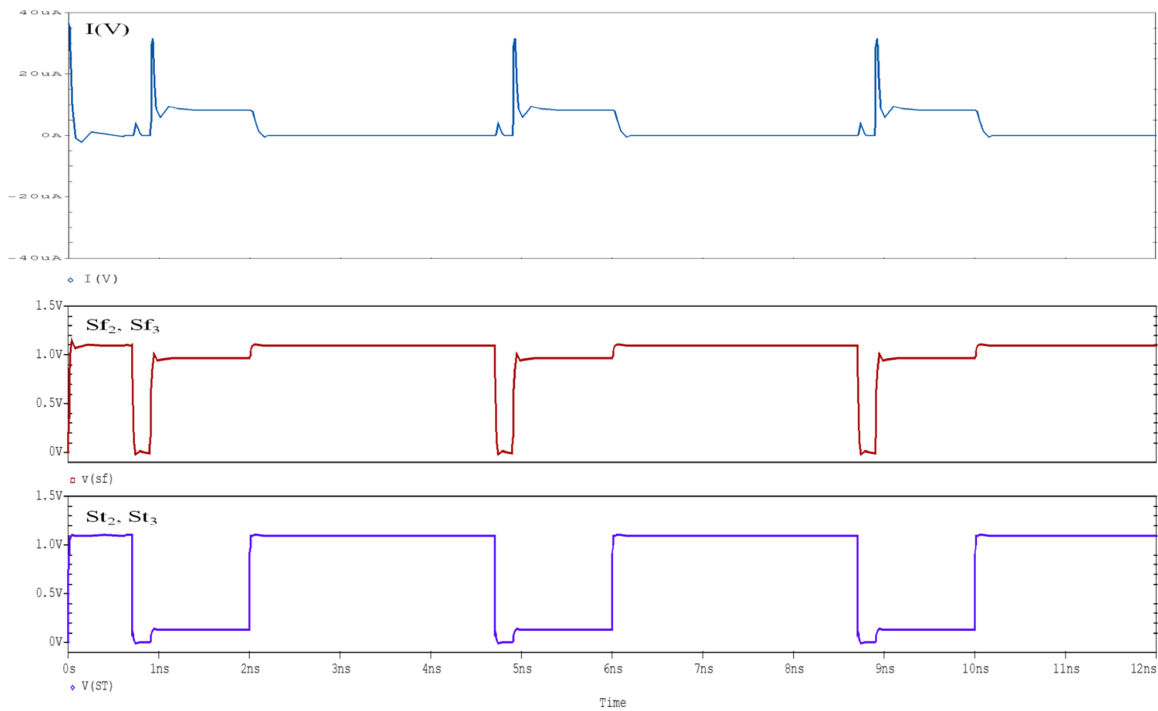
Fig. 7 shows that there is no current peak when the sequences S_2 and S_4 are applied. It should be noted that with or without the sequence $S_1 = [0100]$ the simulation results will be the same, i.e. $(\{S_0 \rightarrow S_1 \rightarrow S_2 \rightarrow S_3\} = \{S_0 \rightarrow S_2 \rightarrow S_3\})$. Sequence $[0100]$ has been generated to check whether for each input transition of QDI circuit a quantity of current is consumed even the presence of the resistive bridge faults. For the sequence $S_4 = [1100]$ the presence of the fault does not affect the operation of the circuit and therefore does not allow fault detection. This sequence produces two transitions which occur at the same time and in the same direction, hence the

break of the conduction path between V_{DD} and the masse. This is the reason why the current consumption peak does not appear.

8.2.3 Simulation for a medium resistance, $R_{br} = 100 \Omega$: Fig. 6c shows other simulation results where the value of the bridge resistance is of 100Ω in TMR AND QDI. In this case, the simulation on the target displays poor results. The conducting path created by these low-ohmic defects would have a very strong influence on the voltage potentials of the shorted nodes and would be able to pull the voltage at S_f below or equal to $V_{DD}/2$ and the voltage at S_t above or equal to $V_{DD}/2$. On the other hand, a high-voltage level appears at the outputs S_t instead of a low-level



a



b

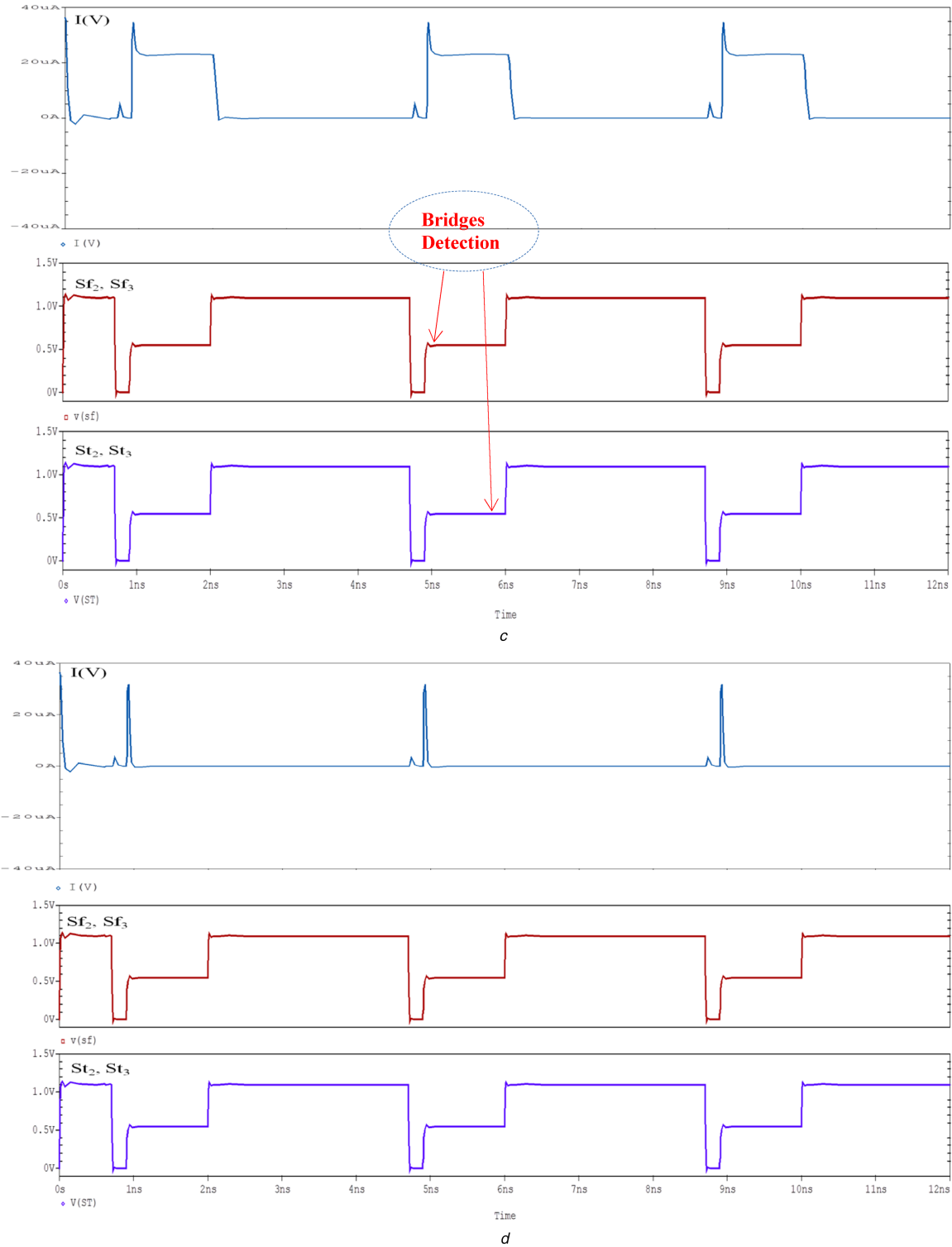


Fig. 6 Behaviour of the defective TMR AND QDI

(a) $R_{br} = \infty$ ($\gg 350 \text{ k}\Omega$), (b) $R_{br} = 350 \text{ k}\Omega$, (c) $R_{br} = 100 \Omega$, (d) $R_{br} = 8 \Omega$

voltage; also a low-level voltage appears at the outputs Sf_2 and Sf_3 while a high-level voltage should normally be present. For example, for $R_{br} = 100 \Omega$ in TMR AND QDI, $(V(Sf_2), V(Sf_3))$ and $(V(Sf_2), V(Sf_3))$ have some identical intermediate voltage which is equal to the threshold voltage when the rising transition occurs. Hence, $V(S_i)$ is interpreted as a logical value of 1, and $V(S_f)$ as a logical value of 0. So, the two resistive bridge faults propagate logical errors towards (St_2, St_3) and (Sf_2, Sf_3) on each faulty gate. The voter V1 receives two wrong values for S_i and the voter V2 receives two wrong values for S_f . So, the values on the two outputs of the TMR design are faulty. The two resistive bridge faults are detected (not tolerated).

On the other hand, the faults have also unbalanced the current-consumption profiles and make them dependent on the data handled. The TMR-based AND QDI becomes insecure against side channel attack. As shown in Fig. 6d, the resistance value influences the fault detection.

When (xt, yt) and (xf, yf) produce inverse transitions that are shifted in time, the current consumption becomes unbalanced. In this case, the faulty outputs cause a wider and higher peak in the measured power traces and make them dependent on the inputs data. This faulty behavioural of TMR design is dependent on the states of the inputs data and can be therefore exploited in power analysis attacks. The power consumption is not only dependent on the inputs data but also on the faulty outputs. From Figs. 6a and b,









xytxfyf	Current peak (μA)	Transition on St	Transition on Sf
S0= 1100	Initial state	1	1
S1= 0100	No peak	+ 	+ 
S2= 0000	small	- 	- 
S3= 0011	High	- 	+ 
S4= 1100	No peak	+ 	+ 

Fig. 7 Current consumption

it is evident that a bridge with a very large resistance ($>350\text{ k}\Omega$) and a large resistance ($350\text{ k}\Omega$) cannot be detected while a smaller resistance bridge ($100\text{ }\Omega$) can be detected. Consequently, the TMR target is not fault tolerant in the case of a small resistance value. This means that a given resistive bridge can be detected by the sequence test if its unknown resistance R_{br} is smaller than a critical resistance value called R_C . Also, when $100\text{ }\Omega < R_{br} \leq 350\text{ k}\Omega$, the TMR AND QDI function correctly but it becomes unsecure against power analysis.

As shown in Fig. 6d, the resistance value influences the fault detection. It is easily detectable, for low resistances values ($R_{br} = 8\text{ }\Omega$). Consequently, the TMR target is not fault tolerant in the case of a small resistance value. This means that a given resistive bridge can be detected by the sequence test if its unknown resistance R_{br} is smaller than a critical resistance value called R_C . So, the DI, the TI and the SI related to the resistive bridges are the following:

$$= [0, R_C^{\max}] = [0, 100\text{ }\Omega] \Rightarrow \text{TI} =]100\text{ }\Omega, \infty[$$

$$\text{SI} =]350\text{ k}\Omega, \infty[.$$

9 Conclusion

This study presents a way to perform fault and power analyses based on the correlation of fault propagation and the value of the faulty TMR QDI circuits. The novelty and the amount of the contribution of this study compared with previous publications is that to evaluate the fault tolerance and the security of the secure TMR, the fault injection is done on the simulation of hardware implementation rather on an algorithm implementation of the AES. The method requires reasonably lower restrictions on fault injection scheme in comparison with previous works. We have shown that both security and fault tolerance depend on the resistance value of a bridge defect. Consequently, the resistive bridge faults can also be used to break the security of the TMR–QDI. The results also showed the existence of a critical resistance below which the fault is detected and the TMR–QDI does not tolerate the resistive bridge faults.

10 References

- [1] Biham, E., Shamir, A.: ‘Differential fault analysis of secret key cryptosystems’. Proc. Int. Conf. on Advances in Cryptology (CRYPTO), Santa Barbara, California, USA, August 1997, pp. 513–525
- [2] Cuiping, S., Huiyun, L., Jianbin, Z.: ‘Fast and automatic security test on cryptographic ICs against fault injection attacks based on design for security test’. *IET Inf. Sec.*, 2017, **11**, (6), pp. 312–318
- [3] Kocher, P.C.: ‘Timing attacks on implementations of Diffie–Hellman, RSA, DSS, and other systems’. Proc. Int. Conf. on Advances in Cryptology (CRYPTO), Santa Barbara, California, USA, August 1996, pp. 104–113
- [4] Quisquater, J.J., Samyde, D.: ‘Electromagnetic analysis (EMA): measures and countermeasures for smart cards’. Proc. Int. Conf. on Research in Smart Cards, Cannes, France, September 2001, pp. 200–201
- [5] Tiri, K., Verbauwhede, I.: ‘A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation’. Proc. Int. Conf. on Design,

- Automation, and Test in Europe. (DATE), Paris, France, February 2004, pp. 246–251
- [6] Popp, T., Mangard, S.: ‘Masked dual-rail pre-charge logic: DPA- resistance without routing constraints’. Proc. Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005), Edinburgh, Scotland, August 2005, pp. 172–186
- [7] Nassar, M., Bhasin, S., Danger, J.L., *et al.*: ‘BCDL: a high speed balanced DPL for FPGA with global precharge and no early evaluation’. Proc. Int. Conf. on Design Automation Test Europe (DATE), Dresden, Germany, March 2010, pp. 849–854
- [8] Sparso, J., Furber, S.: ‘Principles of asynchronous circuit design: a systems perspective’ (Kluwer Academic Publishers, Dordrecht, The Netherlands, 2001)
- [9] Rahbaran, B., Steininger, A.: ‘Is asynchronous logic more robust than synchronous logic’. *IEEE Trans. Dependable Secur. Comput.*, 2009, **6**, (4), pp. 282–294
- [10] Li, Y., Sakiyama, K., Gomisawa, S., *et al.*: ‘Fault sensitivity analysis’. Proc. Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2010), Santa Barbara, USA, August 2010, pp. 320–334
- [11] Robisson, B., Manet, P.: ‘Differential behavioural analysis’. Proc. Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES), Vienna, Austria, September 2007, pp. 413–426
- [12] Li, Y., Ohta, K., Sakiyama, K.: ‘A new type of fault-based attack: fault behaviour analysis’. *IEICE Trans.*, 2013, **E96.A**, (1), pp. 177–184
- [13] Kocher, P.C., Jaffe, J., Jun, B.: ‘Differential power analysis’. Proc. Int. Conf. on Advances in Cryptology, Santa Barbara, CA, USA, August 1999, pp. 388–397
- [14] Mangard, S.: ‘A simple power analysis (SPA) attack on implementations of the AES key expansion’. Int. Conf. on Information Security and Cryptology (ICISC 2002), Seoul Korea, 2003 (LNCS, **2587**), pp. 343–358
- [15] Wang, H., Forte, D., Tehranipoor, M.M., *et al.*: ‘Probing attacks on integrated circuits: challenges and research opportunities’. *IEEE Des. Test*, 2017, **34**, (5), pp. 63–71
- [16] Boneh, D., DeMillo, R.A., Lipton, R.J.: ‘On the importance of checking cryptographic protocols for faults’. Proc. Int. Conf. on Advances in Cryptology (EUROCRYPT), Germany, May 1997, pp. 37–51
- [17] Mischke, O., Moradi, A., Guney, S., T.: ‘Fault sensitivity analysis meets zero-value attack’. Proc. Int. Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), Busan, South Korea, September 2014, pp. 59–67
- [18] Skorobogatov, S.P.: ‘Optically enhanced position-locked power analysis’. Proc. Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2006), Yokohama, Japan, October 2006, pp. 61–75
- [19] Blomer, J., Seifert, J.P.: ‘Fault based cryptanalysis of the advanced encryption standard (AES)’. Proc. Int. Conf. on Financial Cryptography, Guadeloupe, French, West Indies, January 2003, pp. 162–181
- [20] Yu, Z.C., Furber, S.B., Plana, L.A.: ‘An investigation into the security of self-timed circuits’. Proc. Int. Symp. on Asynchronous Circuits and Systems, Vancouver, BC, Canada, Canada, May 2003, pp. 206–215
- [21] Suzuki, D., Saeki, M.: ‘Security evaluation of DPA countermeasures using dual-rail pre-charge logic style’. Proc. Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2006), Yokohama, Japan, October 2006, pp. 255–269
- [22] Tiri, K., Akmal, M., Verbauwhede, I.: ‘A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards’. Proc. Int. Conf. on European Solid-State Circuits Conf. (ESSCIRC), Florence, Italy, September 2002, pp. 403–406
- [23] Martin, A.J., Burns, S.M., Lee, T.K., *et al.*: ‘The first asynchronous microprocessor: the test results’. *ACM SIGARCH Comput. Archit. News*, 1989, **17**, (4), pp. 95–98
- [24] Martin, A.J., Nystrom, M.: ‘Asynchronous techniques for system-on-chip design’. *Proc. IEEE*, 2006, **94**, (6), pp. 1089–1120
- [25] Van Kees Berkel, C.H., Josephs, M.B., Nowick, S.M.: ‘Scanning the technology applications of asynchronous circuits’. *Proc. IEEE*, 1999, **87**, pp. 223–233
- [26] Tang, B.Z., Lane, F.: ‘Low power QDI asynchronous FFT’. Proc. 22nd IEEE Int. Symp. on Asynchronous Circuits and Systems, Porto Alegre, Brazil, May 2016, pp. 87–88
- [27] Jiang, W., Bertozzi, D., Miorandi, G., *et al.*: ‘An asynchronous NoC router in a 14 nm FinFET library: comparison to an industrial synchronous counterpart’. Proc. Int. Conf. on Design, Automation and Test, Lausanne, Switzerland, May 2017, pp. 732–733
- [28] Martin, A.J., Nystrom, M.: ‘Asynchronous techniques for noise tolerant nanoelectronics’. Technical Report Situs-TR-04-01, Situs Logic, Pasadena, CA, USA, 2004
- [29] Bouesse, G.F., Sicard, G., Baixas, A., *et al.*: ‘Quasi delay insensitive asynchronous circuits for low EMI’. Proc. Int. Workshop on Electromagnetic Compatibility of Integrated Circuits, Angers, France, 2004, pp. 27–31
- [30] Chang, I.J., Park, S.P., Roy, K.: ‘Exploring asynchronous design techniques for process-tolerant and energy-efficient sub-threshold operation’. *IEEE J. Solid-State Circuits*, 2010, **45**, pp. 401–410
- [31] David, I., Ginosar, R., Yoeli, M.: ‘Self-timed is self-checking’. *J. Electron. Test., Theory Appl.*, 1995, **6**, (2), pp. 219–228
- [32] Burns, F., Bystrov, A., Koelmans, A., *et al.*: ‘Design and security evaluation of balanced 1-of-n circuits’. *IET Comput. Digit. Tech.*, 2012, **6**, (2), pp. 125–135
- [33] Cilio, W., Linder, M., Porter, C., *et al.*: ‘Mitigating power- and timing based side-channel attacks using dual-spacer dual-rail delay-insensitive asynchronous logic’. *Microelectron. J.*, 2013, **44**, pp. 258–269
- [34] Shams, M., Ebergen, J.C., Elmasry, M.I.: ‘Modeling and comparing CMOS implementations of the C-element’. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, 1998, **6**, (4), pp. 563–567

- [35] Rodriguez-Montanes, R., Volf, P., Pineda de Gyvez, J.: 'Resistance characterization for weak open defects', *IEEE Des. Test Comput.*, 2002, **19**, (5), pp. 18–26
- [36] Li, Z., Lu, X., Qiu, W., *et al.*: 'A circuit level fault model for resistive opens and bridges'. Proc. Int. Symp. 21st VLSI Test, Napa, CA, USA, May 2003, pp. 379–384
- [37] Bar-El, H., Choukri, H., Naccache, D., *et al.*: 'The Sorcerer's apprentice guide to fault attacks', *Proc. IEEE*, 2006, **94**, (2), pp. 370–382
- [38] Lima, F., Carro, L., Reis, R.: 'Designing fault tolerant systems into SRAM-based FPGAs'. Proc. Int. Conf. 40th Annual Design Automation Conf., Anaheim, CA, USA, June 2003, pp. 650–655
- [39] Clavier, C., Feix, B., Gagnerot, G., *et al.*: 'Passive and active combined attacks on AES: combining fault attacks and side channel analysis'. Proc. Conf. on Fault Diagnosis and Tolerance in Cryptography (FDTC), Santa Barbara, CA, USA, 2010, pp. 10–19
- [40] Polian, I., Hayes, J.P.: 'Selective hardening: toward cost-effective error tolerance', *IEEE Des. Test Comput.*, 2011, **28**, (3), pp. 54–63
- [41] Chuang, T.P., Wun Chiou, C., Lin, S.S., *et al.*: 'Fault-tolerant Gaussian normal basis multiplier over GF(2m)', *IET Inf. Sec.*, 2012, **6**, (3), pp. 157–170
- [42] Fang, L., Hsiao, M. S.: 'Bilateral testing of nano-scale fault tolerant circuits'. Proc. Int. Symp. 21st IEEE Defect and Fault Tolerance in VLSI Systems, Arlington, VA, USA, October 2006, pp. 309–317
- [43] Stan, M.R., Franzon, P.D., Goldstein, S.C., *et al.*: 'Molecular electronics: from devices and interconnect to circuits and architecture', *Proc. IEEE*, 2003, **91**, (11), pp. 1940–1957
- [44] Wang, Z., Chakrabarty, K.: 'Built-in self-test of molecular electronics based nanofabrics'. Proc. Int. Symp. IEEE European Test, Tallinn, Estonia, May 2005, pp. 168–173
- [45] Ait Abdelmalek, G., Ziani, R., Laghrouche, M.: 'Testing and fault tolerance of secured circuits', *Int. J. Circuits Syst. Signal Process.*, 2016, **10**, (1), pp. 1–6
- [46] Zhang, G., Song, W., Garside, J., *et al.*: 'Transient fault tolerant QDI interconnects using redundant check code'. Proc. Int. Conf. on Euromicro Digital System Design (DSD), Los Alamitos, CA, USA, October 2013, pp. 3–10
- [47] Kuang, W., Xiao, E., Ibarra, C.M., *et al.*: 'Design asynchronous circuits for soft error tolerance'. Proc. Int. Conf. on IC Design and Technology (ICIDT), Austin, Texas, USA, 30 May–1 June 2007, pp. 1–5
- [48] Teixeira de Sousa, J., Gonçalves, F.M., Teixeira, J.P., *et al.*: 'Defect level evaluation in an IC design environment', *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, 1996, **15**, (10), pp. 1286–1293
- [49] Marzouqi, H., Al-Qutayri, M., Salah, K.: 'Review of gate-level differential power analysis and fault analysis countermeasures', *IET Inf. Sec.*, 2013, **8**, (1), pp. 51–66
- [50] Tiri, K., Verbauwhede, I.: 'A digital design flow for secure integrated circuits', *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, 2006, **25**, (7), pp. 1197–1208