Non-Intrusive Testing Technique for Detection of Trojans in Asynchronous Circuits

Leonel Acunha Guimarães, Thiago Ferreira de Paiva Leite, Rodrigo Possamai Bastos, and Laurent Fesquet
Univ. Grenoble Alpes, CNRS, Grenoble INP*, TIMA, 38000 Grenoble, France
* Institute of Engineering Univ. Grenoble Alpes
{leonel.guimaraes|thiago.leite|rodrigo.bastos|laurent.fesquet}@univ-grenoble-alpes.fr

***Abstract*—Asynchronous circuits, as any IC, are vulnerable to hardware Trojans (HTs), which might be maliciously implanted in IC designs during outsourced fabrication phases. In this paper, a new testing technique to detect HTs by exploiting the regular side-channel properties of quasi-delay insensitive (QDI) asynchronous circuits is proposed. The technique does not need neither additional circuitry nor significant adjustments in the post-fabrication testing phase. Simulation results show that the proposed technique is able to detect HTs with dimensions smaller than 1% of the original circuit.**

I. Introduction

Nowadays IC architectures demand matching robustness against attacks and faults with low power and performance. Clockless circuits, also known as asynchronous circuits are an interesting alternative to deal with power consumption without compromising system's performance [1]. Those architectures employ local communication protocols instead of a global clock for data synchronization, avoiding unnecessary dynamic power consumption in parts of the circuit that have no data to process at a certain point in time. The robustness of Quasi-Delay-Insensitive (QDI) asynchronous circuits against Differential Power Analysis (DPA) [2], transient-faults [3] and EM emissions [1] makes them also a good solution from a security point a view.

Hardware Trojans (HT) are a security issue that currently draws attention of many researchers and engineers. A HT can be a simple layout modification made by an attacker in an untrusted foundry that enables security-oriented systems to leak keys to an adversary [4]. Furthermore, a Trojan can be designed to remain inactive until being triggered by a rare event, leading it to be almost undetectable during regular testing phase. Since a HT, even inactive, causes impacts on side-channel signals, several techniques exploit them for detecting HTs [5]–[9].

Nevertheless, process variations (PV) affect side-channel signals, masking Trojan effects in the circuit. Thus, side-channel analysis detection methods require considerable efforts at design- or test-level to compensate PV. A widely used design-level approach consists of splitting the original circuit in several measurement domains in order to isolate the Trojan impacts to a specific area [6], [7]. This strategy require extra on-chip circuitry or pads to separate the sub-circuits signals and additional post-manufacture tests or dedicated set-ups to generate all required signals, which increases the project cost.

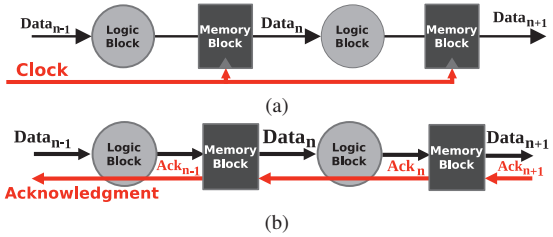

Figure 1. Typical representations of synchronous (a) and asynchronous (b) systems.

Some works were recently published showing that it is possible to implement Trojans in asynchronous circuits [10], [11], while others [12], [13] present strategies to detect threats in mixed macro synchronous micro asynchronous systems. However, for the best of our knowledge, none have ever proposed methods devoted for detecting Trojans inserted in QDI asynchronous circuits.

In this paper, we propose a testing technique for Trojan detection dedicated to QDI asynchronous circuits exploiting the transient current (I_{DDT}) and path delay (Δt) to compare patterns from genuine ICs and devices under Trojan test (DUTT) without adding any extra circuitry nor modifying the original post-silicon test set-up. The proposed technique takes advantage of intrinsic aspects of asynchronous circuits' supply current, which produces separate traces from different blocks that compose the system. We show that it is only required measuring global supply current I_{DD} from the V_{DD} pin to obtain isolated side-channel signals from each block of the circuit.

II. Fundamentals of QDI Asynchronous systems

Circuits that use a local communication protocol for data synchronization, instead of a global clock, are known as clockless or asynchronous circuits. In such architectures, a certain block (sender) only outputs a signal to the following one (receiver) if all its output channels are empty. The receiver, in turn, will only start processing new data when all the necessary inputs are available. These two directives are the basis of a local communication protocol. Respecting them is thus crucial for a correct functioning of asynchronous circuits.

A typical representation of an asynchronous system is shown in Fig.1b. If compared to its synchronous equivalent, the basic difference noted is the absence of a clock signal and the addition of an acknowledgement signal. The latter

978-3-9819263-0-9/DATE18/©2018 EDAA

is part of the local protocol that enables synchronization in asynchronous systems. It signalizes the previous stage that the calculation is completed and new data can be processed.

QDI is a class of asynchronous circuits that can operate correctly with only a few timing constraints [1]. They require a robust data encoding, one that allows data validity to be signaled by the information being propagated itself, hence dual-rail encoding is used for this purpose. In this case, the protocol validity signal (request) is merged into data signals. Thus, there is no physical difference between data and the communication protocol signal. This type of encoding is particularly robust against DPA based attacks, due to its power balance property which masks internal states [2]. Moreover, this class of circuits also features robustness against fault attacks, as discussed in [3]. Consequently, QDI asynchronous architectures are an attractive solution in terms of security.

III. Side Channel Analysis Applied to QDI Asynchronous Circuits

A. Trojan Detection Through Side-Channel Analysis

Several methods have been proposed in literature comparing side-channel signals patterns of DUTTs with golden results from genuine ICs [4]. If the patterns obtained from a DUTT deviate from the golden IC references, a Trojan is detected. Different side-channel signals such as transient current (I_{DDT}) [5], quiescent current (I_{DDQ}) [6], path delay [7] and EM [8] can be exploited.

Despite the multiple options of side-channel signals that can be exploited, dealing with variability is one of the biggest challenges faced by the referred studies. In fact, PV alters circuit parameters such as threshold voltages (V_{th}), channel lengths (L), and oxide thickness (T_{ox}). The detection of slight Trojans relies on alternatives to compensate for parameter fluctuations that could mask HT effects. Several methods [5], [6] propose using multiple power pins in the circuit to highlight the side-channel patterns from a specific regions of the chip, isolating their effects in a smaller region consequently increasing detectability.

Although reliable results are presented covering most of circuit designs against Trojans, such techniques impose substantial area overhead or considerable addition in cost and duration of the testing phase. For instance, the method in [7] proposes using a secondary clock signal to control a set of shadow registers to measure the path delay of logic blocks. The approach in [9] evaluates a pair of parameters (maximal frequency and transient current) to detect Trojans, measuring the signals from multiple power supply pins in order to isolate the Trojan and applying power gating to enhance the detection rate. The methodology in [8] is able to detect Trojans by mapping thermal characteristics with no extra hardware in the original design. However, it requires the use of high resolution devices to generate thermal maps, which increases time-to-market and costs at testing phase, besides the challenging procedures for nanoscale technology nodes.

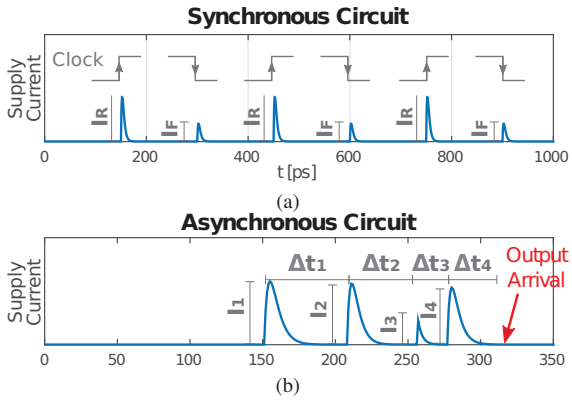

Figure 2. Abstraction of the supply current from synchronous (a) and asynchronous (b) circuits.

B. Side-Channel Signals in QDI Asynchronous Circuits

As presented in section II, locally derived handshake pulses control data propagation in asynchronous circuits. Their generation, which can occur at any moment, are governed by the latency of the successor and the predecessor blocks. Therefore, these pulses tend to be randomized over time, resulting in smoother supply current curves [1], without the large di/dt spikes as in synchronous circuits, as shown in Fig. 2a.

The asynchronous protocol results in a current trace as the one depicted in Fig. 2b. This example represents the current response of a single input vector passing through a 4-stage pipelined asynchronous circuit measured from the global power supply. In case of a single input vector test, whenever the first stage outputs data to be processed by the second stage, the former will no longer have new calculations to do, and will become idle. The same behavior will be observed in every following stage of the asynchronous pipeline until all stages turn inactive. Therefore, only one stage of the pipeline is in fact active at a certain moment, while the other stages stand idle, waiting for new data to process. Thus, each peak in Fig. 2b corresponds to the operation of a single pipeline stage. For this reason, a Trojan inserted in an asynchronous circuit directly impacts the current peak that corresponds to the stage in which it has been inserted. Conversely, in synchronous circuits the global clock governs the switching activity of all pipeline stages simultaneously. Hence, the current peaks depicted in 2a represent the sum of the individual contribution of all elements that composes the circuit. The insertion of a Trojan in this case would impact the supply current response of the system as a whole, not only the pipeline stage in which it has been inserted. Consequently, it is possible to obtain the transient current of each separate pipeline stage and the path delay only with the global supply current trace.

1) Global Path Delay (Δt): In QDI asynchronous circuits, the delay of a pipeline stage can be measured by the difference Δt_i between two current peaks (see Fig. 2b). As the global delay is given by $\Delta t = \sum_{i=1}^{n} \Delta t_i$, the deviation caused by a Trojan in one of its n pipeline stages is propagated to others subsequent blocks, delaying the output. Therefore, measuring the delay Δt between the primary inputs and its arrival at the

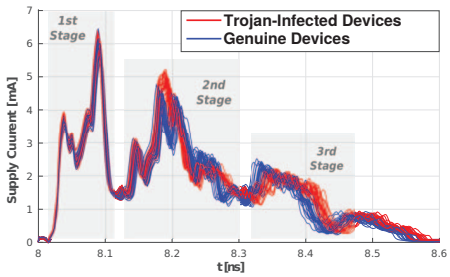

Figure 3. Current curves in a 3-stage pipelined QDI asynchronous circuit obtained with 50-run Monte Carlo simulations. Blue traces were generated by genuine and red by Trojan-infected devices.

system output, is sufficient for malicious circuitry tracking. Obtaining path delay in asynchronous circuit, thus, requires only non-intrusive current measures on the power supply pin, seamlessly fitting in the regular testing phase with no extra cost in terms of design. Additionally, as gate delays is inversely proportional to power supplies levels, two simple actions can increase feasibility of path delay measurements: (1) reduction of the power supply level V_{DD} and; (2) reduction of the substrate voltage V_{DDS}.

2) Transient Current (I_{DDT}): Since only the gates from a specific pipeline stage switches simultaneously, if a Trojan is inserted in a certain stage, its relative current peak is increased, highlighting the Trojan impact. Therefore, a HT insertion in a given stage can be recognized by the variation in its current amplitude.

Path delays and transient currents are correlated and mutually affected by PV. If the variation increases the current, it decreases the delay and vice-versa. The measurement of one variable allows deducing the range of the other, thus reducing the range of possible values of the other one. Therefore, the evaluation of the variables I_{DDT} and Δt allows reducing the impact of PV effects, as similarly demonstrated in [9].

C. Trojan Impacts on Side-Channel Signals

We propose to illustrate the Trojan effects on the current trace by a preliminary test considering PV effects in FD-SOI 28nm technology. Fig. 3 show an example of supply current traces obtained from 3-stage pipelined devices with and without a Trojan implanted in its second stage. The result figure depicts the impacts caused by Trojans (of approximately 1.3% of the original circuit area) in the current trace. It illustrates the motivation for the Trojan detection technique presented in this work. Note that the current in the first stage remains unadulterated, whereas the current peaks in the second stage are clearly increased, and delayed in the third due to the Trojan effects. The necessary steps to perform Trojan detection are thus discussed in the following section.

IV. Proposed HT-Detection Technique for QDI Asynchronous Circuits

A. Test Procedure: Collecting I_{DDT} and Δt

Initially, the proposed test procedure requires collecting side-channel signatures from genuine devices (golden data) as in other methods. Subsequently, the same procedure is applied on each DUTT in order to produce results that will be statistically compared to the golden data.

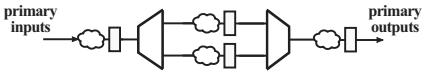

Figure 4. Representation of the pipeline stages from the ALU in [14].

As explained in Section III-B, the supply current trace is enough to obtain I_{DDT} and Δt, which are the necessary parameters for the proposed analysis. Thus, the current trace is directly measured from the global V_{DD} pin of each golden device using a test input vector X, from which the I_{DDT} peaks of each pipeline stage (I_{DDT1}, I_{DDT2}, I_{DDT3}) are extracted and stored. The Δt is obtained with the same test, however using a reduced V_{DD} level to facilitate the delay measurement, as discussed in III-B1. This test is repeated for each available genuine device. By the end, due to the PV effects, the collected parameters form a statistical distribution. Defining limits to such a distribution results in a data range in which measurements from genuine devices are expected to lay on. By performing the same test in each DUTT, it is possible to verify if its parameters belong to the generated distribution, thus classifying it as Trojan-free if the assumption is true, otherwise the DUTT is classified as Trojan-infected.

V. Experiments, Results, and Analysis

The QDI asynchronous 8-bit ALU proposed in [14] is the case-study circuit chosen for this study. It has 3 stages of pipeline and a total of 506 logic gates. Fig. 4 depicts an abstraction of it.

The Trojan model is a gate-level trigger that alters data flow whenever the input is set to a specific value, which is never tested during our simulations to make the detection more challenging. Therefore, the Trojan remains inactivated during all performed tests, which implies that its architecture is not pertinent for the detection. Simulations were done with Trojans representing 1.7%, 1.3% 1%, and 0.8% area of the original design. Both case-study and Trojan were synthesized with low threshold voltage transistors in FD-SOI 28nm technology. Results were obtained by using 400-run Monte Carlo (MC) simulations performed at a reference temperature of 25^oC. Intra- and inter-die PV have been considered.

Two simulations are performed in order to generate results for the technique proposed in IV: one to obtain I_{DDT} with supply voltage V_{DD} of 1V, and the second one to obtain global Δt, with V_{DD} of 0.6V. Data collected from Trojan-free devices produce the signature of golden ICs by following the procedure explained in section IV. Afterwards, the same design is infected with different Trojans, to produce results that are statistically compared with the golden data. The parameter used to evaluate the results is the detection rate, defined as the percentage of Trojan data not pertaining to the Trojan-free distribution.

A. Results and Analysis

Results from MC simulations performed with genuine and Trojan-infected devices are shown in Fig. 5. In these simu-

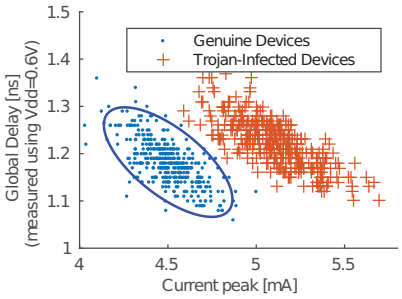

Figure 5. Current peak in the second stage and the global delay obtained from 400-run MC in the Trojan-free and Trojan-infected ALU. The ellipse surrounds the data from genuine devices with a confidence level of 95%.

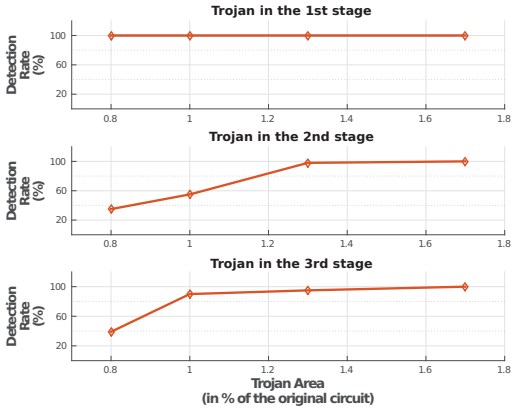

Figure 6. Detection rate obtained considering Trojan infection in different pipeline stages.

lations, the Trojans have a total area of 1.6% of the original circuit area and were inserted in the second pipeline stage. An error ellipse with 95% of confidence level surrounds the golden data, indicating a region in the parameters space where a circuit is accepted as Trojan-free. Note that the impact of the Trojan shifts the data from its original value to a greater current peak and global delay, as previously signaled in Fig. 3. As no point from the Trojan-infected circuit is enclosed by the Trojan-free ellipse, the detection rate is 100%.

The same study is extended to cases in which the HT size and location vary. Fig. 6 depicts the curves of detection rate versus Trojan size. The graphs represent the results for HTs inserted in the first, second, and third stages respectively.

Results in Fig. 6 show that it is possible to detect Trojans representing 1.3% of the original circuit area with a detection rate of 100% if the Trojan is inserted in the first pipeline stage, 98% in the second one, and 95% in the third stage. The curves in different stages are different, since the total number of gates vary in each stage. If the stages were equality balanced, the total dynamic consumption would be divided equally in all stages and, thus the curves would be more homogeneous. Furthermore, systems with more pipeline stages would present its dynamic power divided in more stages, enhancing the relative Trojan overhead in one of their stages. In order to enhance the detection rate, modifications in the original circuit could be made to increase the number of pipeline stages.

VI. Conclusions

We presented an efficient Trojan detection technique dedicated to QDI asynchronous circuits exploiting its inherent transient current and path delay characteristics. The evenly distributed current peaks, intrinsic of asynchronous circuits, make them more sensitive to side-channel deviations than synchronous circuits, thus enhancing HT detection potential. Thus, it is possible to detect modifications smaller than 1.3% of original circuit with a detection rate of 95% without requiring any extra-circuitry. Moreover, the testbench set-up employed in the regular post-silicon testing phase can be reused for this purpose. Still, this technique can also be employed combined with any other methods proposed in the literature in order to enhance the obtained results, thus allowing the detection of even smaller Trojans. Future works will include adapting the proposed detection technique to other classes of asynchronous circuits, e.g. micropipeline.

References

[1] J. Sparsø and S. Furber, *Principles of Asynchronous Circuit Design: A Systems Perspective*, 1st ed. Springer Publishing Company, Incorporated, 2010.

[2] W. G. Ho *et al.*, "Security analysis of asynchronous-logic qdi cell approach for differential power analysis attack," in *2016 International Symposium on Integrated Circuits (ISIC)*, Dec 2016, pp. 1–4.

[3] Y. Monnet *et al.*, "Designing resistant circuits against malicious faults injection using asynchronous logic," *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1104–1115, Sept 2006.

[4] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE Design Test of Computers*, vol. 27, no. 1, pp. 10–25, Jan 2010.

[5] R. Rad *et al.*, "Sensitivity analysis to hardware trojans using power supply transient signals," in *2008 IEEE International Workshop on Hardware-Oriented Security and Trust*, June 2008, pp. 3–7.

[6] J. Aarestad *et al.*, "Detecting trojans through leakage current analysis using multiple supply pad I_{ddq} s," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 893–904, Dec 2010.

[7] B. Cha and S. K. Gupta, "Trojan detection via delay measurements: A new approach to select paths and vectors to maximize effectiveness and minimize cost," in *DATE*, 2013.

[8] K. Hu *et al.*, "High-sensitivity hardware trojan detection using multimodal characterization," in *2013 Design, Automation Test in Europe Conference Exhibition (DATE)*, March 2013, pp. 1271–1276.

[9] S. Narasimhan *et al.*, "Hardware trojan detection by multiple-parameter side-channel analysis," *IEEE Transactions on Computers*, vol. 62, no. 11, pp. 2183–2195, Nov 2013.

[10] T. Y. Koutaro Inaba and M. Imai, "Hardware trojan asynchronous noc router," in *Asynchronous Circuits and Systems (ASYNC), 2017 IEEE 24th International Symposium on*, May 2017, to be published.

[11] S. R. Hasan *et al.*, "Hardware trojans in asynchronous fifo-buffers: From clock domain crossing perspective," in *2015 IEEE 58th International Midwest Symposium on Circuits and Systems (MWSCAS)*, Aug 2015, pp. 1–4.

[12] F. K. Lodhi *et al.*, "Hardware trojan detection in soft error tolerant macro synchronous micro asynchronous (msma) pipeline," in *2014 IEEE 57th International Midwest Symposium on Circuits and Systems (MWSCAS)*, Aug 2014, pp. 659–662.

[13] ——, "Formal analysis of macro synchronous micro asychronous pipeline for hardware trojan detection," in *2015 Nordic Circuits and Systems Conference (NORCAS): NORCHIP International Symposium on System-on-Chip (SoC)*, Oct 2015, pp. 1–4.

[14] T. F. de Paiva Leite *et al.*, "Comparison of low-voltage scaling in synchronous and asynchronous fd-soi circuits," in *2016 26th International Workshop on Power and Timing Modeling, Optimization and Simulation (PATMOS)*, Sept 2016, pp. 229–234.