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 of 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.

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
is part of the local protocol that enables synchronization in asynchronous systems. It signals 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.

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 ($\Delta t$): In QDI asynchronous circuits, the delay of a pipeline stage can be measured by the difference $\Delta t_i$ 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 $\Delta t$ between the primary inputs and its arrival at the
A. Results and Analysis

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

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°C. 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 \(\Delta t\), 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.
representing 1 inserted in the first, second, and third stages respectively. Fig. 6 depicts the curves of detection rate and location vary. 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